



Configuring Password Management Modules (PMMs), Connectors, and Agents

Release 9.1

Core Security SDI Corporation

**1000 Holcomb Woods Parkway
Suite 401**

**Roswell, GA 30076
Phone: (678) 304-4500
Fax: (770) 573-3743**

Trademarks

Copyright © 2018 by Core Security SDI Corporation. All Rights Reserved. The following are trademarks of Core Security Corporation "Core Impact", "Core Vulnerability Insight", "Core Password", "Core Access", "Core Provisioning", "Core Compliance", "Core Access Insight", "Core Mobile Reset", and "Think Like an Attacker". The following are registered trademarks of Core Security Corporation "WebVerify", "CloudInspect", "Core Insight", and "Core Security". The names of actual companies and products mentioned herein may be the trademarks of their respective owners. The names of additional products may be trademarks or registered trademarks of their respective owners.

Table of Contents

Chapter 1 - About Password Management Modules (PMMs) and Connectors	27
Creating Custom Connectors with the Connector Rapid Development Kit	28
Password Management Module (PMM) Functionality	29
Connector Functionality	30
PMM and Connector Agents	31
Connector and PMM Summary	32
Chapter 2 - BMC Remedy Action Request System — PMM and Connector	39
Configuring the PMM for BMC Remedy Action Request System	40
Prerequisites	40
PMM Configuration	40
Creating a Workflow for the Target	42
Updating to Remedy 6.51	42
Configuring the Connector for BMC Remedy Action Request System 3.x	43
Configuring Remedy for Secure (encrypted) Communication	43
Connector Configuration	43
Chapter 3 - CA eTrust SiteMinder — PMM	47
Configuring the PMM for CA eTrust SiteMinder	48
Prerequisites	48
Creating the SiteMinder Agent for the PMM	49
Security Options	49
Allow Reset of Administrative Accounts	49
User must change password during next login	49
PMM Configuration	49
Chapter 4 - Using the Connector Configuration Manager	53
Configuring Connectors and PMMs in a Distributed Installation	54
The Connector Framework and Connector Framework Manager Web Services	54
Assigning Targets to a Connector Framework in a Distributed Installation	54
Privilege Issues in a Distributed Installation	55
Connectors and PMMs that Require Supporting Files	55
Adding and Removing Connectors	56
Prerequisites for Adding a Connector	56
Running the Connector Configuration Manager to Add a Connector	56
Running the Connector Configuration Manager to Delete or Modify a Connector or Target	58
Prerequisites for Configuring a Connector	58
Information Needed for Connector Configuration	58
Connector Configuration Manager Menu Bar Options	59
Assigning Targets to the Default Connector Framework	60
Running the Connector Configuration Manager to Assign Targets to the Default Connector Framework	60
Using the PMM Gateway Connector to Define PMM Targets	61
Chapter 5 - Citrix SSO — Connector	63
Configuring the Connector for Citrix SSO	64
Prerequisites	64
Connector Configuration	64
Chapter 6 - Citrix XenApp — Connector	67
Configuring the Connector for Citrix XenApp	68
Providing Access to Citrix Published Applications	68
Making Checkbox Selections Available for Citrix XenApp Published Applications	69
Prerequisites	71

Installing the Citrix SDK	71
Specifying the Name of the Citrix XenApp	71
Connector Configuration	72
Notes	74
Adding the Citrix XenApp Name to the Microsoft Windows DCOM Settings	74
Provisioning to Multiple Published Applications	74
Updating the Unique Target Data Field Selection Form after Updating the CP Server	75
Using IdentityMap Restrictions to Detect Duplicate CP Server Published Application Access	75
Conflicts in Access	75
Chapter 7 - Core Role Connector	77
Configuring the Role Connector	78
Chapter 8 - Core Connector for SQL Usage	81
Configuring the Connector for SQL Usage	82
Chapter 9 - Core Connector for JavaScript Custom Macros	85
Configuring the Connector for JavaScript Custom Macros	86
Chapter 10 - Core Connector for VBScript Custom Macros	89
Configuring the Connector for VBScript Custom Macros	90
Chapter 11 - Core Connector for Web Services	91
Configuring the Connector for Web Services	92
Chapter 12 - Epic — Connector	95
Configuring the Connector for Epic	96
Prerequisites	96
Connector Configuration	96
Chapter 13 - HP OpenView ServiceCenter — Connector	99
Configuring the Connector for HP Software Service Manager	100
Prerequisites	100
Editing the Services File	100
Connector Configuration	100
Notes and Warnings	102
Chapter 14 - HP-UX System — PMM and Connector	103
Configuring the PMM for HP-UX	104
Prerequisites	104
PMM Configuration	104
Creating a Workflow for a Target	106
Writing Password Management Scripts	107
Installing and Configuring the HP-UX PMM Agent	108
Installing the Agent	108
Configuring the HP-UX PMM Agent	109
Starting and Stopping the Agent	111
Displaying the Version Information	111
Uninstalling the PMM Agent for Upgrading	111
Configuring the Connector for HP-UX	112
Prerequisites	112
Scripts that Support Provisioning on HP-UX Systems	112
Connector Configuration	112
Chapter 15 - HP-UX 11i v1 Trusted Mode — PMM	117
Configuring the PMM for HP-UX 11i v1 Trusted Mode	118
Prerequisites	118
PMM Configuration	118
Creating a Workflow for a Target	120
Installing and Configuring the HP-UX 11i v1 PMM Agent	121
Installing the Agent	121
Configuring the HP-UX 11i V1 PMM Agent	122
Starting and Stopping the Agent	123

Displaying the Version Information	123
Uninstalling the PMM Agent for Upgrading	123
Chapter 16 - HTML Email — Connector	125
Configuring the Connector for HTML Email	126
Configuring the Enhanced Connector for HTML Email	128
Chapter 17 - IBM AIX — PMM and Connector	131
Configuring the PMM for IBM AIX	132
Prerequisites	132
PMM Configuration	132
Creating a Workflow for the Target	134
Notes and Warnings	134
Writing Password Management Scripts	135
Installing and Configuring the AIX PMM Agent	136
Installing the Agent	136
Configuring the Agent	137
Starting and Stopping the Agent	139
Displaying the Version Information	139
Uninstalling the Agent for Upgrading	139
Configuring the Connector for IBM AIX	140
Prerequisites	140
Scripts that Support Provisioning on IBM AIX Systems	140
Connector Configuration	140
Chapter 18 - IBM Lotus — PMMs and Connector	145
Configuring the PMM for IBM Lotus Domino	146
Prerequisites	146
Using the Replication Feature	146
PMM Configuration	147
Creating a Workflow for the Target	149
Configuring the PMM for IBM Lotus Notes	150
Prerequisites	150
ID File Definition	150
PMM Configuration	151
Downloading the Modified ID File to the Client Machine	164
Configuring the Domino ID Vault Feature	165
Creating a Workflow for the Target	166
Notes and Warnings	167
Sample Password Processing Script	168
Configuring the Connector for IBM Lotus	171
Prerequisites	171
Connector Configuration	171
Notes and Warnings	175
Configuring the WorkerTermMinutes Attribute	176
Chapter 19 - IBM z/OS Systems with CA-ACF2 — PMM and Connector	179
Configuring the PMM for z/OS Systems with CA-ACF2	180
Prerequisites	180
z/OS Mainframe Requirements	180
z/OS System Requirements	181
PMM Configuration	181
Configuring TCP/IP Parameters	183
Configuring SNA Parameters	183
Creating a Workflow for the Target	184
Notes and Warnings	184
Configuring the Connector for z/OS Systems with CA-ACF2	185
Prerequisites	185
Connector Configuration	185
Chapter 20 - IBM z/OS Systems with CA-Top Secret — PMM and Connector	189
Configuring the PMM for z/OS Systems with CA-Top Secret	190

Prerequisites	190
z/OS Mainframe	190
z/OS System	191
PMM Configuration	191
Configuring TCP/IP Parameters	193
Configuring SNA Parameters	193
Creating a Workflow for a Target	194
Notes and Warnings	194
Configuring the Connector for z/OS Systems with CA-Top Secret	195
Prerequisites	195
Connector Configuration	195
Chapter 21 - IBM z/OS Systems with RACF — PMM and Connector	199
Configuring the PMM for z/OS Systems with RACF	200
Prerequisites	200
z/OS Mainframe Requirements	200
z/OS PMM Agent Requirement	201
PMM Configuration	201
Configuring TCP/IP Parameters	203
Configuring SNA Parameters	203
Creating a Workflow for the Target	204
Notes and Warnings	204
Configuring the Connector for z/OS Systems with RACF	205
Prerequisites	205
Connector Configuration	205
Chapter 22 - IBM i Systems — PMM and Connector	209
Configuring the PMM for IBM i	210
Prerequisites	210
PMM Configuration	210
Required Forced Password Change	212
Creating a Workflow for the Target	212
Notes and Warnings	212
Using OS/400 PMM Agent Commands and Keywords	214
Installing and Configuring the PMM Agent	217
Installing the PMM Agent	217
Delivered Agent Authority	220
Configuring the PMM Agent	220
Agent Menu	222
Configure Agent (PMMCFG) Commands	223
Start Agent Command (STRPMM)	224
Printing Configuration Files	225
Excluding Profiles from Password Reset	226
Starting and Stopping the PMM Agent	226
Uninstalling the PMM Agent	228
Configuring the Connector for IBM i	230
Connector Configuration	230
Notes	232
Installing and Configuring the Connector Agent	233
Installing the Connector Agent	233
Authority Delivered with the OS/400 Connector Agent	235
OS/400 Connector Agent Menu	236
Configuring the OS/400 Connector Agent	237
Starting the OS/400 Connector Agent	238
Stopping the Agent	239
Uninstalling the OS/400 Connector Agent	240
Stopping the Agent	240
Remove Agent Commands	240
Deleting Product Library and User Profiles	241
Chapter 23 - Imprivata OneSign — Connector	243
Configuring the Connector for Imprivata OneSign	244

Prerequisites	244
Courion Provisioning System Adaptor Configuration	245
Installing the Root OneSign CA Certificate	245
Connector Configuration	247
Configuring the Trigger	249
Chapter 24 - Kronos Workforce Central — PMM and Connector	251
Configuring the PMM for Kronos Workforce Central	252
Prerequisites	252
PMM Configuration	252
Creating a Workflow for a Target	254
Configuring the Connector for Kronos Workforce Central	255
Connector Configuration	255
Chapter 25 - Microsoft Active Directory — PMM and Connector	257
Configuring the PMM for Microsoft Active Directory	258
Prerequisites	258
Security Options for Active Directory	258
Allow Reset of Administrative Accounts	258
Force User To Change Password at Next Logon	259
Conform to System Password History	259
Conform to System Minimum Password Age	259
PMM Configuration	260
Enabling Local Password Cache Updates on the Client Machine	263
Creating a Workflow for the Target	263
Single Domain Model	264
Single or Multiple Master Domain Model	264
Configuring the Connector for Microsoft Active Directory	266
Connector Configuration	266
Notes and Warnings	269
Chapter 26 - Microsoft Active Directory Application Mode (ADAM) — Connector	271
Configuring the Connector for ADAM	272
Connector Configuration	272
Chapter 27 - Microsoft Active Directory Attribute Trigger — Connector	275
Configuring the Connector for Microsoft Active Directory Attribute Trigger	276
Prerequisites	276
Connector Configuration	276
Workflow Configuration	279
Chapter 28 - Microsoft Active Script — Connector	281
Configuring the Connector for Active Script	282
Connector Configuration	282
Chapter 29 - Microsoft ADO (ActiveX Data Objects) — Connector	287
Configuring the Connector for ADO	288
Features that Require a Transaction Repository	288
Using Security Options	289
Adding a Target Data Source	289
Chapter 30 - Microsoft Exchange 5.5 — Connector	295
Configuring the Connector for Microsoft Exchange 5.5	296
Connector Configuration	296
Chapter 31 - Microsoft Exchange 2000 — Connector	299
Configuring the Connector for Microsoft Exchange 2000	300
Prerequisites	300
Connector Configuration	300
Chapter 32 - Microsoft Exchange 2007 and 2010 — Connector	305
Configuring the Connector for Microsoft Exchange 2007 and 2010	306
Prerequisites	306

For Microsoft Exchange 2007 Only	306
For Microsoft Exchange 2010 Only	306
Prerequisites for Microsoft Windows Server 2008 and 2008 R2 and higher	307
Installing Exchange Management Tools on the Connector Framework and Connector Framework Manager Servers for Microsoft Exchange 2007	307
Connector Configuration	308
Chapter 33 - Microsoft Identity Integration Server (MIIS) — Connector	311
Configuring the Connector for Microsoft Identity Integration Server (MIIS)	312
Prerequisites	312
Connector Configuration	312
Chapter 34 - Microsoft ODBC 3.0 — Connector	317
Configuring the Connector for Microsoft ODBC	318
Prerequisites	318
Connector Configuration	318
Adding a New Microsoft Access Data Source	322
Adding a New SQL Server Data Source	325
Adding a New Oracle Data Source	329
Supported Data Types	332
Notes	332
Chapter 35 - Configuring the PMM for Microsoft Office365	333
Configuring the PMM for Microsoft Office365	334
Target Requirements	334
Connector Framework and Connector Framework Manager Server Requirements	334
PMM Configuration	334
Chapter 36 - Configuring the Connector for Microsoft Office365 Exchange Online	339
Configuring the Connector for Microsoft Office365 Exchange Online	340
Prerequisites	340
Connector Configuration	340
Licenses	343
Using Triggers	344
Native Query (Macros)	345
Get Licenses	345
Get Admin Roles	345
Chapter 37 - Configuring the Connector for Microsoft Office365 Lync Online	347
Configuring the Connector for Microsoft Office365 Lync Online	348
Prerequisites	348
Connector Configuration	348
Licenses	351
Native Query (Macros)	352
Get Licenses	352
Get Admin Roles	352
Chapter 38 - Configuring the Connector for Microsoft Office365 SharePoint Online	353
Configuring the Connector for Microsoft Office365 SharePoint Online	354
Prerequisites	354
Connector Configuration	354
Licenses	357
Native Query (Macros)	358
Get Licenses	358
Get Admin Roles	358
Chapter 39 - Microsoft SQL Server — PMM and Connector	359
Configuring the PMM for Microsoft SQL Server	360
Prerequisites	360
Data Source Name Configuration	360
PMM Configuration	361
Sample Password Reset Example	366
Creating a Workflow for the Target	366

Configuring the Connector for Microsoft SQL Server	367
Connector Configuration	367
Chapter 40 - Microsoft-VBScript 5.6 — Connector	369
Configuring the Connector for Microsoft-VBScript 5.6	370
Connector Configuration	370
Chapter 41 - Microsoft Windows 2000 and Windows NT — PMM and Connector	373
Configuring the PMM for Microsoft Windows NT and Windows 2000	374
Prerequisites	374
Using Security Options	374
Allow Reset of Administrative Accounts	374
Conform to System Password History	375
Additional Password Settings for Admin Password Resets	376
Conform to System Minimum Password Age	376
PMM Configuration	377
Enabling Local Password Cache Updates on the Client Machine	380
Creating a Workflow for a Target	380
Notes and Warnings	380
Single Domain Model	381
Single or Multiple Master Domain Model	381
Configuring the Connector for Microsoft Windows NT Domains	383
Prerequisites	383
Connector Configuration	383
Chapter 42 - Netscape Directory Server and iPlanet Directory Server — PMM	387
Configuring the PMM for Netscape Directory Server	388
Prerequisites	388
PMM Configuration	388
Creating a Workflow for a Target	391
Configuring the PMM Agent	392
Starting and Stopping the PMM Agent	393
Support for SHA Hashing	394
Chapter 43 - Netscape SMTP — Connector	395
Configuring the Connector for Netscape SMTP	396
Connector Configuration	396
Chapter 44 - Novell GroupWise — PMM and Connector	399
Configuring the PMM for Novell GroupWise	400
Prerequisites	400
PMM Configuration	400
Creating a Workflow for a Target	402
Configuring the Connector for Novell GroupWise	403
Prerequisites	403
Connector Configuration	403
Chapter 45 - Novell NDS eDirectory — PMM and Connector	407
Configuring the PMM for Novell NDS eDirectory	408
Prerequisites	408
PMM Configuration	408
Creating a Workflow for the Target	410
Notes and Warnings	410
Configuring the Connector for Novell NDS eDirectory	411
Prerequisites	411
Connector Configuration	411
Configuring a Workflow to use more than one Target based on this Connector	413
Chapter 46 - Novell SUSE Linux Enterprise — Connector	415
Configuring the Connector for Novell SUSE Linux Enterprise	416
Prerequisites	416

Connector Configuration	417
Chapter 47 - OpenVMS for VAX, Alpha, and Itanium Systems — PMM and Connector	421
Configuring the PMM for OpenVMS	422
Prerequisites	422
PMM Configuration	422
Creating a Workflow for a Target	424
Notes and Warnings	424
Configuring the Connector for OpenVMS	425
Prerequisites	425
Connector Configuration	425
Installing and Configuring the OpenVMS Agent	427
Installing the Agent	427
Reinstalling the Agent	429
Configuring the OpenVMS Agent	429
Starting the Agent	430
Stopping the Agent	430
Uninstalling the OpenVMS Agent	431
Agent Logging	432
Chapter 48 - Oracle Database 8i and 9i — PMM and Connector	433
Configuring the PMM for Oracle Database	434
Prerequisites	434
PMM Configuration	434
Sample Password Reset Procedure	439
Creating a Workflow for a Target	440
Configuring the Connector for Oracle 8i and 9i	441
Prerequisites	441
Connector Configuration	441
Chapter 49 - Oracle E-Business Suite — PMM and Connectors	445
Configuring the PMM for Oracle E-Business Suite	446
Prerequisites	446
PMM Configuration	446
Running the Install Scripts	446
Adding an Oracle ODBC Driver as a Target Data Source	448
Adding a Microsoft ODBC for Oracle Driver as a Target Data Source	453
Creating a Workflow for a Target	454
Accounts Excluded From Password Reset	455
Configuring the Connector for Oracle E-Business Suite 11i and the Connector for Oracle E-Business Suite R12	456
Upgrading from Oracle E-Business Suite 11i to Oracle E-Business Suite R12:	456
Connector Configuration	456
Configuring the AdminID for a value other than APPS	458
Chapter 50 - Oracle Internet Directory — Connector	463
Configuring the Connector for Oracle Internet Directory	464
Import File Example	468
Chapter 51 - PeopleSoft — PMM and Connector	471
Configuring the PMM for PeopleSoft	472
Prerequisites	472
Using PeopleSoft External APIs	472
Installing the PeopleSoft External APIs on the Connector Framework or Connector Framework Manager	
Servers	472
Installing Java Virtual Machine Versions	473
Configuring PeopleSoft Applications	473
PMM for PeopleSoft Privileged User Permissions	473
PSWDEXPIRED Property in the USER_PROFILE Component Interface	474
Forcing a Password Change on Next Logon	475
PMM Configuration	475
Creating a Workflow for a Target	478

Configuring the Connector for PeopleSoft	479
Prerequisites	479
Privileges Required	479
Configuring the Connector Framework and Connector Framework Manager to Support the PeopleSoft Target	479
Connector Configuration	480
Configuring the Web Services Connector for PeopleSoft Enterprise Applications	483
Configuring PeopleSoft Web Services	483
For PeopleTools 8.44 to 8.46	483
For PeopleTools 8.47 and higher	483
Connector Configuration	483
Notes and Warnings	486
Chapter 52 - Red Hat Enterprise Linux — PMM and Connector	487
Configuring the PMM for Red Hat Enterprise Linux	488
Prerequisites	488
PMM Configuration	488
Creating a Workflow for the Target	490
Writing Password Management Scripts	491
Installing and Configuring the Linux PMM Agent	492
Installing the Agent	492
Configuring the PMM Agent	493
Starting and Stopping the Agent	495
Displaying the Version Information	495
Uninstalling the Agent for Upgrading	495
Configuring the Connector for Red Hat Enterprise Linux	497
Prerequisites	497
Connector Configuration	498
Chapter 53 - Research In Motion BlackBerry 4.x — Connector	501
Configuring the Connector for RIM BlackBerry	502
Connector Configuration	502
Notes and Warnings	504
Chapter 54 - Research In Motion (RIM) BlackBerry 5.x — Connector	505
Installing the BlackBerry Administration Certificate	506
Configuring the Connector for RIM BlackBerry	510
Connector Configuration	510
Notes and Warnings	512
Chapter 55 - RSA Access Manager — PMM	513
Configuring the PMM for RSA Access Manager	514
Prerequisites	514
Note: ExtensionPMM4RSAct.log is the debug log file name for this PMM.	514
Installation	514
PMM Configuration	514
Chapter 56 - RSA Authentication Manager — PMM and Connector	519
Configuring the PMM for RSA Authentication Manager	520
Prerequisites	520
PMM Configuration	520
Notes and Warnings	524
Configuring the Connector for	RSA Authentication Manager 525
Prerequisites	525
Parameters	525
Copying the rsaws.dll file	525
Connector Configuration	525
Notes and Warnings	528
Obtaining the Command Client User Name and Password	529
Obtaining the rsaws.dll File	530

Chapter 57 - RSA SecurID — PMM and Connector	531
Configuring the PMM for RSA SecurID	532
Prerequisites	532
PMM Configuration	533
Creating a Workflow for the Target	535
Notes and Warnings	536
Configuring Targets Using the Token Re-Synchronization Action	536
Configuring Targets using the Generate Emergency One-Time Passcodes Action	536
Configuring the Connector for RSA SecurID	538
Prerequisites	538
Connector Configuration	538
Installing and Configuring the Agent on a UNIX System	540
Installing the Agent on a UNIX System	540
Allowing Resets of Disabled Tokens	541
Configuring the Agent on a UNIX System	541
Starting and Stopping the Agent on a UNIX System	543
Uninstalling the Agent for Upgrading on a UNIX System	543
Installing and Configuring the Agent on a Windows System	544
Installing the Agent on a Windows System	544
Configuring the Agent on a Windows System	544
Reconfiguring the Agent on a Windows System	546
Starting and Stopping the Agent on a Windows System	546
Uninstalling the Agent for Upgrading on a Windows System	546
Chapter 58 - SAP Server — PMMs and Connectors	547
Configuring the PMM for SAP	548
SAP Logon Requirements and Configuration	548
PMM Prerequisites	548
Prerequisites on the Connector Framework and Connector Framework Manager Servers	548
Using the Custom Remote Function Call	548
PMM Configuration	549
Mapping the SAP Servers and Clients Using the Custom Remote Function Call	552
Updated Resource Overrides Administration Manager Form	553
Notes	553
Installing the Remote Function Call (RFC)	554
Creating the Package	554
Creating the Function Group	554
Creating the Function Module	554
Configuring the Connector for SAP	556
SAP Logon Requirements	556
SAP Logon Configuration - Specifying the SAP Server Name	556
Prerequisites	557
Setting the Correct Trust Level	557
SAP Role Support	558
Connector Configuration	558
Notes	562
Configuring the PMM for SAP Logon	563
SAP Logon Prerequisites and Configuration	563
PMM Prerequisites	563
PMM Configuration	563
Notes Regarding the PMMForSAPLogon.vbs Script	566
Configuring the Connector for SAP Logon	567
SAP Logon Requirements and Configuration	567
Connector Configuration	567
Using the SAP Account Discovery Tool	570
Chapter 59 - mySAP.com — PMM	573
Configuring the PMM for mySAP.com	574
Prerequisites	574
Business Connector SAP Configuration	574
Using Multiple R/3 Servers with a Single Business Connector	578
SSL Certificate	579

Privileges Required by the Privileged User	580
PMM Configuration	585
Advanced Properties	588
Specifying Template Files for non-SAP R/3 version 4.6c	588
User Must Change Password at Next Logon	590
Creating a Workflow for the Target	591
Notes and Warnings	591
Chapter 60 - Sun Directory Server — Connector	593
Configuring the Connector for Sun Directory Server	594
Import File Example	598
Authentication Configuration	599
Support for SHA Hashing	600
Chapter 61 - Sun Kerberos — PMM	601
Configuring the PMM for Sun Kerberos	602
Prerequisites	602
PMM Configuration	602
Advanced Properties	605
Creating a Workflow for the Target	605
Chapter 62 - Sun Solaris — PMM and Connector	607
Configuring the PMM for Sun Solaris	608
Prerequisites	608
PMM Configuration	608
Creating a Workflow for a Target	610
Writing Password Management Scripts	611
Installing and Configuring the Sun Solaris PMM Agent	612
Installing the Agent	612
Configuring the Agent	613
Starting and Stopping the Agent	615
Displaying the Version Information	615
Uninstalling the Agent for Upgrading	615
Configuring the Connector for Sun Solaris	616
Prerequisites	616
Scripts that Support Provisioning on Sun Solaris Systems	616
Connector Configuration	616
Chapter 63 - Sybase Adaptive Server Enterprise — PMM and Connector	621
Configuring the PMM for Sybase Adaptive Server Enterprise	622
Prerequisites	622
PMM Configuration	622
Creating a Workflow for a Target	627
Sybase Password Limitations	627
Configuring the Connector for Sybase Adaptive Server Enterprise	628
Sybase ASE Data Source Configuration	628
Connector Configuration	629
Chapter 64 - Using the Cour390 Agent	631
About the Cour390 Agent	632
Cour390 Agent Requirements	632
Installing or Upgrading the Cour390 Agent	633
Configuring the Cour390 Agent	635
Modifying the Sample JCL To Run the Agent	635
Creating the GLOBAL Member	635
Configuring the Security Interface	642
Configuring the RACF Security Interface	642
Sample RACF Member	646
Coexisting with RACF Exits and Other Password Maintenance Products	648
Configuring the CA-ACF2 Security Interface	649
Sample CA-ACF2 Member	651
Configuring the CA-Top Secret Security Interface	653

Sample CA-Top Secret Member	656
Providing Information to the Core Server Administrator	658
Defining Words that Cannot Be Used As Passwords	659
Defining the Reserved Word List	659
Checking and Refreshing the Reserved Word List	659
Using the Cour390 Authorization Checking File	660
Creating the Authorization Checking File	660
Refreshing the Authorization Checking File	661
Operating the Cour390 Agent	662
Commands to the Cour390 Agent	662
FTP Communications Tracing	663
Troubleshooting	664
Members Distributed with the Cour390 Agent	666
Cour390 SMF Report	667
Cour390 SMF Report Program (ESSMFRPT)	667
Format of Cour390 Log Records	668
Cour390 Return Codes	670
Error and Status Messages	672
Appendix A - Installing ActivePerl	695
Installing Required Perl Modules	695

List of Tables

Table 1: Connector Functions	30
Table 2: PMMs and Connectors That Use Agents.	31
Table 3: Core Access Assurance Suite PMMs and Connectors	32
Table 4: Connector Data Types and Control Types for Citrix Published Applications	71
Table 5: PMM Agent for HP-UX Components	108
Table 6: PMM Agent for HP-UX Configuration Parameters Core Server	109
Table 7: Scripts that Support Provisioning on HP-UX Systems.	112
Table 8: PMM Agent for HP-UX 11i v1 Components.	121
Table 9: PMM Agent for HP-UX 11i v1 Configuration Parameters	122
Table 10: PMM Agent for IBM AIX Components	136
Table 11: AIX PMM Agent Configuration ParametersCore Server	137
Table 12: Scripts that Support Provisioning on IBM AIX Systems.	140
Table 13: PMM Agent for OS/400 Commands and KeywordsCore Server	214
Table 14: Configurable Attributes Used for Account Create Trigger to OneSign.	249
Table 15: PMM Configuration Parameters.	337
Table 16: Connector Configuration Parameters	342
Table 17: Support for Provisioning Licenses	343
Table 18: Connector Configuration Parameters	350
Table 19: Support for Provisioning Licenses	351
Table 20: Connector Configuration Parameters	356
Table 21: Support for Provisioning Licenses	357
Table 22: OpenVMS Agents	427
Table 23: OpenVMS Agent Files Core Server	429
Table 24: Parameters for the create_cour_sys.sql script.	459
Table 25: Parameters for APPS connection	460
Table 26: PMM Agent for Linux Components	492
Table 27: PMM agent for Linux Configuration Parameters	493
Table 28: System Parameters	517
Table 29: PMM Configuration Parameters.	522
Table 30: Connector Configuration Parameters	527
Table 31: PMM Agent Configuration Information, RSA SecurID on UNIX Systems Core Server	542
Table 32: Agent Configuration Information for RSA SecurID on Windows	544
Table 33: Configuration parameters for SAP Logon PMM.	565
Table 34: Configuration parameters for Sun Kerberos PMM.	604
Table 35: PMM Agent Components for Sun Solaris	612

Table 36: PMM agent for Sun Solaris Configuration Parameters	613
Table 37: Scripts that Support Provisioning on Sun Solaris Systems	616
Table 38: Essential Parameters in the GLOBAL Member	636
Table 39: Agent Control Parameters	637
Table 40: Cour390 Password Reset Parameters	638
Table 41: Commands to the Cour390 Agent	662
Table 42: Troubleshooting Cour390 Errors.	664
Table 43: Z/OS Members Used with the Cour390 Agent	666
Table 44: Cour390 Relocate Sections	668
Table 45: Cour390 Return Codes	670

List of Figures

Figure 1: PMM and System Components	29
Figure 2: PMM Configuration Manager for BMC Remedy Action Request System	40
Figure 3: Add / Edit Target Configuration for BMC Remedy Action Request System	41
Figure 4: Properties	42
Figure 5: Add BMC Remedy Action Request System Target	44
Figure 6: Connector Configuration Manager for BMC Remedy Action Request System	45
Figure 7: PMM Configuration Manager for CA eTrust SiteMinder	50
Figure 8: Add/Edit Target Configuration for CA eTrust SiteMinder	51
Figure 9: Connector Configuration Manager Main Window	56
Figure 10: Selecting a Connector to Add	57
Figure 11: Add Target Dialog Box	61
Figure 12: Connector Configuration for PMM Targets Dialog Box	62
Figure 13: Add Citrix Target	64
Figure 14: Connector Configuration Manager for Citrix-SSO	65
Figure 15: Enter Account Attributes Screen with Citrix Applications	69
Figure 16: Applications Not Available	70
Figure 17: Control Type on the Unique Target Data Form	71
Figure 18: Add Citrix-CPS-Cnctr Target	72
Figure 19: Connector Configuration Manager for Technology Connector	73
Figure 20: Add Role Connector Target	78
Figure 21: Role Connector Configuration Manager	79
Figure 22: Add SQL Usage Target	82
Figure 23: Connector Configuration Manager for SQL Usage	83
Figure 24: Add JavaScript Macros Target	86
Figure 25: Add VBScript Macros Target	90
Figure 26: Add Web Services Target	92
Figure 27: Connector Configuration Manager for Web Services	93
Figure 28: Add Epic Target	96
Figure 29: Connector Configuration Manager for Epic	97
Figure 30: Add HP OpenView ServiceCenter Target	101
Figure 31: Connector Configuration Manager for HP Software Service Manager	101
Figure 32: PMM Configuration Manager	104
Figure 33: Add/Edit UNIX System User	105
Figure 34: Add HP-UX Target	113
Figure 35: Connector Configuration Manager for HP-UX	113

Figure 36: Connector Configuration Manager for HP-UX (2)	114
Figure 37: PMM Configuration Manager	118
Figure 38: Add/Edit HPUX 11i v1 System PMM Configuration	119
Figure 39: Add HTML Email Target	126
Figure 40: Connector Configuration Manager for HTML Email	127
Figure 41: Add HTML Email Target	128
Figure 42: Connector Configuration Manager for HTML Email	129
Figure 43: PMM Configuration Manager for IBM AIX	132
Figure 44: Add / Edit UNIX System PMM Configuration for IBM AIX	133
Figure 45: Add IBM AIX Target	141
Figure 46: Connector Configuration Manager for IBM AIX	141
Figure 47: Connector Configuration Manager for IBM AIX (2)	142
Figure 48: PMM Configuration Manager for IBM Lotus Domino	147
Figure 49: PMM Configuration Manager for IBM Lotus Notes	151
Figure 50: Target Information	152
Figure 51: Temporary Directory Information	154
Figure 52: Domino Privileged User Information	155
Figure 53: Logon Username Identification	156
Figure 54: Network Server Information	158
Figure 55: Download Path Location	160
Figure 56: Password Digest Information	161
Figure 57: ID Database Information	162
Figure 58: ID Filename Information	163
Figure 59: Password Database Information	164
Figure 60: ID Vault Privileged Information	166
Figure 61: Add IBM Lotus Target	172
Figure 62: Connector Configuration Manager for IBM Lotus	173
Figure 63: PMM Configuration Manager for z/OS (OS/390)	181
Figure 64: Add/Edit Target Configuration with TCP/IP selected	182
Figure 65: Add/Edit Target Configuration with SNA selected	183
Figure 66: Add CA-ACF2 Target	186
Figure 67: Connector Configuration Manager for CA-ACF2 - TCP/IP	186
Figure 68: Connector Configuration Manager for CA-ACF2 - SNA	187
Figure 69: PMM Configuration Manager for z/OS (OS/390)	191
Figure 70: Add/Edit Target Configuration with TCP/IP selected	192
Figure 71: Add/Edit Target Configuration with SNA selected	193
Figure 72: Add CA-Top Secret Target	196
Figure 73: Connector Configuration Manager for CA-Top Secret	196
Figure 74: PMM Configuration Manager for z/OS (OS/390)	201
Figure 75: Add/Edit Target Configuration with TCP/IP selected	202
Figure 76: Add/Edit Target Configuration with SNA selected	203
Figure 77: Add RACF Target	206
Figure 78: Connector Configuration Manager for RACF - TCP/IP	206

Figure 79: Connector Configuration Manager for RACF - SNA	207
Figure 80: PMM Configuration Manager for OS/400	210
Figure 81: PMM for OS/400 Configuration Parameters	211
Figure 82: PMM Agent for OS/400 Menu	221
Figure 83: PMM Agent for OS/400 Configuration (PMMCFG)	221
Figure 84: PMM Agent for OS/400 Start Screen.	222
Figure 85: PMM Agent for OS/400 Menu	222
Figure 86: PMM Agent for OS/400 Configuration (PMMCFG), Screen One.	223
Figure 87: PMM Agent for OS/400 Configuration (PMMCFG), Screen Two.	224
Figure 88: PMM Agent for OS/400 Start (STRPMM)	225
Figure 89: PMM Agent for OS/400 Print Configuration Files	225
Figure 90: PMM for OS/400 Maintain Excluded Profiles Table.	226
Figure 91: PMM Agent for OS/400 End	227
Figure 92: PMM Agent for OS/400 Active Jobs	227
Figure 93: PMM Agent for OS/400 Inactive Job	228
Figure 94: Add OS/400 Target	230
Figure 95: Connector Configuration Manager for IBM OS/400.	231
Figure 96: AMM (Connector) Agent for OS/400 Menu	236
Figure 97: AMM (Connector) Agent for OS/400 Configuration (AMMCFG) Screen 1	237
Figure 98: AMM (Connector) Agent for OS/400 Configuration (AMMCFG) Screen 2	238
Figure 99: AMM (Connector) Agent for OS/400 Start Menu.	238
Figure 100: AMM (Connector) Agent for OS/400 End	239
Figure 101: AMM (Connector) Agent for OS/400 Active Jobs Screen	240
Figure 102: Imprivata Certificate Download	246
Figure 103: Add Imprivata OneSign Target	247
Figure 104: Connector Configuration Manager for Imprivata OneSign.	248
Figure 105: PMM Configuration Manager for Kronos Workforce Central	252
Figure 106: Add/Edit Target Configuration for Kronos Workforce Central	253
Figure 107: Add Kronos Workforce Central Target.	255
Figure 108: Connector Configuration Manager for Kronos Workforce Central.	256
Figure 109: PMM Configuration Manager for Active Directory	260
Figure 110: Add/Edit Target Configuration for Active Directory	261
Figure 111: Add Active Directory Target.	266
Figure 112: Connector Configuration Manager for Active Directory	267
Figure 113: Add Microsoft ADAM Target	272
Figure 114: Connector Configuration Manager for Microsoft ADAM	273
Figure 115: Add Microsoft Active Directory Attribute Trigger Target	277
Figure 116: Connector Configuration Manager for Microsoft Active Directory Attribute Trigger.	277
Figure 117: Trigger Subform.	279
Figure 118: Add Microsoft ActiveScript Target	282
Figure 119: Connector Configuration Manager for Microsoft ActiveScript	283
Figure 120: Connector Configuration Manager for Microsoft ActiveScript (2)	284
Figure 121: Add Microsoft ADO Target.	290

Figure 122: Connector Configuration Manager for ADO	291
Figure 123: Data Link Properties (Provider)	291
Figure 124: Data Link Properties (Connection)	292
Figure 125: Add Microsoft Exchange 5.5 Target	296
Figure 126: Connector Configuration Manager for Microsoft Exchange 5.5	297
Figure 127: Add Microsoft Exchange 2000 Target	301
Figure 128: Connector Configuration Manager for Microsoft Exchange 2000	302
Figure 129: Add Microsoft Exchange 2007 or 2010 Target	308
Figure 130: Connector Configuration Manager for Microsoft Exchange 2007 and 2010	309
Figure 131: Add MIIIS Target	313
Figure 132: Connector Configuration Manager for MIIIS	314
Figure 133: Data Link Properties 1	314
Figure 134: Data Link Properties 2	315
Figure 135: Connector Configuration Manager Dialog Box Partially Completed	316
Figure 136: Add ODBC Target	319
Figure 137: Connector Configuration Manager for ODBC	320
Figure 138: Select System Data Source	320
Figure 139: Authorize ODBC Database Access	321
Figure 140: Create New Microsoft Access Data Source	322
Figure 141: Select Microsoft Access Driver	323
Figure 142: New Microsoft Access Data Source - Summary	323
Figure 143: Set Up Microsoft Access Data Source	324
Figure 144: Select Microsoft Access Database	324
Figure 145: Setup Microsoft Access Data Source - Done	324
Figure 146: Select System for Microsoft Access Data Source - Done	325
Figure 147: Create New Microsoft SQL Server Data Source	325
Figure 148: Select Microsoft SQL Server Driver	326
Figure 149: New Microsoft SQL Server Data Source - Summary	326
Figure 150: Setup Microsoft SQL Server Data Source	327
Figure 151: Setup Microsoft SQL Server Data Source - Authentication	327
Figure 152: Setup Microsoft SQL Server Data Source - Select Database	328
Figure 153: Setup Microsoft SQL Server Data Source - Log Files	328
Figure 154: Setup Microsoft SQL Server Data Source - Summary	329
Figure 155: Setup Microsoft SQL Server Data Source - Successful Configuration	329
Figure 156: Create New Oracle Data Source	330
Figure 157: Select Oracle Driver	330
Figure 158: New Oracle Data Source - Summary	331
Figure 159: Set Up Oracle Data Source	331
Figure 160: PMM Configuration Manager for Office365	335
Figure 161: Add/Edit Target Configuration	336
Figure 162: Advanced Properties	337
Figure 163: Add Microsoft Office365 Exchange Online Target	341
Figure 164: Connector Configuration Manager	341

Figure 165: Add Microsoft Office365 Lync Online Target.	349
Figure 166: Connector Configuration Manager.	349
Figure 167: Add Microsoft Office365 SharePoint Online Target.	355
Figure 168: Connector Configuration Manager.	355
Figure 169: PMM Configuration Manager for Microsoft SQL Server	361
Figure 170: Add/Edit Target for Microsoft SQL Server	362
Figure 171: Machine Data Source	362
Figure 172: Create New Data Source Screen	363
Figure 173: Data Source Driver Selection Screen	363
Figure 174: Create New Data Source Summary Screen	364
Figure 175: Create a New Data Source to SQL Server Dialog Box	364
Figure 176: Partially Completed Add/Edit Target Databases	365
Figure 177: Add Microsoft SQL Server.	367
Figure 178: Connector Configuration Manager for Microsoft SQL Server	368
Figure 179: Add Microsoft VBScript Target	370
Figure 180: Connector Configuration Manager for Microsoft VBScript.	371
Figure 181: Connector Configuration Manager for Microsoft VBScript (2)	372
Figure 182: PMM Configuration Manager for Windows NT and Windows 2000.	377
Figure 183: Add/Edit Target Configuration for Windows NT and Windows 2000	378
Figure 184: Add Windows NT Target	383
Figure 185: Connector Configuration Manager for Windows NT	384
Figure 186: PMM Configuration Manager for Netscape Directory Server	389
Figure 187: Add / Edit for Netscape Directory Server.	390
Figure 188: PMM Agent for Netscape Directory Server and iPlanet Directory Server	392
Figure 189: Add Netscape SMTP Target	396
Figure 190: Connector Configuration Manager for Netscape SMTP	397
Figure 191: PMM Configuration Manager for Novell GroupWise	400
Figure 192: Add/Edit Target Configuration for Novell GroupWise	401
Figure 193: Add Novell GroupWise Target.	404
Figure 194: Connector Configuration Manager for Novell GroupWise	404
Figure 195: PMM Configuration Manager for Novell NDS eDirectory.	409
Figure 196: Add Novell NDS eDirectory Target	412
Figure 197: Connector Configuration Manager for Novell NDS eDirectory	412
Figure 198: Linux Target User Prompt	416
Figure 199: Linux Password Verification Prompt	416
Figure 200: New and Verify New Password Prompt.	417
Figure 201: Add Red Hat Enterprise Linux Target	418
Figure 202: Connector Configuration Manager for Red Hat Enterprise Linux	418
Figure 203: PMM Configuration Manager for OpenVMS	423
Figure 204: PMM Parameters for OpenVMS	423
Figure 205: Add OpenVMS Target	425
Figure 206: Connector Configuration Manager for OpenVMS	426
Figure 207: PMM Configuration Manager for Oracle 8i/9i	435

Figure 208: Add/Edit Target for Oracle 8i/9i	435
Figure 209: Machine Data Source	436
Figure 210: Create New Data Source	437
Figure 211: Driver Selection	437
Figure 212: Oracle ODBC Driver Setup	438
Figure 213: Partially Completed Add/Edit Target Databases	438
Figure 214: Add Oracle 8i/9i Target	441
Figure 215: Connector Configuration Manager for Oracle 8i/9i	442
Figure 216: SQL PLus Logon	447
Figure 217: Logon Successful Message	447
Figure 218: PMM Configuration Manager for Oracle E-Business	448
Figure 219: Add/Edit Target Configuration Dialog Box for Oracle E-Business	449
Figure 220: Select Data Source	449
Figure 221: Machine Data Source List	450
Figure 222: Create a New Data Source	450
Figure 223: List of Drives in Create New Data Source	451
Figure 224: Oracle8 ODBC Driver Setup	451
Figure 225: Oracle8 ODBC Driver Connect	452
Figure 226: Add/Edit Configuration Target with Oracle Target	452
Figure 227: Microsoft ODBC for Oracle Setup	453
Figure 228: Microsoft ODBC for Oracle Connect	453
Figure 229: Add/Edit Target Configuration	454
Figure 230: Add Oracle E-Business Target	457
Figure 231: Connector Configuration Manager for Oracle E-Business	457
Figure 232: Run create_cour_sys.sql	459
Figure 233: Parameters for the create_cour_sys.sql script	460
Figure 234: Prompt for the Connector User Name	461
Figure 235: Run create_synonyms_cour.sql	461
Figure 236: Add Oracle Internet Directory Target	464
Figure 237: Connector Configuration Manager for Oracle Internet Directory	465
Figure 238: Connector Configuration Manager for Oracle Internet Directory Server (2)	466
Figure 239: Connector Configuration Manager for Oracle Internet Directory Server (3)	467
Figure 240: Component Interface Permissions	474
Figure 241: PMM Configuration Manager for PeopleSoft	475
Figure 242: PMM Configuration Manager for PeopleSoft- Add Target	476
Figure 243: Add PeopleSoft Target	481
Figure 244: Connector Configuration Manager for PeopleSoft	481
Figure 245: Add PeopleSoft PeopleTools 8.48 Target	484
Figure 246: Connector Configuration Manager for PeopleSoft PeopleTools 8.48	484
Figure 247: Connector Configuration Manager for PeopleSoft PeopleTools 8.48	485
Figure 248: PMM Configuration Manager for Red Hat Enterprise Linux	488
Figure 249: Add / Edit UNIX System PMM Configuration for Red Hat Enterprise Linux	489
Figure 250: Linux Target User Prompt	497

Figure 251: Linux Password Verification Prompt	497
Figure 252: New and Verify New Password Prompt.	498
Figure 253: Add Red Hat Enterprise Linux Target	499
Figure 254: Connector Configuration Manager for Red Hat Enterprise Linux	499
Figure 255: Add RIM BlackBerry Target.	503
Figure 256: Connector Configuration Manager for RIM BlackBerry	503
Figure 257: BlackBerry Administration Service.	506
Figure 258: Viewing the Administration Certificate	507
Figure 259: Install Certificate	508
Figure 260: Certificate Import Wizard	508
Figure 261: Select Certificate Store	509
Figure 262: Certificate Import Wizard with Certificate Store Populated	509
Figure 263: Add RIM BlackBerry Target.	511
Figure 264: Connector Configuration Manager for RIM BlackBerry	511
Figure 265: Add Target Dialog Box.	515
Figure 266: The Add/Edit Target Configuration Dialog Box for RSA Access Manager	516
Figure 267: Advanced Properties Dialog Box.	517
Figure 268: PMM Configuration Manager for RSA Authentication Manager 7	521
Figure 269: Add/Edit Target Configuration for RSA Authentication Manager.	522
Figure 270: Advanced Properties Dialog Box.	524
Figure 271: Add RSA Authentication Manager Target	526
Figure 272: Connector Configuration Manager for RSA Authentication Manager	527
Figure 273: C# API Reference Guide	530
Figure 274: PMM Configuration Manager for RSA SecurID	533
Figure 275: Add/Edit RSA SecurID System PMM Configuration	534
Figure 276: Add RSA SecurID Target.	538
Figure 277: Connector Configuration Manager for RSA SecurID	539
Figure 278: PMM Configuration Manager for SAP	549
Figure 279: Add/Edit Target Configuration for SAP	550
Figure 280: Resource Overrides Administration Manager Form	553
Figure 281: SAP Logon Configuration	556
Figure 282: SAP Logon Properties Dialog Box.	557
Figure 283: Add SAP Target.	559
Figure 284: Connector Configuration Manager for SAP	559
Figure 285: Connector for SAP Advanced Properties	561
Figure 286: PMM Configuration Manager for SAP Logon	564
Figure 287: Add/Edit Target Configuration for SAP Logon.	565
Figure 288: Add SAP Logon Target	568
Figure 289: Connector Configuration Manager for SAP Logon	568
Figure 290: SAP Servers Defined in the Business Connector	575
Figure 291: Routing Rules in the Business Connector	575
Figure 292: SAP Routing Rule Defined 1	576
Figure 293: SAP Routing Rule Defined 2	576

Figure 294: SAP Routing Rule Defined 3	577
Figure 295: SAP Routing Rule Defined 4	577
Figure 296: SAP Routing Rule Defined 5	578
Figure 297: Create New User	581
Figure 298: Create New Group	581
Figure 299: Add New User to New Group	582
Figure 300: Associate Group to SAPUsers ACL	582
Figure 301: Associate Group to Internal ACL	583
Figure 302: User Assigned to System User Type	584
Figure 303: User Assigned to Profiles	585
Figure 304: PMM Configuration Manager for mySAP.com	586
Figure 305: Add / Edit Target Configuration for mySAP.com	587
Figure 306: Advanced Properties	588
Figure 307: SAP Business Connector Interface	589
Figure 308: SAP Adapters	589
Figure 309: bXML Template	590
Figure 310: Add Sun Directory Server Target	594
Figure 311: Connector Configuration Manager for Sun Directory Server	595
Figure 312: Connector Configuration Manager for Sun Directory Server (2)	596
Figure 313: Connector Configuration Manager for Sun Directory Server (3)	597
Figure 314: PMM Configuration Manager for Sun Kerberos	602
Figure 315: Add / Edit Target Configuration for Sun Kerberos	603
Figure 316: Advanced Properties	605
Figure 317: PMM Configuration Manager for Sun Solaris	609
Figure 318: Add / Edit UNIX System PMM Configuration for Sun Solaris	609
Figure 319: Add Sun Solaris Target	617
Figure 320: Connector Configuration Manager for Sun Solaris	617
Figure 321: Connector Configuration Manager for Sun Solaris (2)	618
Figure 322: PMM Configuration Manager for Sybase ASE	623
Figure 323: Add/Edit Target for Sybase ASE	623
Figure 324: Machine Data Source	624
Figure 325: Create New Data Source	625
Figure 326: Data Source Driver Selection	625
Figure 327: Create New Data Source Summary	626
Figure 328: ODBC Sybase Driver Setup	626
Figure 329: Sybase ASE Data Source Configuration	628
Figure 330: Sybase ASE Test Connection	629
Figure 331: Add Sybase ASE Target	629
Figure 332: Connector Configuration Manager for Sybase ASE	630
Figure 333: Sample RACF Member	646
Figure 334: Sample CA-ACF2 Member	651
Figure 335: Sample CA-Top Secret Member	656
Figure 336: Sample CA-Top Secret Member (Continued)	657

Chapter 1: About Password Management Modules (PMMs) and Connectors

This manual explains how to install and configure Core Access Assurance Suite Password Management Modules (PMMs) and Connectors. PMMs and Connectors provide an interface between Core Access Assurance Suite applications and target systems.

PMMs are interfaces to the target systems where you want to reset passwords. Connectors are interfaces for provisioning platform applications (the Core Provisioning[®] solution, the RoleCourier[®] role management solution, the Core Compliance[™] policy verification solution, the ProfileCourier profile management solution, and the Core Password[®] provisioning solution).

This chapter includes the following topics:

- [*"Password Management Module \(PMM\) Functionality" on page 29*](#)
- [*"Password Management Module \(PMM\) Functionality" on page 29*](#)
- [*"Connector Functionality" on page 30*](#)
- [*"Connector and PMM Summary" on page 32*](#)

Creating Custom Connectors with the Connector Rapid Development Kit

For targets not supported by a specific Core Access Assurance Suite connector, you can create your own using the connector Rapid Development Kit (RDK). Contact your Core Security sales representative for information about how to obtain the connector Rapid Development Kit (RDK).

Password Management Module (PMM) Functionality

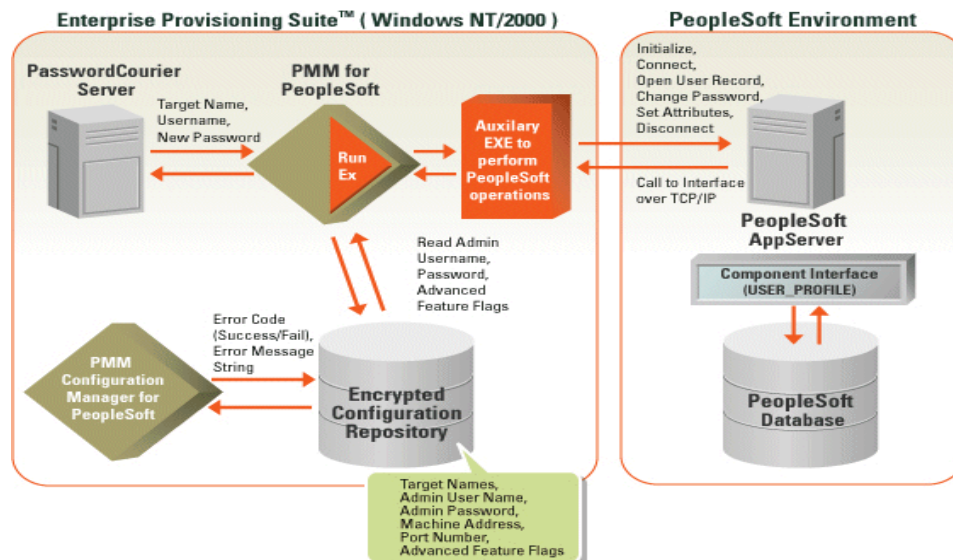
A Password Management Module (PMM) provides these functions:

- Resets user passwords on targets (host systems)
- Enforces security rules specified on targets
- Provides synchronization of a user's password on multiple targets

As with connectors, Core Security offers PMMs for various manufacturers' platforms. The PMMs enabled at your site depend on the access keys you ordered with the Core Access Assurance Suite.

[Figure 1](#) shows the PMM for PeopleSoft as it works with system components.

Figure 1: PMM and System Components



Connector Functionality

A connector provides these functions:

- Adding modifying, and deleting configurations for target systems
- Interacting with the Administration Manager during configuration of workflows
- Fulfilling provisioning, compliance, password reset, and other requests from the provisioner

Core Security offers connectors for various manufacturers' platforms. The connectors enabled at your site depend on the access keys you ordered with the Core Access Assurance Suite.

Different connectors support the following different functions, as follows.

Table 1: Connector Functions

Connector Type	Function
Provisioning and Compliance Actions	Enables an application to execute provisioning and compliance actions and password resets on a target system. For example, a connector can create a user account on a Microsoft Active Directory domain. Note: When you configure a connector to add a target for actions, you make that target available for all actions appropriate to the connector. You cannot make targets available for individual provisioning actions. (However, once the connector is available for actions, you still need to configure the connector for individual actions within a workflow, using the Administration Manager.)
Authentication	Enables an application to authenticate end users against supported target data sources, such as ODBC-compliant databases and LDAP-enabled directories.
Query	Enables an application to retrieve data from supported target data sources, such as ODBC-compliant databases, using native query statements.
Ticketing	Enables an application to create and update tickets for provisioning events in target Help Desk applications, such as the BMC Remedy Action Request System or the HP OpenView ServiceCenter (previously known as Peregrine Service Center). Ticketing is also available for ODBC data sources.
Notification	Enables an application to send SMTP-based e-mail messages to end users that can note event success or failure, or include the URL that enables an end user to launch a provisioning workflow.
IdentityMap™	Enables an application to create IdentityMap records.
Transaction Repository	Provides a persistent storage for request records, delegation records, verification information, and password history.
Gateway	Provides access to password management modules (PMMs).

PMM and Connector Agents

Some PMMs and Connectors require agents. Each agent acts as the interface between a PMM or connector and the platform. The platform chapters of this manual describe installing and using any agents required, except for the Cour390 agent. The Cour390 agent is explained in its own chapter, [“Using the Cour390 Agent” on page 631](#)

The PMMs and connectors that use agents are listed in [Table 2](#).

Table 2: PMMs and Connectors That Use Agents

Platform	Agent Name
HP-UX® operating system, PMM agent	pwdcour_unixpxy
IBM AIX operating system, PMM agent	pwdcour_unixpxy
IBM z/OS systems with CA-ACF2, PMM agent	Cour390
IBM z/OS systems with RACF, PMM agent	Cour390
IBM i5/OS systems Connector agent	COURAMM
IBM i5/OS systems PMM agent	COURAGENT
Linux™ PMM agent	pwdcour_unixpxy
Netscape Directory Server and iPlanet Directory Server, PMM agent	CourNSLDAPAgent
OpenVMS™ for VAX® and Alpha Platforms, PMM and connector agent	COURION_PROXY.EXE
RSA SecurID, PMM and connector agent (connector agent on Windows only)	AIX: pwdcour_SecurIDpxy HP-UX and Sun Solaris: S99pwdcour_SecurIDpxy Windows: CourSecurIDAgent
Sun Solaris operating system, PMM	pwdcour_unixpxy

Connector and PMM Summary

[Table 3](#) lists the Core Access Assurance Suite PMMs and Connectors alphabetically by platform.

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
BMC Remedy Action Request System Version 3.X	Remedy-ARSAPI-3.x, page 43	Add, Change, Create, Delete, Disable, Enable, Verify, View Audit: Create Ticket, Update Ticket Authentication, Query	Remedy Action Request System, page 40
CA eTrust SiteMinder (previously known as Netegrity SiteMinder)	none	n/a	CA eTrust-Netegrity Siteminder, page 49
Citrix XenApp (previously known as Citrix Presentation Server)	Citrix-CPS-Cnctr, page 68	Add, Change, Create, Delete, Verify, View	none
Citrix SSO	Citrix-SSO-Cnctr, page 64	Trigger	none
Core Function	Core-Function-Cnctr	Used when you create Functions (see <i>Configuring Workflows with the Core Access Assurance Suite Administration Manager</i>); no configuration required	none
Courion Role Connector	Courion-Role-Cnctr, page 78	Add, Change, Create, Delete, Disable, Enable, Verify, View Query, Trigger	none
Courion SQL Usage	Cour-SQLUsage-1.0, page 82	Trigger	none
Courion JavaScript Custom Macros	Courion-JavaScriptMacro-10, page 27	Query, Trigger	non
Courion VBScript Custom Macros	Courion-VBScriptMacro-1.0, page 90	Query	none
Courion Web Services	Courion-WebService-Cnctr, page 92	Add, Change, Create, Delete, Disable, and Enable	Courion Web Services
Epic	Epic, page 96	Add, Change, Create, Delete, Disable, Enable	none

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
HP Software Service Manager (previously known as Peregrine ServiceCenter)	Peregrine-ServiceCenter-SCAuto, page 100	Audit: Create Ticket, Update Ticket	none
HP-UX Operating System	HP-UP-UX-Cnctr page 112	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication	HP-UX, page 104
HTML Email	Microsoft-CDO.Message-Cnctr, page 126 Courion-HTML Email-Cnctr2 (enhanced with support for character sets), page 128	Notification	none
IBM AIX Operating System	IBM-AIX-Cnctr, page 140	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication	IBM AIX, page 132
IBM Lotus	IBM-Lotus, page 171	Add, Change, Create, Delete, Disable, Enable, Verify, View Trigger	IBM Lotus Domino, page 146 IBM Lotus Notes, page 150
IBM z/OS Systems (previously known as OS/390) with CA-ACF2	CA-ACF2-Cnctr, page 185	Add, Change, Create, Delete, Disable, Enable, Verify, View	CA-ACF2, page 180
IBM z/OS Systems (previously known as OS/390) with CA-Top Secret	CA-TopSecret-Cnctr, page 195	Add, Change, Create, Delete, Disable, Enable, Verify, View	CA-Top Secret page 190
IBM z/OS Systems (previously known as OS/390) with RACF	IBM-RACF-2.x page 205	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication, Query	RACF, page 200
IBM i (previously known as OS/400, i5/OS)	IBM-OS400-V4R5, page 230	Add, Change, Create, Delete, Disable, Enable, Verify, View	OS400, page 210
Imprivata OneSign	Imprivata-OneSign-Cnctr, page 244	Trigger	none

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
Kronos Workforce Central	Kronos-WFC-Cnctr, page 255	Add, Change, Create, Delete, Disable, Enable, Verify, View	Kronos Workforce Central, page 252
Microsoft Active Directory (AD)	Microsoft-ADS-5.x, page 266	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication, Query	Active Directory, page 258
Microsoft Active Directory Application Mode (ADAM)	Microsoft-ADAM-Cnctr, page 272	Add, Change, Create, Delete, Disable, Enable, Verify, View Trigger	none
Microsoft Active Directory Attribute Trigger	ADAttribute-Trigger_Cnctr, page 27	Trigger	none
Microsoft Active Script	Microsoft-ActiveScript-Cnctr, page 282	Add, Change, Create, Delete, Disable, Enable, Verify, View Audit: Create Ticket, Update Ticket Authentication, Notification, Query, Triggers	none
Microsoft ADO (ActiveX Data Objects)	Microsoft-ADO-3.0, page 288	Change, Create, Delete, Verify, View Audit: Create Ticket, Update Ticket Authentication, Query, Trigger Transaction Repository,	none
Microsoft Exchange 5.5	Microsoft-Exchange-5.5, page 296	Add, Change, Create, Delete, Disable, Enable, Verify, View	none
Microsoft Exchange 2000	Microsoft-Exchange-2000, page 300	Add, Change, Create, Delete, Disable, Enable, Verify, View	none
Microsoft Exchange 2007	Microsoft-Exchange-2007, page 306	Add, Change, Create, Delete, Disable, Enable, Verify, View	none
Microsoft Identity Integration Server (MIIS)	Microsoft-MIIS-Cnctr, page 312	Verify, View Authentication, Query	none
Microsoft ODBC-3.0	Microsoft-ODBC-3.0, page 318	Change, Create, Delete, Verify, View Audit: Create Ticket, Update Ticket Authentication, Query	none
Microsoft Office365	none	n/a	Microsoft Office365, page 333

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
Microsoft Office365 Exchange Online	Microsoft-Office365-ExchangeOnline-v1.0, page 339	Add, Change, Create, Delete, Disable, Enable, Verify, View Native Query Collector, Trigger	none
Microsoft Office365 Lync Online	Microsoft-Office365-LyncOnline-v1.0, page 347	Add, Change, Create, Delete, Disable, Enable, Verify, View Native Query, Collector	none
Microsoft Office365 SharePoint Online	Microsoft-Office365-SharePointOnline-v1.0, page 353	Add, Change, Create, Delete, Disable, Enable, Verify, View Native Query, and Collector	none
Microsoft SQL Server	MSFT-SQL Server-Cnctr, page 367	Add, Change, Create, Delete, Disable, Enable, Verify, View	Microsoft SQL Server page 360
Microsoft Windows 2000, Windows NT	Microsoft-WNTDomain-4.x, page 383	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication, Query	Windows NT and Windows 2000, page 374
Microsoft VBScript-5.6	Microsoft-VBScript-5.6, page 370	Add, Change, Create, Delete, Disable, Enable, Verify, View Audit: Create Ticket, Update Ticket Authentication, Notification, Query, Trigger	none
Netscape/iPlanet Directory Server	See Sun Directory Server	n/a	Netscape Directory Server, page 388
Netscape SMTP	Netscape-SMTP-3.5, page 395	Notification	none
Novell GroupWise	Novell-Groupwise-Cnctr, page 403	Add, Change, Create, Delete, Disable, Enable, Verify, View	Novell GroupWise, page 400
Novell NDS eDirectory	Novell-NDS-4.x, page 411	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication	Novell NDS, page 408
Novell NetWare Bindery	none	n/a	Novell Netware Bindery, page 408
Novell SUSE Linux Enterprise	Novell SUSE-Linux Enterprise-Cnctr, page 416	Add, Change, Create, Delete, Disable, Enable, Verify, View	none
OpenVMS for VAX and Alpha Platforms	HP-OpenVMS-Cnctr, page 425	Add, Change, Create, Delete, Disable, Enable, Verify, View	OpenVMS, page 422

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
Oracle Database 8i 9i	Oracle-Databases-8i/9i, page 441	Add, Change, Create, Delete, Disable, Enable, Verify, View	Oracle Database, page 434
Oracle E-Business Suite 11i and Oracle E-Business Suite R12	Oracle E-Business, page 456	Add, Change, Create, Disable, Enable, Verify, View	Oracle E-Business Suite, page 446
Oracle Internet Directory and Oracle Directory Server Enterprise.	Oracle-InternetDirectoryServer-Cnctr, page 464	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication, Query, Trigger	none
PeopleSoft	Peoplesoft-CI-8.x, page 479 PS-PT848WS-Cnctr, page 483	Add, Change, Create, Delete, Disable, Enable, Verify, View Add, Change, Create, Delete, Disable, Enable, View	PeopleSoft, page 472
Perl	Perl-Perl-5.8 See "Installing ActivePerl" on page 695.	Same as connector it works with	none
PMM Gateway	PMM-Gateway-Cnctr, page 61	Password Reset	none
Red Hat Linux Enterprise	Red Hat-Enterprise Linux-Cnctr, page 497	Add, Change, Create, Delete, Disable, Enable, Verify, View	Linux, page 488
Research in Motion Blackberry 4.x	Research In Motion-BlackBerry-Cnctr, page 502	Add, Change, Create, Delete, Disable, Verify, View	none
Research in Motion Blackberry 5.x	Research In Motion-Blackberry5x-Cnctr, page 505	Add, Change, Create, Delete, Disable, Enable, Verify, and View	none
RSA Access Manager	none	n/a	RSA Access Manager, page 514
RSA Authentication Manager	RSA-Authentication Manager-71, page 525	Add, Change, Create, Delete, Disable, Enable, Verify, View, Authentication, Query	RSA Authentication Manager, page 520
RSA SecurID	RSA-SecurID-Cnctr, page 538	Add, Change, Create, Delete, Disable, Enable, Verify, View	RSA SecurID, page 532
SAP R/3 Systems	SAP-Cnctr, page 556 SAP Logon-Cnctr, page 567	Add, Change, Create, Delete, Disable, Enable, Verify, View Add, Change, Create, Delete, Disable, Enable	SAP R/3, page 548 SAP Logon, page 563
mySAP.com	none	n/a	mySAP.com, page 574

Table 3: Core Access Assurance Suite PMMs and Connectors

Target System	Provisioning Connector	Connector Operations Supported	PMM
Sun Directory Server (for PMM, see Sun Solaris)	Sun-Directory-Server-Cnctr, page 593 Netscape/iPlanet Server, NscplPlanetCnctr.dll	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication, Query, Trigger	none
Sun Kerberos	none	n/a	Sun Kerberos, page 602
Sun Solaris Operating System	Sun-Solaris-Cnctr, page 616	Add, Change, Create, Delete, Disable, Enable, Verify, View Authentication	Sun Solaris, page 608
Sybase Adaptive Server Enterprise	Sybase-ASE-Cnctr, page 628	Add, Change, Create, Delete, Disable, Enable, View	Sybase, page 622

See the following manuals to create workflows that use the connectors and PMMs you configure:

Configuring Workflows with the Core Access Assurance Suite Administration Manager, for applications on the provisioning platform.

Using PasswordCourier and PasswordCourier Support, for PasswordCourier and PasswordCourier Support Staff on the Classic Platform.

Chapter 2: BMC Remedy Action Request System — PMM and Connector

This chapter explains how to configure the PMM and Connector for the BMC® Remedy® Action Request System® (formerly known as Remedy Action Request System):

- [*“Configuring the PMM for BMC Remedy Action Request System” on page 40*](#)
- [*“Configuring the Connector for BMC Remedy Action Request System 3.x” on page 43*](#)

Configuring the PMM for BMC Remedy Action Request System

The Password Management Module (PMM) for BMC Remedy Action Request System enables PasswordCourier or PasswordCourier Support Staff to automatically reset passwords for end users of the BMC Remedy Action Request System. This PMM is installed when the Access Assurance Suite is installed.

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Security.

Prerequisites

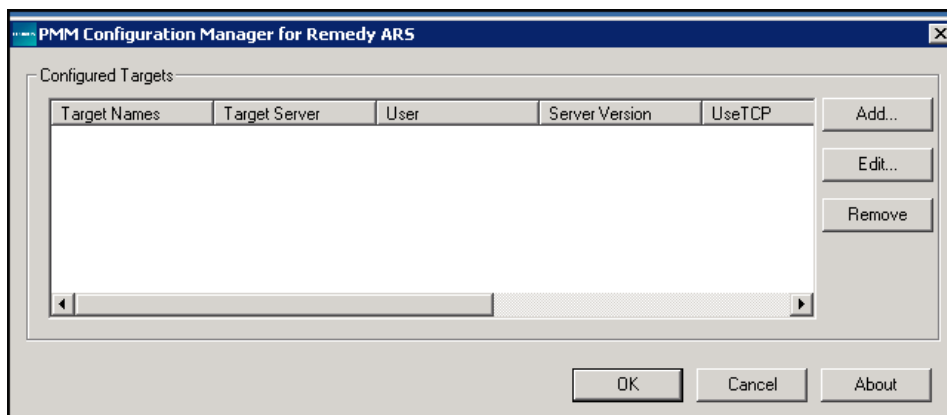
The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

This version of the PMM for BMC Remedy Action Request System supports password resets for one or more BMC Remedy Action Request System servers.

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Password Management Modules
>Remedy Action Request System
The PMM Configuration Manager appears.

Figure 2: PMM Configuration Manager for BMC Remedy Action Request System



2. From this dialog box, you can
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.

- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the **ADD** or **EDIT** option from the PMM, the **ADD/EDIT TARGET CONFIGURATION** dialog box appears.

Figure 3: Add / Edit Target Configuration for BMC Remedy Action Request System

3. **ADD/EDIT TARGET CONFIGURATION**

- AR TARGET NAME** — Enter a descriptive target name. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
- AR SERVER** — Enter the name of the Action Request Server on which passwords are reset.
- ADMINISTRATIVE USER** — Enter a Remedy Administrative username and password for that server.
- REMEDY SERVER VERSION** — Select the correct Remedy Server version.

4. **TCP PORT:**

- USE DYNAMIC TCP PORT** — This option specifies that the PMM uses an available TCP port on the Remedy server. If the Remedy server is configured to use the Port Mapper feature, select this option.
- USE TCP PORT** — If you do not check **USE DYNAMIC TCP PORT**, enter a specific TCP port on the Remedy AR System server here.

5. **RPC NUMBER:**

- CONNECTOR FRAMEWORK USE RPC NUMBER** — Enter a specific RPC port.

Note: The RPC number feature can help balance the load on the Remedy server. The RPC number specifies the thread to use within the Remedy server. The administrator on the Remedy server can assign a thread to a

specific RPC number. Each thread can be configured to perform certain functions and handle a certain number of connections.

6. When done, click **OK** to save the PMM configuration and skip to [“Creating a Workflow for the Target” on page 42](#), unless you have modified or created a new schema from the default.

If you have modified a schema or created a new schema, click **PROPERTIES**. When you click on properties, the **PROPERTIES** dialog box appears.

Figure 4: Properties

The screenshot shows a dialog box titled "Properties" with a close button (X) in the top right corner. It contains two sections: "AR User Schema" and "AR Group Schema".

AR User Schema:

- Schema Name: User
- Request ID Field: Request ID
- Login Name Field: Login Name
- Password Field: (empty)
- Group List Field: Group List

AR Group Schema:

- Schema Name: Group
- Request ID Field: Group ID
- Group Name Field: Group Name

At the bottom of the dialog box are three buttons: **OK**, **Cancel**, and **Remove**.

7. **PROPERTIES**

The dialog box indicates the schemas to use when updating the passwords for Remedy users. If you use defaults, the **PROPERTIES** dialog box are preconfigured with the default User and Group Schema names, and the default fields of the two schemas.

If you use different schemas or create new ones, then provide the field names of the new schemas that correspond to each of the labels in the dialog box.

8. Click **OK** to save the configuration.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff* explains how to do this on the classic platform.

Updating to Remedy 6.51

After upgrading to 6.51, edit and resave any configured Remedy Action Request System targets. Failure to do so results in “Error initializing Remedy API” error message, when resetting the password on the target.

Configuring the Connector for BMC Remedy Action Request System 3.x

The Connector for BMC Remedy Action Request System 3.x enables the Access Assurance Suite to integrate with the Remedy AR System application. This integration provides ticketing services for operations, such as end user authentication and provisioning actions.

Adding a target to the connector identifies the system on which the Remedy AR System application is installed.

Configuring Remedy for Secure (encrypted) Communication

To enable encrypted communications between the Remedy server and the Connector Framework, you need to alter a configuration setting on the Remedy server. Edit the file `Remedy\CONF\ar.cfg`:

1. Open the file `Remedy\CONF\ar.cfg` and look for a line beginning with:
Encrypt-Security-Policy:
2. If no such line exists, add a line of text, as written above (be sure to include the ":").
3. Add (or change, if the line previously existed) a numeral after the colon. Values are as follows:
0 — Encryption between the client and server is allowed, but not required.
1 — Encryption between the client and server is required; unencrypted communication is not allowed.
2 — Encryption between the client and server is disabled. This is the default value.
4. Once you have saved the configuration file with a change, you need to restart the Remedy Service on the Remedy Server. The service name is typically: Remedy Action Request System Server.

Connector Configuration

Follow these steps to add a Remedy ARS connector target:

1. From the Start menu, select:
Program >Core Access Assurance Suite>Connector Configuration Manager
2. Select **REMEDY-ARSAPI-3.x**
3. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 5: Add BMC Remedy Action Request System Target

The screenshot shows a Windows-style dialog box titled "Add Connector Target". It has a "Target Name:" label followed by a text input field containing "Remedy-ARSAPI-3.x". Below this is a section titled "Operations Supported" which contains a list box. The list box has four items: "Action" (which is selected and highlighted in blue), "Audit", "Authentication", and "Query". At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

Select **ACTION** to enable these provisioning actions: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

Select **AUDIT** to enable ticketing on this Remedy AR System target data source. This includes two operations: "Create Ticket" and "Update Ticket". "Create Ticket" and "Update Ticket" are collectively called "Audit" because a target cannot be added to a single ticketing operation (for example, a target cannot be added to "Create Ticket" only).

Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Provisioning.

Select **QUERY** to enable Core Provisioning or Core Compliance to use queries to find data in this Remedy AR System target data source.

5. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box.

Figure 6: Connector Configuration Manager for BMC Remedy Action Request System

The screenshot shows a Windows-style dialog box titled "Connector Configuration Manager for Remedy". It contains a group box labeled "Remedy ARS Information" with the following fields and options:

- Remedy server:** A text input field.
- Require Remedy administrator:** A checked checkbox.
- Privileged Remedy user:** A text input field.
- Password:** A text input field.
- Use dynamic TCP port:** A checked checkbox.
- Remedy server TCP port:** A text input field with "0" entered.
- Use default RPC number:** A checked checkbox.
- Private server RPC number:** A text input field with "0" entered.
- Perform case insensitive compares:** An unchecked checkbox.

At the bottom of the dialog box are three buttons: "< Back", "Finish", and "Cancel".

6. This dialog box requires the following information.

- **REMEDY SERVER** — Enter the name of the server on which Remedy AR System is installed.
- **REQUIRE REMEDY ADMINISTRATOR** — Determines if the user name specified in the "Privileged Remedy User:" field must have Remedy Administrator privileges.
- **PRIVILEGED REMEDY USER** — Enter the user name for an account with access to the schemas/forms needed for ticketing on the Remedy AR System server. If the "Require Remedy Administrator" check box is selected, the user must have Remedy Administrator privileges.
- **PASSWORD** — Enter the password for the account.
- **USE DYNAMIC TCP PORT** — This option specifies that the connector uses an available TCP port on the Remedy server. If the Remedy server is configured to use the Port Mapper feature, select this option.
- **REMEDY SERVER TCP PORT** — If you do not check Use dynamic TCP port, enter a specific TCP port on the Remedy AR System server here.
- **USE DEFAULT RPC NUMBER** — This option specifies that the Connector Framework uses an available Remote Procedure Call (RPC) port on the Remedy server.
- **PRIVATE SERVER RPC NUMBER** — Enter a specific RPC port.

Note: The RPC number is used to specify which thread to use within the Remedy AR System server. The administrator on the Remedy server can assign a thread to a specific RPC number. The threads can be configured to perform certain functions and to be able to handle a certain number of connections. This feature is used to help load balance the Remedy server.

For example, you can send all tickets from Core Password to one thread and all tickets from Core Provisioning to another thread. This helps balance the load on the Remedy server. The thread for Core Password may be able to handle ten connections, while the thread for Core Provisioning may only need to handle two.

- **PERFORM CASE INSENSITIVE COMPARES** — This option enables you to control whether the connector queries Remedy in a case sensitive or insensitive manner. Some examples of where this option might be applied are custom macros, refining a community, and community restrictions.

7. Click **FINISH**.

Note: Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

8. Select **Yes** to implement the new selections.

Chapter 3: CA eTrust SiteMinder — PMM

This chapter explains how to configure the PMM for CA eTrust SiteMinder (previously known as Netegrity SiteMinder):

- [*“Configuring the PMM for CA eTrust SiteMinder” on page 48*](#)

Configuring the PMM for CA eTrust SiteMinder

The Password Management Module (PMM) for CA eTrust SiteMinder enables end users to automatically reset passwords on eTrust SiteMinder policy servers.

Note: The PMM for CA eTrust SiteMinder does not reset passwords for administratively disabled accounts. This PMM does reset passwords that are disabled because a user exceeded the maximum number of attempts to enter a correct password as configured on the SiteMinder policy server.

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Security.

Prerequisites

Before configuring the PMM for CA eTrust SiteMinder, complete the following procedures.

1. Download Java™ SDK version 1.3.1_9 or higher from the Sun Microsystems™ web site onto the server where the Access Assurance Suite is installed, and then install the SDK on this server.

Download the Java SDK, not just the Java Runtime Environment (JRE). You can download the Java SDK from the Sun Microsystems web site at

<http://www.sun.com>

Follow the instructions from the web site to download this SDK.

2. Download the SiteMinder SDK (this step) or install the SiteMinder Web Agent on each server in which the Connector Framework or Connector Framework Manager is installed (step 3).

To download the SiteMinder SDK: Contact CA support personnel for information about how to obtain the SiteMinder SDK. Download the eTrust SiteMinder SDK onto any machine in the network. Follow the instructions in the SDK Installation Guide to install the SDK.

- a. After you have installed the SDK, copy the following files into the CourionService directory on each server in which the Connector Framework or Connector Framework Manager is installed:

```
smjavaagentapi.dll  
smjavaagentapi.jar  
smjavasdk2.jar
```

Skip to the next section.

3. To install the SiteMinder Web Agent, obtain the web agent from the CA/Netegrity Support site at the following URL:

<http://support.netegrity.com>

- a. After you have logged in to the support site, use the following path to search for the web agent:

Tools > Download manager > SiteMinder Web Agent

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Creating the SiteMinder Agent for the PMM

This PMM requires that you create a SiteMinder agent on the SiteMinder policy server. When you create the agent, check the **SUPPORT 4.X AGENTS** check box. The PMM uses the “agent name” and the “shared secret” that you enter during the PMM configuration to establish a secure communication channel with the SiteMinder policy server to ensure secure password resets.

Refer to the Etrust SiteMinder documentation for information about how to configure the agent on the SiteMinder policy server.

Security Options

The PMM for CA eTrust SiteMinder provides the following options that support secure password resets on the eTrust SiteMinder policy servers:

- Allow Reset of Administrative Account
- User must change password during next login

Allow Reset of Administrative Accounts

The **ALLOW RESET OF ADMINISTRATIVE ACCOUNTS** option enables you to specify whether or not the PMM for eTrust SiteMinder resets passwords for users that are members of certain administrative groups such as CN = Directory Managers.

LDAP administrators can configure their own administrative groups that the PMM includes or excludes from password resets based on the setting of this option.

See the **ALLOW RESET OF ADMINISTRATIVE ACCOUNTS** option in the Add/Edit Target Configuration dialog box on page 51.

User must change password during next login

This option forces end users to change their passwords the first time they log on to the SiteMinder protected resource. See the **USER MUST CHANGE PASSWORD DURING NEXT LOGIN OPTION** on page 51.

PMM Configuration

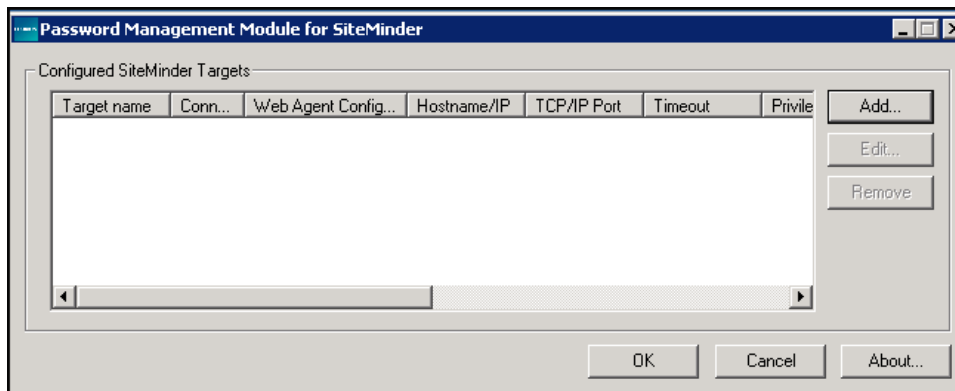
The PMM for CA eTrust SiteMinder provides two methods to specify a SiteMinder policy server during target configuration.

The Add/Edit Target Configuration dialog box lets you identify a policy server or specify the SiteMinder agent configuration file, which can contain information about multiple policy servers. Configuring a target with the SiteMinder agent configuration file lets the PMM leverage the capabilities of a SiteMinder web agent.

The download pre-configuration requirements apply for either method. If you identify a policy server you can choose either the SiteMinder SDK or SiteMinder Agent for the second option. If you specify a configuration file you need to choose the SiteMinder Agent for the second option.

1. From the Start menu, select:
Programs>Access Assurance Suite >Password Management Modules>CA eTrust-Netegrity SiteMinder
2. Click **YES** to start the PMM Configuration Manager.
The PMM Configuration Manager dialog box appears.

Figure 7: PMM Configuration Manager for CA eTrust SiteMinder



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 8: Add/Edit Target Configuration for CA eTrust SiteMinder

Target name:

Target connection information:

☒ SiteMinder policy server information:

Hostname or IP address: TCP/IP port: 44442

Timeout (seconds): 60

Agent name: Agent shared secret:

☐ SiteMinder agent configuration file: Browse...

Administrator information:

Privileged username: Password:

Directory information:

User directory name:

Options:

☐ User must change password at next login

☐ Allow reset of administrative accounts

OK Cancel

4. **TARGET NAME** — Enter a target name for the eTrust SiteMinder policy server that you use as the target. (You cannot edit the name of an existing target.) You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
5. **TARGET CONNECTION INFORMATION** — Select either the SiteMinder policy server or the SiteMinder agent configuration file to use as the target connection.
6. **SITEMINDER POLICY SERVER INFORMATION** — Click this radio button to select a specific policy server and enter information about that server.
7. **HOSTNAME OR IP ADDRESS** — Specify The hostname or IP address of the eTrust SiteMinder policy server target.
8. **TCP/IP PORT** — Enter the TCP/IP port that the SiteMinder agent is listening to on the SiteMinder policy server. The default value is 44442.
9. **TIMEOUT (SECONDS)** — The number of seconds that the PMM waits for a response from the SiteMinder policy server before it terminates the connection. The default is 60 seconds.
10. **AGENT NAME** — The name of the agent on the SiteMinder policy server.
11. **AGENT SHARED SECRET** — The shared secret of the SiteMinder policy server agent.

Note: Core Password uses the values in these two fields to establish a secure communication channel with the SiteMinder policy server. The values you enter in these fields must match the agent name and agent shared secret configured on the policy server.

SITEMINDER AGENT CONFIGURATION FILE — Click this radio button to use the web agent configuration file attributes to connect to the policy servers. Use the **BROWSE...** button to select the file located on the same system as this PMM.

This file is the file created by SiteMinder Web Agent Client wizard, when you register a Host. It is usually called SMHost.conf, but can also be a WebAgent.conf or any `.conf` file for that matter. It needs to include the list of "policyserver" attributes and the "hostconfigobject" attribute that the PMM uses to establish a connection with the SiteMinder Policy Server

Refer to the SiteMinder documentation for instructions on using the SiteMinder Web Agent Client wizard.

Note: When configuring the PMM for CA eTrust SiteMinder to use the Web Agent configuration file for the connection, the size of that file affects the performance of the password reset functionality. The more entries that are present in the web agent configuration used in the target configuration, the longer it takes for a password reset to complete. This is true even if the first policy server listed in the Web Agent configuration file is reachable. If a large Web Agent configuration file is needed, Core Security recommends increasing the timeout value on the PMM and perhaps increasing the ASP session timeout for end user client pages. Core Security Customer Support can provide details for how to do both of these items.

ADMINISTRATION INFORMATION

12. **PRIVILEGED USERNAME** — Specify the privileged user on the SiteMinder policy server. This user must have the **MANAGE USERS IN THE DIRECTORY** privilege. Core Security recommends using a privileged user whose password never expires.
13. **PASSWORD** — Enter the password for the privileged user.

DIRECTORY INFORMATION

14. **USER DIRECTORY NAME** — The name of the user directory on the SiteMinder policy server that is used by the PMM to perform password resets.
15. **USER MUST CHANGE PASSWORD DURING NEXT LOGIN** — Select this option to force the end users to change their passwords the first time they log on to the SiteMinder protected resource.
16. **ALLOW RESET OF ADMINISTRATIVE ACCOUNTS** — Decide whether or not to allow administrators to reset their passwords. To allow administrative resets, select this check box.
17. Click **OK** to save the changes and exit from the PMM Configuration Manager.

You have configured the CA eTrust SiteMinder PMM.

Chapter 4: Using the Connector Configuration Manager

This chapter describes how to add and remove connectors using the Connector Configuration Manager. It also describes configuration issues in a distributed installation. Finally, it includes information on how to use the PMM Gateway connector, which is needed for configuring a PMM on the provisioning platform.

- [*“Configuring Connectors and PMMs in a Distributed Installation” on page 54*](#)
- [*“Adding and Removing Connectors” on page 56*](#)
- [*“Assigning Targets to the Default Connector Framework” on page 60*](#)
- [*“Using the PMM Gateway Connector to Define PMM Targets” on page 61*](#)

Configuring Connectors and PMMs in a Distributed Installation

There are four main components in the Access Assurance Suite: the Core Server, the Connector Framework web service, the Connector Framework Manager web service, and the Publisher web service. During installation, you choose whether you want to install the Access Assurance Suite on a single server or to install different components of the suite on different servers in the network (a distributed installation).

Distributed installations are flexible. You can separate out one of the components while grouping the others onto a single server, break out all components onto different servers, or any other combination. Additionally, you can install multiple instances of the Connector Framework and Connector Framework Manager on multiple servers. (You can install only one instance of a specific component on a server). For more details on distributed installation, see the manual *Installing the Suite*.

The Connector Framework and Connector Framework Manager Web Services

The functions of these components are as follows:

- The Connector Framework web service provides connectivity to the various targets in your enterprise.
- The Connector Framework web service manages the target configuration of all supported connectors and PMMs.

When you install a Connector Framework (CF) and a Connector Framework Manager (CFM) on different servers, the supporting connector and PMM files are installed on both servers. The CF uses these files for communication with the individual targets, while the CFM uses the files to access configuration information. To configure a connector, you need to run the Connector Configuration Manager on the server where the CFM is installed. You also need to run individual PMM configurations on the server where the CFM is installed.

Assigning Targets to a Connector Framework in a Distributed Installation

You need to assign each of your configured targets to one or more Connector Frameworks, which use connectors to communicate with targets. There are two categories of connectors in a distributed installation:

- **Single-Location Connector** — A connector that can have a specific target configured on a single Connector Framework, but can have different targets on many Connector Frameworks.
- **Distributable Connector** — A connector that can have the same target on more than one Connector Framework.

When you configure two or more CFs, you designate one as the default CF. Once you configure a target in the Connector Configuration Manager, that target is automatically assigned to the default CF. If you want to access that target from a different or additional CF, you need to change its CF assignment. You assign targets to CFs in the CFM Configuration option of the Web Services Configuration Manager.

If the target uses a single-location connector, the target can be assigned to only one CF but you can move the target from one CF to another. If the target uses a distributable connector, you can move the target to a new CF or assign the target to additional CFs. See the chapter “Configuring the Web Service Options” in the manual *Installing the Suite* for more details.

Privilege Issues in a Distributed Installation

If your company has multiple domains, and you install the Courion Server and the Connector Framework Manager in Domain A, you may need to access targets in Domain B. If you install a Connector Framework on Domain B, the administrator who configures the connectors in Domain B only needs privileges in Domain A, because connectors are configured on the server on which the Connector Framework Manager is installed. In this situation, when the administrator clicks **FINISH** to complete configuration of the connector in the Connector Configuration Manager, a warning message appears stating that the configuration cannot be validated. This is because the administrator has privileges on one domain but not the other. However, as long as the connector has been configured correctly, the CFM and the CF moves information back and forth between the two.

Connectors and PMMs that Require Supporting Files

Some connectors and PMMs require that you install supporting files. These include the following:

- Script based connectors, such as those for Epic, IBM AIX, and Sun Solaris
- Connectors with client software, such as Microsoft Exchange, Oracle Databases, and Peoplesoft
- Connectors and PMMs that use agents, such as IBM i5/OS, Open VMS, and RSA SecurID
- Connectors and PMMs that require a DSN, such as Microsoft ODBC and Oracle E-Business

If you install the CF and CFM on different servers, you need to install these files on both servers, and if you install them on multiple servers, you need to install the files on each server. You only need to install the files on a server that is used for communication with the connector. For example, if you have one CFM and two CFs but only one CF is configured for PeopleSoft, you only need to install the client software on the CFM and the single CF.

Adding and Removing Connectors

This section explains using the Connector Configuration Manager to add, modify, or delete a connector.

Note: In a distributed installation, you run the Connector Configuration Manager on the server in which the Connector Framework Manager is installed.

Prerequisites for Adding a Connector

Before you begin adding a connector, ensure that you have configured an access key for the connector. Access keys are added during installation of the Access Assurance Suite. You can also add them from the Start menu at:

All Programs>Core Access Assurance Suite>Access Keys

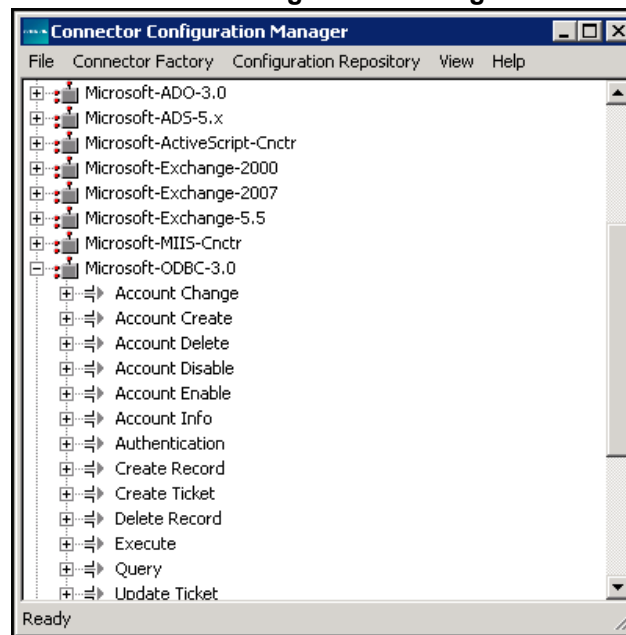
Running the Connector Configuration Manager to Add a Connector

1. On the server in which the Connector Framework Manager was installed, start the Connector Configuration Manager:

Start>All Programs>Core Access Assurance Suite>Connector Configuration Manager

The Connector Configuration Manager main window appears as in [Figure 9](#) (shown with some connectors already added). By default, any connectors for which you have an access key are automatically added.

Figure 9: Connector Configuration Manager Main Window



The  icon identifies a connector. Click the plus sign (+) next to a connector to show the operations available with that connector.

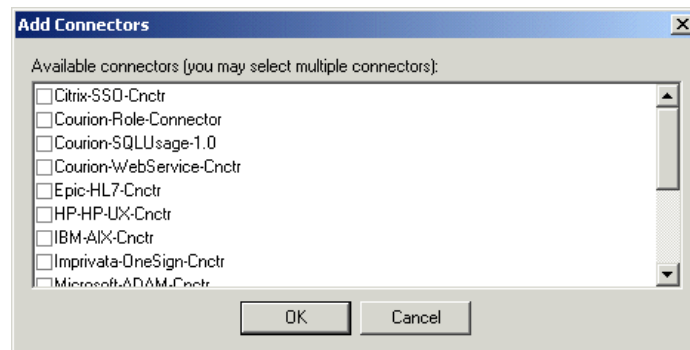
The  icon identifies a operation. Click the plus sign (+) next to a operation to show the target defined for that operation.

The  icon identifies a specific target.

2. From the **FILE** menu, choose **ADD CONNECTOR....**

The software displays a list of connectors for which your site has access keys and that have not already been added (see [Figure 10](#)).

Figure 10: Selecting a Connector to Add



3. Select one or more connectors to add (by checking the box next to each) and click **OK**.

The Connector Configuration Manager screen appears showing the connector you added.

4. To configure a target for the connector, right-click the connector. The software leads you through target configuration, explained for each connector shown in [“Core Access Assurance Suite PMMs and Connectors” on page 32](#).

Note: do not use single quote ('), double quote ("), or back slash (\) characters when naming a target. These rules apply to all types of connectors.

5. When done, close the Connector Configuration Manager screen.

Adding or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Access Assurance Suite and web services. The software prompts you to stop and restart.

6. Select **YES** to implement the new selections.

Note: You must also perform Application Pool reset after making any changes to CCM targets that are being used in data collection rules by taking the following steps:

- a. In Internet Information Services Manager, right-click the DefaultAppPool service.
- b. In the context menu, select Restart.

Running the Connector Configuration Manager to Delete or Modify a Connector or Target

1. On the server in which the Connector Framework Manager was installed, start the Connector Configuration Manager:
 Start>All Programs >Core Access Assurance Suite>Connector Configuration Manager
 The Connector Configuration Manager main window appears as in [Figure 9](#) above.
2. To remove a connector, from the **FILE** pull-down menu, select **REMOVE CONNECTOR**; or click the right mouse button on the target and from the pop-up menu select **REMOVE CONNECTOR**. Then confirm.
 To remove or modify a target, from the **FILE** pull-down menu, select **REMOVE TARGET** or **MODIFY TARGET....** or
 Click the right mouse button on the target and select either **REMOVE CONNECTOR** or **MODIFY TARGET...** from the pop-up menu. Then modify and confirm or confirm.

Prerequisites for Configuring a Connector

Before you begin configuring a connector complete the following steps:

- Install the connector agent, if required.

Information Needed for Connector Configuration

To configure a target for the connector, you need to provide the following information:

- Specify the operation or operations for the connector-target combination.
- Provide the information required for communication with a target.
- Some connectors require that you install other software, such as Admin tools for the Microsoft Exchange 2000 connector. If you have not installed the prerequisite software for these connectors, they do not appear on the list of connectors
- To configure the Connector for Microsoft Exchange 2000, the Connector Framework server used to access Exchange 2000 must be a member of the Active Directory Domain where the Exchange 2000 server resides, or it must have a trust with this server. Additionally the following two tools must be installed on each server in which the Connector Framework or Connector Framework Manager is installed:
 - Active Directory Users and Computers Administration Tool
 - Microsoft Exchange 2000 Administration Tool
- Some connectors (Epic, HP-UX, Sun Solaris, etc.) require that you install ActivePerl. See [“Installing ActivePerl” on page 695](#) for information about how to install ActivePerl.

- If you use the Create action, you need to configure at least one connector that supports the Create profile records (entries) operation. To create a resource on a target system, the Access Assurance Suite must first create an initial profile for the user in a profile datasource. The profile data source can be a table in an ODBC-compliant database or object class in an LDAP-enabled directory. The profile entry for a user includes a unique identifier (badge number, for example). The profile is linked to the IdentityMap table through the user's unique identifier.

If you use the Requester/Approver or Delegation features, the Core Password Password History feature, store compliance information for reports using Core Compliance Verify action, or the Configuration Repository option to store shared data, you need to configure a Microsoft ADO connector with a transaction repository.

- Optionally, you can configure the connector for a supported Help Desk application to enable ticketing of events. The SMTP connector can be configured to enable e-mail notification of events.

Connector Configuration Manager Menu Bar Options

FILE pull-down menu options:

- Add Connector
- Remove Connector
- Add Target
- Modify Target
- Remove Target
- Refresh the window
- Exit the Connector Configuration Manager

CONNECTOR FACTORY menu options

- Create your own connector with the connector Rapid Development Kit (RDK). Contact your Core Security sales representative for information about how to obtain the connector Rapid Development Kit (RDK).

CONFIGURATION REPOSITORY pull-down menu option

- Configuration management (transition shared data to a transaction repository on the network). See the *Access Assurance Suite Implementation Guide* for more information about this feature.

VIEW pull-down menu toggles on or off the status display at the bottom of the window.

HELP pull-down menu displays version and copyright information about the Connector Configuration Manager.

Assigning Targets to the Default Connector Framework

By default, new targets are assigned to the CourionService. Using the Connector Configuration Manager, you have the option to place the first target for a connector into the remote default Connector Framework. This option only applies to the first target configured for a connector. If a connector already has a target associated with it, then the CF assignment for any additional targets is implemented as follows:

- If the target is assigned to the CourionService, then the new target is assigned to the CourionService.
- If the new target is assigned to any distributed CF, then the target is assigned to the default distributed CF.

You can use the Web Service Configuration Manager to change these assignments. If you use Web Service Configuration Manager to move targets for a connector onto distributed CFs, any subsequent targets you create for that connector are placed on the default CF. See the manual *Installing the Suite* for more information about using the Web Service Configuration manager.

Running the Connector Configuration Manager to Assign Targets to the Default Connector Framework

1. On the server in which the Connector Framework Manager was installed, start the Connector Configuration Manager:
Start>All Programs>Core Access Assurance Suite>Connector Configuration Manager
2. From the File menu, select **ASSIGN TARGETS BY DEFAULT TO**
3. Select **COURIONSERVICE** or **DEFAULT CONNECTOR FRAMEWORK**.

Using the PMM Gateway Connector to Define PMM Targets

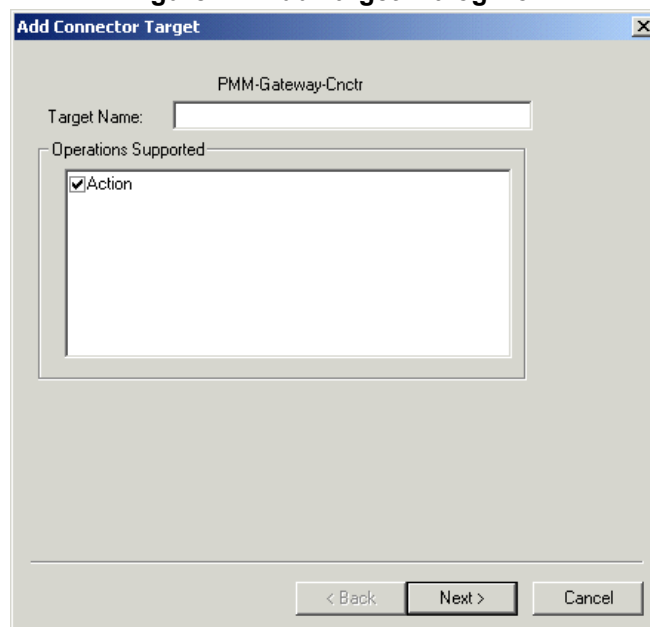
The PMM Gateway connector provides an interface between Core Password and a PMM target.

If you have previously defined the target you want for a PMM, then you need only specify the target name to the Gateway connector. If you have not defined a target, then you can add it using this connector.

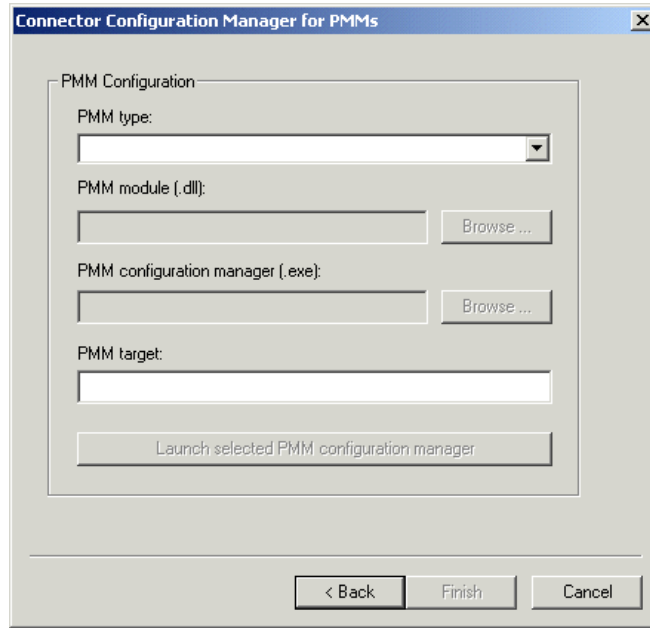
Follow these steps to identify a PMM target to the Access Assurance Suite:

1. From the Start menu, select:
Start>All Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **PMM-GATEWAY-CNCTR**
If this connector name does not appear, select File>Add and select the connector from the list. Then right-click **PMM-GATEWAY-CNCTR** and select **ADD**.
The Add Target dialog box appears.

Figure 11: Add Target Dialog Box



3. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
4. Click **NEXT**.
The Connector Configuration Manager displays the Connector Configuration for PMM Targets dialog box.

Figure 12: Connector Configuration for PMM Targets Dialog Box


The dialog box is titled "Connector Configuration Manager for PMMs". It contains a "PMM Configuration" section with the following fields and controls:

- PMM type:** A drop-down menu.
- PMM module (.dll):** A text input field with a "Browse..." button to its right.
- PMM configuration manager (.exe):** A text input field with a "Browse..." button to its right.
- PMM target:** A text input field.
- Launch selected PMM configuration manager:** A button located below the PMM target field.

At the bottom of the dialog box are three buttons: "< Back", "Finish", and "Cancel".

5. **PMM TYPE** — From the drop-down list, select the type of PMM you want to configure.

For any PMM you select, Core Security provides the PMM module (.dll) filename and configuration manager (.exe) filename. If you select a custom PMM (**SELECT CUSTOM PMM**, which is last on the drop-down list), you need to provide the path to the custom .dll file and configuration manager filename.

6. **PMM TARGET** — If you have already configured a target for this PMM using the PMM configuration manager, enter the name of the target here. The name must match the name of the target you configured. Click **FINISH**.

If you have not configured a PMM target, go to step 7.

7. To configure the PMM target, click the **LAUNCH SELECTED PMM CONFIGURATION MANAGER** button and skip to the appropriate chapter for the PMM. See [“Core Access Assurance Suite PMMs and Connectors” on page 32](#) for a list of platforms with PMMs.

Once you finish configuring the PMM and click **OK** to exit the PMM configuration manager, you are returned to the Connector Configuration for PMM Targets dialog box.

In the **PMM TARGET** field, enter the name of the target you just configured. The name must match the name of the target you configured. Click **FINISH**.

Chapter 5: Citrix SSO — Connector

This chapter explains how to configure the Connector for Citrix SSO:

- [*“Configuring the Connector for Citrix SSO” on page 64*](#)

Configuring the Connector for Citrix SSO

The connector for Citrix-SSO systems can send a trigger to a target, based on the results of the following actions: Add, Create, Change, Delete, Disable, Enable, Verify, and View.

Prerequisites

Configuring a target requires the following information:

- Citrix server name
- Privileged domain name
- Privilege user password
- Privileged username

The domain, username, and password are used as privileged credentials for communicating with the Citrix server specified by server name. They must allow login at the time you configure the target.

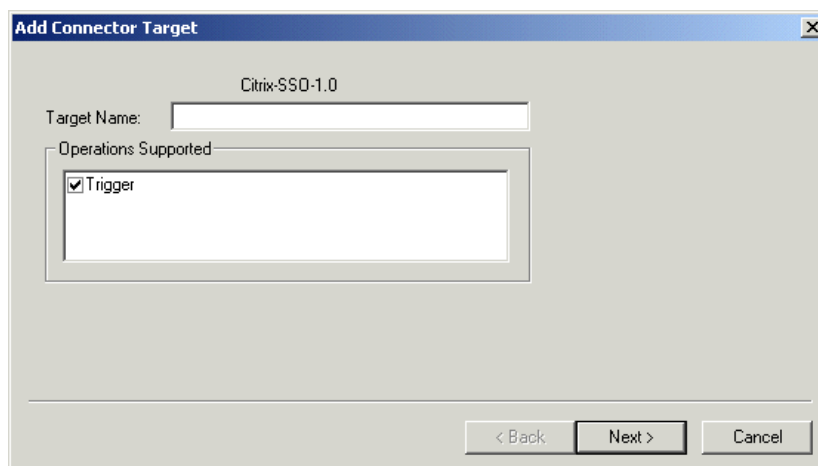
Connector Configuration

Follow these steps to add a Citrix-SSO connector and target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **CITRIX-SSO**, and click **OK**.
3. Select **CITRIX-SSO**
4. Right click on Citrix-SSO and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 13: Add Citrix Target



5. Enter a name (alias) for the target in the Target Name text box. This name identifies the target in the Administration Manager interface.
6. The only supported operation is Trigger, selected by default. Click **NEXT**.
The Connector Configuration Manager for Technology Connector screen appears.

Figure 14: Connector Configuration Manager for Citrix-SSO

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **CITRIX SERVER** — This represents the Fully-Qualified Domain Name of the server housing the Citrix Provisioning Webservice. This must match the name used when you acquired a certificate from a certificate authority for running the web service. An example is myserver.corp.xyz.com. This is a required field.
 - **PRIV DOMAIN** — This represents the domain of the privileged user who has access rights to the Citrix Webservice. This is a required field.
 - **PRIV PASSWORD** — This represents the password of the privileged user who has access rights to the Citrix Webservice. This is an optional field.
 - **PRIV USER** — This represents the account of the privileged user who has access rights to the Citrix Webservice. This is a required field.

Notes:

- The password and username values must allow log in to the Citrix server in the domain specified.
 - You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.
8. When you have configured the correct server, domain, password and user values, click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services. The target is now available for each provisioning action for the selected connector.

Chapter 6: Citrix XenApp — Connector

This chapter explains how to configure the Connector for Citrix XenApp (formerly known as Citrix Presentation Server):

- [*“Configuring the Connector for Citrix XenApp” on page 68*](#)

Configuring the Connector for Citrix XenApp

The Connector for Citrix XenApp provisions Citrix XenApp published applications to users and recertifies (attests) access to these published applications. To do this, the connector maps Microsoft Active Directory group management to Citrix XenApp access policies. The connector supports the following actions on a target: Add, Create, Change, Delete, View, and Verify.

Note: You cannot delete a user from the user's primary security group. If the user's primary security group controls the application you are attempting to delete, the Delete action fails.

Providing Access to Citrix Published Applications

The Connector for Citrix XenApp supports different directory structures that determine how Active Directory groups control access to Citrix published applications. Provisioners can select which applications they make available to a provisionee on the Enter Account Attributes screen using one of these methods:

- By selecting an Active Directory group that controls the application from a drop-down list of groups that all control the application.
- By selecting a checkbox next to the application name to give access to the application to the provisionee.

Note: Any time you make a change on the Citrix target, such as adding or deleting applications, or adding or removing group access to applications, restart the CourionService. From the Start menu, select:

Start>Administrative Tools>Services

Select CourionService, and then Restart the service.

[Figure 15](#) shows the Enter Account Attributes screen with both of these methods available.

Figure 15: Enter Account Attributes Screen with Citrix Applications

Enter Account Attributes

This form is used to gather information related to each of the accounts.

Allow access to selected CPS applications		
Calculator	☐	?
Courion	[None]	?
Desktop	[None] Citrix Admins Citrix Users Windows Account	?
Dialer		?
Notepad	☐	?
Notepad2	☐	?
Notepad3	☐	?
Paint Brush	☐	?
WinHelp	☐	?
Yahoo	☐	?

To make the Core Security application in [Figure 15](#) available to a provisionee, the provisioner selects an Active Directory group associated with the application from the drop-down list. To make any other application available, the provisioner simply checks the box next to the application name.

Making Checkbox Selections Available for Citrix XenApp Published Applications

To make the checkbox method available, select the **USE CHECKBOXES** configuration parameter in the Connector Configuration for Technology Connector dialog box, as shown in [Figure 19](#). You can set the configuration parameter value to **TRUE**, **YES**, or **1** (values are not case sensitive). If you do not select this parameter, the provisioner needs to select an Active Directory group from the drop-down list of groups controlling the application.

The checkbox method also requires that the Active Directory groups and the applications they control conform to one of the following directory structures:

1x1 Structure

In this organization, one Active Directory group controls access to one Citrix XenApp published application. There are no nested sub-groups under the Active Directory group and the Active Directory group is not part of another group or sub-group.

Nested Structure

In this organization, an Active Directory parent group has nested sub-groups that control access to Citrix XenApp published applications assuming the following conditions:

- A parent group can have only one level of nested groups.
- Any nested group can have only one parent group.

- Each nested group controls access to only one published application.

In this type of nested structure, the parent group can also control access to published applications directly. When a parent group controls access to a published application directly, the provisionee still needs to be a member of a sub-group to access the application:

- If one or more sub-groups exists in the structure with no other applications associated with them, the connector assigns the provisionee to one of these sub-groups (the provisioner does not control this assignment).
- If no other sub-groups exists without applications associated with them, the provisioner must assign the provisionee to another sub-group by selecting one of the applications that belong to that group.

If the provisionee is already a member of the parent group, any other published applications that are associated with the parent group appear with read-only (grayed-out) checkboxes on the Enter Account Attributes screen, as shown in [Figure 16](#). The provisioner cannot change the availability of these applications to the provisionee.

Figure 16: Applications Not Available

Allow access to "Desktop"	☒
Allow access to "Dialer"	☐
Allow access to "Google"	☒
Allow access to "Internet Explorer"	☒
Allow access to "Notepad"	☐
Allow access to "Outlook Express"	☐

Changing an Application's Control Type in a Nested Structure

In the nested structure configured with the Use Checkbox configuration parameter, you can change the Active Directory group associated with the Citrix XenApp published application. If you do this, complete the following steps:

Change the application's Control Type for the Attribute Display Options on the Unique Target Data form, based on the new group association. The Connector Data Type on this form is updated automatically. For example, if the application is initially configured to have a Boolean Control Type for the Attribute Display Option and you change the group association to one that requires the Multi-State Boolean Control Type, you need to manually change the Control Type on the Unique Target Data form in the administration manager.

[Figure 17](#) shows how the Control Type drop-down list and the Connector Data Type field would appear in this example on the Unique Target Data form after you changed the group association. The Control Type remains Boolean (as it was before the group association changed), and the Connector Data Type updated to BOOL_MSTATE. You need to select Multi-State Boolean from the Control Type drop-down list.

Figure 17: Control Type on the Unique Target Data Form

The screenshot shows a form with the following elements:

- Control Type:** A dropdown menu currently showing "Boolean".
- Default Value:** A checkbox that is currently unchecked.
- Text Input:** A text box containing "[N/A]".
- Label:** The text "BOOL_MSTATE" is displayed to the right of the text input.

Citrix Published Applications have one of three Connector Data Types. Table 4 lists these Connector Data Types and their corresponding Control Types.

Table 4: Connector Data Types and Control Types for Citrix Published Applications

Control Type	Connector Data Type
List	ENUM
Boolean	BOOL
Multi-State Boolean	BOOL_MSTATE

See the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for more information about the Unique Target Data form.

Prerequisites

Configuring a target requires the following information:

- Administrator domain name
- Administrator password
- Administrator username

The domain, username and password are used as privileged credentials for communicating with the Citrix XenApp specified by server name. They must allow login at the time you configure the target.

Installing the Citrix SDK

Prior to configuring the Connector for Citrix XenApp, install the Citrix SDK.

Specifying the Name of the Citrix XenApp

Specify the name of the Citrix XenApp you provision against when you install the Citrix SDK. The Access Assurance Suite can provision against a Citrix XenApp running version 4.0 or 4.5. During the SDK installation, enter the name when prompted at the MetaFrame COM Server dialogue box.

Note: If you do not provide the server name, you cannot configure the Citrix XenApp target through the Administration Manager Provisioning Targets Configuration Form. If you do not enter the server name when you install the SDK, you can add the Citrix XenApp name to the Microsoft Windows DCOM settings. See [“Adding the Citrix XenApp Name to the Microsoft Windows DCOM Settings” on page 74](#) for information about how to do this.

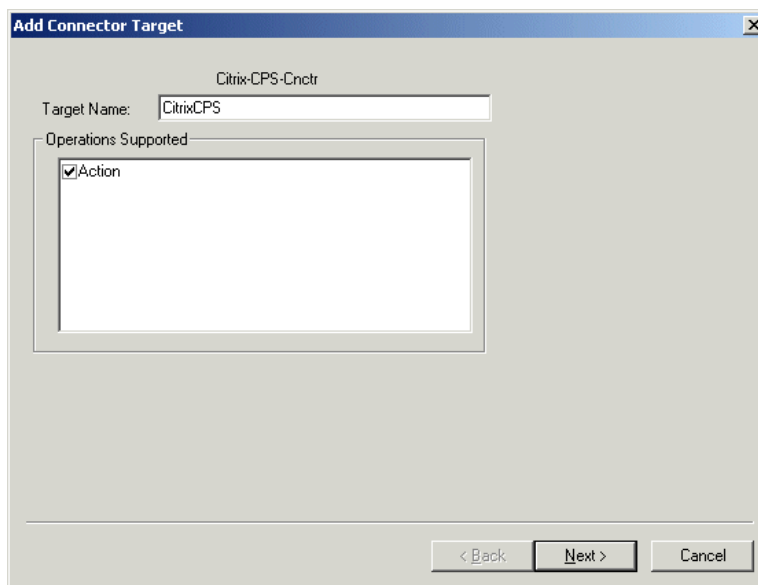
Connector Configuration

Follow these steps to add a Citrix XenApp connector and target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE**, **ADD CONNECTOR**, and select **CITRIX-CPS-CNCTR**, and click **OK**.
3. Select **CITRIX-CPS-CNCTR**
4. Right click on Citrix-CPS-Cnctr and choose **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 18: Add Citrix-CPS-Cnctr Target



5. Enter a name (alias) for the target in the Target Name text box. This name identifies the target in the Administration Manager interface. In this example, CitrixCPS is the target name.
6. Action is selected by default (Add, Create, Change, Delete, View, and Verify). Click **NEXT**.

The Connector Configuration Manager for Technology Connector screen appears.

Figure 19: Connector Configuration Manager for Technology Connector

- The drop-down list, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Values always appear as asterisks (“*”) for security.

The parameters are:

- **USE CHECKBOXES** — Displays a checkbox next to the Citrix XenApp application on the Enter Account Attributes screen. The provisioner can grant access to the application by checking the box. To enable this parameter set the configuration parameter value to **TRUE**, **YES**, or **1** (values are not case sensitive).
- **ADMINISTRATOR DOMAIN** — The domain of the user who has access rights to the Citrix XenApp. This is a required field.
- **ADMINISTRATOR PASSWORD** — The password of the user who that has access rights to the Citrix XenApp. This is an optional field.
- **ADMINISTRATOR USERNAME** — The account of the user who has access rights to the Citrix XenApp. This is a required field.

Notes:

- The password and username values must allow log in to the Citrix XenApp in the domain specified. The Citrix XenApp administrator must have the “Full Administration” privilege.
- You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. When you have configured the correct server, domain, password and user values, click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services. The target is now available for each provisioning action for the selected connector.

Notes

The following notes apply to the Connector for Citrix XenApp:

- [*“Adding the Citrix XenApp Name to the Microsoft Windows DCOM Settings” on page 74*](#)
- [*“Provisioning to Multiple Published Applications” on page 74*](#)
- [*“Updating the Unique Target Data Field Selection Form after Updating the CP Server” on page 75*](#)
- [*“Using IdentityMap Restrictions to Detect Duplicate CP Server Published Application Access” on page 75*](#)
- [*“Conflicts in Access” on page 75*](#)

Adding the Citrix XenApp Name to the Microsoft Windows DCOM Settings

If you did not enter the name of the Citrix XenApp during the installation of the Citrix SDK, you can enter it in the Microsoft Windows DCOM settings by following these steps:

1. Select Component Services from the Start menu or the Control Panel:
From the Start menu, select:
Start>Administrative Tools>Component Services
From the Control Panel, click on Administrative Tools. From Administrative Tools, click on Component Services.
2. From the Component Services window, expand Component Services under the Console Root folder.
3. Expand the Computers folder and select My Computer.
4. Click on the DCOM Config folder.
5. In the DCOM Config folder, right click on MetaFrame COM Server. Select Properties, and enter the name of the Citrix XenApp in the Location box.

Note: Enter the name of the server running the version Citrix XenApp that you want to provision against. The Access Assurance Suite can provision against Citrix XenApp version 4.0 or 4.5.

Provisioning to Multiple Published Applications

If there is any failure when provisioning to multiple Citrix published applications, a user might still have access to applications that were successfully provisioned even after Core Security issues a Non-Success status summary screen.

For example, during a provisioning action for Citrix applications A and B, Core Security gives access to application A but fails to give access to Application B. Core Security issues a Non-Success status message. However, a user may still access application A even though there was a Non-Success status message for the provisioning action.

Updating the Unique Target Data Field Selection Form after Updating the CP Server

If changes are made on the Citrix XenApp, you need to update the Citrix XenApp target information on the Unique Target Data Field Selection Form in the Administration Manager. Do this for each action in each workflow that uses the Citrix XenApp target. These changes can include adding or removing applications, adding groups to applications, and removing groups from applications.

Using IdentityMap Restrictions to Detect Duplicate CP Server Published Application Access

Because the Add action does not automatically detect duplicate Citrix XenApp published application access entries, Core Security recommends that you use an IdentityMap restriction in the form of a custom macro. The restriction can check for an existing entry of the provisionee. This approach provides a mechanism to prevent the addition of duplicate published application access and the resulting IdentityMap entries. You add an IdentityMap restriction on the IdentityMap Field Connection Form in the Administration Manager.

Conflicts in Access

If there is a conflict in the way you are granting user access to a published application because of overlapping groups or direct Windows account access, the connector does not grant the access and reports a Non-Success status. In the event of a conflict, the administrator can determine the cause of the conflict by examining the Active Directory groups listed for each application on the Resource Overrides page.

Chapter 7: Core Role Connector

This chapter explains how to configure the Role Connector:

- [*“Configuring the Role Connector” on page 78*](#)

Configuring the Role Connector

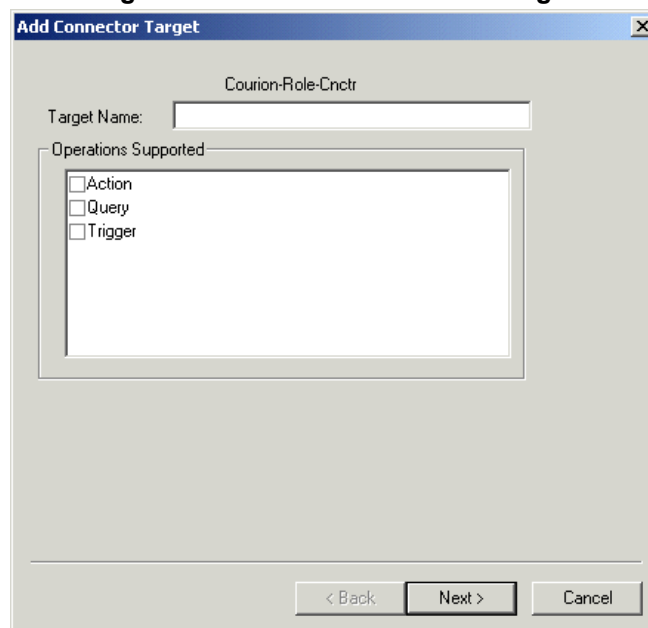
The Role Connector is used to connect a workflow to the role information stored in the Transaction Repository. The connector supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Query
- Event Triggers

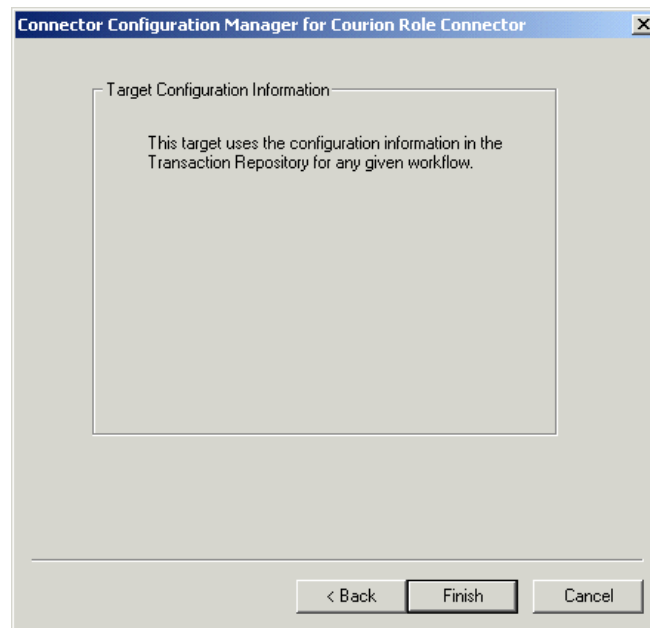
Follow these steps to configure the Role Connector:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **CORE-ROLE-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target Dialog box appears.

Figure 20: Add Role Connector Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select **ACTION** to enable all provisioning actions on a target.
Select **QUERY** to enable RoleCourier to use queries to find data in the target data source.
Select **TRIGGER** to configure event triggers that initiate functions that you associate with certain events.
6. Click **NEXT**. The Connector Configuration Manager for Core Role Connector appears.

Figure 21: Role Connector Configuration Manager

7. Click the **FINISH** button. There are no parameters to configure for the Role Connector.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Chapter 8: Core Connector for SQL Usage

This chapter explains how to configure the Connector for SQL Usage:

- [*“Configuring the Connector for SQL Usage” on page 82*](#)

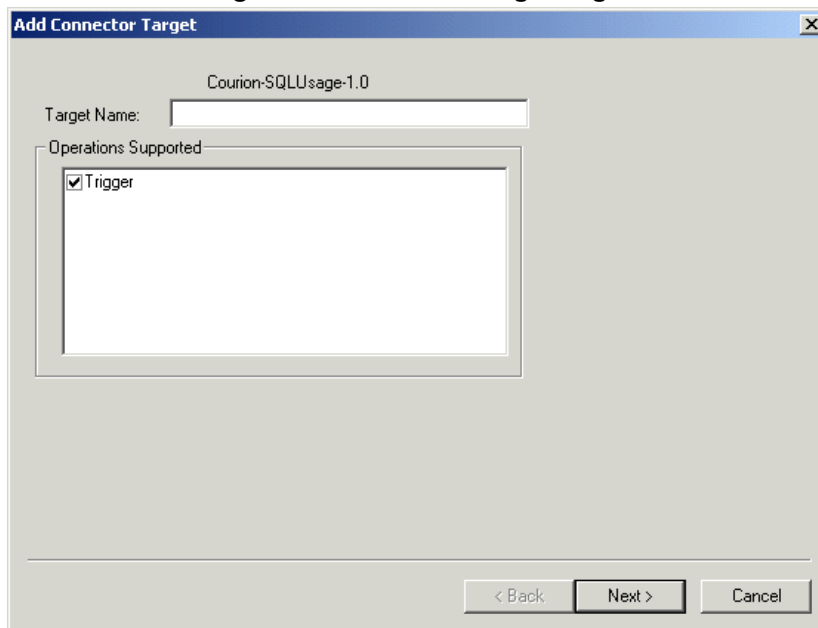
Configuring the Connector for SQL Usage

The connector for SQL Usage enables you to execute one or more SQL statements, using a trigger, based on the results of the following actions: Add, Change, Create, Delete, Disable, Enable, Password Reset, Verify, and View.

Follow these steps to configure the Connector for SQL Usage:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **COUR-SQLUSAGE-1.0**, and click **OK**.
3. Select **COUR-SQLUSAGE-1.0**
4. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target Dialog box appears.

Figure 22: Add SQL Usage Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. **TRIGGER** is checked by default. Click **NEXT**. The Connector Configuration Manager for Technology Connector appears.

Figure 23: Connector Configuration Manager for SQL Usage

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **Administrator Password** — Enter the password of the administrator with access to the SQL database.
 - **Administrator User** — Enter the user name of the administrator with access to the SQL database.
 - **Data Source** — Enter the name of the Data Source that is used to connect to the SQL server that the SQL command is executed against.
 - **Initial Catalog** — Enter the SQL database name.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Chapter 9: Core Connector for JavaScript Custom Macros

This chapter explains how to configure the Connector for JavaScript Custom Macros:

- [*“Configuring the Connector for JavaScript Custom Macros” on page 86*](#)

Configuring the Connector for JavaScript Custom Macros

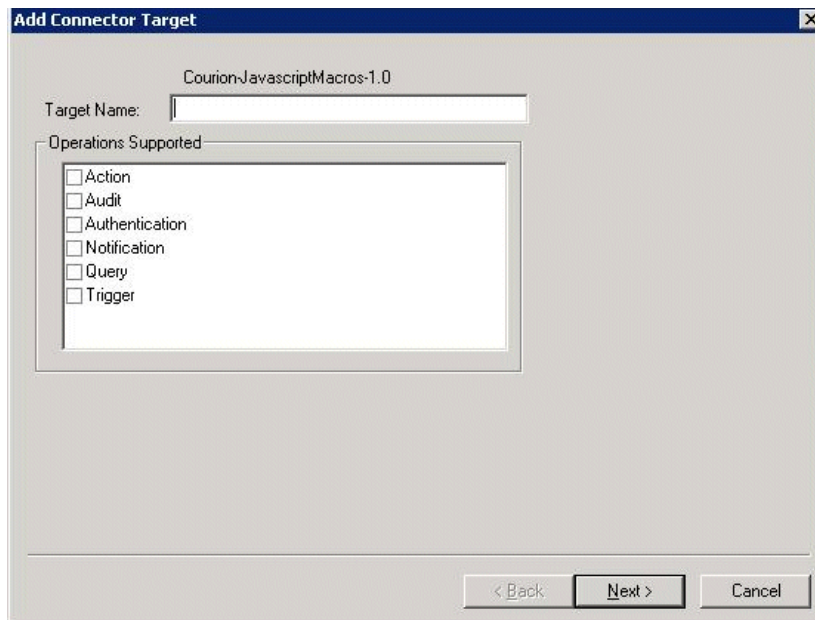
The Connector for JavaScript Custom Macros enables you to write custom macros using JavaScript within the provisioning application. This connector supports the Query and Trigger operations.

After you add a JavaScript Custom Macros target, the target name appears in the Administration Manager Create Custom Macros form (see the manual *Configuring Workflows with the Access Assurance Suite Administration Manager*).

Follow these steps to configure the Connector for JavaScript Custom Macros:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **COURION-JAVASCRIPTMACRO-1.0**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target Dialog box appears.

Figure 24: Add JavaScript Macros Target



4. Add a target name.
5. Select **QUERY** to enable provisioning actions to use queries to find data in the target datasource.
Select **TRIGGER** to configure event triggers that initiate functions that you associate with certain events.
NOTE: Other operations that appear in this dialog box are not supported.
6. Click **NEXT**. The Connector Configuration Manager for Technology Connector appears.
7. Click **FINISH** (there are no parameters available to select).

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each of the provisioning actions for the selected connector.

Chapter 10: Core Connector for VBScript Custom Macros

This chapter explains how to configure the Connector for VBScript Custom Macros:

- [*“Configuring the Connector for VBScript Custom Macros” on page 90*](#)

Configuring the Connector for VBScript Custom Macros

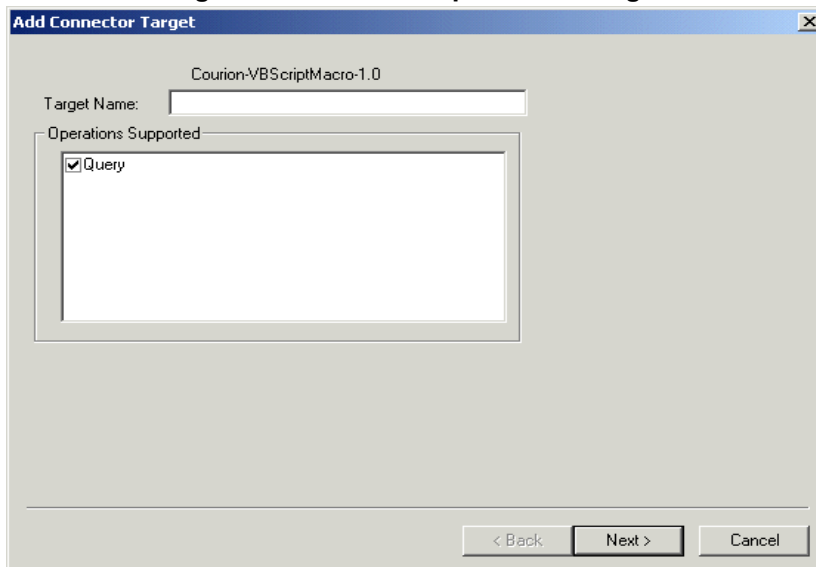
The Connector for VBScript Custom Macros enables you to write custom macros using VBScript within the provisioning application. This connector supports the Query operation.

After you add a VBScript Custom Macros target, the target name appears in the Administration Manager Create Custom Macros form (see the manual *Configuring Workflows with the Access Assurance Suite Administration Manager*).

Follow these steps to configure the Connector for VBScript Custom Macros:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **COURION-VBSCRIPTMACRO-1.0**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target Dialog box appears.

Figure 25: Add VBScript Macros Target



4. Add a target name. The Query box is checked by default. Click **NEXT**. The Connector Configuration Manager for Technology Connector appears.
5. Click **FINISH** (there are no parameters available to select).

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each of the provisioning actions for the selected connector.

Chapter 11: Core Connector for Web Services

This chapter explains how to configure the Connector for Web Services:

- [*“Configuring the Connector for Web Services” on page 92*](#)

Configuring the Connector for Web Services

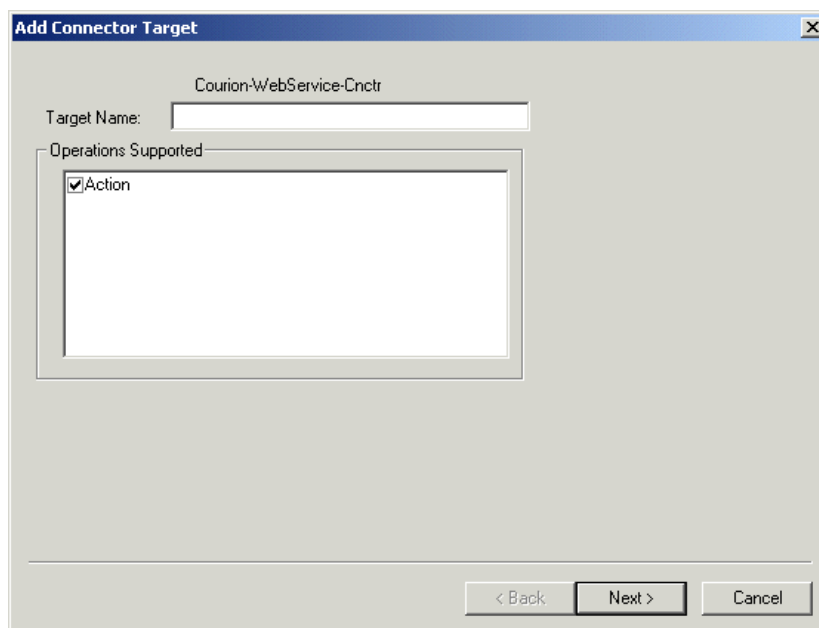
The connector for Web Services enables you to connect to other applications that support web services. The connector has the ability to auto-discover published Web Services Description Language (WSDL) files via HTTP. The following actions are supported: Add, Change, Create, Delete, Disable, and Enable.

Details on implementing this connector can be found in *The Access Assurance Suite Implementation Guide*.

Follow these steps to configure the Connector for Web Services:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **ADD CONNECTOR** from the File menu. Place check in the checkbox next to **COURION-WEB-SERVICE-CNCTR**. Click **OK**.
3. Select **COURION-WEB-SERVICE-CNCTR**. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target Dialog box appears.

Figure 26: Add Web Services Target



4. Add a target name. Click **NEXT**. The Connector Configuration Manager for Technology Connector appears.

Figure 27: Connector Configuration Manager for Web Services

5. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **WSDLUrl** — The URL of the WSDL document you are trying to access
 - **WSPassword** — The password of the account used to access the WSDL doc
 - **WSUsername** — The user name of the account used to access the WSDL doc
 - **XSLT For AcctChangeResults** — The name of the XSLT file used to process Account Change results
 - **XSLT For AcctCreateResults** — The name of the XSLT file used to process Account Create results
 - **XSLT For AcctDeleteResults** — The name of the XSLT file used to process Account Delete results
 - **XSLT For AcctDisableResults** — The name of the XSLT file used to process Account Disable results
 - **XSLT For AcctEnableResult** — The name of the XSLT file used to process Account Enable results
 - **XSLT For AcctInfoResults** — The name of the XSLT file used to process Account Info results
6. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Chapter 12: Epic — Connector

Please contact Customer Support to get the newer connectors used to integrate to EPIC. There is the Connector for Epic SER and the Connector for Epic EMP. One or both of these should be used instead of this connector that is available in the suite installation kit.

This chapter explains how to configure the Connector for Epic[®]:

- [*“Configuring the Connector for Epic” on page 96*](#)

Configuring the Connector for Epic

The Connector for Epic establishes a TCP/IP connection to the specified server and port and passes HL7 formatted messages to the server. The server simply acknowledges that the message was received. At some point the message is processed by the Epic system and the requested action is processed. The actual status of the request can be viewed by checking the Epic system. This means Core Provisioning only knows that the request was posted, not the status of the request.

The connector for Epic supports the following actions on a target: Add, Change, Create, Enable, Delete, and Disable.

Prerequisites

Epic server with the Bridges™ Standard HL7 Incoming Personnel Management Interface.

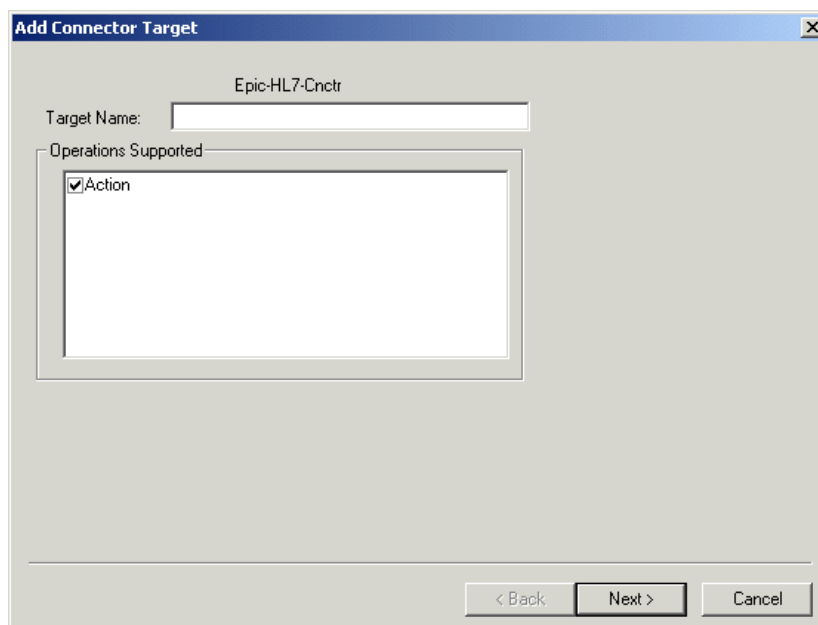
Connector Configuration

Follow these steps to add a target domain:

1. From the Start menu, select:
Programs > Core Access Assurance Suite> Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **EPIC-HL7-CNCTR**, and click **OK**.
3. Select **EPIC-HL7-CNCTR**.
4. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 28: Add Epic Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**.
The configuration screen for Epic appears.

Figure 29: Connector Configuration Manager for Epic

6. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **IP Address (required)** — IP address of the Epic system
 - **MSH:Processing ID (required)** — Accepted values: D=Debugging, P=Production, T=Training
 - **MSH:Receiving Application** — A value can be entered but is not required
 - **MSH:Receiving Facility** — A value can be entered but is not required
 - **MSH:Sending Application** — A value can be entered but is not required
 - **MSH:Sending Facility** — A value can be entered but is not required
 - **TCP Port (required)** — Port the Epic system listens on

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by the connector.

Chapter 13: HP OpenView ServiceCenter — Connector

This chapter explains how to configure the Connector for HP OpenView ServiceCenter (previously known as Peregrine ServiceCenter):

- [*“Configuring the Connector for HP Software Service Manager” on page 100*](#)

Configuring the Connector for HP Software Service Manager

The connector for HP Software Service Manager® enables provisioning applications to integrate with the HP OpenView ServiceCenter application. This integration provides ticketing services for Access Assurance Suite operations, such as end user authentication and provisioning actions.

Adding a target to the connector identifies the system on which the HP OpenView ServiceCenter application is installed.

Prerequisites

This connector requires a license key from HP called `SCAuto\SDK`. Contact HP for information about how to obtain this license key.

The TCP port number you specify during connector configuration must also be configured on the ServiceCenter according to HP OpenView Systems documentation.

In a distributed installation, the Courion Server and Connector Framework Manager (CFM) components must be installed on the same server. This is because HP OpenView ServiceCenter needs to update a configuration attribute to keep track of the next ticket ID. For details on distributed installation, see [“Configuring Connectors and PMMs in a Distributed Installation” on page 54](#).

Editing the Services File

1. On the drive where the Windows Server 2003 operating system is installed, locate the file `\winnt\system32\drivers\etc\services` and open it with a text editor (for example, Notepad).
2. Add the following two lines at the end of the file:

```
scauto [portnum]/tcp  
scauto [portnum]/udp
```

where *portnum* is the TCP/IP port number. The default value is 12690.
3. Save and close the services file.

Connector Configuration

Follow these steps to add an HP Software Service Manager target:

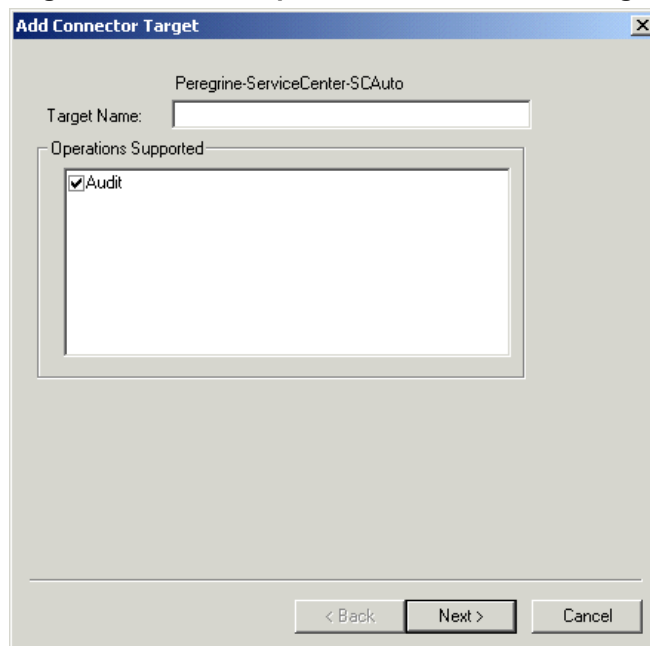
1. From the Start menu, select:
Programs>Core SAccess Assurance Suite>Connector Configuration Manager
2. Select **PEREGRINE-SERVICECENTER-SCAUTO**
3. Click the right mouse button and choose **ADD TARGET....**

Note: The connector lists two supported operations: “Create Ticket” and “Update Ticket”. A target cannot be added to a single operation (for example, a target

cannot be added to “Create Ticket” only). By default, an added target is available to both operations.

The Add Connector Target dialog box appears.

Figure 30: Add HP OpenView ServiceCenter Target



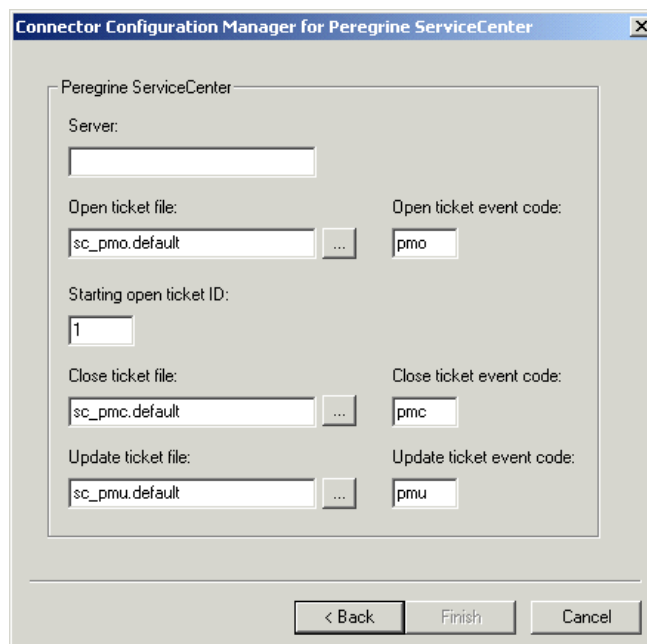
4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **AUDIT** check box is selected by default.

5. Click **NEXT**.

The Add Connector Target dialog box appears.

Figure 31: Connector Configuration Manager for HP Software Service Manager



When adding a target for the Connector for HP OpenView ServiceCenter, the only required field is **SERVER**.

6. **SERVER** — Enter the name of the server on which HP OpenView ServiceCenter is installed.

Accept the default values for the other fields unless these fields have been previously configured for different values.

7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

Ticketing is now available on the connector.

Notes and Warnings

If you are using HP Software Service Manager in Core Password, Core Provisioning, Core Compliance, or RoleCourier, the configurations must be identical. The HP Software Service Manager connection for Core Password is setup during the configuration of the Courion Server, and the HP Software Service Manager connection for Core Provisioning, Core Compliance, and RoleCourier is setup using the Connector Configuration Manager.

These items must be identical and are case-sensitive:

- The Server name must be identical between Core Provisioning, Core Compliance, or RoleCourier and Core Password.
- The Ticket Event Codes (all three of them), must be identical between Core Provisioning, Core Compliance, or RoleCourier and Core Password.
- The Ticket File (all three of them), must be identical between Core Provisioning, Core Compliance, or RoleCourier and Core Password.

Failure to follow these rules results in unpredictable behavior by the Courion Server.

Chapter 14: HP-UX System — PMM and Connector

This chapter explains how to configure the PMM and Connector for HP-UX. It also explains how to install and configure the agent required by the PMM:

- [*“Configuring the PMM for HP-UX” on page 104*](#)
- [*“Writing Password Management Scripts” on page 107*](#)
- [*“Installing and Configuring the HP-UX PMM Agent” on page 108*](#)
- [*“Configuring the Connector for HP-UX” on page 112*](#)

Configuring the PMM for HP-UX

The Password Management Module (PMM) for HP-UX enables Core Password applications to reset passwords automatically on HP-UX systems. The PMM is a component of the Access Assurance Suite and is installed when the suite is installed.

You can specify the user and password pair that is appropriate for the server on which a reset is requested. Additionally, you can mark one privileged user entry as the default username and password pair for all servers not explicitly configured.

The correct access key is needed for this PMM. For details on access keys, please contact Core Security.

Prerequisites

You need to install a PMM agent for HP-UX on each HP-UX machine that is a configured password reset target for Core Password.

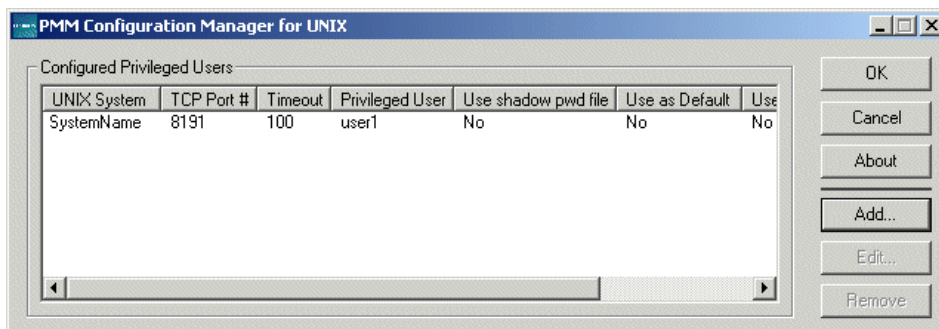
To use the Trusted Mode and Shadow Password File features of the PMM for HP-UX, the HP-UX client needs to have the hp-gcc 4.4.3 library installed on it before the Unix proxy agent is installed. Refer to the HP-UX documentation for information about how to install the hp-gcc 4.4.3 library. These features apply only to HP-UX versions of UNIX.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Start>All Programs>Core Server Core Server>Password Management Modules>HP-UX
2. When prompted, click **YES** to begin the configuration.
The PMM Configuration Manager dialog box appears.

Figure 32: PMM Configuration Manager



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit UNIX System PMM Configuration dialog box appears.

Figure 33: Add/Edit UNIX System User

4. To configure a privileged user for the PMM, follow these steps:
 - a. **UNIX SYSTEM** — Specify the HP-UX server where password resets occur. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
 - b. **TCP/IP PORT** — Specify the TCP/IP port on which the HP-UX agent is listening. The default is 8191.
 - c. **TIMEOUT (SECS)** — Specify the amount of time (in seconds) before password resets timeout. The default is 10 seconds.
 - d. **PRIVILEGED USERNAME** — Specify the username of the privileged user.
Note: The privileged user configured here requires no special privileges; the account is used only to activate the password reset executed by the agent.
 - e. **PASSWORD** — Enter and verify the password for the privileged user.
5. **RESET TYPE**

Determine the reset type to be performed and select “Local Workstation” or “NIS” as appropriate.

- If you select **LOCAL WORKSTATION** and the HP-UX system uses a shadow password file to authenticate users, check the **USE SHADOW PASSWORD FILE** check box.
 - If you select **NIS** and the privileged user exists in the local database and not in the NIS map, check the **USE LOCAL PASSWORD FILE FOR VERIFYING THIS PRIVILEGED USER** check box. Additionally, if the local database where the privileged user's password file uses a shadow file, check the **USE SHADOW PASSWORD FILE** check box.
6. **USE TRUSTED MODE** - Check this box to use trusted mode.
 7. **USE SHADOW PASSWORD FILE** — If the password file is stored in a shadow file, check this box.
 8. **USE LOCAL PASSWORD FILE FOR VERIFYING THIS ADMINISTRATIVE USER** — If you want this user's password to be authenticated using the local system password file, check the box.
 9. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — If you want this username to be the default username for all servers not specifically configured in the PMM Configuration Manager, check the box.
 10. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — If you want to allow password resets of users with a UID or GID of zero, check this box.
 11. Click the **OK** button to save the configuration.
 12. If desired, continue to configure additional users for other servers.
 13. You have finish configuring the PMM. Click the **OK** button to save the changes and exit the configuration program.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and Password Courier Support Staff Classic* explains how to do this on the classic platform.

Writing Password Management Scripts

The PMM for HP-UX can run a sequence of UNIX shell commands to perform a password reset. This allows the PMM for HP-UX to reset any password which has an administrative password reset available via the UNIX shell.

The PMM agent for HP-UX reads a specialized script language. The language syntax is as follows:

- **S N send-string** - Send 'send-string' to a pseudo terminal (pty) and pause for N number of seconds before continuing. The send string can contain any of the following substitution macros:
 %u - The user name to be reset
 %p - the plain text password
 %e - the encrypted password
- **V N verify-string** - Verify that 'verify-string' is found in the output from the pty after waiting N number of seconds for a response and continue when a response is received. The verify string can contain any of the substitution macros described in the send command. It is necessary to have a verify string at the end. If the final verify command isn't received, the end user receives a failure message.
- **;** comment-string - A comment string. Comments must be alone on a line. Commands cannot have trailing comments.

Use a scripting language such as Perl or shell script to write a script that performs a password reset.

The following is an example of a script that uses a custom Perl script to reset a user's password:

```
; Send to launch custom reset script
s 2 perl password_reset_cmd %u %p
; Verify successful message
v 2 "Password reset was successful"
```

Note: Arguments to the “s” and “v” commands must be enclosed with quotation marks.

To tell the PMM agent for HP-UX to use the script for performing resets, go to the directory where the agent was installed and locate the `pxy_def` file. Open the file with a text editor and add the following line:

```
SCRIPT_NAME:pwd.scr
```

where `pwd.scr` is the name of the created script file.

For the change to take effect, start and stop the agent (page 109).

Installing and Configuring the HP-UX PMM Agent

This section explains how to install, configure, remove, start, and stop the PMM agent.

Installing the Agent

The PMM agent runs as a daemon on the UNIX machine. Table 5 describes the agent installation components included with the PMM for HP-UX.

Table 5: PMM Agent for HP-UX Components

PMM for HP-UX agent files	pwdcour_unixpxy pxy_def install uninstall
PMM for HP-UX agent tar file	unixhp.tar

Copy the tar file for the HP-UX system from the UNIX folder located in the folder where the Core Server Core Server is installed to a temporary directory on the HP-UX machine on which the agent is being installed. Log on to the machine as a superuser and proceed to the directory where the tar file was placed.

Note: If it is not performed by a user with superuser privileges, the install fails.

Extract the installation files for the platform using the following command:

```
tar -xvf unixhp.tar
```

This creates and places all of the install files inside of a subdirectory named Core Server.

Change to that directory and then execute the installation shell script by typing `./install`.

Follow the prompts and answer the questions needed for installation. The following information is required:

1. The install directory for the agent (the default is `/usr/local/Core Server`)
2. The password file (the default is `/etc/passwd`)
3. Whether or not NIS is being used (if NIS is being used, the agent must be installed on the same machine as the NIS master.)
 - a. If NIS is being used, the following information is required:
 - The default path to yp database directory (`/var/yp`).
 - The path to make (`/var/yp`)
4. The TCP/IP port available to the agent (default is 8191)

Note: The agent installation is complete when these four steps are performed. If any changes need to be made, make them before finishing step 4.

After installing the agent, launch it by rebooting or by executing the following command:

```
/sbin/rc3.d/S99pwdcour_unixpxy start
```

Configuring the HP-UX PMM Agent

Installing the agent on an HP-UX host creates a configuration file in the agent installation directory (default: `/usr/local/Core Server`). The configuration file is called `pxy_def`. This file has several parameters that control the agent's actions and configuration. You can use a text editor such as `vi` to change the `pxy_def` file. Table 6 describes the agent parameters.

Table 6: PMM Agent for HP-UX Configuration Parameters Core Server

Parameter Syntax	Description
<code>INST_DIR:install_dir</code>	This is the directory in which the agent is installed. By default, the agent is installed in <code>/usr/local/Core Server</code> .
<code>LOG_FILE:log_file</code>	This is the name of the file to which the agent logs all messages. If the directory is omitted, the <code>log_file</code> is automatically created in the directory specified by <code>INST_DIR</code> . If this parameter is omitted, the default value is <code>pxy.log</code> .
<code>LOG_LEVEL:n</code>	Log messages have a log level 'n' associated with them. The log level ranges from 0-2. Depending on the log level you specify in the <code>pxy_def</code> file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the <code>pxy_def</code> file. By default, the log level specified is 0.
<code>MAKE_DIR:make_directory</code>	This is the directory in which the make command can be found. It is used to rebuild the NIS password map. If the directory is omitted, the default is <code>/var/yp</code> . Note: This argument is only relevant when the PMM is configured for native NIS reset support.
<code>NIS_YMAKE_CMD:make_cmd</code>	This command line is used to rebuild and/or push the NIS password map. If it is omitted, the default command is: <code>cd%s;%s/make passwd NOPUSH=TRUE.</code> The first “%s” is a substitution macro for the value specified by <code>Y_DIR</code> . The second “%s” is a substitution macro for the value specified by <code>MAKE_DIR</code> . Note: This argument is only relevant when the PMM is configured for native NIS reset support.
<code>NIS_UPMAKE_RESP:response</code>	This is the expected response from the command used to rebuild and/or push the NIS password map. If this value is omitted, the default response is “updated passwd.” Note: This argument is only relevant when configured for native NIS reset support.

Table 6: PMM Agent for HP-UX Configuration Parameters Core Server

Parameter Syntax	Description
NIS_PASSWORD_FILE	This parameter is used to specify the path to the NIS password file on the local machine. It is necessary to use this file when NIS password files that are not /etc/passwd are being used.
PASSWORD_FILE: <i>passwd_file</i>	This represents the fully qualified file name of the password file against which users are validated and native workstation and/or NIS resets are performed. If the file is omitted, the default is /etc/passwd.
PWD_ERR_MSG: <i>err_msg</i>	This is a custom error message displayed to the user when an error occurs during a password reset. If it is omitted, a technical error description is displayed.
SCRIPT_NAME: <i>script_file</i>	This is the name of the script file to run for resets. For more information on scripts, see “Creating a Workflow for a Target” on page 106 . If this parameter is omitted, a native password reset (either workstation or NIS) is performed.
SHDW_FILE: <i>shadow_file</i>	This is the fully qualified file name of the shadow file against which users are validated and native workstation resets are performed. This value is consulted if the PMM Configuration Manager is configured with the USE SHADOW PASSWORD FILE check box checked. If it is omitted, the default is /etc/security/shadow.
SVR_NAME: <i>server</i>	This represents the host name of the server on which the agent is installed. There is no default value. This value must be valid.
SVR_PORT: <i>port_number</i>	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value and the port number specified here must be the same as the one used during PMM configuration. This value is required.
VALIDATION_USER: <i>username</i>	This user name must match the user configured for this server on the machine running on the Connector Framework Manager. If this parameter is omitted, the default value is root. Note: The privileged user configured requires no special privileges; the account is only used to activate the password reset executed by the agent software.
YP_DIR: <i>yp_dir</i>	This is the directory where the NIS password file exists. If it is omitted, the default value is /var/yp. Note: This argument is only relevant when the PMM is configured for native NIS password reset support.

Starting and Stopping the Agent

For any changes to take effect, stop and then start the agent using the startup script. To start the PMM agent, run the startup script with the argument **START**. Run the script with the **STOP** argument to stop the agent.

- To start: `/etc/pwdcour_unixpxy start`
- To stop: `/etc/pwdcour_unixpxy stop`

Displaying the Version Information

To output the version of the proxy, execute the following command from the UNIX prompt: `/usr/local/courion/pwdcour_unixpxy -v`

This outputs the version information to the command window, e.g. 7.50.00.113

There is not an option in the `/etc/pwdcour_unixpxy` file to output the version information; you have to run it directly from the install directory (default for AIX is `/usr/local/courion`).

The default install directory is the same for each platform the proxy is installed on (`/usr/local/courion`)

Uninstalling the PMM Agent for Upgrading

To upgrade the PMM agent for HP-UX, uninstall the previous agent and then install the new agent. The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

To uninstall the PMM agent for HP-UX execute the uninstall script by typing `installdir/uninstall`.

Note: Before beginning the uninstall process, back up the `installdir/pxy_def` file to another directory, where *installdir* is the installation directory, typically `/usr/local/Core Server`. Also back up the reset script file to another directory if scripted resets are being used.

- Follow the prompts and answer the questions. You must know the install path.
- After untarring the distribution files for the new PMM agent for HP-UX, install the new agent by following the steps outlined in [“Installing the Agent” on page 108](#).
- Merge custom entries from the backed up `pxy_def` file into the new `installdir/pxy_def` file.
- Restore the backup reset script to the desired directory. Make sure the new `pxy_def` file refers to that script.

Configuring the Connector for HP-UX

The Connector for HP-UX supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Authentication

Prerequisites

ActivePerl must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. See [“Installing ActivePerl” on page 695](#) for information on installing ActivePerl. Reboot the servers after you have installed ActivePerl.

Scripts that Support Provisioning on HP-UX Systems

Table 7 shows the scripts and connection methods you can use with versions of HP-UX systems.

Table 7: Scripts that Support Provisioning on HP-UX Systems

Script	HP-UX System	Connection Method
hpux11sshtss.pl	Hewlett Packard HP-UX v11	Trusted secure system using SSH
hpux11sshtss_sudo.pl	Hewlett Packard HP-UX v11	Trusted secure system using SSH with the <code>sudo</code> command

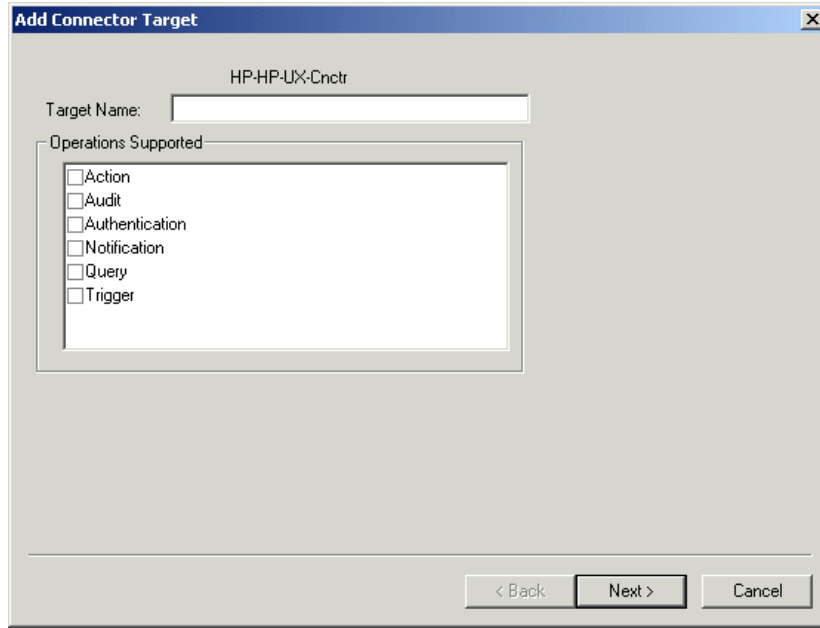
Note: The `sudo` command can assign a specific user account with minimum privileges, other than root, on the HP-UX system to perform provisioning actions.

Note: You may need to modify these scripts for your customized UNIX environment.

Connector Configuration

Follow these steps to add an HP-UX target:

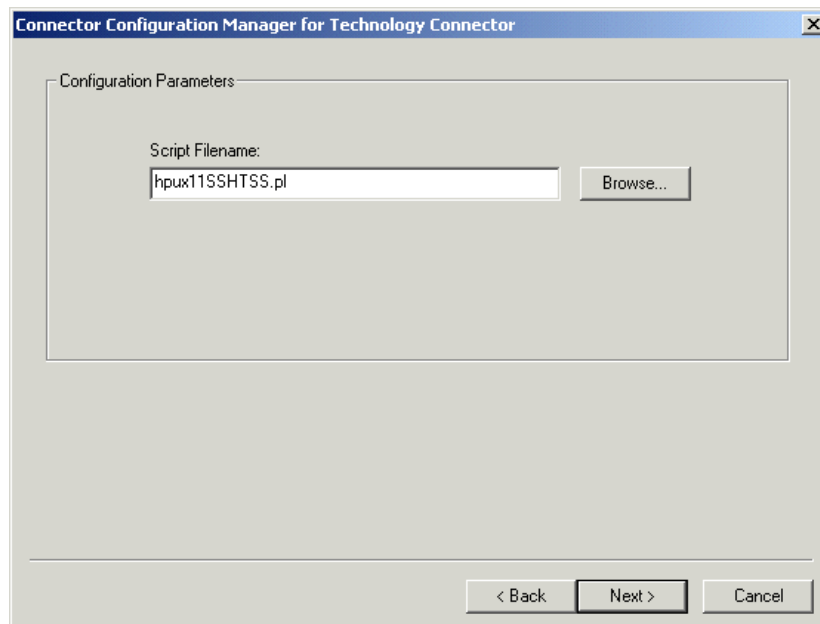
1. From the Start menu, select:
Programs >Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **HP-HP-UX-CNCTR**, and click **OK**.
3. Select **HP-HP-UX-CNCTR**
4. Right click and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 34: Add HP-UX Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
 - Choose the operations you want:
Select **ACTION** to enable operations on a target.
 - Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Server or Core Server.
6. Click **NEXT**.

NOTE: Other operations that appear in this dialog box are not supported.

The Configuration Manager for Technology Connector screen appears.

Figure 35: Connector Configuration Manager for HP-UX

7. The default `hpux11SSHTSS.pl` script providing the functionality for performing connector operations is entered for the **SCRIPT FILENAME**. If you want to use a different script, browse to the location and name of that script. Click the **NEXT** button.

The second window for HP-UX appears.

Figure 36: Connector Configuration Manager for HP-UX (2)

8. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

SSH Parameters:

- a. **ROOT PASSWORD** — The password value of the superuser. Use this parameter only if you do not want to connect to the server directly as "root" but as a normal user. In that case, the root password value is required to change a normal user to the superuser so that the application can execute commands. To connect directly to the HP-UX server as "root", make sure the SSH server is configured to set the "PermitRootLogin" option to "yes."
- b. **SSH AUTHENTICATION METHOD** — Two authentication methods are supported for SSH: password authentication and public key authentication. Password authentication is the default value, or you can enter `password` to specify this value. Enter the value `publickey` to use public key authentication.
- c. **SSH CIPHER TYPE** — The cipher type used to encrypt the session. The three supported cipher types are: 3DES, AES and Blowfish. Enter the value `3des` for 3DES; `aes` for AES; or `blowfish`. If you omit a value for cipher type, the connector negotiates with the SSH server to select the appropriate cipher for encrypting the session.
- d. **SSH PRIVATE KEY** — The full path of private key file of the SSH User. The path needs to be in one of these formats:

drive-letter:\\yourdir\\your-private-key-file
or
drive-letter/yourdir/your-private-key-file

This private key file is generated using the ssh key generator tool on the SSH server. Make sure the public key of the same type (RSA or DSA) of this user is in the `authorized_keys` file for it to work properly. This parameter is required only if the authentication method is public key authentication.

- e. **SSH PRIVATE KEY TYPE** — Specify the type of the private key: RSA or DSA. The default key type is RSA or you can enter the value `rsa`. To specify that the private key is a DSA key, enter the value `dsa`.
 - f. **SSH PRIVATE KEY'S PASSPHRASE** — The pass phrase of the private key. If the private key provided is protected by a pass phrase, then enter that pass phrase. Otherwise, leave it blank.
 - g. **SSH SERVER** — The name of the HP-UX server that has SSH server installed.
 - h. **SSH USER** — The account name used to connect to the HP-UX server.
 - i. **SSH USER'S PASSWORD** — The password of the SSH User. This parameter is required only if the authentication method is a password authentication.
9. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 15: HP-UX 11i v1 Trusted Mode — PMM

This chapter explains how to configure the PMM for HP-UX 11i v1 Trusted Mode. It also explains how to install and configure the agent required by the PMM:

- [*“Configuring the PMM for HP-UX 11i v1 Trusted Mode” on page 118*](#)
- [*“Installing and Configuring the HP-UX 11i v1 PMM Agent” on page 121*](#)

Configuring the PMM for HP-UX 11i v1 Trusted Mode

The Password Management Module (PMM) for HP-UX 11i v1 Trusted Mode enables Core Server applications to reset passwords automatically on HP-UX 11i v1 systems. The PMM is a component of the Core Server and is installed when the suite is installed.

Note: This PMM works only with the HP-UX 11i v1 (11.11) in Trusted Mode. For password resets for other versions of HP-UX, see [“HP-UX System — PMM and Connector” on page 103](#).

Prerequisites

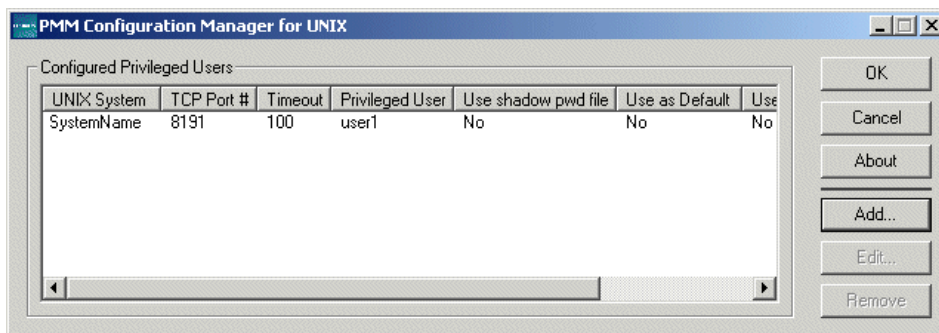
You need to install a PMM agent for HP-UX 11i v1 Trusted Mode on each HP-UX 11i v1 machine that is a configured password reset target for Core Password.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Start>All Programs>Core Server Core Server>Password Management Modules>HP UX 11i v1 Trusted Mode
2. When prompted, click **YES** to begin the configuration.
The PMM Configuration Manager dialog box appears.

Figure 37: PMM Configuration Manager



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.

- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit HP-UX 11i v1 System PMM Configuration dialog box appears.

Figure 38: Add/Edit HP-UX 11i v1 System PMM Configuration

4. To configure a privileged user for the PMM, follow these steps:
 - a. **UNIX SYSTEM** — Specify the HP-UX 11i v1 server where password resets occur. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
 - b. **TCP/IP PORT** — Specify the TCP/IP port on which the HP-UX 11i v1 agent is listening. The default is 8191.
 - c. **TIMEOUT (SECS)** — Specify the amount of time (in seconds) before password resets timeout. The default is 10 seconds.
 - d. **PRIVILEGED USERNAME** — Specify the username of the privileged user.
Note: The privileged user configured here requires no special privileges; the account is used only to activate the password reset executed by the agent.
 - e. **PASSWORD** — Enter and verify the password for the privileged user.
5. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — If you want to allow password resets of users with a UID or GID of zero, check this box.
6. Click the **OK** button to save the configuration.
7. If desired, continue to configure additional users for other servers.
8. You have finish configuring the PMM. Click the **OK** button to save the changes and exit the configuration program.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff* explains how to do this on the classic platform.

Installing and Configuring the HP-UX 11i v1 PMM Agent

This section explains how to install, configure, remove, start, and stop the PMM agent.

Installing the Agent

The PMM agent runs as a daemon on the UNIX machine.

This agent requires that the hp-gcc-4.4.5 compiler be installed on the HP-UX 11i v1 system.

Table 8 describes the agent installation components included with the PMM for HP-UX 11i v1 Trusted Mode.

Table 8: PMM Agent for HP-UX 11i v1 Components

PMM for HP-UX 11i v1 Trusted Mode agent files	pwdcour_unixpxy pxy_def install uninstall
PMM for HP-UX 11i v1 Trusted Mode agent tar file	hpux11_11_RISC.tar

Copy the hpux11_11_RISC.tar file that is located in the UNIX folder under the Core Core Server directory to a temporary directory on the HP-UX 11i v1 system. Log on to the machine as a Superuser and navigate to the directory where the tar file was placed.

Note: If you are not logged on as a Superuser, the installation fails.

Extract the installation files for the platform using the following command:

```
tar -xvf hpux11_11_RISC.tar
```

This creates a subdirectory named courion and places all of the installation files inside the directory.

Change to the courion directory and execute the installation shell script by typing the command:

```
./install
```

To answer the prompts, you need the following information:

- The install directory for the agent (the default is /usr/local/courion)
- The password file (the default is /etc/passwd)
- The TCP/IP port available to the agent (default is 8191)

Note: The agent installation is complete when you have completed these three steps. If any changes need to be made, make them before finishing step 3.

After installing the agent, launch it by rebooting or by executing the following command using a Superuser account:

```
/sbin/rc3.d/S99pwdcour_unixpxy start
```

Configuring the HP-UX 11i V1 PMM Agent

Installation of the agent on an HP-UX 11i v1 creates a configuration file in the installation directory for the agent (default: /usr/local/courion). The configuration file is called pxy_def. This file has several parameters that control the agent's actions and configuration. You can use a text editor such as vi to change the pxy_def file. Table 9 describes the agent parameters.

Table 9: PMM Agent for HP-UX 11i v1 Configuration Parameters

Parameter Syntax	Description
INST_DIR: <i>install_dir</i>	This is the directory in which the agent is installed. By default, the agent is installed in /usr/local/courion.
LOG_FILE: <i>log_file</i>	This is the name of the file to which the agent logs all messages. If the directory is omitted, the log_file is automatically created in the directory specified by INST_DIR. If this parameter is omitted, the default value is pxy.log.
LOG_LEVEL: <i>n</i>	Log messages have a log level 'n' associated with them. The log level ranges from 0-2. Depending on the log level you specify in the pxy_def file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the pxy_def file. By default, the log level specified is 0.
PASSWORD_FILE: <i>passwd_file</i>	This represents the fully qualified file name of the password file against which users are validated and native workstation and/or NIS resets are performed. If the file is omitted, the default is /etc/passwd.
PWD_ERR_MSG: <i>err_msg</i>	This is a custom error message displayed to the user when an error occurs during a password reset. If it is omitted, a technical error description is displayed.
SCRIPT_NAME: <i>script_file</i>	This is the name of the script file to run for resets. For more information on scripts, see “Creating a Workflow for a Target” on page 120 . If this parameter is omitted, a native password reset (either workstation or NIS) is performed.
SVR_NAME: <i>server</i>	This represents the host name of the server on which the agent is installed. There is no default value. This value must be valid.
SVR_PORT: <i>port_number</i>	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value and the port number specified here must be the same as the one used during PMM configuration. This value is required.

Table 9: PMM Agent for HP-UX 11i v1 Configuration Parameters

Parameter Syntax	Description
VALIDATION_USER: <i>username</i>	This user name must match the user configured for this server on the machine running on the Connector Framework Manager. If this parameter is omitted, the default value is root. Note: The privileged user configured requires no special privileges; the account is only used to activate the password reset executed by the agent software.

Starting and Stopping the Agent

For any changes to take effect, stop and then start the agent daemon using the startup script. To start the PMM agent, run the startup script with the argument START. Run the script with the STOP argument to stop the agent.

- To start: `/sbin/init.d/pwdcour_unixpxy start`
- To stop: `/sbin/init.d/pwdcour_unixpxy stop`

Displaying the Version Information

To output the version of the PMM agent, execute the following command from the UNIX prompt: `/usr/local/courion/pwdcour_unixpxy -v`

This outputs the version information to the command window, e.g. 7.50.00.113

The default install directory is the same for each platform the daemon agent is installed on (`/usr/local/courion`).

Uninstalling the PMM Agent for Upgrading

To upgrade the PMM agent for HP-UX 11i v1, uninstall the previous agent and then install the new agent. The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

To uninstall the existing PMM agent for HP-UX 11i v1 by execute the uninstall script located in the PMM agent installation directory.

Note: Before beginning the uninstall process, back up the `pxy_def` file located in the installation directory to another directory. default: `/usr/local/courion`. Back up the reset script file to another directory if scripted resets are being used.

- Follow the prompts and answer the questions. You must know the install path.
- After extracting the new distribution file for the new PMM agent, install it by following the steps outlined in [“Installing the Agent” on page 121](#).

- Merge custom entries from the backed up pxy_def file into the new pxy_def file located in the installation directory.
- Restore the backup reset script to the installation directory. Make sure the new pxy_def file refers to that script.

Chapter 16: HTML Email — Connector

There are two different connectors for HTML Email—the standard connector, and an enhanced connector that supports character sets.

It is recommended to use the Enhanced Connector for HTML Email as it is more robust and has more features.

This chapter explains how to configure both connectors for HTML Email:

- [*“Configuring the Connector for HTML Email” on page 126*](#)
- [*“Configuring the Enhanced Connector for HTML Email” on page 128*](#)

Configuring the Connector for HTML Email

The standard Connector for HTML Email supports Notification on a target and enables Core Server applications to integrate with an SMTP e-mail server. This integration provides e-mail notification services for operations, such as end user authentication and provisioning actions. Adding a target to the connector identifies the server on which the SMTP application is installed.

The Connector for HTML Email enables you to include rich HTML content in the body of the message.

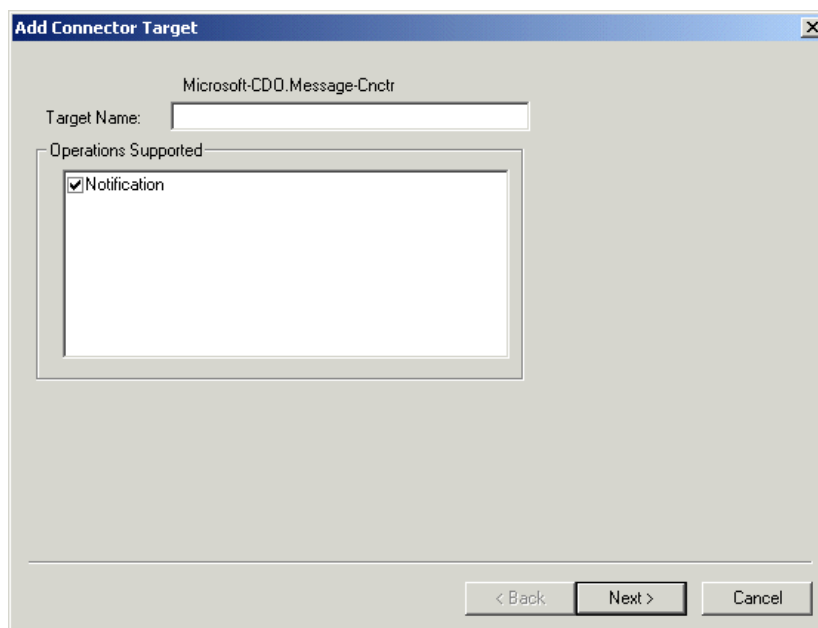
Each server in which the Connector Framework or Connector Framework Manager is installed must have Internet access.

Follow these steps to add an SMTP target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-CDO.MESSAGE-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 39: Add HTML Email Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **NOTIFICATION** check box is selected by default.

Click **NEXT**. The Core Server dialog box appears.

Figure 40: Connector Configuration Manager for HTML Email

5. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

SMTP Port — Enter an SMTP port number. In most environments, the SMTP port is 25.

SMTP Server — Enter the IP address or the DNS server name for the SMTP server.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

6. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Configuring the Enhanced Connector for HTML Email

The enhanced Connector for HTML Email supports all of the features of the regular Connector for HTML Email. In addition, it provides support for character sets.

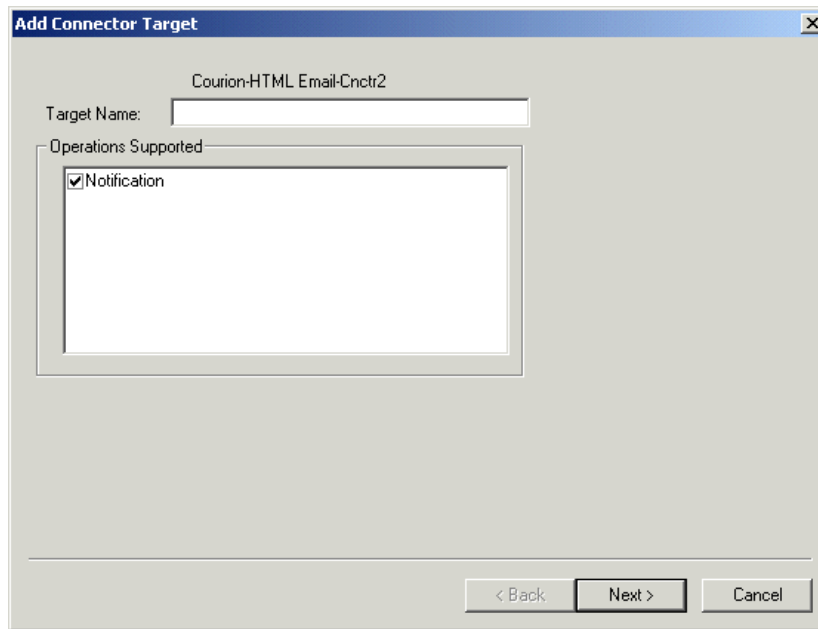
Each server in which the Connector Framework or Connector Framework Manager is installed must have Internet access.

Follow these steps to add an SMTP target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **COURION-HTML EMAIL-CNCTR2**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 41: Add HTML Email Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **NOTIFICATION** check box is selected by default.

Click **NEXT**. The Core Server dialog box appears.

Figure 42: Connector Configuration Manager for HTML Email

5. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

Email Charset — Enter the character set to be used for the email. The default value is “utf-8”. For a list of valid character sets, see <http://msdn2.microsoft.com/en-us/library/ms526296.aspx>

Email Server — Enter the IP address or the DNS server name for the SMTP server.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

6. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 17: IBM AIX — PMM and Connector

This chapter explains how to configure the PMM and Connector for IBM AIX. It also explains installing and operating the AIX PMM agent. This chapter includes the following sections:

- [*“Configuring the PMM for IBM AIX” on page 132*](#)
- [*“Writing Password Management Scripts” on page 135*](#)
- [*“Installing and Configuring the AIX PMM Agent” on page 136*](#)
- [*“Configuring the Connector for IBM AIX” on page 140*](#)

Configuring the PMM for IBM AIX

The Password Management Module (PMM) for IBM AIX enables Core Server applications to reset passwords automatically on IBM AIX systems. The PMM is a component of the Core Server and is installed when the suite is installed.

You can specify the user and password pair that is appropriate for the server on which a reset is requested. Additionally, you can mark one privileged user entry as the default username and password pair for all servers not explicitly configured.

The correct access key is needed for this PMM. For details on access keys, please contact Core Server.

Prerequisites

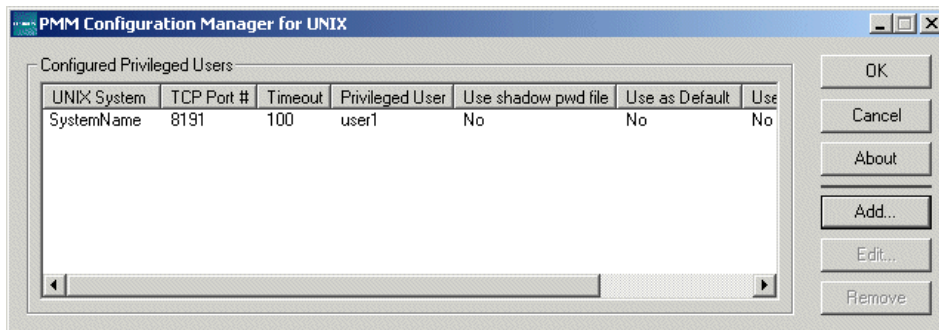
The PMM agent for IBM AIX must be installed on each IBM AIX machine on which password resets are to be performed. Installing the agent is described later in this chapter.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>IBM AIX
2. Click on **IBM AIX** and, when prompted, click **YES** to begin the configuration.
The PMM Configuration Manager appears.

Figure 43: PMM Configuration Manager for IBM AIX



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.

- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 44: Add / Edit UNIX System PMM Configuration for IBM AIX

4. **UNIX SYSTEM** — Enter the name of the IBM AIX server where password resets occur. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
5. **TCP/IP PORT** — Enter the TCP/IP port on which the IBM AIX agent is listening. The default is 8191.
6. **TIMEOUT (SECS)** — Enter the amount of time (in seconds) before password reset timeout. The default is 10 seconds.

7. **PRIVILEGED USER** — Enter the username of the privileged user.

Note: The Privileged AIX user must have permissions to reset passwords at a minimum. The AIX user must be a Privileged User (an Authorized User) but does not require ROOT and no other specific permissions are required.

8. **PASSWORD** — Enter and verify the password for the privileged user.

9. **RESET TYPE**

Determine the reset type to be performed and select “Local Workstation” or “NIS” as appropriate.

- If you select **LOCAL WORKSTATION** and the IBM AIX system uses a shadow password file to authenticate users, check the **USE SHADOW PASSWORD FILE** check box.

- If you select **NIS** and the privileged user exists in the local database and not in the NIS map, check the **USE LOCAL PASSWORD FILE FOR VERIFYING THIS PRIVILEGED USER** check box. Additionally, if the local database where the privileged user's password file uses a shadow file, check the **USE SHADOW PASSWORD FILE** check box.
10. **USE SHADOW PASSWORD FILE** — If the password file is stored in a shadow file, check this box.
 11. **USE LOCAL PASSWORD FILE FOR VERIFYING THIS ADMINISTRATIVE USER** — If you want this user's password to be authenticated using the local system password file, check the box.
 12. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — If you want this username to be the default username for all servers not specifically configured in the PMM Configuration Manager, check the box.
 13. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — If you want to allow password resets of users with a UID or GID of zero, check this box.
 14. Click the **OK** button to save the configuration.
 15. If desired, continue to configure additional users for other servers.
 16. You have finish configuring the PMM. Click the **OK** button to save the changes and exit the configuration program.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- If the ADMIN attribute is set for a user on AIX, the PMM does not allow that user to change his password through Core Server.
- If the ADMCHG attribute is set for a user on AIX, the PMM removes this attribute after a user resets his/her password through Core Server. The user is not forced to change password at the next login unless Core Server is configured to force a password change at next login.
- The PMM resets the unsuccessful login count to zero (0) for AIX users who reset their passwords through Core Server after one or more unsuccessful logins.

Writing Password Management Scripts

The PMM can run a sequence of UNIX shell commands to perform a password reset. This allows the PMM to reset any password which has an administrative password reset available via the UNIX shell.

Note: Use of password management scripts is only required if you have a non-standard or custom configuration on your AIX server (such as running third party software on your AIX server). In such a case, Courion's AIX PMM would then execute those shell scripts. If however your AIX server accepts standard commands, then no password management scripts need to be written.

The IBM AIX agent reads a specialized script language. The syntax of the language is as follows:

- S N send-string - Send 'send-string' to a pseudo terminal (pty) and pause for N number of seconds before continuing. The send string can contain any of the following substitution macros:
 %u - The username to be reset
 %p - the plain text password
 %e - the encrypted password
- V N verify-string - Verify that 'verify-string' is found in the output from the pty after waiting N number of seconds for a response and continue when a response is received. The verify string can contain any of the substitution macros described in the send command. It is necessary to have a verify string at the end. If the final verify command isn't received, the end user receives a failure message.
- ; comment-string - A comment string. Comments must be alone on a line. Commands cannot have trailing comments.

Use a scripting language such as Perl or shell script to write a script that performs a password reset.

The following is an example of a script that uses a custom Perl script to reset a user's password:

```
; Send to launch custom reset script
s 2 perl password_reset_cmd %u %p
; Verify successful message
v 2 "Password reset was successful"
```

Note: Arguments to the “s” and “v” commands must be enclosed with quotation marks.

To tell the PMM for IBM AIX agent to use the script for performing resets, go to the directory where the agent was installed and locate the pxy_def file. Open the file with a text editor and add the following line:

```
SCRIPT_NAME:pwd.scr
where pwd.scr is the name of the created script file.
```

For the change to take effect, start and stop the agent ([“Starting and Stopping the Agent” on page 139](#)).

Installing and Configuring the AIX PMM Agent

This section explains how to install, configure, remove, start, and stop the PMM agent.

Installing the Agent

The PMM agent runs as a daemon on the UNIX machine. Table 10 describes the agent installation components included with the PMM for IBM AIX.

Table 10: PMM Agent for IBM AIX Components

PMM for IBM AIX agent files	pwdcour_unixpxy pxy_def install uninstall
PMM for IBM AIX agent tar file	unixaix.tar

1. Copy the tar file for the IBM AIX system from the UNIX folder located in the directory where the Core Server Core Server is installed to a temporary directory on the IBM AIX machine on which the agent is being installed. Log on to the machine as a superuser and proceed to the directory where the tar file was placed.

Note: If it is not performed by a user with superuser privileges, the install fails.

2. Extract the installation files for the platform using the following command:

```
tar -xvf unixaix.tar
```

This creates and places all of the install files inside of a subdirectory named Core Server.

3. Change to that directory and then execute the installation shell script by typing `./install`.
4. Follow the prompts and answer the questions needed for installation. The following information is required:
 - a. The install directory for the agent (the default is `/usr/local/Core Server`)
 - b. The password file (the default is `/etc/passwd`)
 - c. Whether or not NIS is being used (if NIS is being used, the agent must be installed on the same machine as the NIS master.)
If NIS is being used, the following information is required:
 - d. The default path to yp database directory (`/var/yp`)
 - e. The path to make (`/var/yp`)
 - f. The TCP/IP port available to the agent (default is 8191)

The agent installation is complete when these four steps are performed. If any changes need to be made, make them before finishing step 4.

Once it is installed, launch the agent by rebooting or by executing the following command:

```
/etc/pwdcour_unixpxy start
```


Configuring the Agent

Installation on the IBM AIX host creates a configuration file in the agent's installation directory (the default is `/usr/local/Core Server`). The configuration file is called `pxy_def`. This file has several parameters that control the agent's actions and configuration. You can use a text editor such as `vi` to change the `pxy_def` file. Table 11 describes the parameters.

Table 11: AIX PMM Agent Configuration ParametersCore Server

Parameter Syntax	Description
<code>INST_DIR:install_dir</code>	This is the directory in which the agent is installed. By default, the agent is installed in <code>/usr/local/Core Server</code> .
<code>LOG_FILE:log_file</code>	This is the name of the file to which the agent logs all messages. If the directory is omitted, the <code>log_file</code> is automatically created in the directory specified by <code>INST_DIR</code> . If this parameter is omitted, the default value is <code>pxy.log</code> .
<code>LOG_LEVEL:n</code>	Log messages have a log level 'n' associated with them. The log level ranges from 0-2. Depending on the log level you specify in the <code>pxy_def</code> file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the <code>pxy_def</code> file. By default, the log level specified is 0.
<code>MAKE_DIR:make_directory</code>	This is the directory in which the make command can be found. It is used to rebuild the NIS password map. If the directory is omitted, the default is <code>/var/yp</code> . Note: This argument is only relevant when the PMM is configured for native NIS reset support.
<code>NIS_YMAKE_CMD:make_cmd</code>	This the command line used to rebuild and/or push the NIS password map. If it is omitted, the default command is: <code>cd%s;%s/make passwd NOPUSH=TRUE.</code> The first “%s” is a substitution macro for the value specified by <code>Y_DIR</code> . The second “%s” is a substitution macro for the value specified by <code>MAKE_DIR</code> . Note: This argument is only relevant when the PMM is configured for native NIS reset support.
<code>NIS_UPMAKE_RESP:response</code>	This is the expected response from the command used to rebuild and/or push the NIS password map. If this value is omitted, the default response is “updated passwd.” Note: This argument is only relevant when configured for native NIS reset support.
<code>NIS_PASSWORD_FILE</code>	This parameter is used to specify the path to the NIS password file on the local machine. It is necessary to use this file when NIS password files that are not <code>/etc/passwd</code> are being used.

Table 11: AIX PMM Agent Configuration ParametersCore Server

Parameter Syntax	Description
PASSWORD_FILE:passwd_file	This represents the fully qualified filename of the password file against which users are validated and native workstation and/or NIS resets are performed. If the file is omitted, the default is /etc/passwd.
PWD_ERR_MSG:err_msg	This is a custom error message displayed to the user when an error occurs during a password reset. If it is omitted, a technical error description is displayed.
SCRIPT_NAME:script_file	This is the name of the script file to run for resets. For more information on scripts, see “Creating a Workflow for the Target” on page 134 . If this parameter is omitted, a native password reset (either workstation or NIS) is performed.
SHDW_FILE:shadow_file	This is the fully qualified filename of the shadow file against which users are validated and native workstation resets are performed. This value is consulted if the PMM Configuration Manager is configured with the USE SHADOW PASSWORD FILE check box checked. If it is omitted, the default is /etc/security/shadow.
SVR_NAME:server	This represents the host name of the server on which the agent is installed. There is no default value. This value must be valid.
SVR_PORT:port_number	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value and the port number specified here must be the same as the one used during PMM configuration. This value must be present.
USE_ADMIN_FLAG:x	When this variable is set to 1 (enabled) it prevents Core Server-driven password resets from occurring on accounts that have the ADMIN flag set. Note: This variable is not in the sample <i>pxy_def</i> file. If you want to use this variable, you must add it to your file.
VALIDATION_USER:username	This username must match the user configured for this server on the machine running on the Connector Framework Manager. If this parameter is omitted, the default value is <code>root</code> . Note: The privileged user configured requires no special privileges. The account is used only to activate the password reset executed by the agent software.
YP_DIR:yp_dir	This is the directory where the NIS password file exists. If it is omitted, the default value is <code>/var/yp</code> . Note: This argument is only relevant when the PMM is configured for native NIS password reset support.

Starting and Stopping the Agent

For any changes to take effect, stop and then start the agent using the startup script. To start the PMM agent, run the startup script with the argument **START**. Run the script with the **STOP** argument to stop the agent.

- To start: `/etc/pwdcour_unixpxy start`
- To stop: `/etc/pwdcour_unixpxy stop`

Displaying the Version Information

To output the version of the proxy, execute the following command from the UNIX prompt: `/usr/local/courion/pwdcour_unixpxy -v`

This outputs the version information to the command window, e.g. 7.50.00.113

There is not an option in the `/etc/pwdcour_unixpxy` file to output the version information; you have to run it directly from the install directory (default for AIX is `/usr/local/courion`).

The default install directory is the same for each platform the proxy is installed on (`/usr/local/courion`).

Uninstalling the Agent for Upgrading

To upgrade the PMM agent for IBM AIX, uninstall the previous agent and then install the new agent. The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

To uninstall the PMM agent for IBM AIX, execute the uninstall script by typing `installdir/uninstall`.

Note: Before beginning the uninstall process, back up the `installdir/pxy_def` file to another directory, where `installdir` is the installation directory, typically `/usr/local/Core Server`. Also back up the reset script file to another directory if scripted resets are being used.

- Follow the prompts and answer the questions. It is necessary to know the install path.
- After untarring the distribution files for the new PMM agent for IBM AIX, install the new agent by following the steps outlined in [“Installing and Configuring the AIX PMM Agent” on page 136](#).
- Merge custom entries from the backed up `pxy_def` file into the new `installdir/pxy_def` file.
- Restore the backup reset script to the desired directory. Make sure the new `pxy_def` file refers to that script.

Configuring the Connector for IBM AIX

The connector for IBM AIX supports the following operations on a target: Add, Authentication, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

ActivePerl must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. See [“Installing ActivePerl” on page 695](#) for information on installing ActivePerl. Reboot the servers after you have installed ActivePerl.

Scripts that Support Provisioning on IBM AIX Systems

Table 12 shows the scripts and connection methods that you can use with IBM AIX systems.

Table 12: Scripts that Support Provisioning on IBM AIX Systems

Script	Connection Method
IBMAIXCnctr_SSH.pl	Standard, using SSH
IBMAIXCnctr_SSH_SUDO.pl	Standard, using SSH with the <code>sudo</code> command
IBMAIXCnctr_SSH_NON_SU.pl	Standard, using SSH without Super User privileges. Note: To use this script, the SSH User you specify in the connector configuration must have the following privileges: - The user must be a member of the “security” group - The user’s primary group must be “security”

Note: The `sudo` command can assign a specific user account with minimum privileges, other than root, on the IBM AIX system to perform provisioning actions.

Note: You may need to modify these scripts for your customized UNIX environment.

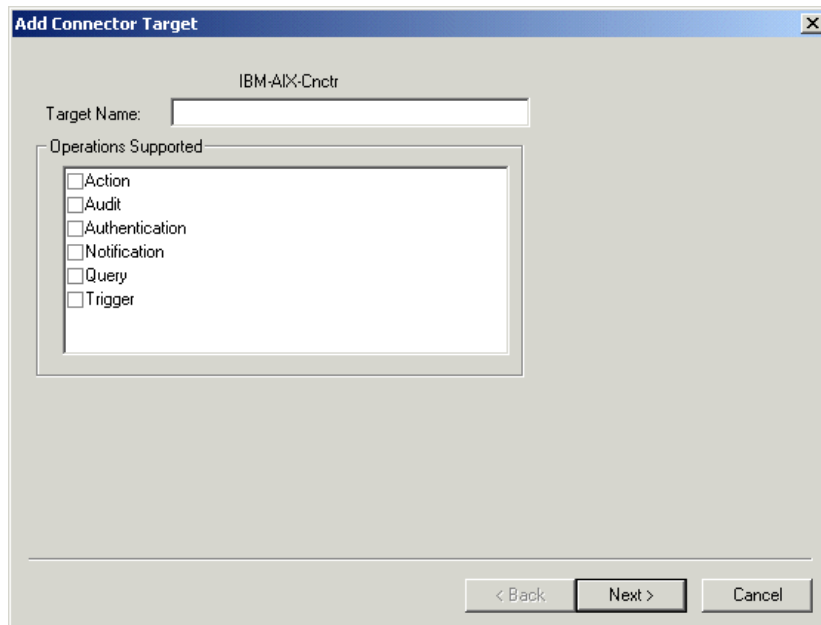
Connector Configuration

Follow these steps to add an IBM AIX target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **IBM-AIX-CNCTR**, and click **OK**.
3. Select **IBM-AIX-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

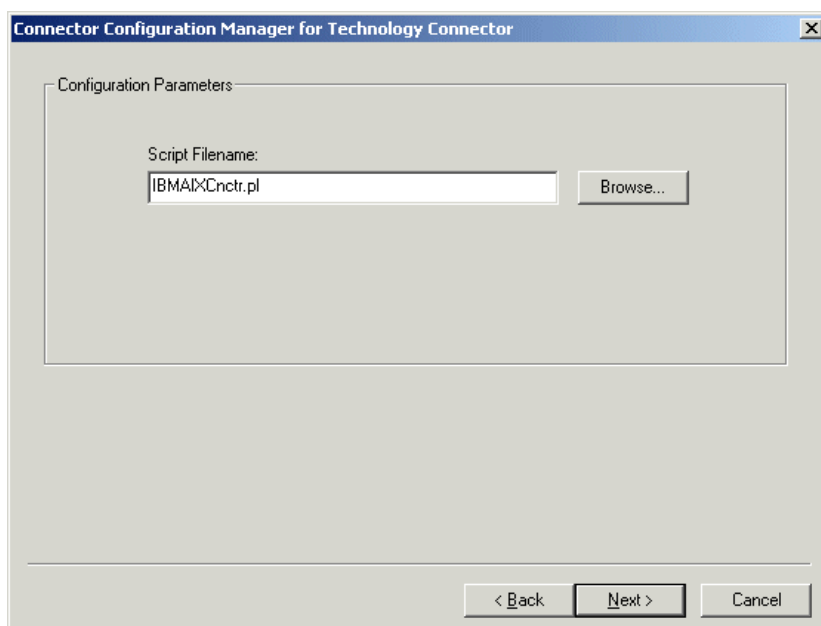
Figure 45: Add IBM AIX Target

The dialog box is titled "Add Connector Target". It has a text field for "Target Name" with the value "IBM-AIX-Cnctr". Below this is a section titled "Operations Supported" containing a list of checkboxes: Action, Audit, Authentication, Notification, Query, and Trigger. The "Action" checkbox is selected. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. Select **ACTION** to enable all provisioning and compliance actions.
Select **AUTHENTICATION** to use the target datasource for authenticating end user access to Core Server or Core Server.
Note: Other operations that appear in this dialog box are not supported.
7. Click **NEXT**.

The Configuration Manager for Technology Connector dialog box appears.

Figure 46: Connector Configuration Manager for IBM AIX

The dialog box is titled "Connector Configuration Manager for Technology Connector". It has a section titled "Configuration Parameters" containing a text field for "Script Filename:" with the value "IBMAIXCnctr.pl". To the right of the text field is a "Browse..." button. At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

8. The default script providing the functionality for performing connector operations is entered for the **SCRIPT FILENAME**. To use a different script, browse to the location and select the name of that script. Click the **NEXT** button.

Note: You may need to modify this script for your customized UNIX environment. Core Security recommends that you save any modified script under a different name. To use a different script, browse to the location and name of that script. Click the **NEXT** button.

The second window of the IBM AIX Connector Configuration Manager appears.

Figure 47: Connector Configuration Manager for IBM AIX (2)

9. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.

SSH Parameters:

- **ROOT PASSWORD** — (Applies to the `IBMAIXCnctr_SSH.pl` script only.) This is the password value of the super user. Use this configuration parameter only if you do not want to connect to the server directly as "root" but as a normal user. In that case, the root password value is used to change a normal user to become the super user to execute commands sent from the provisioning application. To connect directly to the IBM AIX server as "root", make sure the SSH server is configured to set the "PermitRootLogin" option to "yes."
- **SSH AUTHENTICATION METHOD** — Two authentication methods are supported for SSH: password authentication and public key authentication. Password authentication is the default value, or you can enter `password` to specify this value. Enter the value `publickey` to use public key authentication.

- **SSH CIPHER TYPE** — The cipher type used to encrypt the session. The three supported cipher types are: 3DES, AES and Blowfish. Enter the value `3des` for 3DES cipher type; `aes` for AES cipher type; and `blowfish` for Blowfish cipher type. If you do not configure a value for the cipher type, the Connector for IBM AIX negotiates with the SSH server to select the appropriate cipher to use for encrypting the session.
- **SSH PRIVATE KEY** — The full path of private key file of the SSH User. The path must be in one of these formats:

drive:\\yourdir\\your-private-key-file

or

drive/yourdir/your-private-key-file

This private key file is generated using the SSH key generator tool on the SSH server. Make sure the public key of the same type (RSA or DSA) of this user is in the `authorized_keys` file for it to work properly. This configuration parameter is only required if the authentication method is public key authentication.

- **SSH PRIVATE KEY TYPE** — Specify the type of the private key: RSA or DSA. The default key type is RSA or you can enter the value `rsa`. To specify that the private key is a DSA key, enter the value `dsa`.
- **SSH PRIVATE KEY'S PASSPHRASE** — The passphrase of the private key. If the private key provided is protected by a passphrase, then enter that passphrase. Otherwise, leave it blank.
- **SSH SERVER** — The IBM AIX server that has SSH server installed.
- **SSH USER** — The account name used to connect to the IBM AIX server.
- **SSH USER'S PASSWORD** — The password of the SSH User. This configuration is only required if the authentication method is a password authentication.

10. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 18: IBM Lotus — PMMs and Connector

This chapter explains how to configure the PMMs and Connector for IBM Lotus:

- [*“Configuring the PMM for IBM Lotus Domino” on page 146*](#)
- [*“Configuring the PMM for IBM Lotus Notes” on page 150*](#)
- [*“Sample Password Processing Script” on page 168*](#)
- [*“Configuring the Connector for IBM Lotus” on page 171*](#)
- [*“Configuring the WorkerTermMinutes Attribute” on page 176*](#)

Configuring the PMM for IBM Lotus Domino

The Password Management Module (PMM) for IBM Lotus Domino® enables end users who access Lotus Domino with a web browser to automatically reset the HTTP/Internet password.

The PMM for IBM Lotus Domino is installed as a component of the Core Server. The correct access keys are necessary to configure this PMM.

Prerequisites

The Lotus Notes® client software must be installed on the server hosting the Connector Framework Manager. Install the Notes client in “Single user” mode. “Multi-user” installations are not supported.

The ID file that you specify during PMM configuration (on the server hosting the Connector Framework Manager) must also exist on each server hosting a Connector Framework and must have the exact same file path.

Verify that the path to the Lotus Notes client executable files to the PATH System Environment Variable exists.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Using the Replication Feature

The optional Replication feature replicates the end user’s internet password to a specified Mail server, Sametime server, and any other Domino servers you specify after a successful password reset. To use this feature, which you enable through the PMM Configuration Manager dialog box, you first need to create a local replica of the Domino Directory on each server on which the Connector Framework or Connector Framework Manager is installed. To do this, follow these steps:

1. Launch the Lotus Notes client.
2. Open a copy of the Domino Directory. For example, using the Lotus Notes client version 8.5.2, from the menu select File>Open>Lotus Notes Application.
 - a. Select a server (example: Server/Corp).
 - b. Select the Domino Directory (names.nsf) as the database (example: Corporate Address Book).
 - c. Click Open.
3. Create a local replica of the Domino Directory.
 - a. Go to the View menu option in the Lotus Notes client and select Advanced Menus if not already selected.
 - b. From the menu, select File>Replication>New Replica
 - c. Set the server as Local in the dialog box.

- d. There is already a file named names.nsf on the local system. You need to name the local replica of the corporate address book to something different, such as corp_names.nsf. This is used in the PMM configuration.
- e. Uncheck Encrypt the replica using.
- f. Click OK.

PMM Configuration

1. From the Start menu, select:

Programs>Core Server Core Server>Password Management Modules>Lotus Domino

The PMM Configuration Manager for IBM Lotus Domino appears.

Figure 48: PMM Configuration Manager for IBM Lotus Domino

2. This dialog box requires the following information:

DOMINO SERVER NAME — Provide the Domino server name. This is the name of the Lotus Domino server that hosts the copy of Domino Directory that is to be modified. Due to replication issues, this would generally be a 'hub' server rather than a 'spoke' server in a hub & spoke configuration. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

Note: It is recommended that this connector use the same server as the one used for the two Lotus PMMs, to avoid replication conflicts that would arise from changing the same person document from the three possible connectors. The IBM Lotus Connector, PMM for IBM Lotus Notes, and PMM for IBM Lotus Domino

can all potentially manipulate the same person document. If each action is performed on separate servers before replication occurs, the Domino administrator must resolve replication conflicts.

DOMINO DIRECTORY NAME — Provide the Domino directory name.

3. **VIEW NAME TO SEARCH** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the ID file.

If you have not configured a target, the default value of this field is the (\$Users) view. This is a hidden view, not viewable in the Lotus client, that contains multiple username formats. The selected view must have a sorted column where the name format matches the IdentityMap table entry for the username.

For example, if the value of the username field for Cathy Courion's account is Cathy Courion/Engineering/Courion/US, then an example of a valid name formula for the name format of the sorted column would be "@Name([Abbreviate]; FullName)" where FullName would evaluate to "CN=Cathy Courion/OU=Engineering/O=Courion/C=US".

CASE-SENSITIVE SEARCH FOR USERNAME — Enable this check box to require that the supplied username exactly matches the username stored in the Domino directory. The PMM default is for case-insensitive searches.

FULL PATH TO ID FILE — Provide the full path to the Privileged User's ID file.

Note: The Privileged User needs to have at least "AUTHOR" access, with the right to "Write public documents" and the "[UserModifier]" role, in the Domino directory ACL.

PASSWORD — Provide the password associated with the Privileged User's ID file.

4. **ENABLE ENHANCED LOGGING** — This option provides you with detailed information about the Domino database, views, and forms accessed by the PMM, and enables you to track configuration issues. Check this option when you are setting up the PMM for the first time. Core Security recommends that you uncheck this option after all the configuration issues are resolved.
5. **REPLICATION** — The optional Replication feature replicates the end user's internet password to a specified Mail server, Sametime server, and any other Domino servers you specify after a successful password reset. To use this feature, you first need to create a local replica of the Domino Directory on each server on which the Connector Framework or Connector Framework Manager is installed. See ["Using the Replication Feature" on page 146](#) for information about how to do this. To enable Replication, provide the following information

FILE NAME OF THE LOCAL REPLICA — Enter the file name of the local replica that you created in the Lotus Client, in this example, corp_names.nsf. By default, Lotus uses the Notes "data" directory for all local database access. You can also specify a pathname or a path relative to the data directory. Examples:

Assuming the data directory is C:\Program Files\IBM\Lotus\Notes\data, "corp_names.nsf" accesses the file as "C:\Program Files\IBM\Lotus\Notes\data\corp_names.nsf".

If "local\corp_names.nsf" accesses the file as "C:\Program Files\IBM\Lotus\Notes\data\local\corp_names.nsf", the "local" subdirectory must already exist.

"E:\local\corp_names.nsf" accesses the file as specified.

Note: Specifying the local replica database and at least one of the options to replicate to the mail, Sametime, or other servers, enables the Replication feature.

REPLICATE WITH THE USER'S MAIL SERVER — Check this option to replicate the user's internet password with the user's mail server. The connector looks up this information on the user's Person Document during the password reset process.

REPLICATE WITH THE USER'S SAMETIME SERVER — Check this option to replicate the user's internet password with the user's Sametime server. The connector looks up this information on the user's Person Document during the password reset process.

REPLICATE WITH SERVER — If you want to replicate the user's internet password to other servers, enter the server names here. Separate server names with a semi-colon (;). Example:

Server08/Corp;Server14/Corp;Server22/Corp

Note: Although new passwords are replicated to the specified servers immediately, users cannot use the new internet passwords for several minutes as the Domino administration server must process the new passwords. Users can use their old passwords until the new ones are available.

6. Click the **OK** button to save the changes and exit the configuration program.

The PMM for IBM Lotus Domino configuration is complete.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the PMM for IBM Lotus Notes

The Password Management Module (PMM) for IBM Lotus Notes enables end users to reset passwords on a Lotus Notes ID file or by updating the password in ID Vault. The PMM for IBM Lotus Notes performs a password reset by replacing a user's Notes ID file. The PMM supports target configurations against multiple databases, views, and fields. Core Security recommends that you use Lotus Domino Designer to determine the unique configuration of your Lotus Notes environment to help determine how best to configure the PMM for IBM Lotus Notes.

The PMM supports three options to save an ID file: you can download the ID file to a local directory or save the ID file to a network location or update the password in an ID Vault. To use the download option, configure the **DOWNLOAD INFORMATION** dialog box. To configure the PMM to save the ID file to a network location, supply the details in the **NETWORK SERVER INFORMATION** dialog box during the PMM configuration.

Note: Core Security recommends that you download the ID file to a local directory, as well as save the ID file to a network location. In case the download fails but the reset succeeds, the Help Desk can direct you to the network location.

The PMM for IBM Lotus Notes is installed as a component of the Core Server. The correct access keys are necessary to run this PMM.

Prerequisites

The Lotus Notes® client software must be installed on the server hosting the Connector Framework Manager. Install the Notes client in “Single user” mode. “Multi-user” installations are not supported.

If you are using the Domino ID Vault feature, all users for this target must be using the Notes 8.5.x client. See [“Configuring the Domino ID Vault Feature” on page 165](#) for more information.

The path to the Lotus Notes executable files must be added to the PATH System Environment Variable.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

ID File Definition

The Domino administrator creates the ID file to identify a legitimate Domino server or Notes user. The ID file includes:

- The name of the ID owner and possibly one alternate name
- Password
- A permanent Notes license number
- A pair of Notes Certificates from a Certifier ID
- A public and private key

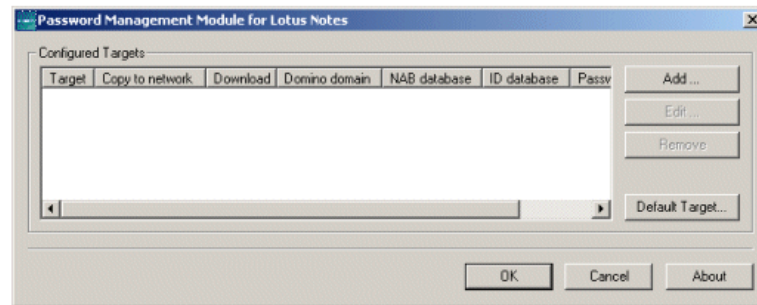
- Ancestral certificates
- An Internet certificate issued by a Certification Authority (CA) to secure SSL connections, and encrypt and sign S/MIME mail messages (optional for Notes client only).
- One or more secret encryption keys

For more information on the ID file definition, please refer to Lotus Notes/Domino documentation.

PMM Configuration

1. From the Start menu, select:
Programs >Core Server Core Server >Password Management Modules >Lotus Notes
The PMM Configuration Manager for IBM Lotus Notes appears.

Figure 49: PMM Configuration Manager for IBM Lotus Notes



2. From this dialog box, you can
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Edit a target created with an earlier version of the PMM Configuration Manager with the **DEFAULT TARGET** button.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the **ADD** or **EDIT** option from the PMM, the **TARGET INFORMATION** dialog box appears.

Figure 50: Target Information

3. **UNIQUE TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **DELIVERY OPTIONS FOR THE UPDATED ID FILE** — Here you can choose to save the updated ID file to a network location, or download the ID file to the local computer.
5. **NETWORK OPTIONS:**
 - **NEVER WRITE TO NETWORK** — Select this option if you do not want to save the updated ID file to a network location. By default, this option is selected.
 - **ALWAYS WRITE TO NETWORK** — Select this option if you want to save the updated ID file to a network location.
6. **DOWNLOAD OPTIONS:**
 - **NEVER DOWNLOAD** — Select this option if you do not want to download the ID file to the local computer. By default, this option is selected.
 - **ALWAYS ATTEMPT TO DOWNLOAD** — Select this option if you want to download the ID file to the local computer.

When you finish configuring this PMM, enable Courion's ActiveX control, CourLocal. The Courion ActiveX control lets an end user update the Lotus Notes ID file stored locally on their client system. This feature places the ID file with the updated password on the end-user system after using the Access Assurance Suite Web Access Option to change the password on the ID file. For details on using CourLocal, refer to the manual *The Access Assurance Suite Implementation Guide*, in the chapter Web Access (ASP Page) Configuration.

Note: XP end users might have their downloads of the ActiveX control blocked. A user can eliminate the blocking problem 1) by setting Internet Explorer's configuration option "Automatic prompting for ActiveX controls" to

“Enable” or 2) configuring Internet Explorer to trust ActiveX Controls and trust the domain that serves the this ActiveX control.

- **DOWNLOAD IF ID FILE EXISTS IN THE CONFIGURED DIRECTORY** — Select this option if you already have an ID file in the configured directory. By default, this option is not selected.

If the downloaded ID filename does not match an ID file that already exists in the configured directory, the download attempt fails. To display a custom error message, enter it in the **MESSAGE TO DISPLAY WHEN ID FILE DOES NOT EXIST** text box. By default, the message text box is empty. However, the ActiveX control displays a default message, “The ID file was not downloaded.”

If you select the **DOWNLOAD IF ID FILE EXISTS IN THE CONFIGURED DIRECTORY** option, the ActiveX control checks if the ID file already exists in the configured directory. If not, the custom error is displayed; otherwise, the ID file that already exists is overwritten.

Note: To use this option, enable ActiveX downloads; see **ALWAYS ATTEMPT TO DOWNLOAD** above.

7. **IGNORE NETWORK WRITE FAILURE AND ATTEMPT TO DOWNLOAD** — When enabled, this option ignores network copy failures and treats them as successes. To enable this option, select **ALWAYS WRITE TO THE NETWORK** for the **DELIVERY OPTIONS FOR THE UPDATED ID FILE** and either the **ALWAYS ATTEMPT TO DOWNLOAD** option or the **DOWNLOAD IF ID FILE EXISTS IN THE CONFIGURED DIRECTORY** from the **DOWNLOAD OPTIONS** section. The **IGNORE NETWORK WRITE FAILURE AND ATTEMPT TO DOWNLOAD** option is unavailable by default.
8. **ID VAULT** — See [“Configuring the Domino ID Vault Feature” on page 165](#) for information about this feature and how to configure it.
9. **CASE INSENSITIVE SEARCHES FOR USERNAME** — Select the checkbox to allow case insensitive search on username.
10. **ENABLE ENHANCED LOGGING** — This option provides you with detailed information about the Notes databases, views, and forms accessed by the PMM, and enables you to track configuration issues. Check this option when you are setting up the PMM for the first time. Core Security recommends that you uncheck this option after all the configuration issues are resolved.
11. Click **NEXT**.

The **TEMPORARY DIRECTORY INFORMATION** dialog box appears as in [Figure 51](#).

The **NEXT** button remains disabled until you select at least one delivery option.

Figure 51: Temporary Directory Information

The screenshot shows a Windows-style dialog box titled "PMM for Lotus Notes: Temporary Directory Information". It has a close button (X) in the top right corner. The dialog is divided into two main sections. The first section, "Temporary directory information", contains a label "Detach ID file to:" followed by a text input field and a browse button (three dots). The second section, "Network user information", contains a checkbox labeled "Use network credentials to access temporary directory". Below this checkbox are two text input fields, one labeled "Name:" and one labeled "Password:". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

You need to have a temporary directory configured to save a temporary copy of the ID file. When you configure the PMM to save the temporary copy of the ID file to the location you selected, the PMM:

- looks for the ID file in a Notes database
- performs the password change
- saves the updated file to a network location and /or downloads it to the user's desktop. The temporary copy of the ID file and the subdirectory that contains the ID file are then deleted.

Note: The PMM creates subdirectories to uniquely identify an ID file for a particular user.

When a password reset occurs, the PMM is running the SYSTEM context. Core Security recommends that you configure the network credentials, which include username and password, to allow temporary logon for the PMM configuration to access network resources.

12. To set up the temporary directory information:

- DETACH ID FILE TO** — Select the path where the PMM can save temporary copies of the ID files. You can create a new directory to hold the temporary copy of the ID file.

Note: Provide the network credentials if you are saving the ID file to a network location. If the directory is local to the machine, then network credentials are not required.

Note: Network credentials include the username and the password.

- USE NETWORK CREDENTIALS TO ACCESS TEMPORARY DIRECTORY** — Select the checkbox if you want the PMM to use the network credentials you enter.
- Enter the network credentials in the **NAME** and **PASSWORD** fields to access the network resources.

13. Click **NEXT**.

The **DOMINO PRIVILEGED USER INFORMATION** dialog box appears.

Figure 52: Domino Privileged User Information

14. **FULL PATH TO ID FILE** — Enter the ID file path, and the password associated with it in the **PASSWORD** field to access the databases.

Note: The Privileged User must have at least "READER" access to the database(s) ACL where the ID file and password are stored (see [Figure 57](#) through [Figure 59](#)). For each database encryption key used for field or document level encryption, the required encryption key(s) must be imported into the privileged user's ID file.

Note: If the PMM is configured to clear the password digest (see [Figure 56](#)) the Privileged User must have at least "AUTHOR" access, with the right to "Write public documents" and the "[UserModifier]" role, in the Domino directory ACL.

15. **ALLOW PASSWORD RESET OF PRIVILEGED USER ID** — Select the checkbox to allow the owner of the ID file to reset his / her password. If this checkbox is not selected, attempts to reset the password for the user fail. Also, this option prevents the accidental disabling of the PMM.

16. In **NETWORK USER INFORMATION**:

Select the **USE NETWORK CREDENTIALS TO ACCESS NOTES ID FILE** checkbox to allow the use of network credentials to access the Notes ID File.

Note: Network credentials include the username and the password.

Enter the network credentials in the **NAME** and **PASSWORD** fields.

17. Click **NEXT**. The **LOGON USERNAME IDENTIFICATION** dialog box appears, as in [Figure 53](#).

Figure 53: Logon Username Identification

18. **DETERMINE WINDOWS LOGON USERNAME FROM** — Determine where the PMM obtains the Microsoft Windows logon username. This information is used for saving an ID file to the network and the ID file download. The PMM can determine the Windows username from:

IDENTITYMAP ENTRY — Obtain the Windows username from the IdentityMap.

ID FILENAME — Obtain the username from the ID file on the end-user system.

SCRIPT COMMAND LINE — Use a script to obtain the username. Enter the name of the script in the box below this option. The following formats are examples only. Use any one of the formats for this option.

```
cscript.exe /nologo /b sample.vbs
c:\winnt\system32\cscript.exe /nologo /b sample.vbs
cscript.exe /nologo /b "c:\Program Files (x86)\Courion Corporation\CourionService\sample.vbs"
c:\winnt\system32\cscript.exe /nologo /b
"c:\Progra~1\Courio~1\CourionService\sample.vbs"
```

When you use the **SCRIPT COMMAND LINE**, an XML fragment gets generated based on the target and user information of the reset. The XML fragment is passed to a script, which then takes action on a particular target / user combination based on the XML input.

The input XML takes the form:

```
<message>
<resetpasswordex>
<attributes></attributes>
<usertoreset>someuser</usertoreset>
<pwdtarget>sometarget</pwdtarget>
</resetpasswordex>
```

```
</message>
```

If you specify additional XML attributes in the **ADDITIONAL XML ATTRIBUTES** section, the attributes also get passed to the script in the <attributes> tag. For example, if the script needs to access another machine with a set of administrator credentials, you could enter the following additional XML attributes in this section:

```
<adminuser>bob</adminuser><adminpassword>thepassword</ad
minpassword><host>myhost</host><port>121</port>
```

The format of XML with the additional XML attributes:

```
<message>
<resetpasswordex>
<attributes>
    <adminuser>bob</adminuser>
    <adminpassword>thepassword</adminpassword>
    <host>myhost</host>
    <port>121</port>
</attributes>
<usertoreset>CCourion</usertoreset>
<pwdtarget>MyNotesTarget</pwdtarget>
</resetpasswordex>
</message>
```

To find out whether or not the script executed successfully, the script returns two XML tags: <status></status> and <statusmsg></statusmsg>.

A value of 0 (zero) in the <status> field indicates success. Any other value, for example, 10, indicates a failure. On success, the contents of <statusmsg> contains the desired information, or an error message if the status indicates a failure.

DATABASE ENTRY — This option queries the database field for the Windows username. You need to supply the following:

- **SERVER NAME (BLANK FOR LOCAL DATABASE)** — Enter the name of the server where the database resides in the field.
- **DATABASE FILENAME** — Enter the name of the database that holds the Windows username in the field.
- **VIEW NAME OR ALIAS** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the Windows username.
- **FIELD CONTAINING WINDOWS LOGON USERNAME** — Enter the name of the field that contains the username.

19. Click **NEXT**. The **NETWORK SERVER INFORMATION** dialog box appears, [Figure 54](#).

Note: This dialog box only appears if you selected the option to save the updated ID file to a network location in [Figure 50](#).

Figure 54: Network Server Information

20. Select the **USE NETWORK CREDENTIALS TO ACCESS NETWORK SERVER(S)** checkbox to allow the network credentials at runtime to access the network location where the ID files are saved.
21. Enter the network credentials in the **NAME** and **PASSWORD** fields to access the network location.
22. **SERVER PATH CONSTRUCTION** — You can provide a single server or multiple server configuration.

- **Single Server Configuration**

Under **SERVER BASE**, enter the **SINGLE SERVER ROOT** details.

To combine the username after server base, select the **INSERT USERNAME AFTER SERVER BASE** checkbox.

Enter **ADDITIONAL PATH INFORMATION**

Select **APPEND USERNAME AT END OF PATH** to include the username at the end of path name.

For example, if you entered the following details for a single server configuration:

'Single server root' = \\singleserver\profiles

'Insert username after server base' = checked and username is CCourion

'Additional path information' = Notes\data

The ID file would be saved to:

\\singleserver\profiles\CCourion\Notes\data\id_filename.id

- **Multiple Server Configuration**

If you want to save the ID files to multiple network locations based on the username, you must write a script to determine the correct server and return that information to the PMM.

SCRIPT COMMAND LINE — Enter the name of a script. The formats given below are examples only. Use any one of the formats for this option.

```
cscript.exe /nologo /b sample.vbs
c:\winnt\system32\cscript.exe /nologo /b sample.vbs
cscript.exe /nologo /b "c:\Program Files (x86)\Courion
Corporation\CourionService\sample.vbs"
c:\winnt\system32\cscript.exe /nologo /b
"c:\Progra~1\Courio~1\CourionService\sample.vbs"
```

When you use the **SCRIPT COMMAND LINE**, an XML fragment gets generated based on the target and user information of the reset. The XML fragment is passed to a script, which then takes action on a particular target / user combination based on the XML input.

The input XML takes the form:

```
<message>
<resetpasswordex>
<attributes></attributes>
<usertoreset>someuser</usertoreset>
<pwdtarget>sometarget</pwdtarget>
</resetpasswordex>
</message>
```

If you specify additional XML attributes in the **ADDITIONAL XML ATTRIBUTES** section, the attributes also get passed to the script in the <attributes> tag. For example, if the script needs to access another machine with a set of administrator credentials, you could enter the following additional XML attributes in this section:

```
<adminuser>bob</adminuser><adminpassword>thepassword</ad
minpassword><host>myhost</host><port>121</port>
```

The format of XML with the additional XML attributes:

```
<message>
<resetpasswordex>
<attributes>
    <adminuser>bob</adminuser>
    <adminpassword>thepassword</adminpassword>
    <host>myhost</host>
    <port>121</port>
</attributes>
<usertoreset>CCourion</usertoreset>
<pwdtarget>MyNotesTarget</pwdtarget>
</resetpasswordex>
</message>
```

To find out whether or not the script executed successfully, the script returns two XML tags: <status></status> and <statusmsg></statusmsg>.

A value of 0 (zero) in the <status> field indicates success. Any other value, for example, 10, indicates a failure. On success, the contents of <statusmsg> contains the desired information, or an error message if the status indicates a failure.

To combine the username after server base, select the **INSERT USERNAME AFTER SERVER BASE** checkbox. For more information, see [“Single Server Configuration” on page 158](#)

23. Enter **ADDITIONAL PATH INFORMATION**. For more information, see [“Single Server Configuration”](#) above.

Select **APPEND USERNAME AT END OF PATH** to include the username at the end of path name. For more information, see [“Single Server Configuration”](#) above.

24. Click **NEXT**.

The **DOWNLOAD PATH LOCATION** dialog box appears.

Figure 55: Download Path Location

Note: This screen appears enabled if you selected the option to download the updated ID file to the local computer in [Figure 50](#).

25. **DETERMINE BASE DIRECTORY FOR DOWNLOAD FROM** offers the following options:
- **LOGGED ON USER'S PROFILE DIRECTORY** informs the ActiveX control to find the Profiles directory and save the path/file in that location.
 - **PATH SPECIFIED IN NOTES.INI** informs the ActiveX control to locate a local copy of the NOTES.INI file and query the KeyFilename and Directory entries to determine the location where the ID file is saved.
 - **PATH (MUST BE FULLY QUALIFIED)** is for cases where there is a common drive mapping on all end-user machines. For example, H:\settings.
 - **SCRIPT COMMAND LINE** calls a script to be run for any other standard configuration. For this option, please see [“Multiple Server Configuration” on page 158](#).
26. **INSERT USERNAME AFTER SERVER BASE** — Select the checkbox to combine the username after server base.
27. **ADDITIONAL PATH INFORMATION** — For more information, see [“Single Server Configuration” on page 158](#).
28. **APPEND USERNAME AT END OF PATH** — Select the checkbox to include the username at the end of path name.

29. Click **NEXT**.

The **PASSWORD DIGEST INFORMATION** dialog box appears.

Figure 56: Password Digest Information

30. **PASSWORD DIGEST OPTIONS**

If the Domino server is enabled for password checking, then the server maintains a password history list in a password digest for each user. When password checking is on, the administrator may also specify which databases and/or users to apply password checking to.

When a Notes user opens the Lotus Notes client, he/she is prompted to select an ID file and supply the password for that file. When the user attempts to open a database on a Domino server for which password checking is turned on, the password used to unlock the ID file is compared to the most recent password in the digest. If the password used to unlock the ID file does not match the latest password in the password digest, the user is denied access to the database.

- a. You can choose to either clear or retain the password digest on the Domino server or the mail server.

DO NOT CLEAR — If you do not want the password digest to be cleared on the Domino server, select the option.

The PMM for IBM Lotus Notes only queries the database if one of the two options to clear the digest mentioned below is checked.

CLEAR ON SERVER SPECIFIED BELOW — If you want to clear the password digest on the Domino server, select this.

CLEAR ON USER'S HOME SERVER (MAILSERVER FIELD) — If you want to clear the password digest specified in the MailServer setting of the Person document, select this.

- b. **SERVER NAME (BLANK FOR LOCAL DATABASES)** — Enter the server name where replication happens in a timely manner. This server is usually a hub server.

- c. **DATABASE FILENAME** — Enter the name of the database
 - d. **VIEW NAME OR ALIAS** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the name of the mailserver (when the password digest is set to be cleared on the user's home mailserver).
31. Click **NEXT**.

The **ID DATABASE INFORMATION** dialog box appears.

Figure 57: ID Database Information

The screenshot shows a dialog box titled "PMM for Lotus Notes: ID Database Information". Inside the dialog, there is a section titled "ID database information" which contains four text input fields: "Server name (blank for local database):", "Database filename:", "View name or alias:", and "Field containing attached ID file:". Below these fields is a checkbox labeled "Ignore attachments that do not end with *.ID". At the bottom of the dialog box, there are three buttons: "< Back", "Next >", and "Cancel".

- 32. **SERVER NAME (BLANK FOR LOCAL DATABASE)** — Enter the name of the server where the database resides.
 - 33. **DATABASE FILENAME** — Enter the name of the database that holds the archived ID files.
 - 34. **VIEW NAME OR ALIAS** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the ID file.
 - 35. **FIELD CONTAINING ATTACHED ID FILE** — Enter the name of the field where the ID file attachment is stored. This field is optional. If you do not specify a name in this field, all attachments on the form are processed.
 - 36. **IGNORE ATTACHMENTS THAT DO NOT END WITH *.ID** - This option enables the administrator to only process attachments with the extension of .ID.
37. Click **NEXT**.

The **ID FILENAME INFORMATION** dialog box appears.

Figure 58: ID Filename Information

38. **DETERMINE ID FILENAME FROM** information. Select one of the options as follows.

- **ATTACHMENT NAME** — Select to use the name of the attachment.
- **KEYFILENAME IN NOTES.INI** — Select to inform the ActiveX control to locate the local copy of the NOTES.INI file, and query the KeyFilename entry to determine the ID filename.

Note: This option is disabled if **DOWNLOAD IF ID FILE EXISTS IN THE CONFIGURED DIRECTORY** is enabled in [Figure 50](#).

If you previously configured a target with the **KEYFILENAME IN NOTES.INI** option enabled, and if you also enabled the option **DOWNLOAD IF ID FILE EXISTS IN THE CONFIGURED DIRECTORY**, then all options on this screen are cleared and the **NEXT** button is disabled. To enable the **NEXT** button, you must select an option on this screen.

- **SCRIPT COMMAND LINE**, please see [“Multiple Server Configuration” on page 158](#).
- **DATABASE ENTRY** option queries the database field for the ID filename.
 - **SERVER NAME (BLANK FOR LOCAL DATABASE)** — Enter the name of the server where the database resides in the field.
 - **DATABASE FILENAME** — Enter the name of the database that holds the ID files in the field.
 - **VIEW NAME OR ALIAS** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the ID filename.
 - **FIELD CONTAINING ID FILENAME** — Enter the name of the field that contains the filename.

39. Click **NEXT**.

The **PASSWORD DATABASE INFORMATION** dialog box appears.

Figure 59: Password Database Information

40. **SERVER NAME (BLANK FOR LOCAL DATABASE)** — Enter the name of the server where the database that holds the archived passwords resides.
41. **DATABASE FILENAME** — Enter the name of the database that holds the archived passwords.
42. **VIEW NAME OR ALIAS** — Enter the view name or alias of that view where the user is uniquely identified, and the form it opens contains the password to unlock the ID file.
43. **FIELD CONTAINING PASSWORD** — Enter the name of the field that contains the password
44. Click **FINISH** to complete the PMM configuration.

You have configured a PMM target for IBM Lotus Notes.

Downloading the Modified ID File to the Client Machine

Core Server's ActiveX control, CourLocal, is available with this PMM. This ActiveX control downloads the modified Lotus Notes ID file to the local machine. This feature can replace the ID file that has the forgotten or expired password with the ID file that has the user-selected password. For details on using CourLocal, refer to *The Core Server Core Server Implementation Guide*, chapter *Web Access (ASP Page) Configuration*.

Note: Mozilla Firefox and Google Chrome may not support some Microsoft technologies such as ActiveX. If you require local password cache synchronization, Core Security recommends using one of the supported versions of Internet Explorer.

Configuring the Domino ID Vault Feature

The PMM for Lotus Notes supports the Domino ID Vault configuration for a password reset. This feature resets the password on a vaulted ID file. Lotus Domino mechanisms deploy the updated ID file after the reset. To support the native mechanisms, an ID Vault configuration disables the "Network" and "Download" options.

All users for this target must be using the Notes 8.5.x client.

On the "ID Vault" tab of the Lotus Notes Security Settings document:

- **ENFORCE PASSWORD CHANGE AFTER PASSWORD HAS BEEN RESET** — If you set up a self-service password reset application, you may want to set this field to **No** so users who reset their own passwords do not immediately have to change passwords again.
- Set **ALLOW AUTOMATIC ID DOWNLOADS** to Yes.

Other Domino ID Vault considerations: For non-vaulted users, the configuration remains unchanged. For vaulted users:

- The PMM for IBM Lotus Domino is not affected by an implementation of the ID Vault in a Domino environment.
- When performing a Connector for IBM Lotus Create or Change action with a certifier that enforces or inherits an ID Vault policy, the workflow does not require the Trigger option to be configured to populate a Notes database with the created or updated ID file. Domino automatically updates the vault for any relevant additions or updates.

To configure this feature with the PMM configuration manager:

1. Select **PASSWORD RESET USING ID VAULT** on the Target Information dialog box of the PMM configuration manager (see [Figure 50](#) on page 152). **CLICK NEXT**.
2. Click **NEXT** on the Domino Privileged User information dialog box (no changes necessary). The ID Vault Information dialog box appears:

Figure 60: ID Vault Privileged Information

PMM for Lotus Notes: ID Vault Information

ID Vault server information

Server name:

Database filename:

Replication

File name of the local ID Vault replica

Replicate with ID Vault server

< Back Next > Cancel

3. Enter the following ID Vault information:

- **SERVER NAME** — Enter the name of the server that contains a copy of the ID Vault.
- **DATABASE FILENAME** — Enter a database filename for the ID vault. Example: IBM_ID_VAULTCVault.nsf

(This information is used during configuration to verify the configured privileged user has access to the ID Vault.)

File name of the local ID Vault replica and Replicate with ID Vault server - Optional: Specify the file name of the local ID Vault replica and one or more servers to replicate with after an ID Vault reset.

Click **NEXT**.

The Password Digest Information dialog box appears. Click **FINISH**.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- If the archived database entry for a given user contains more than one copy of the ID file, and the date/time stamps of the ID files are identical, then preference is given to the ID file that was found first.
- To continue to the next screen during configuration, you need to provide details for the required fields on all screens.

Sample Password Processing Script

The following script takes a full name of the form *Firstname Lastname* and returns the first initial, last name followed by ".id."

```
' Sample script that takes a full name of the form
'   Firstname Lastname
' and returns the first initial, last name + ".id"
' Here's how to use this script with the PMM for Lotus Notes
'   1. put this script in your CourionService directory
'   2. Run the PMM config program.
'   3. Use one of the following formats for a script command line
'       cscript.exe /nologo /b sample.vbs
'       c:\winnt\system32\cscript.exe /nologo /b sample.vbs
'       cscript.exe /nologo /b "c:\Program Files (x86)\Courion
Corporation\CourionService\sample.vbs"
'       c:\winnt\system32\cscript.exe /nologo /b
"c:\Progra~1\Courio~1\CourionService\sample.vbs"
'
' Here's a sample of the incoming XML
' <message>
'   <resetpasswordex>
'     <attributes>
'       <adminuser>bob</adminuser>
'       <adminpassword>thepassword</adminpassword>
'       <host>myhost</host>
'       <port>121</port>
'     </attributes>
'     <usertoreset>ccourion</usertoreset>
'     <pwdtarget>MyNotesTarget</pwdtarget>
'   </resetpasswordex>
' </message>
'
' The outgoing XML has the form
' <status>0</status>
' <statusmsg>some information</statusmsg>
'
' <status> = 0 indicates success (no errors). Any other status is
interpreted as non-success.
' <statusmsg> on non-success is returned as the error string
'           on success is used by the PMM to perform the required function
'
```



```

Option Explicit
'*****

'* Read XML request from stdin
'*****

Function GetInputData()
Dim Input
Dim stdin
set stdin = WScript.StdIn
Input = ""
Do While Not StdIn.AtEndOfStream
    Input = Input & StdIn.ReadAll
Loop
GetInputData = Input
End Function
'*****

'* Main part of the PMM
'*****

Dim stdout
Dim Input
Dim xmlDomdoc
Dim strAccount
Dim ElementList
Dim ElementList2
Dim attributesNode
Dim item
Dim returnMsg
Dim ShortName
On error resume next
Input = GetInputData()
set stdout = WScript.Stdout
'*****

'* Parse the XML doc and get the acct
'* and password for reset.
'*****

Set xmlDomdoc = CreateObject("Microsoft.XMLDOM")
xmlDomdoc.async = False
xmlDomdoc.validateOnParse = False
xmlDomdoc.preserveWhiteSpace = False
xmlDomdoc.resolveExternals = False
xmlDomdoc.LoadXml(Input)
'xmlDomdoc.Save("MyTEST.xml") ' DEBUGGING

```

```

'*****
'* get the account name from the request
'*****

Set ElementList = xmlDomDoc.getElementsByTagName("usertoreset")
strAccount = ElementList.item(0).text
ShortName = Left(strAccount, 1) & Mid(strAccount, Instr(strAccount, " ")+ 1)
'*****

'* get the custom attributes
'*****

Set ElementList = xmlDomDoc.getElementsByTagName("Attributes")
Set attributesNode = ElementList.item(0)
set ElementList2 = attributesNode.childNodes
For Each Item In ElementList2
returnMsg = returnMsg & Item.nodeName & "=" & Item.text & " "
Next
'*****

'* Write XML response to stdout
'*****

Stdout.Write "<status>0</status>"
Stdout.Write "<statusmsg>"
Stdout.Write ShortName & ".id"
stdout.write "</statusmsg>"
'*****

' DONE!
'*****

```

Configuring the Connector for IBM Lotus

The Connector for IBM Lotus supports the following actions on a target: Add, Change, Create, Delete, Disable, Verify, View, Trigger, Authentication, and Query. The trigger allows the ID file and password for an account to be stored in Lotus Notes, which makes them available to the PMM for Lotus Notes.

Prerequisites

The Lotus Notes® client software must be installed on the server hosting the Connector Framework Manager. Install the Notes client in “Single user” mode. “Multi-user” installations are not supported.

The Certifier ID file that you specify during connector configuration (on the server hosting the Connector Framework Manager) must also exist on each server hosting a Connector Framework and must have the exact same file path.

The Lotus Notes client software must be run once prior to installing the Core Server (this sets up the connection information with the Domino environment).

The SYSTEM PATH environment variable must include the Notes executable path (for 7.0 this is \Program Files\Lotus\Notes). If the Notes client is installed prior to installing the Suite, this environment variable is set automatically. If the Suite is installed first, the system path must be modified as a manual step and requires a reboot for the CourierService to pick up this environment change.

For a client machine to perform Lotus Notes resets through web access, the Microsoft Internet Explorer security setting must allow signed ActiveX® controls to run.

Connector Configuration

Follow these steps to add an IBM Lotus target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **IBM-LOTUS-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 61: Add IBM Lotus Target

The screenshot shows a Windows-style dialog box titled "Add Connector Target". It features a "Target Name:" label and a text input field containing "IBM-Lotus-Cnctr". Below the text field is a section titled "Operations Supported" which contains a list of four items, each with a checkbox: "Action" (checked), "Authentication", "Query", and "Trigger". At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager.

Select **ACTION** to enable these Core Server actions: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

Select **AUTHENTICATION** to enable end users to authenticate against the target data source.

Select **QUERY** to retrieve data from the target data source.

Select **TRIGGER** to trigger a script during a workflow.

5. Click **NEXT**.

The configuration screen for IBM Lotus appears.

Figure 62: Connector Configuration Manager for IBM Lotus

6. This dialog box requires the following information:

DOMINO SERVER — Provide the Domino server name. This is the name of the Lotus Domino server that hosts the copy of Domino Directory that is to be modified. Due to replication issues, this would generally be a 'hub' server rather than a 'spoke' server in a hub & spoke configuration.

Note: It is recommended that this connector use the same server as the one used for the two Lotus PMMs, to avoid replication conflicts that would arise from changing the same person document from the three possible connectors. The IBM Lotus Connector, PMM for Lotus Notes, and PMM for Lotus Domino can all potentially manipulate the same person document. If each action is performed on separate servers before replication occurs, the Domino administrator must resolve replication conflicts.

PRIVILEGED USER ID PATH — Provide the full path to the Privileged User's ID file. This file needs to be located on the server in which the Connector Framework is installed.

A privileged user needs one of the two following minimum access levels to the Domino server:

Author with

- a. [UserCreator] role
- b. [UserModifier] role
- c. [GroupModifer] role

- d. Create documents access
- e. Delete documents access

Editor with

- a. [UserModifier] role
- b. Delete documents access

PASSWORD — Provide the password associated with the Privileged User's ID file.

CERTIFIER ID PATH — Provide the full path to the Certifier's ID file. This file needs to be located on the server in which the Connector Framework is installed.

Note: Some actions (such as Create, Delete, and some aspects of Change) create requests by the privileged user that are submitted to the "administration process". These requests require the person submitting the request to not only have their own ID file and password, but also have the Certifier ID file and password.

CERTIFIER ID PASSWORD — Provide the password associated with the Certifier's ID file.

UNIQUE USER IDENTIFIER DIRECTORY FIELD — Provide the field to be used as the unique user identifier. FullName is generated by Domino during user registration (in the Create/Add actions). The canonical FullName is the preferred unique identifier since it is guaranteed to be unique in the directory.

Note: Both the FullName and ShortName are generated when the account is created, therefore when doing a create/add action if FullName or ShortName is used as the Unique Attribute, that value must be set explicitly during the create action.

LOG LEVEL (0-5) — Select the level of logging for the connector. The default is 0. Options are:

- 0 Standard logging (all error messages and Action Success messages)
- 1 Lotus API calls
- 2 Lotus session and logon/logoff information
- 3 Call stack logging
- 5 Process and thread logging

ENABLE GROUP NESTING — Enable this option to expose attributes that allow groups to be nested. When you attempt to add a user to a group that is full and the Enable group nesting option is enabled, the connector looks for an existing nested group with room and adds the user to that group. If no existing nested group with room exists, the connectors creates a new nested group where it can add the user.

The connector only recognizes nested group names with the specific format "<Group Name> ##". For example: with "All Web Users" as the target group name, nested group names appear as "All Web Users 01" through "All Web Users 99"

RETRY INTERVAL — Specify the wait period before the connector retries an action. You can specify between 0 and 999 seconds. The default is 3 seconds.

7. Click **FINISH**.

Notes and Warnings

When moving users between certifiers, name changes in the Domino Directory do not appear until the administration process (adminp) executes Interval requests. Changes to the Domino Directory on additional servers happen according to the replication schedule.

Configuring the WorkerTermMinutes Attribute

This section explains how to create the WorkerTermMinutes attribute for the PMM for IBM Lotus Domino, the PMM for IBM Lotus Notes, and the Connector for IBM Lotus that enables a worker process to be terminated if it becomes unresponsive. Create this attribute through the Microsoft CIM Studio settings. Once you create the attribute, modify the encrypted attribute values in the Configuration Editor (CfgEdit2.exe).

If this attribute does not exist, or the value is set to zero, worker processes may continue until they complete all operations. When the attribute exists with a timeout value, it initiates a timeout thread to wait a maximum number of minutes for an individual worker process. When the timeout is reached, the specific worker process associated with the timer is terminated and the action reports a failure.

Download the Microsoft CIM Studio from the Microsoft website.

Attribute values:

- 0 = no timeout
- 1 – 9999 indicates the number of minutes to wait for a worker process that may be unresponsive.

To add the value to a Lotus Connector target, launch Microsoft CIM Studio:

1. Open root\Courion\CourCntrFrameworkMgr.
2. In the left pane, select CourTarget.
3. In the right pane, click the fourth icon from the right Instances.
4. Scroll to the right to find the Connector and Name columns.
5. Double-click the row with the IBM-Lotus-Cntr target instance with the name you want to set the timeout value for.

Note: For PMMs, do not select the connector instance without a value in the Name column. For example, find an instance where the Connector column contains *Lotus Domino* and the Name column contains the target name.

Modify the arrays as suggested. To modify an array, click the Array button in the Value column. On the empty line at the bottom of the list, add the value as described:

- AttrDescriptionArray – Default Description
- AttributeNameArray – WorkerTermMinutes
- AttrMetaInfoArray

All connector values are encrypted. For the Connector for IBM Lotus target, this must be Yes.

PMM values may be encrypted or clear text. This value is not encrypted. For the PMM for IBM Lotus Domino and the PMM for IBM Lotus Notes targets, this value must be NO.

- AttrvalueArray

For the Connector for IBM Lotus target, enter zero for now. Because the value is encrypted, use CfgEdit2 to set the encrypted value.

For the PMM for IBM Lotus Domino and the PMM for IBM Lotus Notes targets, you can set the value directly in Microsoft CIM Studio and omit the steps below for CfgEdit2.exe.

It is important that each of these arrays has the same number of items or the connector does not load. Also, do not add empty rows by pressing <Enter>. There is always one empty row at the end of each array, and there should only be one.

After you add all the array entries, click the Save icon (fifth from the right) to save the information.

Next, launch CfgEdit2.exe from the Start Menu:

1. Go to **ALL PROGRAMS > CORE SECURITY ACCESS ASSURANCE SUITE > CONFIGURATION EDITOR**.
2. Navigate to **WMI – COURCNCTRFRAMEWORKMGR – COURTARGET - <name of the target you edited> - ATTRVALUEARRAY**.
3. Double click the last item in the list.
You can verify this is the correct item by checking that the same number item in the AttributeNameArray has the WorkerTermMintues value.
4. Enter the timeout value (1 - 9999).
5. Click **ENCRYPT DATA FOR CONNECTORS**.
6. Click **OK**.

Restart services for the connector or PMM to incorporate this change.

Chapter 19: IBM z/OS Systems with CA-ACF2 — PMM and Connector

This chapter explains how to configure the PMM and Connector for IBM z/OS Systems (formerly known as OS/390) with CA-CAF2:

- [*“Configuring the PMM for z/OS Systems with CA-ACF2” on page 180*](#)
- [*“Configuring the Connector for z/OS Systems with CA-ACF2” on page 185*](#)

Configuring the PMM for z/OS Systems with CA-ACF2

The Password Management Module (PMM) for CA-ACF2® enables an Core Server application to reset passwords automatically on z/OS® systems using CA-ACF2. The correct access keys are required to configure and use this PMM.

The PMM for CA-ACF2 uses a simple algorithm for resetting passwords:

1. Verify that the username to reset exists on the system.
2. Obtain the account with "READ" access to the \$COURIER facility to make the connection to the Mainframe Reset agent which carries out the reset request.
3. Verify that the specially configured account for the system where the username to reset exists.
4. If the account is configured, then attempt the reset.

The PMM for CA-ACF2 includes the following components:

- PMM for CA-ACF2 library (.dll) Mainframe.dll
- PwReset.dll
- Configuration Application MainframeConfig.exe
- The Courion Mainframe Reset Agent os390agent.exe

Prerequisites

You need to install the PMM agent for Cour390 on the z/OS systems where the resets occur. The Cour390 agent is explained in [“Using the Cour390 Agent” on page 631](#).

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

z/OS Mainframe Requirements

1. z/OS Systems Programmer.
 - Ability to upload the mainframe SAMPLIB and LOADLIB into data sets defined on the host.
 - Ability to APF authorize the LOADLIB with either the z/OS Console Commands and entries in the PROGxx member or the IEAAPFxx member.
2. VTAM Systems Programmer.
 - Ability to Add VTAM Definitions and Activate them with z/OS Console Commands.
3. Security System Systems Programmer/Administrator.
 - Ability to enter Security definitions for the applicable Host Security System.

z/OS System Requirements

The PMM agent for CA-ACF2 must be installed for password resets on the z/OS system. The os390agent.exe file is located in the OS390 folder within the Core Server Core Server installation folder.

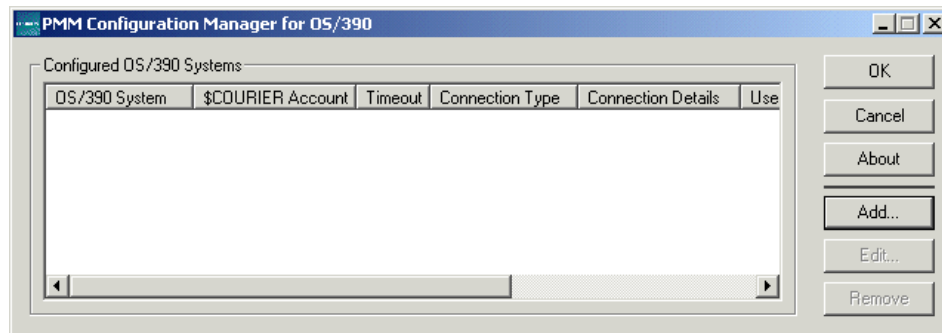
Before running this PMM, be sure to have the following information:

- Determine if the connection to the z/OS system is via TCP/IP or an SNA Server. The TCP/IP port for the agent on the z/OS system is needed for a TCP/IP connection. For a SNA connection, the LU Name and ModeName for the Agent on the z/OS system are required. The SNA client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- Select the username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the PMM for CA-ACF2 and the Cour390 Agent.

PMM Configuration

1. From the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>CA-ACF2
The PMM Configuration Manager for z/OS appears.

Figure 63: PMM Configuration Manager for z/OS (OS/390)



2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.

A Global parameter, ACF2_ENABLE=(SUS,CAN,EXP), added to the SAMPLIB. It is a Cour390 agent global parameter that causes the CANCEL and SUSPEND flags to be reset to the active state and the EXPIRE date to be set to zero. This is functionally equivalent to ACF2_ENABLE=ALL. See [“Configuring the Cour390 Agent” on page 635](#) for details on the ACF2_ENABLE parameter.

 - View the targets already configured in the **CONFIGURED TARGETS** list.

- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box displays.

Figure 64: Add/Edit Target Configuration with TCP/IP selected

3. CONFIGURE OS/390 SYSTEM

- OS/390 SYSTEM** — Enter the target (either an IP address or a resolvable DNS) of the z/OS system in which the password resets are to be performed. Select the appropriate connection method (SNA or TCP/IP). The target should be an IP address, not a host name. The IP address must equal the IP address of the target z/OS system. The port specified must match that specified in the TCPIPPORT parameter of the GLOBAL member.

You need to use this same address for the **PMM TARGET** name when you configure the target in the PMM Gateway Connector configuration. Both fields should use the IP address or both should use the DNS.

Note: The TCP/IP address or DSN must be the same as that specified in the IPADDR field of the SAMPLIB member containing the TCP Configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

- \$COURIER** — Enter an account name for the \$COURIER facility to use in connecting the PMM for CA-Top Secret with the Cour390 agent.
 - ACCOUNT PASSWORD** — Enter a password for the specially configured account created in the **\$COURIER ACCOUNT** field.
- Note:** This account name and password must match that of the Logon Definition for the z/OS. See [“Using the Cour390 Agent” on page 631](#).
- TIMEOUT (SECS)** — Enter the amount of time (in seconds) before password reset timeout. The default value for this field is 10 seconds.
 - SECURITY PHRASE** — Enter the security phrase that initializes Triple DES Encryption. This phrase must match the phrase (called the 3DES_SEED GLOBAL parameter) configured on the z/OS agent.

- f. **USE STRONG PASSWORD RULES** — Select this option to enforce strong password rules.
- g. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — Select this option to allow password resets for administrator accounts with Core Server.
If you do not select this option, the Core Server does not reset accounts with these privileges: Security Officer, Account, Auditor, Consultant, or Project Leader.

Depending on your connection type, continue to [“Configuring TCP/IP Parameters”](#) or [“Configuring SNA Parameters”](#)

Configuring TCP/IP Parameters

- a. **CONNECTION** — Choose the **TCP/IP** Connector option.
- b. **TCP/IP PORT** — Enter the TCP/IP port that the agent is listening to on the z/OS System.

Note: The port address must be the same as that specified in the IPPORT field of the SAMPLIB member containing the TCP configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

Configuring SNA Parameters

Figure 65: Add/Edit Target Configuration with SNA selected

- a. **LU NAME** — Enter the SNA LU Name for the z/OS system agent.
 - b. **MODE NAME** — Enter the mode name for the z/OS system agent.
Note: The SNA LU Name and Mode Name must be the same as that specified in the LU_NAME and MODENAME fields of the SAMPLIB member containing the SNA configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is SNANODE.
4. You have configured the PMM. Click the **OK** button to save the configuration

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- The controls provided by the ACF2_ENABLE option apply to all disabled users that Cour390 enables. There is no option to selectively apply these options to any subset of users.
- Core Server only enables disabled end users when the z/OS target is configured with the **RESUME REVOKED/SUSPENDED ACCOUNTS** property set.
- As with all GLOBAL parameters, Cour390 reads and processes ACF2_ENABLE and RRSF_PASSWORD_SUPPORT only at Cour390 initialization or in response to the GLOBALREFRESH Modify command.
- Punctuation is not supported for password resets. De-select the **ALLOW PUNCTUATION** check box on the Password Strength Composition screen. (Additionally, password reset via the PMM for Synchronization does not take place on the CA-ACF2 system unless the **ALLOW PUNCTUATION** check box is deselected.)

Configuring the Connector for z/OS Systems with CA-ACF2

The Connector for z/OS Systems with CA-ACF2 supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

An Core Server application manages accounts on z/OS systems with CA-ACF2 through the Cour390 agent, which must be installed on the target z/OS system. For information on the agent, see [“Using the Cour390 Agent” on page 631](#).

Prerequisites

Configuring a target requires the following information:

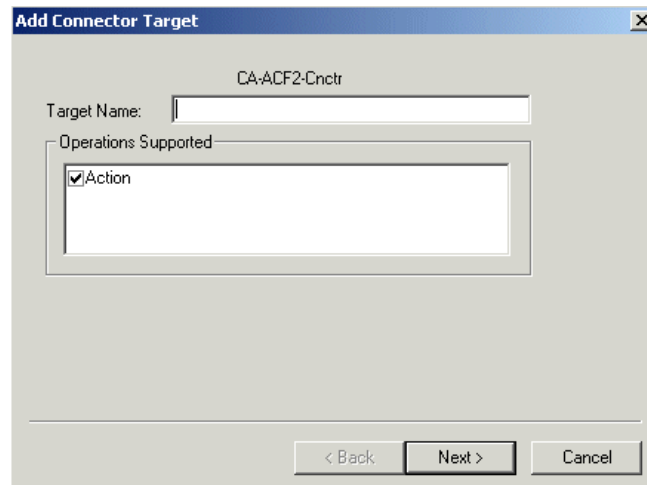
- Knowledge of whether the connection to the z/OS system is via TCP/IP or an SNA Server. TCP/IP connections require the TCP/IP port for the agent on the z/OS system. SNA connections require the LU Name and ModeName for the agent on the z/OS system. The SNA client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- Knowledge of the username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the Connector for CA-ACF2 and the Cour390 agent.

Connector Configuration

Follow these steps to add an z/OS system with CA-ACF2 target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **CA-ACF2-CNCTR**
3. Click the right mouse button on the name of the connector and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 66: Add CA-ACF2 Target


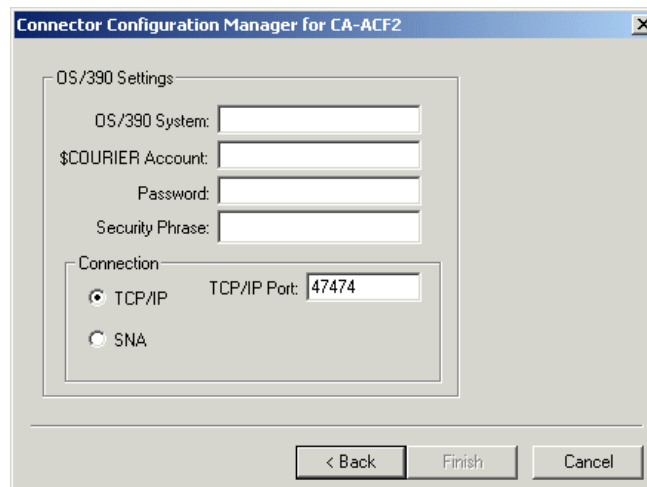
The dialog box is titled "Add Connector Target". It contains a "Target Name:" label followed by a text box containing "CA-ACF2-Cnctr". Below this is a section labeled "Operations Supported" containing a list box with "Action" checked. At the bottom are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **ACTION** check box is selected by default.

5. Click **NEXT**.

The Core Server displays the following dialog box.

Figure 67: Connector Configuration Manager for CA-ACF2 - TCP/IP


The dialog box is titled "Connector Configuration Manager for CA-ACF2". It has two main sections. The "OS/390 Settings" section contains four text boxes: "OS/390 System:", "\$COURIER Account:", "Password:", and "Security Phrase:". The "Connection" section contains two radio buttons: "TCP/IP" (which is selected) and "SNA". Next to the "TCP/IP" radio button is a text box labeled "TCP/IP Port:" containing the value "47474". At the bottom are three buttons: "< Back", "Finish", and "Cancel".

Figure 68: Connector Configuration Manager for CA-ACF2 - SNA

6. Enter the following information:
 - a. **OS/390 SYSTEM** - hostname or IP address.
 - b. **\$COURIER ACCOUNT** — The LogonID of the CA-ACF2[®] Account, with access permitted to the \$COURIER facility. (See SAMPLIB member ACF2 in [“Sample CA-ACF2 Member” on page 651](#) for an example of how to define this LogonID.)
 - c. **PASSWORD** — the password of the \$COURIER account.
 - d. **SECURITY PHRASE** — A character string, 8 to 32 bytes long, used to create encryption keys. This value must match that specified in the Cour390 Global parameter 3DES_SEED (see [“Creating the GLOBAL Member” on page 635](#)).
 - e. **TCP/IP OR SNA CONNECTION** — Select the communication protocol to use between the Connector for CA-ACF2 and the Cour390 agent. The selection here determines which of the following fields are displayed in the Configuration Manager.
 - f. **TCP/IP PORT** — The port on which the Cour390 agent listens for requests. This value must match that specified in the Cour390 Global parameter TCPIPSPORT.
 - g. **LU NAME** — The SNA LU Name for the Cour390 agent.
 - h. **MODE NAME** — The SNA Mode Name for the Cour390 agent. This value must match that specified in the Cour390 Global parameter MODENAME (or be the VTAM default, if MODENAME is not specified in the Global Member).
 - i. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 20: IBM z/OS Systems with CA-Top Secret — PMM and Connector

This chapter explains how to configure the PMM and Connector for IBM z/OS Systems (formerly known as OS/390) with CA-Top Secret:

- [*“Configuring the PMM for z/OS Systems with CA-Top Secret” on page 190*](#)
- [*“Configuring the Connector for z/OS Systems with CA-Top Secret” on page 195*](#)

Configuring the PMM for z/OS Systems with CA-Top Secret

The Password Management Module (PMM) for CA-Top Secret enables an Core Access Assurance Suite application to reset passwords automatically for z/OS systems using CA-Top Secret.

This password management module is installed automatically with the Core Access Assurance Suite. The correct access key(s) are required to configure it.

The PMM for z/OS systems with CA-Top Secret uses a simple algorithm for resetting passwords:

1. Verify that the username to reset exists on the system.
2. Obtain the account with "READ" access to the \$COURIER facility to make the connection to the Mainframe Reset Agent which carries out the reset request.
3. Verify the specially configured account for the system where the username to reset exists.
4. If one is configured, then attempt the reset.

The PMM for z/OS systems with CA-Top Secret includes the following components:

- PMM for CA-Top Secret library (.dll) Mainframe.dll
- PwReset.dll
- Configuration Application MainframeConfig.exe
- Courion Mainframe Reset Agent `os390agent.exe`

Prerequisites

You need to install the PMM agent for CA-Top Secret on the z/OS systems where the resets occur.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

The PMM requires the most recent version of the Core Access Assurance Suite. Previous versions may not be able to communicate with the current versions of the Cour390 agent.

z/OS Mainframe

- z/OS Systems Programmer.
Ability to upload the mainframe SAMPLIB and LOADLIB into data sets defined on the host.
Ability to APF authorize the LOADLIB with either the z/OS Console Commands and entries in the PROGxx member, or the IEAAPFxx member.
- VTAM Systems Programmer.
Ability to Add VTAM Definitions and Activate them with z/OS Console Commands.

- Security System Systems Programmer/Administrator.
Ability to enter Security definitions for the applicable Host Security System.

z/OS System

The PMM agent for CA-Top Secret must be installed for password resets on the z/OS system. The `os390agent.exe` file is located in the OS390 folder within the Core Access Assurance Suite installation folder. For information on installing, configuring, and maintaining Core's z/OS Agent, please see ["Using the Cour390 Agent" on page 631](#).

Before installing this PMM, be sure to have the following information:

- Determine if the connection to the z/OS system is via TCP/IP or an SNA Server. The TCP/IP port for the agent on the z/OS system is needed for a TCP/IP connection. For an SNA connection, the LU Name and ModeName for the Agent on the z/OS system are required. The SNA client must be installed on the same system as each server in which the Connector Framework or Connector Framework manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- Select the username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the PMM for z/OS systems with CA-Top Secret and the Cour390 Agent.

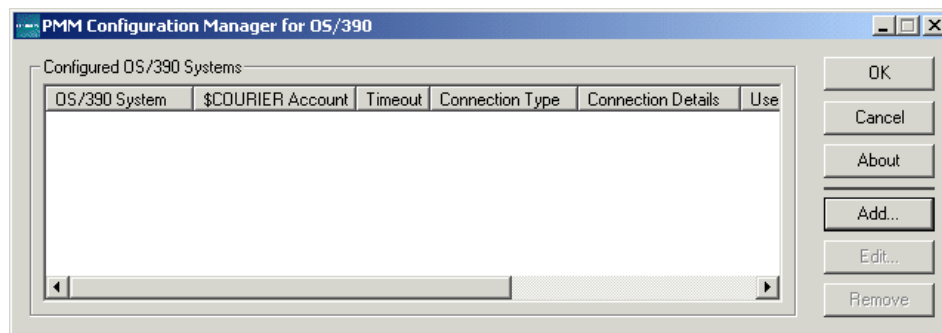
PMM Configuration

1. From the Start menu, select:

Programs>Core Access Assurance Suite >Password Management Modules>CA-Top Secret

The PMM Configuration Manager for z/OS screen appears.

Figure 69: PMM Configuration Manager for z/OS (OS/390)



2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.

- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box displays.

Figure 70: Add/Edit Target Configuration with TCP/IP selected

3. CONFIGURE OS/390 SYSTEM

- OS/390 SYSTEM** — Enter the target (either an IP address or a resolvable DNS) of the z/OS system in which the password resets are to be performed. Select the appropriate connection method (SNA or TCP/IP). The target should be an IP address, not a host name. The IP address must equal the IP address of the target z/OS system. The port specified must match that specified in the TCPIPPORT parameter of the GLOBAL member.

You need to use this same address for the **PMM TARGET** name when you configure the target in the PMM Gateway Connector configuration. Both fields should use the IP address or both should use the DNS.

Note: The TCP/IP address or DSN must be the same as that specified in the IPADDR field of the SAMPLIB member containing the TCP Configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

- \$COURIER** — Enter an account name for the \$COURIER facility to use in connecting the PMM for z/OS systems with CA-Top Secret with the Cour390 Agent.
- ACCOUNT PASSWORD** — Enter a password for the specially configured account created in the **\$COURIER ACCOUNT** field.

Note: This account name and password must match that of the Logon Definition for the z/OS. See [“Using the Cour390 Agent” on page 631](#).

- TIMEOUT (SECS)** — Enter the amount of time (in seconds) before password reset timeout. The default value for this field is 10 seconds.

- e. **SECURITY PHRASE** — Enter the security phrase that initializes Triple DES Encryption. This phrase must match the phrase (called the 3DES_SEED GLOBAL parameter) configured on the z/OS Agent.
- f. **USE STRONG PASSWORD RULES** — Select this option to enforce strong password rules.
- g. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — Select this option to allow password resets for administrator accounts with Core Password.

If you do not select this option, the Core Access Assurance Suite does not reset accounts with either the Special, Operations, or Auditor attributes.

Depending on your connection type, continue to [“Configuring TCP/IP Parameters”](#) or [“Configuring SNA Parameters”](#)

Configuring TCP/IP Parameters

- a. **CONNECTION** — Choose the **TCP/IP** Connector option.
- b. **TCP/IP PORT** — Enter the TCP/IP port that the agent is listening to on the z/OS System.

Note: The port address must be the same as that specified in the IPPORT field of the SAMPLIB member containing the TCP configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

Configuring SNA Parameters

Figure 71: Add/Edit Target Configuration with SNA selected

- a. **LU NAME** — Enter the SNA LU Name for the z/OS system agent.
- b. **MODE NAME** — Enter the mode name for the z/OS system agent.

Note: The SNA LU Name and Mode Name must be the same as that specified in the LU_NAME and MODENAME fields of the SAMPLIB member containing the SNA configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is SNANODE.

4. You have configured the PMM. Click the **OK** button to save the configuration

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

Punctuation is not supported for password resets. De-select the **ALLOW PUNCTUATION** check box on the Password Strength Composition screen.

Configuring the Connector for z/OS Systems with CA-Top Secret

The connector for z/OS systems with CA-Top Secret® systems supports the following actions on a target: Add, Create, Change, Delete, Disable, Enable, Verify, and View.

Prerequisites

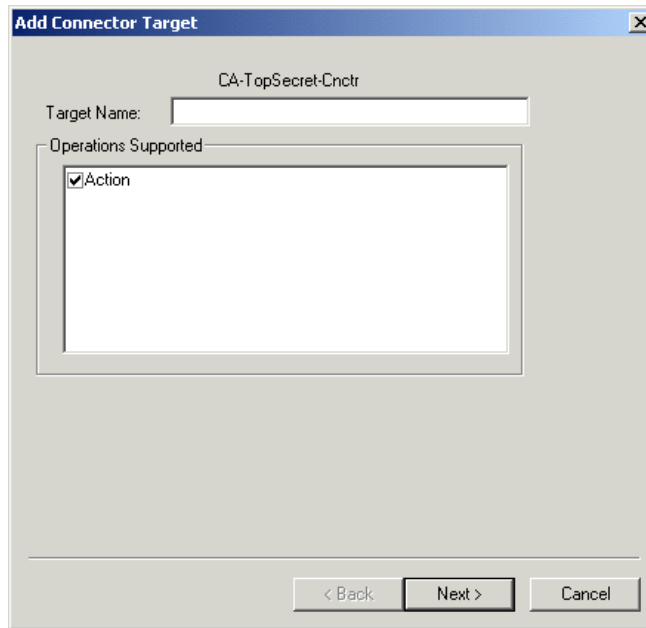
Core Provisioning and Core Compliance manage accounts on z/OS® systems with CA-Top Secret through the Cour390 Agent, which you install on the target z/OS® system. Configuring a target (specifically, step 6 in the following procedure) requires the following information:

- Determine if the connection to the z/OS system is through TCP/IP or an SNA Server. TCP/IP connections require the TCP/IP port for the agent on the z/OS system. SNA connections require the LU Name and ModeName for the Agent on the z/OS system. The SNA client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- Determine the username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the Connector for z/OS systems with CA-Top Secret and the Cour390 Agent.
- Determine the security phrase used to create encryption keys. This value must match the value specified in the Cour390 Global parameter 3DES_SEED (see [“Configuring the Cour390 Agent” on page 635](#)).
- For information on installing the Agent, see [“Installing or Upgrading the Cour390 Agent” on page 633](#).

Connector Configuration

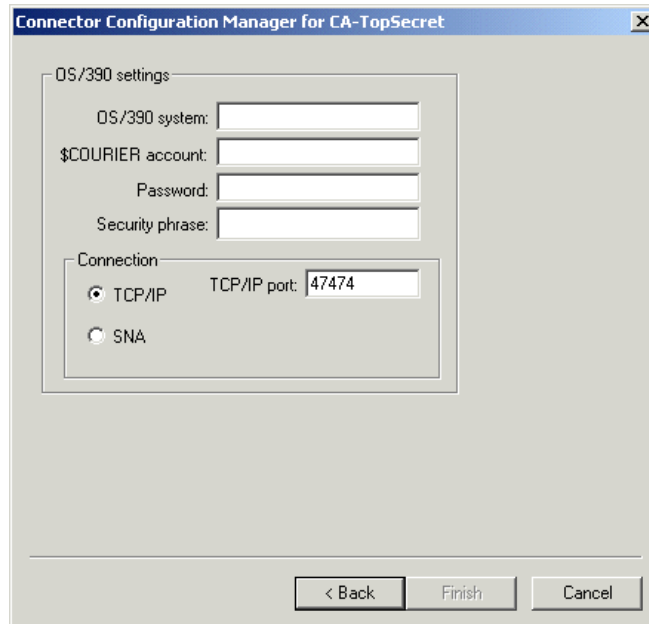
Follow these steps to add a z/OS system with a CA-Top Secret target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **CA-TOPSECRET-CNCTR**
3. Click the right mouse button on the connector name and choose **ADD TARGET...**
The Add Connector Target dialog box appears, as shown in [Figure 72](#).

Figure 72: Add CA-Top Secret Target


The dialog box is titled "Add Connector Target". It contains a "Target Name:" label followed by a text box containing "CA-TopSecret-Cnctr". Below this is a section titled "Operations Supported" which contains a list box with a single item "Action" that is checked. At the bottom of the dialog are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the Target Name text box. This name identifies the target in the Administration Manager interface.
The Action check box is selected by default.
5. Click **NEXT**. The Connector Configuration Manager dialog box appears.

Figure 73: Connector Configuration Manager for CA-Top Secret


The dialog box is titled "Connector Configuration Manager for CA-TopSecret". It has two main sections. The first section, "OS/390 settings", contains four text boxes: "OS/390 system:", "\$COURIER account:", "Password:", and "Security phrase:". The second section, "Connection", contains two radio buttons: "TCP/IP" (which is selected) and "SNA". To the right of the "TCP/IP" radio button is a text box labeled "TCP/IP port:" containing the value "47474". At the bottom of the dialog are three buttons: "< Back", "Finish", and "Cancel".

6. Enter the following information:
 - a. **OS/390 SYSTEM** — The hostname or IP address of the z/OS or OS/390 system.

- b. **\$COURIER ACCOUNT** — The LogonID of the CA-Top Secret Account, with access permitted to the \$COURIER facility. (See SAMPLIB member ACF2 in [“Sample CA-ACF2 Member” on page 651](#) for an example of how to define this LogonID.)
 - c. **PASSWORD** — The password of the \$COURIER account.
 - d. **SECURITY PHRASE** — A character string, 8 to 32 bytes long, used to create encryption keys. This value must match that specified in the Cour390 Global parameter 3DES_SEED ().
 - e. **CONNECTION** — Select the communication protocol, **TCP/IP** or **SNA**, to use between the Connector for z/OS systems with CA-Top Secret and the Cour390 Agent. The selection here determines which of the following fields are displayed in the Configuration Manager.
 - f. **TCP/IP PORT** — The port on which the Cour390 Agent listens for requests. This value must match that specified in the Cour390 Global parameter TCPIPPORT.
 - g. **LU NAME** — The SNA LU Name for the Cour390 Agent.
 - h. **MODE NAME** — The SNA Mode Name for the Cour390 Agent. This value must match that specified in the Cour390 Global parameter MODENAME (or be the VTAM default, if MODENAME is not specified in the Global Member).
7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services. The target is now available for each action supported by this connector.

Chapter 21: IBM z/OS Systems with RACF — PMM and Connector

This chapter explains how to configure the PMM and Connector for IBM z/OS Systems (formerly known as OS/390) with RACF:

- [*“Configuring the PMM for z/OS Systems with RACF” on page 200*](#)
- [*“Configuring the Connector for z/OS Systems with RACF” on page 205*](#)

Configuring the PMM for z/OS Systems with RACF

The Password Management Module (PMM) for RACF enables Core Server applications automatically to reset passwords for z/OS systems using RACF.

The correct access key(s) are required to configure this module.

The PMM for RACF uses a simple algorithm for resetting passwords:

1. Verifies that the username to reset exists on the system.
2. Connects to the PMM for z/OS agent that submits the reset request.
3. Verifies that the PMM configuration allows resets on this system, by validating the \$COURIER account and password that was specified during PMM configuration.
4. If resets are allowed, attempts the reset.

The PMM for RACF includes the following components:

- PMM for RACF library (.dll's) Mainframe.dll
- PwReset.dll
- Configuration Application MainframeConfig.exe
- PMM for z/OS agent os390agent.exe, needed for RACF password resets to occur. This file is located in the OS390 folder within the Core Server Core Server installation folder.

Prerequisites

You need to install the Cour390 agent on the z/OS systems where the password resets occur. Installing and configuring the Cour390 agent is explained in [“Using the Cour390 Agent”](#) starting on page [631](#).

The PMM requires the most recent version of the Core Server. Previous versions may not be able to communicate with current versions of the PMM for z/OS agent.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

z/OS Mainframe Requirements

1. z/OS Systems Programmer.
 - Ability to upload the mainframe SAMPLIB and LOADLIB into datasets defined on the host.
 - Ability to APF authorize the LOADLIB with either the z/OS Console Commands and entries in the PROGxx member, or the IEAAPFxx member.
2. VTAM Systems Programmer.

Ability to Add VTAM Definitions and Activate them with z/OS Console Commands.

3. Security System Systems Programmer/Administrator.

Ability to enter Security definitions for the applicable Host Security System.

z/OS PMM Agent Requirement

RACF requires the z/OS PMM agent for password resets on the z/OS system to occur. The os390agent.exe file is located in the OS390 folder within the Core Server Core Server installation folder.

To allow the PMM for RACF to propagate password changes under control of the RACF Remote Sharing Facility (RRSF), include the parameter RRSF_PASSWORD_SUPPORT=YES in the z/OS Agent GLOBAL file. See [“Cour390 Password Reset Parameters” on page 638](#) for a detailed description of the RRSF_PASSWORD_SUPPORT parameter. When this parameter is specified to the agent, the agent performs the equivalent of an administrative reset and forces the user to change their password at their next log on to the system unless parameter ESS_EXPIRE_PASSWORD is set to NO.

PMM Configuration

Be sure to have the following information:

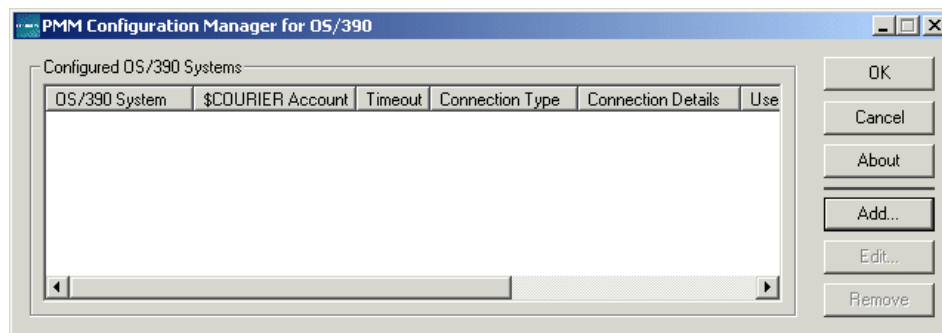
- The type of connection to the z/OS system: TCP/IP or SNA. The TCP/IP port for the agent on the z/OS system is needed for a TCP/IP connection. For an SNA connection, the LU Name and ModeName for the agent on the z/OS system are required. The SNA client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- A username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the PMM for RACF and the Cour390 Agent.

1. From the Start menu, select:

Programs>Core Server Core Server >Password Management Modules>RACF

The PMM Configuration Manager for z/OS appears.

Figure 74: PMM Configuration Manager for z/OS (OS/390)



2. From this dialog box, you can

- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box displays.

Figure 75: Add/Edit Target Configuration with TCP/IP selected

3. **CONFIGURE OS/390 SYSTEM**

- a. **OS/390 SYSTEM** — Enter the target (either an IP address or a resolvable DNS) of the z/OS system in which the password resets are to be performed. Select the appropriate connection method (SNA or TCP/IP). The target should be an IP address, not a host name. The IP address must equal the IP address of the target z/OS system. The port specified must match that specified in the TCPIPPORT parameter of the GLOBAL member.

You need to use this same address for the **PMM TARGET** name when you configure the target in the PMM Gateway Connector configuration. Both fields should use the IP address or both should use the DNS.

Note: The TCP/IP address or DSN must be the same as that specified in the IPADDR field of the SAMPLIB member containing the TCP Configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

- b. **\$COURIER** — Enter an account name for the \$COURIER facility to use in connecting the PMM for CA-Top Secret with the Cour390 Agent.
- c. **ACCOUNT PASSWORD** — Enter a password for the specially configured account created in the **\$COURIER ACCOUNT** field.

Note: This account name and password must match that of the Logon Definition for the z/OS. See [“Using the Cour390 Agent” on page 631](#).

- d. **TIMEOUT (SECS)** — Enter the amount of time (in seconds) before password reset timeout. The default value for this field is 10 seconds.
- e. **SECURITY PHRASE** — Enter the security phrase that initializes Triple DES Encryption. This phrase must match the phrase (called the 3DES_SEED GLOBAL parameter) configured on the z/OS Agent.
- f. **USE STRONG PASSWORD RULES** — Select this option to enforce strong password rules.
- g. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — Select this option to allow password resets for administrator accounts with Core Server.
If you do not select this option, the Core Server does not reset accounts with Special, Operations, or Auditor attributes.

Depending on your connection type, continue to [“Configuring TCP/IP Parameters”](#) or [“Configuring SNA Parameters”](#)

Configuring TCP/IP Parameters

- a. **CONNECTION** — Choose the **TCP/IP** Connector option.
- b. **TCP/IP PORT** — Enter the TCP/IP port that the agent is listening to on the z/OS System.

Note: The port address must be the same as that specified in the IPPORT field of the SAMPLIB member containing the TCP configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is TCPNODE.

Configuring SNA Parameters

Figure 76: Add/Edit Target Configuration with SNA selected

- a. **LU NAME** — Enter the SNA LU Name for the z/OS system agent.
- b. **MODE NAME** — Enter the mode name for the z/OS system agent.

Note: The SNA LU Name and Mode Name must be the same as that specified in the LU_NAME and MODENAME fields of the SAMPLIB member

containing the SNA configuration information. This member is named in the CONFIG member of SAMPLIB; the default member name is SNANODE.

4. You have configured the PMM. Click the **OK** button to save the configuration

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- This PMM supports access to the RACF Remote Sharing Facility (RRSF). To access this feature, set RRSF_PASSWORD_SUPPORT to YES in the GLOBAL member of the SAMPLIB.
- Punctuation is not supported for password resets. De-select the **ALLOW PUNCTUATION** check box on the Password Strength Composition screen.

Configuring the Connector for z/OS Systems with RACF

The connector for z/OS Systems with RACF supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, View, Authentication, and Query.

The Core Server manages accounts on z/OS Systems with RACF through the Cour390 Agent, which must be installed on the target z/OS system. For information on the agent, see [“Using the Cour390 Agent” on page 631](#).

Prerequisites

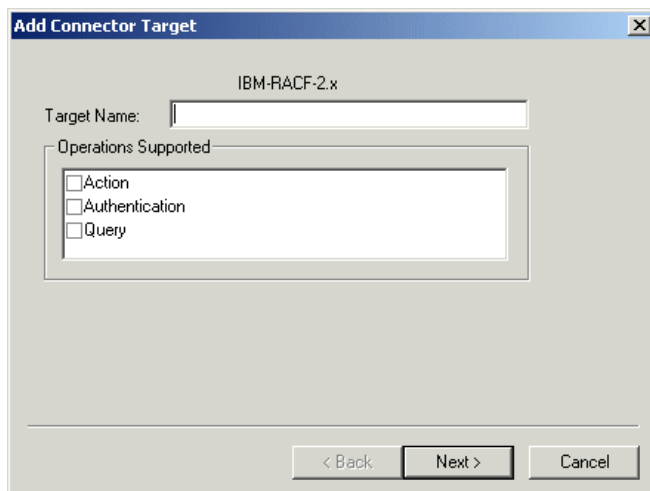
Configuring a target requires the following information:

- Knowledge whether the connection to the z/OS system is via TCP/IP or an SNA Server. TCP/IP connections require the TCP/IP port for the agent on the z/OS system. SNA connections require the LU Name and ModeName for the agent on the z/OS system. The SNA client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. The system must be in the same domain or a domain that is trusted by the domain where the SNA Server is running.
- Knowledge of the username/password pair of an account that has "READ" access in the user-defined facility \$COURIER. This account is used to validate the connection between the Connector for RACF and the Cour390 Agent.
- Information shown in step 7 of the following section: [“Connector Configuration”](#).

Connector Configuration

Follow these steps to add an z/OS Systems with RACF target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **IBM-RACF-2.x**
3. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 77: Add RACF Target


The dialog box is titled "Add Connector Target". It contains a text field for "Target Name" with the value "IBM-RACF-2.x". Below this is a section titled "Operations Supported" containing three checkboxes: "Action", "Authentication", and "Query". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

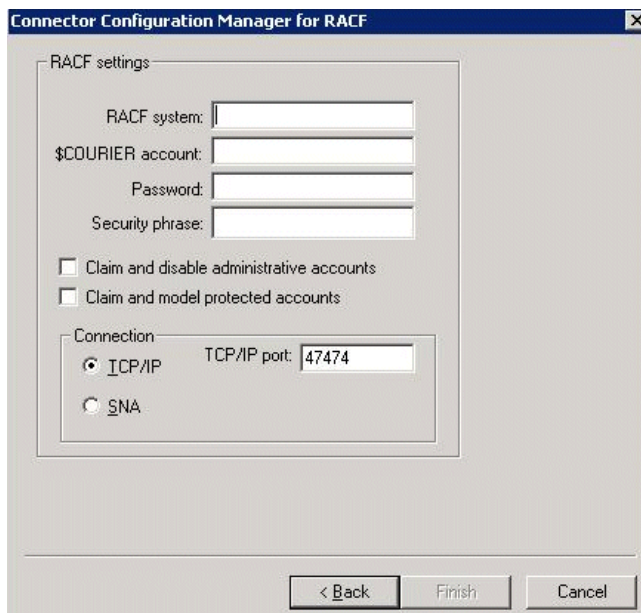
5. Select **Action** to enable all provisioning actions on the target.

Select **AUTHENTICATION** to use the target datasource for authenticating end user access to Core Server or Core Server.

Select **QUERY** to enable provisioning actions to use queries to find data in the target datasource.

6. Click **NEXT**.

The Core Server displays the following dialog box:

Figure 78: Connector Configuration Manager for RACF - TCP/IP


The dialog box is titled "Connector Configuration Manager for RACF". It contains a section titled "RACF settings" with four text fields: "RACF system:", "\$COURIER account:", "Password:", and "Security phrase:". Below these are two checkboxes: "Claim and disable administrative accounts" and "Claim and model protected accounts". A section titled "Connection" contains two radio buttons: "TCP/IP" (selected) and "SNA". Next to the "TCP/IP" radio button is a text field for "TCP/IP port:" with the value "47474". At the bottom are three buttons: "< Back", "Finish", and "Cancel".

7. This dialog box requires the following information.

- **RACF SYSTEM** — Enter the name or IP address of the z/OS System with RACF server where the provisioning actions occur.

- **\$COURIER ACCOUNT** — Enter the user id of an account with access to the facility class profile on the specified system.
- **PASSWORD** — Enter the password for the user id.
- **SECURITY PHRASE** — Enter the security phrase that initializes Triple DES Encryption. This phrase must match the phrase configured on the Cour390 Agent, and is case-sensitive. The phrase is configured on the agent in the 3DES_SEED parameter of the GLOBAL file.
- **CLAIM AND ADMINISTRATIVE ACCOUNTS** — Select this option to disable any administrative accounts associated with this target.
- **CLAIM AND MODEL PROTECTED ACCOUNTS** — Select this option to use any protected accounts on this target as models for new accounts.

Note: To claim either protected or administrative accounts, you also need to configure the Resource Suggestion Details form in the Administration Manager to allow either protected accounts or administrative accounts to be claimed. They must be active to be claimed. To make them active, check the checkbox in the “Active” column that is next to either Protected Account or Administrator Account on this form. See the manual *Configuring Workflows with the Core Server Administration Manager* for more information about the Resource Suggestion Details form.

These options also enable you to view administrative or protected accounts using the View action.

- In the **CONNECTION** section, select the type of connection:

For TCP/IP, enter the port number in the **TCP/IP PORT** text box.

For SNA, enter the logical unit name in the **LU NAME** text box and a valid logon mode for the logical unit in the **MODE NAME** text box.

Figure 79: Connector Configuration Manager for RACF - SNA

8. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 22: IBM i Systems — PMM and Connector

This chapter explains how to configure the PMM and Connector for IBM i (previously known as OS/400, i5/OS). The PMM and Connector each have an agent that must be installed and configured which is also explained in this chapter.

Major topics are:

- [*“Configuring the PMM for IBM i” on page 210*](#)
- [*“Installing and Configuring the PMM Agent” on page 217*](#)
- [*“Configuring the Connector for IBM i” on page 230*](#)
- [*“Installing and Configuring the Connector Agent” on page 233*](#)

Note: IBM has renamed their OS/400, i5/OS operating system to IBM i. The PMM, Connector, and agents in the Core Security Core Server are still named OS/400. The terms OS/400 and IBM i can be used interchangeably in this documentation.

- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 81: PMM for OS/400 Configuration Parameters

3. **TARGET NAME** — Enter a logical name for the target. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **OS/400 SYSTEM** — Enter the OS/400 server name on which password resets are being performed and on which the agent is installed and configured. The name must be that of either the OS/400 server or IP address.
5. **TCP PORT** — Enter the TCP Port number on which the PMM Agent for OS/400 is listening. The default port number is 8191. Acceptable port numbers range from 1024 to 65535.
6. **TIMEOUT (SECS.)** — Enter the Timeout information. The default is 30 seconds. Timeouts may range from 1 to 360 seconds. Core Security recommends setting the minimum timeout to 30 seconds or greater.
7. **PRIVILEGED USERNAME** — Enter the Privileged Username. The user must have *ALLOBJ and *SECADM authorities.
8. **PASSWORD** — Enter the Password associated with the specified privileged user.
9. **ALLOW RESET AND ENABLE OF ADMINISTRATIVE PROFILES** — Select this check box to allow users to **PASSWORD RESET AND ENABLE** for user profiles with *SECADM privileges that are not on the excluded profiles list.

10. **PASSWORD RESET** — Choose this option to allow password resets only. It does not enable *DISABLED user profiles.
11. **PASSWORD RESET AND ENABLE *DISABLED PROFILES** — Choose this option to allow both password resets and enabling of *DISABLED user profiles at the same time.
12. **ENABLE *DISABLED PROFILES** — Choose this option to enable *DISABLED user profiles. It does not allow password resets.
13. Click **OK** to save the configuration.

Required Forced Password Change

Required Forced password change upon next login is a feature you can configure with the Administration Manager (see the manual *Configuring Workflows with the Core Server Administration Manager*). When turned on, this parameter sets the end user profile to expire as soon as the user profile reset.

- The PMM for OS/400 does not allow password resets for *DISABLED user profiles or profiles with the password of *NONE.
- Password resets are executed similarly to administrative password resets which do not enforce the password strength rules on the OS/400 system.
- The spool file QPRINT, where the trace messages logged by the agent are stored, is delivered by IBM with a default maximum size (MAXRCDS) of 100,000 spooled output records (approximately 1800 pages).

If the PMM Agent for OS/400 is started with ETRACE(*YES), then about 2200 resets can be issued before the spool file QPRINT fills up. When it is full, the message CPA4072 "Reached maximum number of spooled records for file QPRINT in library QGPL. (C R NOMAX 1-999999)" is issued to the system operator (QSYSOPR) message queue. At this point, the agent is frozen and waits for the spool file issue to be resolved.

Once the system operator answers the message, the agent terminates. Restart the agent for password resets to be accepted.

- The first password reset attempt made after the agent is started is known to take longer than any subsequent reset.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff* explains how to do this on the classic platform.

Notes and Warnings

- The PMM for OS/400 does not allow password resets for *DISABLED user profiles or profiles with the password of *NONE.

- Password resets are executed similarly to administrative password resets which do not enforce the password strength rules on the OS/400 system.
- The spool file QPRINT, where the trace messages logged by the agent are stored, is delivered by IBM with a default maximum size (MAXRCDS) of 100,000 spooled output records (approximately 1800 pages).

If the PMM Agent for OS/400 is started with ETRACE(*YES), then about 2200 resets can be issued before the spool file QPRINT fills up. When it is full, the message CPA4072 "Reached maximum number of spooled records for file QPRINT in library QGPL. (C R NOMAX 1-999999)" is issued to the system operator (QSYSOPR) message queue. At this point, the agent is frozen and waits for the spool file issue to be resolved.

Once the system operator answers the message, the agent terminates. Restart the agent for password resets to be accepted.

- The first password reset attempt made after the agent is started is known to take longer than any subsequent reset.

Using OS/400 PMM Agent Commands and Keywords

Table 13: PMM Agent for OS/400 Commands and KeywordsCore Server

Command	Keyword	Allowed Values	Default	Description
COURAGENT /PMMCFG				
	PMMLIB	COURAGENT	COURAGENT	Specify the name of the library where the PMM Agent for OS/400 is installed. Note: This configuration command "PMMCFG" must be running in the installed library.
	SUBSYS	Any valid subsystem	QSYSWRK	Specify the name of the Subsystem where the PMM Agent for OS/400 SSL Server should execute.
		Library where subsystem description exists	QSYS	Specify the name of the Library where the Subsystem is defined.
	JOBQ	Any valid jobq within the above subsystem	QSYSNOMAX	Specify the name of the Job Queue where PMM Agent for OS/400 batch jobs should be run.
		Library where jobq description exists	QSYS	Specify the name of the Library where the Job Queue is defined.
	PORT	1024-65535	8191	Specify the Port where the PMM Agent for OS/400 should listen for SSL messages from requesting clients.
	MSGPRGDAY S	1-99	07	Specify the number of days that error and traces messages should be kept in the message queue before they may be purged using the Purge Message and Output Queues option.
	IFSPATH	see below ¹	see below ¹	Specify the fully qualified path to the PMM Agent for OS/400 files.

Table 13: PMM Agent for OS/400 Commands and KeywordsCore Server

Command	Keyword	Allowed Values	Default	Description
COURAGENT /PMMCFG (continued)	CLASS	see below ²	see below ²	This field should contain the name of the Java Class to be run. This value must match the actual name of a Java class and should not be changed unless a newly named Java class is installed.
	CLASSPATH	see below ³	see below ³	Specify the fully qualified Class Path environment variable.
	JVERSION	'1.1.8'	'1.1.8'	This field must contain the JVM version number that the Java code is designed to be run within. This JVM must be installed and configured.
	PMMOWNER	COURAGENT	COURAGENT	This field should contain the name of the Owner of the PMM Agent for OS/400 Library. This value is used to ensure that the program is initiated in the correct environment.
COURAGENT /PMMPRG				
	SELDAYS	1-99	07	Enter the number of days worth of entries that should remain in the queues after the purge has completed.

Table 13: PMM Agent for OS/400 Commands and KeywordsCore Server

Command	Keyword	Allowed Values	Default	Description
COURAGENT /STRPMM				
	ETRACE	*NO, *YES	*NO	This parameter is used to indicate whether the PMM Agent for OS/400 should be started in Trace mode or not. Selecting *YES causes the program to be initiated with Tracing enabled which causes additional program detail to be logged, to assist in problem determination.
	CMSGQ	*NO, *YES	*NO	This command is for clearing the message queue. Selecting *YES causes the message logging queue to be cleared before the program is initiated.
	COUTQ	*NO, *YES	*NO	This command is for clearing the output queue. *YES causes the logging output print queue to be cleared before the program is initiated.

Note: these values are supplied as defaults by PMM for OS/400 and should not be changed unless instructed by the PMM for OS/400 software vendor.

¹Path to jar files in IFS: '/couragent'

²Java class to run:'com.courion.os400.AgentController'

³Class path:

```
' :.:./QIBM/ProdData/Java400/jt400ntv.jar:/couragent/
pmm400.jar:/couragent/os400.jar:/QIBM/ProdData/HTTP/Public/
jt400/lib/jt400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/
data400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/x4j400.jar '
```


Installing and Configuring the PMM Agent

This section explains how to install, configure, start, and stop the PMM agent.

Select the OS/400 agent SAVF file (couragent.savf) that corresponds to your version of OS/400 (iSeries).

iSeries 7.1: <install drive>:\<install folder>\Courion Corporation\iSeries 7.1\PMM
 OS/400 V5RM10: <install drive>:\<install folder>\Courion Corporation\OS400 V5RM10\PMM
 OS/400 V5R4: <install drive>:\<install folder>\Courion Corporation\OS400 V5R4\PMM
 OS/400 V4R5: <install drive>:\<install folder>\Courion Corporation\OS400\PMM

Installing the PMM Agent

The user profile used in this install process must have *SECADM and *ALLOBJ special authorities. Core Security recommends using QSECOFR for installation. To install the PMM Agent for OS/400:

1. Sign on to the AS/400 as QSECOFR or a user profile with *ALLOBJ and *SECADM authority.
2. Bring up a Command Entry screen by typing:

```
CALL QCMD
```

3. Establish new user profiles before installing the product library

Create the following user profiles:

- a. Name: COURAGENT

Purpose: owns all the objects provided and is the user profile which runs the PMM Agent for OS/400

```
CRTUSRPRF USRPRF(COURAGENT)
          PASSWORD(some-password)
          USRCLS(*USER)
          LMTCPB(*NO)
          TEXT('PMM for OS/400 Object Owner/Group
Profile')
          SPCAUT(*USRCLS)
          HOMEDIR('/couragent')
```

Note: the following messages display:

```
Special authorities granted *NONE
User profile COURAGENT created
```

- b. Name: COURAGSEC

Purpose: has *SECADM and *ALLOBJ special authorities and is the privileged user profile under which the Java SSL Agent runs. The COURAGESEC user profile must allow the privileged user to log in. The COURAGSEC user profile is optional if an existing "Security Officer" user profile is being used for password resets.

```
CRTUSRPRF USRPRF(COURAGSEC)
          PASSWORD(some-password)
          USRCLS(*SECADM)
```

```
INLMNU(*SIGNOFF)
LMTCPB(*NO)
TEXT('PMM Agent for OS/400 Security Officer')
SPCAUT(*SECADM *ALLOBJ)
PWDEXPITV(*NOMAX)
GRPPRF(COURAGENT)
OWNER(*GRPPRF)
```

Note: The following messages appear:

User class and special authorities do not match system supplied values.

User profile COURAGSEC created.

4. Grant temporary authority

- a. The COURAGENT user profile temporarily needs authority to the RSTLIB and RST commands.
- b. Temporarily grant authority to RSTLIB and RST commands to COURAGENT to perform product restore operations.

```
GRTOBJAUT OBJ(RSTLIB) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*USE)
```

```
GRTOBJAUT OBJ(RST) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*USE)
```

- c. Sign-off as QSECOFR or the user ID used to create the above user profiles.

5. Use FTP to transfer the .savf file to the AS/400

- a. Sign-on to the AS/400 as COURAGENT.

Note: It is important that the FTP, RST and RSTLIB commands issued below be entered under the COURAGENT user profile. The system does not set up correctly if the administrator configuring it does not sign on as COURAGENT.

- b. Create a save file in QGPL:

```
CRTSAVF QGPL/COURAGENT
```

The extracted AS/400 programs are delivered in a *SAVF file and must be uploaded to the AS/400 system.

- c. Copy the COURAGENT.savf file from the Core Server install directory (OS400 subfolder) to the root directory of C:\
- d. Using FTP enter the following commands from the PC where the COURAGENT.savf file is stored and perform the following steps:

```
FTP myAS400ipAddress
User: COURAGENT
Password: (COURAGENT password)
cd QGPL
lcd C:\
binary
put COURAGENT.savf COURAGENT
bye
```

6. Restore the product library

- a. On the AS/400, signed on as COURAGENT, issue this restore command:

```
RSTLIB SAVLIB(COURAGENT) DEV(*SAVF) SAVF(QGPL/COURAGENT)
OUTPUT(*PRINT)
```

7. Run the PMM Agent for OS/400 install program.

This creates the folder '/couragent' in the IFS and restores the .jar files. It then deletes the QGPL/COURAGENT save-file and revokes *PUBLIC authority to the Product Library COURAGENT.

a. CALL COURAGENT/INSTALLPMM

Note: the following messages display when the program is run:

```
Step 1- Create IFS root directory /couragent.
Step 2- Restore jar files into directory /couragent.
Step 3 - Delete *SAVF QGPL/COURAGENT.
Step 4 - Remove *PUBLIC authority from library COURAGENT.
Installation of PMM Agent for OS/400 has completed.
Type DSPJOB and select options 4 and 10 to review
installation logs.
```

8. Revoke Temporary Authority

Now that PMM Agent for OS/400 is installed, remove the temporary authority that was granted to the RSTLIB and RST commands.

- a. Sign-off as the user COURAGENT.
- b. Sign-on again as QSECOFR or a user profile with *ALLOBJ and *SECADM authority.
- c. Revoke the authority that had been given to COURAGENT to restore objects:

```
RVKOBJAUT OBJ(RSTLIB) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*ALL)
```

```
RVKOBJAUT OBJ(RST) OBJTYPE(*CMD) USER(COURAGENT)
AUT(*ALL)
```

- d. Update the COURAGENT user profile, adding the default menu and pmmoutq.

```
CHGUSRPRF USRPRF(COURAGENT) INLMNU(COURAGENT/PMMMNU)
OUTQ(COURAGENT/PMMOUTQ)
```

- e. Sign-off as QSECOFR.

Note: You may add the following commands to the QSTRUP job after all of the TCP/IP jobs are up and running. Adding these commands starts the OS/400 PMM Agent for OS/400 automatically after each IPL:

```
/* Start PMM for OS/400 */
COURAGENT/STRPMM
MONMSG CPF0000
```

IBM Delivers the QSTRUPJD *JOBID "Autostart job JOBID", as being owned by QPGMR and the USER parameter in the QSTRUPJD *JOBID is QPGMR. If the command COURAGENT/STRPMM is placed into the QSTRUP program, it is possible that during IPL, PMM Agent for OS/400 may fail to start with an error message stating QPGMR is not authorized to COURAGENT/STRPMM. (See the QSTRUPJD job log spool file in the QEZJOBLOG output queue.)

Delivered Agent Authority

For security reasons, PMM Agent for OS/400 Product Library is delivered with COURAGENT *ALL and *PUBLIC *EXCLUDE library authorities. This authority only allows COURAGENT or an AS/400 Security Officer into the PMM Agent for OS/400 Product Library to execute commands or bring up the PMMMNU.

To correct this authority problem, grant QPGMR *USE authority to the COURAGENT library and the COURAGENT user profile. This gives QPGMR the minimum authority needed to run the STRPMM command from the QSTRUP job during IPL.

Sign-on as QSECOFR or a user profile with *SECADM and *ALLOBJ special authorities and enter these commands:

```
GRTOBJAUT OBJ(COURAGENT) OBJTYPE(*LIB) USER(QPGMR) AUT(*USE)
GRTOBJAUT OBJ(COURAGENT) OBJTYPE(*USRPRF) USER(QPGMR)
AUT(*USE)
```

QPGMR now has sufficient authority to start the PMM Agent for OS/400 STRPMM command in the QSTRUP job during IPL.

The user profile QPGMR must have *USE authority to the library COURAGENT

The user profile QPGMR must have *USE authority to the user profile COURAGENT

Configuring the PMM Agent

Once the PMM Agent for OS/400 installed, it is ready for configuration. Help text is available by pressing F1.

1. On the AS/400, sign on as COURAGENT and enter the following command:

```
GO COURAGENT/PMMMNU (Figure 82)
```

Figure 82: PMM Agent for OS/400 Menu

```

PMMMNNU                      PMM Agent for OS/400 Menu                      System:   OS400A

Select one of the following:

    1. Start PMM Agent for OS/400
    2. End PMM Agent for OS/400
    3. Configure PMM Agent for OS/400
    4. Maintain Excluded Profiles
    5. Purge Message and Output Queues
    6. Print Configuration Files
    7. Print Message Queue
    8. Display Message Queue
    9. Display Output Queue

    90. Sign Off

Selection or command
===> _____

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
COPYRIGHT (C) 2002 COURION CORPORATION.

```

- From the PMM for OS/400 menu, select option 3: **CONFIGURE PMM AGENT FOR OS/400**.
- If entering COURAGENT/PMMCFG from the command line, enter the value COURAGENT for the keyword pmmlib when prompted.

The Configure PMM Agent screen appears ([Figure 83](#)).

Figure 83: PMM Agent for OS/400 Configuration (PMMCFG)

```

Configure PMM Agent for OS/400 (PMMCFG)

Type choices, press Enter.

Library where installed . . . . > COURAGENT      Name
Subsystem name . . . . . QSYSWRK                Name
Library . . . . . QSYS                          Name
Job queue name . . . . . QSYSNOMAX              Name
Library . . . . . QSYS                          Name
TCP Port . . . . . 08191                        1024-65535
#Days to keep before purge . . . 07              01-99
Execute CHGPWD cmd on reset . . N                Y, N

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys

MA a MW A 12/037

```

- Change the subsystem name, subsystem library name and job queue to what is appropriate on the system being used. The default is the subsystem QSYS/QSYSWRK, job queue QSYS/QSYSNOMAX.

To enable the Conform to Native Password History feature, Enter Y in the **EXECUTE CHGPWD CMD ON RESET** field.

- To start the PMM Agent for OS/400 on the AS/400, select option 1: **START PMM AGENT FOR OS/400** from the PMM Agent for OS/400 menu (PMMMNU) ([Figure 82](#)).

This submits the PMM Agent for OS/400 to the job queue specified in the configuration ([Figure 84](#)).

Figure 84: PMM Agent for OS/400 Start Screen

```

                                Start PMM Agent for OS/400 (STRPMM)

Type choices, press Enter.

Enable trace? . . . . . *NO          *NO, *YES

                                Additional Parameters

Clear the message queue? . . . . *NO          *NO, *YES
Clear the output queue? . . . . *NO          *NO, *YES


                                                                    Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

```

Agent Menu

- To display this menu, type GO COURAGENT/PMMMNU at a command line. It is necessary to be signed on as COURAGENT or as a Security Officer when working from this menu ([Figure 85](#)).

Figure 85: PMM Agent for OS/400 Menu

```

PMMMNU                                PMM Agent for OS/400 Menu                                System:    OS400A

Select one of the following:

    1. Start PMM Agent for OS/400
    2. End PMM Agent for OS/400
    3. Configure PMM Agent for OS/400
    4. Maintain Excluded Profiles
    5. Purge Message and Output Queues
    6. Print Configuration Files
    7. Print Message Queue
    8. Display Message Queue
    9. Display Output Queue

    90. Sign Off

Selection or command
===> _____

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
COPYRIGHT (C) 2002 COURION CORPORATION.

```

Note: After a command is entered in the PMM Agent for OS/400, a status message is provided at the bottom of the menu screen.

Configure Agent (PMMCFG) Commands

You can run the following Agent commands from the PMM Agent for OS/400 Menu command line:

- Start PMM Agent for OS/400
- End PMM Agent for OS/400
- Configure PMM Agent for OS/400
- Purge Message and Output Queues
- Print Configuration Files
- Print Message Queue

For more information on commands and their associated keywords and descriptions see [“Using OS/400 PMM Agent Commands and Keywords” on page 214](#)

By default, the TCP Port is 8191. If changing this port, remember to change the port specified in the PMM for OS/400 Configuration Manager ([Figure 83](#)).

If running the purge (PMMPRG) command, specify the number of days to keep messages and output queue log entries in the COURAGENT library. Run the PMMPRG command to purge the old log entries.

7. Select option 3, **CONFIGURE PMM AGENT FOR OS/400** to configure the PMM agent ([Figure 86](#)).

Figure 86: PMM Agent for OS/400 Configuration (PMMCFG), Screen One

Configure PMM Agent for OS/400 (PMMCFG)		
Type choices, press Enter.		
Library where installed	> COURAGENT	Name
Subsystem name	QSYSWRK	Name
Library	QSYS	Name
Job queue name	QSYSNOMAX	Name
Library	QSYS	Name
TCP Port	08191	1024-65535
#Days to keep before purge . . .	07	01-99
Execute CHGPWD cmd on reset . .	N	Y, N
Additional Parameters		
Path to jar files in IFS	'/_couragent'	
More... F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display F24=More keys		
MA	a	MW 06/037

Note: the “Path to jar files in IFS” field is reserved for future use.

8. Press F10 to view more information ([Figure 87](#)).

Figure 87: PMM Agent for OS/400 Configuration (PMMCFG), Screen Two

Configure PMM Agent for OS/400 (PMMCFG)		
Type choices, press Enter.		
Java class to run	'com.courion.os400.AgentController'	
Class path '.:./QIBM/ProdData/Java400/jt400ntv.jar:/couragent/pmm400.jar:/couragent/os400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/jt400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/data400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/x4j400.jar'		
Java version	'1.1.8'	Character value
Object Owner	COURAGENT	Name
Bottom F3=Exit F4=Prompt F5=Refresh F12=Cancel F13=How to use this display F24=More keys		
MA	a	MW 05/037

Note: The Java™ version entered in the configuration screen should match the JVM™ version installed with the Java Programmer's Toolkit on the system. The PMM Agent for OS/400 may fail to start if the Java version does not match.

Start Agent Command (STRPMM)

From the PMM Agent for OS/400 Menu, select option 1 **START PMM AGENT FOR OS/400** ([Figure 88](#)). To see additional parameters, press F10.

ENABLE TRACE? is set to *NO by default. If **ENABLE TRACE?** is set to *YES, the program is initiated with Tracing enabled, which causes additional program detail to be logged in to assist in problem determination. Please see [“Notes and Warnings” on page 212](#) for more information before setting this feature to *YES.

To clear the message queue and output queue log entries, specify *YES for the additional parameters ([Figure 88](#)).

Figure 88: PMM Agent for OS/400 Start (STRPMM)

```

                                Start PMM Agent for OS/400 (STRPMM)

Type choices, press Enter.

Enable trace? . . . . . *NO          *NO, *YES

                                Additional Parameters

Clear the message queue? . . . . *NO          *NO, *YES
Clear the output queue? . . . . *NO          *NO, *YES


                                                                 Bottom
F3=Exit   F4=Prompt   F5=Refresh   F12=Cancel   F13=How to use this display
F24=More keys

```

Printing Configuration Files

To determine the PMM Agent for OS/400 version number, go to the PMM Agent for OS/400 Menu and select option 6 **PRINT CONFIGURATION FILES** ([Figure 89](#)).

Figure 89: PMM Agent for OS/400 Print Configuration Files

```

                                Print Configuration Files (PMMPRTCFG)


                                                                 Bottom
F3=Exit   F5=Refresh   F12=Cancel   F13=How to use this display   F24=More keys

No parameters to show; press Enter to run, F3 to exit.

```

Using option 9 from the PMM Agent for OS/400 Menu, **DISPLAY OUTPUT QUEUE**, look for the spool file PMMPRTCFCG. Place a "5" on the line next to the PMMPRTCFCG spool file. The spool file displays the version number of PMM Agent for OS/400.

1. Sign-on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL special authorities. If working off of a PC and not the OS/400 console, it is necessary to have access to a 5250-emulation session.
2. Display the PMM Agent for OS/400 menu.
3. Select option 2 **END PMM AGENT FOR OS/400** ([Figure 91](#)).

Figure 91: PMM Agent for OS/400 End

```

End PMM Agent for OS/400 (ENDPMM)

F3=Exit  F5=Refresh  F12=Cancel  F13=How to use this display  F24=More keys

No parameters to show; press Enter to run, F3 to exit.

```

4. Press **ENTER** to confirm. The system displays user jobs.

Figure 92: PMM Agent for OS/400 Active Jobs

```

Work with User Jobs                                OS400A
                                                    02/27/02 15:07:33
Type options, press Enter.
 2=Change  3=Hold  4=End  5=Work with  6=Release  7=Display message
 8=Work with spooled files 13=Disconnect

Opt  Job      User      Type  -----Status-----  Function
---  ---      ---      ---
---  QJVACMSRV  COURAGENT  BATCHI  ACTIVE
---  QZRCRSRV   COURAGENT  BATCHI  ACTIVE
---  SSLAG08191  COURAGENT  BATCH   ACTIVE              CMD-STRPMM

Parameters or command                                Bottom
====>
F3=Exit  F4=Prompt  F5=Refresh  F9=Retrieve  F11=Display schedule data
F12=Cancel  F17=Top  F18=Bottom  F21=Select assistance level
Intermediate assistance level used.

```

5. Make sure PMM Agent for OS/400 is no longer active by using the WRKUSRJOB command as follows ([Figure 92](#)):

```
WRKUSRJOB USER(COURAGENT) STATUS(*ACTIVE)
```

6. There should not be any active jobs for COURAGENT ([Figure 93](#)).

Figure 93: PMM Agent for OS/400 Inactive Job

Work with User Jobs				OS400A 02/27/02 15:53:28	
Type options, press Enter.					
2=Change		3=Hold	4=End	5=Work with	6=Release
8=Work with spooled files		13=Disconnect		7=Display message	
Opt	Job	User	Type	-----Status-----	Function
(No jobs to display)					
Parameters or command					Bottom
==>					
F3=Exit	F4=Prompt	F5=Refresh	F9=Retrieve	F11=Display schedule data	
F12=Cancel	F17=Top	F18=Bottom	F21=Select assistance level		

Uninstalling the PMM Agent

To uninstall the agent, sign on as QSECOFR or as a user with security officer privileges on the AS/400. The security officer must have *SECADM, *ALLOBJ, and *SPLCTL special authorities. It is also necessary to have access to a 5250 emulation session.

Commands to Remove the Agent

If any PMM Agent for OS/400 commands have been added to the QSTRUP program or to the OS/400 Job Scheduled (WRKJOBSCDE), then remove these entries before proceeding with the uninstall. Look for any of the following commands and remove these commands. Recompile the QSTRUP program if it was changed by removing any of the following commands:

```
COURAGENT/ENDPMM - PMM for OS/400 End TCP Server
COURAGENT/PMMCFCG - PMM for OS/400 Configuration
COURAGENT/PMMPRG - PMM for OS/400 Message & Output Queue
Purge
COURAGENT/PMMPRTCFG - PMM for OS/400 Print Configuration
COURAGENT/PMMPRTMSG - PMM for OS/400 Print Message Queue
COURAGENT/STRPMM - PMM for OS/400 Start TCP Server
```

For more information on commands and keywords, see [“Using OS/400 PMM Agent Commands and Keywords” on page 214](#).

Deleting Product Library and User Profiles

Remain signed on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL authorities and perform the following actions:

1. Clear the PMMOUTQ and PMMMSGQ entries:

```
CLROUTQ COURAGENT/PMOUTQ
```

```
CLRMSGQ COURAGENT/PMMSGQ
```

2. Delete the COURAGENT Product Library:

```
DLTLIB COURAGENT
```

3. Delete the two .jar files and one IFS directory:

```
RMVLNK OBJLNK('/couragent/os400.jar')
```

```
RMVLNK OBJLNK('/couragent/pmm400.jar')
```

```
RMVDIR DIR('/couragent')
```

4. Delete any user profiles created in the install process:

```
DLTUSRPRF USRPRF(COURAGSEC)
```

```
DLTUSRPRF USRPRF(COURAGENT)
```

5. Sign-off as QSECOFR

6. The PMM for OS/400 has now been removed from the system.

Configuring the Connector for IBM i

The connector for IBM i (OS/400, i5/OS) Systems supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

This connector requires the IBM OS/400 agent on the IBM i system. Installing the agent is explained later in this chapter.

An OS/400 privileged account needs to share the same authorities as those accounts it uses as models for an Account Create or Add action. It needs these authorities to create accounts with the same authorities. You enter the username for the privileged account during target configuration.

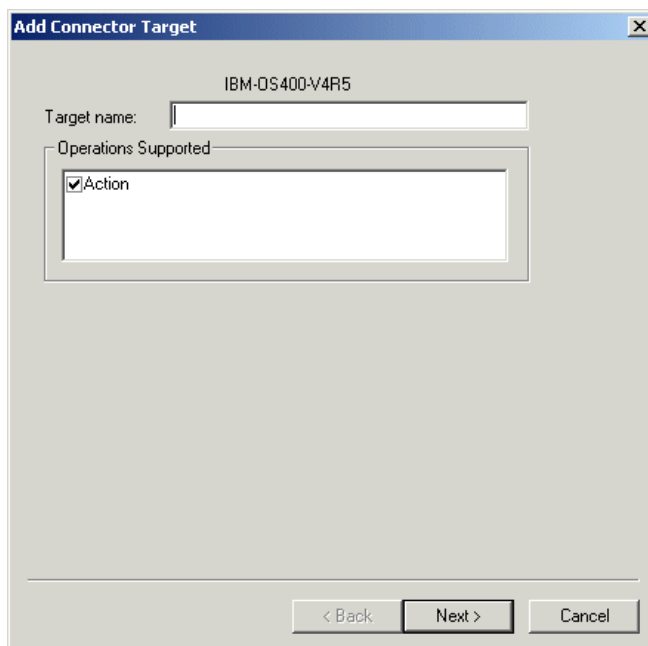
Connector Configuration

Follow these steps to add a target:

1. From the Start menu, select:
Programs >Core Security Core Server>Connector Configuration Manager
2. Select IBM-OS400-V4R5
3. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 94: Add OS/400 Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

5. Select **ACTION** to enable all operations on the target.
6. Click Next. The Connector Configuration Manager for IBM OS/400 dialog box appears.

Figure 95: Connector Configuration Manager for IBM OS/400

7. Enter the following information about the target:
 - a. **OS/400 SYSTEM** — The fully-qualified domain name or IP address of the OS/400 system where the agent is running.
 - b. **TCP/IP PORT** — The port on the OS/400 system where the agent is running.
 - c. **TIMEOUT (SECONDS)** — The length of time, in seconds, that the OS/400 system waits for communications from the Connector Framework before it times out the connection.
 - d. **PRIVILEGED USERNAME** — The name of the privileged user in the OS/400 database. The username you enter must have the appropriate authorities associated with the privileged account. Any attempt to create a user profile with authorities that the privileged user does not possess fails.
 - e. You must check **ALLOW MODELING OF ADMINISTRATIVE ACCOUNTS** to allow users to create accounts based on administrative accounts.
 - f. **PASSWORD** — The password on the target system of the privileged user.
 - g. **ALLOW MODELING OF ADMINISTRATIVE ACCOUNTS** — Allow users to create new accounts by modeling an existing account with administrative privileges. The minimum privilege that characterizes an administrative account on OS/400 is ALLOBJ or AUDIT or IOSYSCFG or JOBCTL or SAVSYS or SERVICE or SPLCTL or SECADM.
8. Click the **FINISH** button.

The target is now available for each action supported by this connector.

Notes

If you set the IBM i “Job Description” attribute to Ignore in the Administration Manager, then you must set the “Job Description Library” attribute to Ignore also.

Installing and Configuring the Connector Agent

This section describes how to install, configure, start, stop, and uninstall the connector agent.

Select the OS/400 agent SAVF file (couramm.savf) that corresponds to your version of OS/400 (iSeries).

iSeries 7.1: <install drive>:\<install folder>\Courion Corporation\iSeries 7.1\AMM
 OS/400 V5RM10: <install drive>:\<install folder>\Courion Corporation\OS400 V5RM10\AMM
 OS/400 V5R4: <install drive>:\<install folder>\Courion Corporation\OS400 V5R4\AMM
 OS/400 V4R5: <install drive>:\<install folder>\Courion Corporation\OS400\AMM

Installing the Connector Agent

The Connector for IBM OS/400 requires the IBM OS/400 agent on the IBM OS/400 system. If you have already installed the Connector for OS/400 agent, you do not need to install it now

Note: To upgrade or re-install the OS/400 Connector agent, you must uninstall it first, as explained in [“Uninstalling the OS/400 Connector Agent” on page 240](#).

The user profile used in this install process needs to have *SECADM and *ALLOBJ special authorities. Core Security recommends using QSECOFR during the installation process.

To install the Connector Agent for OS/400:

1. Sign on to the AS/400 as QSECOFR or a user profile with *ALLOBJ and *SECADM authority.
2. Bring up a Command Entry screen by typing:

```
CALL QCMD
```

3. Establish new user profiles before installing the product library.

Create the following user profiles:

COURAMM

This profile owns all the objects provided and is the user profile which runs the Connector Agent for OS/400.

```
CRTUSRPRF USRPRF (COURAMM)
          PASSWORD (some-password)
          USRCLS (*USER)
          LMTCPB (*NO)
          TEXT ('AMM for OS/400 Object Owner/Group
          Profile')
          SPCAUT (*USRCLS)
          HOMEDIR ('/couramm')
```

The following messages display:

```
Special authorities granted *NONE
User profile COURAMM created
```

COURAMMSC

This profile has *SECADM and *ALLOBJ special authorities and is the privileged user profile under which the Java SSL AMM Agent runs. The COURAMMSC user profile is optional if an existing "Security Officer" user profile is being used for password resets.

```
CRTUSRPRF USRPRF(COURAMMSC)
          PASSWORD(some-password)
          USRCLS(*SECOFR)
          INLMNU(*SIGNOFF)
          LMTCPB(*NO)
          TEXT('AMM Agent for OS/400 Security Officer')
          SPCAUT(*USRCLS)
          PWDEXPITV(*NOMAX)
          GRPPRF(COURAMM)
          OWNER(*GRPPRF)
```

The following messages display:

```
Special authorities granted *ALLOBJ *AUDIT *IOSYSCFG
*JOBCTL *SAVSYS *SECADM *SERVICE *SPLCTL.
User profile COURAMMSC created.
```

4. Grant temporary authority.

The COURAMM user profile temporarily needs authority to the RSTLIB and RST commands. Temporarily grant authority to RSTLIB and RST commands to COURAMM to perform product restore operations.

```
GRTOBJAUT OBJ(RSTLIB) OBJTYPE(*CMD) USER(COURAMM)
AUT(*USE)
GRTOBJAUT OBJ(RST) OBJTYPE(*CMD) USER(COURAMM) AUT(*USE)
```

5. Sign-off as QSECOFR or the user ID used to create the previous user profiles.

6. Use FTP to send the .savf file to the AS/400 system.

7. Sign on to the AS/400 system as COURAMM.

Note: Issue the FTP, RST and RSTLIB commands below under the COURAMM user profile. The system does not be set up correctly if you sign-on as QSECOFR.

8. Create a save file in QGPL:

```
CRTSAVF QGPL/COURAMM
```

The extracted AS/400 programs are delivered in a *SAVF file and must be uploaded to the AS/400 system.

9. Copy the COURAMM.savf file from the Core Server install directory (OS400/AMM sub-folder) to the root directory of C:\

10. Using FTP, enter the following commands from the PC where the COURAMM.savf is stored and perform the following steps:

```
FTP myAS400ipAddress
User: COURAMM
Password: (COURAMM password)
cd QGPL
```

```
lcd C:\
binary
put COURAMM.savf COURAMM
bye
```

11. Restore the product library.

On the AS/400, issue these restore commands (signed on as COURAMM):

```
RSTLIB SAVLIB (COURAMM) DEV (*SAVF) SAVF (QGPL/COURAMM)
OUTPUT (*PRINT)
```

12. Execute the Connector for OS/400 Install Program. It deletes the QGPL/ COURAMM save-file and revokes *PUBLIC authority to the product library COURAMM.

```
CALL COURAMM/INSTALLAMM
```

13. Now that the Connector Agent for OS/400 is installed, remove the temporary authority that was granted to the RSTLIB and RST commands.

- a. Sign-off as the user COURAMM.
- b. Sign-on again as QSECOFR or a user profile with *ALLOBJ and *SECADM authority.
- c. Revoke the authority that had been given to COURAMM to restore objects:


```
RVKOBJAUT OBJ (RSTLIB) OBJTYPE (*CMD) USER (COURAMM)
AUT (*ALL)
RVKOBJAUT OBJ (RST) OBJTYPE (*CMD) USER (COURAMM) AUT (*ALL)
```
- d. Update the COURAMM user profile adding the default menu and output queue.


```
CHGUSRPRF USRPRF (COURAMM) INLMNU (COURAMM/AMMMNU)
OUTQ (COURAMM/AMMOUTQ)
```
- e. Sign-off as QSECOFR.

Authority Delivered with the OS/400 Connector Agent

For security reasons, the Connector Agent for OS/400 Product Library is delivered with COURAMM *ALL and *PUBLIC *EXCLUDE library authorities. This authority only allows COURAMM or an AS/400 Security Officer into the Connector Agent for OS/400 Product Library to execute commands or bring up the AMMMNU.

To correct this authority problem, grant QPGMR *USE authority to the COURAMM library and the COURAMM user profile. This gives QPGMR the minimum authority needed to run the STRAMM command from the QSTRUP job during IPL.

Sign-on as QSECOFR or a user profile with *SECADM and *ALLOBJ special authorities and enter these commands:

```
GRTOBJAUT OBJ (COURAMM) OBJTYPE (*LIB) USER (QPGMR)
AUT (*USE)

GRTOBJAUT OBJ (COURAMM) OBJTYPE (*USRPRF) USER (QPGMR)
AUT (*USE)
```

QPGMR now has sufficient authority to start the Connector Agent for OS/400 STRAMM command in the QSTRUP job during IPL.

The user profile QPGMR must have *USE authority to the library and to the user profile COURAMM.

OS/400 Connector Agent Menu

After installing the connector agent for OS/400 installed, you can configure it. You can display Help text by pressing F1.

1. On the AS/400, sign on as COURAMM and enter the following command:

```
GO COURAMM/AMMNNU
```

The AMM (Connector) Agent for OS/400 Menu appears, as shown in [Figure 96](#).

Figure 96: AMM (Connector) Agent for OS/400 Menu

```

AMMNNU                AMM Agent for OS/400 Menu                System:  ELVIS
Select one of the following:

  1. Start AMM Agent for OS/400
  2. End AMM Agent for OS/400
  3. Configure AMM Agent for OS/400
  4. Maintain Excluded Profiles
  5. Purge Message and Output Queues
  6. Print Configuration Files
  7. Print Message Queue
  8. Display Message Queue
  9. Display Output Queue

 99. Sign Off

Selection or command
==>

F1=Help  F3=Exit  F4=Prompt  F9=Retrieve  F12=Cancel
COPYRIGHT (C) 2003 COURION CORPORATION.

```

You can run the following commands from the (Connector) AMM Agent for OS/400 Menu command line:

- Start AMM Agent for OS/400
- End AMM Agent for OS/400
- Configure AMM Agent for OS/400
- Purge Message and Output Queues
- Print Configuration Files
- Print Message Queue

Note: After you enter a command, a status message appears at the bottom of the menu screen.

Configuring the OS/400 Connector Agent

To configure the agent:

- From the AMM for OS/400 menu ([Figure 96](#)), select option 3: **CONFIGURE AMM AGENT FOR OS/400**.

If entering COURAMM/AMMCFG from the command line, enter the value COURAMM for the keyword pmmlib when prompted. The AMM Agent for OS/400 Configuration (AMMCFG) menu appears as in [Figure 97](#).

Figure 97: AMM (Connector) Agent for OS/400 Configuration (AMMCFG) Screen 1

```

          Configure AMM Agent for OS/400 (AMMCFG)

Type choices, press Enter.

Library where installed . . . . > COURAMM      Name
Subsystem name . . . . . QSYSWRK              Name
Library . . . . . QSYS                        Name
Job queue name . . . . . QSYSNOMAX            Name
Library . . . . . QSYS                        Name
TCP Port . . . . . 08182                      1024-65535
#Days to keep before purge . . . 07            01-99

F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys
Current values could not be retrieved.

MP a MW 11/037

```

- Change the subsystem name, subsystem library name and job queue to what is appropriate on the system being used. The default is the subsystem QSYS/QSYSWRK, job queue QSYS/QSYSNOMAX.

Note: By default, the TCP Port is 8192. If you change this port, remember to change the port specified in the Connector Configuration Manager for IBM OS/400.

Note: You can Press F10 to view more configuration items ([Figure 98](#)).

Figure 98: AMM (Connector) Agent for OS/400 Configuration (AMMCFG) Screen 2

```

Configure AMM Agent for OS/400 (AMMCFG)

Type choices, press Enter.

Class path . . . . . '1.:QIBM/ProdData/Java400/jt400ntv.jar:/cou
ramm/amm400.jar:/couramm/os400.jar:/QIBM/ProdData/HTTP/Public/jt400/lib/jt400.ja
r:/QIBM/ProdData/HTTP/Public/jt400/lib/data400.jar:/QIBM/ProdData/HTTP/Public/jt
400/lib/x4j400.jar'
Java version . . . . . '1.2'          Character value
Object Owner . . . . . COURAMM        Name
Admin User Authority . . . . . *SECADM  *SECADM, *ALLOBJ, *SPLCTL...
      + for more values

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F12=Cancel  F13=How to use this display
F24=More keys

MM  a                                     05/037

```

Note: The Java version entered in the configuration screen should match the JVM version installed with the Java Programmer's Toolkit on the system. The Connector Agent for OS/400 may fail to start if the Java™ version does not match.

Starting the OS/400 Connector Agent

From the AMM (another term for Connector) for OS/400 menu ([Figure 96](#)), select option 1: **START AMM AGENT FOR OS/400**. This submits the AMM Agent for OS/400 to the job queue specified in the configuration. The Start AMM Agent for OS/400 (STRAMM) start menu appears as in [Figure 99](#)

Figure 99: AMM (Connector) Agent for OS/400 Start Menu

```

Start AMM Agent for OS/400 (STRAMM)

Type choices, press Enter.

Enable trace? . . . . . *NO          *NO, *YES

Bottom
F3=Exit  F4=Prompt  F5=Refresh  F10=Additional parameters  F12=Cancel
F13=How to use this display  F24=More keys

MM  a          MM          A                                     05/037

```

The option **ENABLE TRACE?** is set to *NO by default, which is the correct setting in most situations.

Note: Do not set the Enable Trace option to *YES unless instructed to do so by Core Server Technical Support staff.

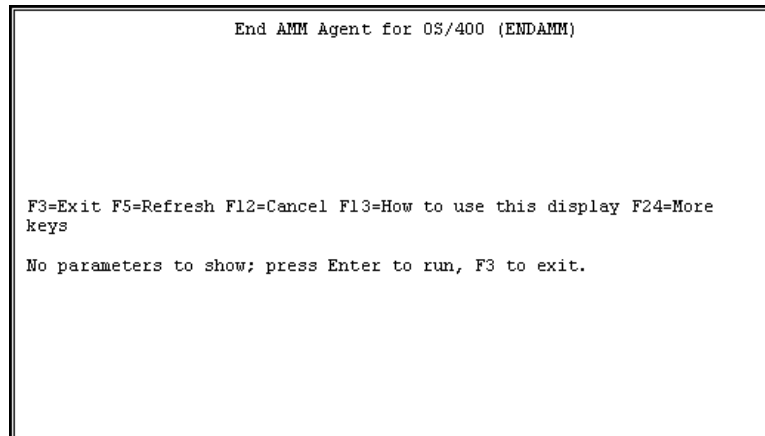
If the Connector Agent for OS/400 is started with ETRACE(*YES), then about 2200 resets can be issued before the spool file QPRINT fills up. When it is full, the message CPA4072 "Reached maximum number of spooled records for file QPRINT in library QGPL. (C R NOMAX 1-999999)" is issued to the system operator (QSYSOPR) message queue. At this point, the agent does not respond and waits for the spool file issue to be resolved. Once the system operator answers the message, the agent terminates. You must then restart it.

Stopping the Agent

To stop the Connector Agent for OS/400:

1. Sign-on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL special authorities. If you are working from a PC and not the OS/400 console, you need access to a 5250-emulation session.
2. From the AMM Agent for OS/400 menu ([Figure 96](#)) select option 2 **END AMM AGENT FOR OS/400**. The screen in [Figure 100](#) appears.

Figure 100: AMM (Connector) Agent for OS/400 End



3. Press Enter to stop the agent.
4. Log out of the AMM agent menu. To confirm that the agent is no longer active, run the following command:

```
WRKUSRJOB USER(COURAMM) STATUS (*ACTIVE)
```

5. The AMM Agent for OS/400 Active Jobs screen appears with no active jobs as in [Figure 101](#).

Figure 101: AMM (Connector) Agent for OS/400 Active Jobs Screen

```

                                Work with User Jobs                                A2TTEST
                                                                                   16/05/03 11:47:43

Type options, press Enter.
2=Change  3=Hold  4=End  5=Work with  6=Release  7=Display message
8=Work with spooled files  13=Disconnect

Opt Job      User      Type      -----Status-----  Function
  (No jobs to display)

Parameters or command
====>
F3=Exit      F4=Prompt  F5=Refresh  F9=Retrieve  F11=Display schedule data
F12=Cancel   F17=Top      F18=Bottom  F21=Select assistance level

```

Uninstalling the OS/400 Connector Agent

To uninstall the agent, sign on as QSECOFR or as a user with security officer privileges on the AS/400. The security officer must have *SECADM, *ALLOBJ, and *SPLCTL special authorities. It is also necessary to have access to a 5250-emulation session.

Stopping the Agent

Before you uninstall the OS/400 agent, you must stop it. See [“Stopping the Agent” on page 239](#) for information about how to do this.

Remove Agent Commands

If any Connector Agent for OS/400 commands have been added to the QSTRUP program or to the OS/400 Job Scheduled (WRKJOBSCDE), then remove these entries before proceeding with the uninstall. Look for any of the following commands and remove these commands. Recompile the QSTRUP program, if it was changed for removing any of the following commands:

COURAMM/ENDAMM - AMM for OS/400 End TCP Server

COURAMM/AMMCFG - AMM for OS/400 Configuration

COURAMM/AMMPRG - AMM for OS/400 Message & Output Queue Purge

COURAMM/AMMPRTCFG - AMM for OS/400 Print Configuration

COURAMM/AMMPRTMSG - AMM for OS/400 Print Message Queue

COURAMM/STRAMM - AMM for OS/400 Start TCP Server

Deleting Product Library and User Profiles

Remain signed on as QSECOFR or a user profile with *ALLOBJ, *SECADM, and *SPLCTL authorities. To confirm that there are no locks on the COURAMM library, enter the following command:

```
WRKOBJLCK OBJ(COURAMM) OBJTYPE(*LIB)
```

Remove any active locks attributed to COURAMM before proceeding with the uninstall.

Follow these steps:

1. Clear the AMMOUTQ and AMMSGQ entries:

```
CLROUTQ COURAMM/AMMOUTQ  
CLRMSGQ COURAMM/AMMSGQ
```

2. Delete the COURAMM Product Library:

```
DLTLIB COURAMM
```

3. Delete the two .jar files, a CSV file, and one IFS directory:

```
RMVLNK OBJLNK('/COURAMM/os400.jar')  
RMVLNK OBJLNK('/COURAMM/amm400.jar')  
RMVLNK OBJLNK('/COURAMM/AMMPRFCSV')  
RMVDIR DIR('/COURAMM')
```

4. Delete any user profiles created in the install process:

```
DLTUSRPRF USRPRF(COURAMMSC)  
DLTUSRPRF USRPRF(COURAMM)
```

5. Sign-off from the 5250 session signed on as QSECOFR.

The AMM (connector) for OS/400 removed from the system.

Chapter 23: Imprivata OneSign — Connector

This chapter explains how to configure the Connector for Imprivata OneSign™:

- [*“Configuring the Connector for Imprivata OneSign” on page 244*](#)

Configuring the Connector for Imprivata OneSign

The Connector for Imprivata OneSign™ integrates the Core Security Core Server with Imprivata OneSign Enterprise Single Sign On (ESSO). This provides the Core Server with the following beneficial functions:

- New users provisioned with the Core Security Core Server are also automatically added as Subscribers in Imprivata OneSign.
- Users provisioned with additional resources have their credentials for these resources added as accounts within Imprivata OneSign and associated with the appropriate Subscriber.
- Users provisioned as noted above experience day 1 ESSO through Imprivata OneSign without having to register credentials for each application.
- Users deprovisioned (terminated or disabled) through the Core Security Core Server are automatically removed (or disabled) within Imprivata OneSign.
- During an initial rollout of Imprivata OneSign, you can use the Core Security Core Server to automatically register all existing enterprise users and their applications within Imprivata OneSign by leveraging this connector during password reset operations.

The Connector for Imprivata OneSign is implemented to support trigger capabilities. It exposes the following triggers:

- `ProvisionOneSignUser` — Adds the user as a OneSign Subscriber
- `AddImprivataCredential` — Adds application credentials to a OneSign user, enabling ESSO for that user and application.
- `ModifyImprivataPassword` — Updates Imprivata accounts with new passwords, preserving seamless ESSO despite external password changes. This object also allows for creating Subscribers and accounts if they do not already exist.
- `DeleteImprivataAccountMapping` — Removes application credentials from a OneSign user, disabling ESSO for that user's application.
- `DeleteImprivataAccount` — Removes a OneSign Subscriber and all associated accounts.

The Connector for Imprivata OneSign can send a trigger to a target, based on the results of the following actions: Add, Create, Change, and Delete.

Prerequisites

There are two prerequisites for configuring the Connector for Imprivata OneSign:

- You need to configure the Courion Provisioning System Adaptor in the OneSign Administrator.
- You need to install the root certificate from the OneSign CA on each server in which the Connector Framework is installed. Core Security also recommends that you install the root certificate on the server in which the Connector Framework

Manager is installed. If the certificate is not installed on the CFM, you receive a validation error when you configure the connector (although the connector still functions correctly as long as it properly configured).

Courion Provisioning System Adaptor Configuration

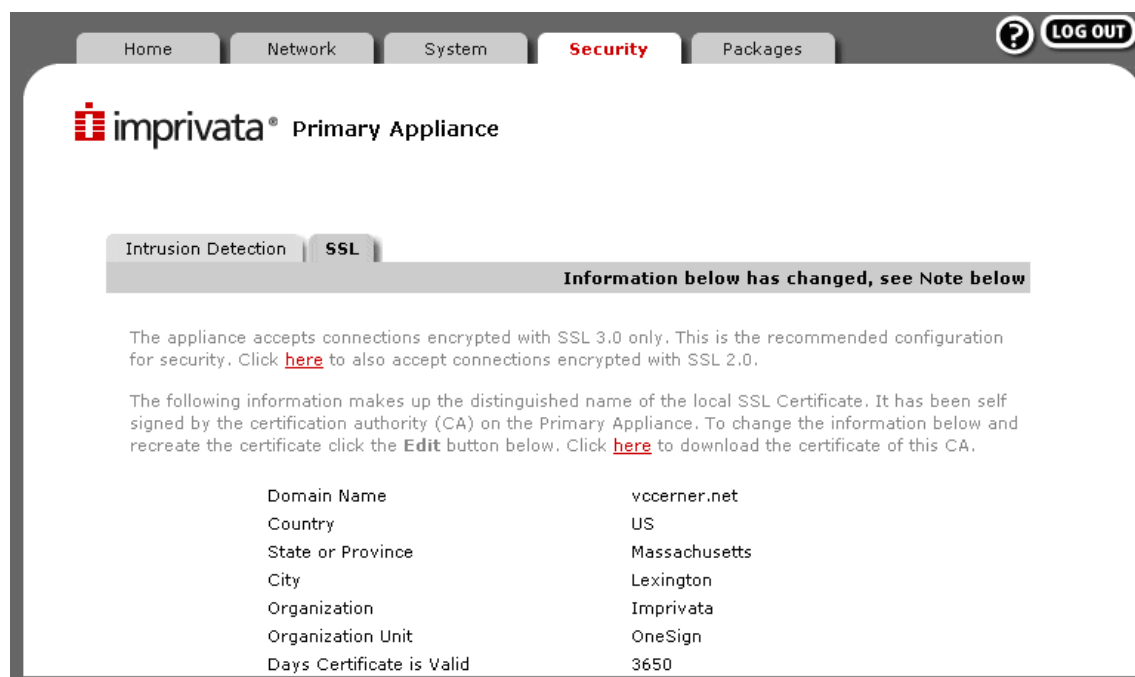
These tasks should be performed by a OneSign Administrator familiar with the OneSign administration interface.

1. Log into the OneSign Administrator
2. Select the "ESSO" tab
3. Select the "Provisioning" tab
4. Select the "Courion" adaptor
5. Enable the adaptor and set the "Provisioning System Hostname or IP Address" to the fully qualified domain name or IP address of the Connector Framework server.

Installing the Root OneSign CA Certificate

1. Download the root certificate
 - a. Log into the OneSign Appliance Administrator
 - b. Select the "Security" tab
 - c. Select the "SSL" tab (as shown in [Figure 102](#)).
 - d. Click "Click here to download the certificate of this CA" link
 - e. Save certificate file and copy to Connector Framework Server

Note: As mentioned in the Product Requirements section, Core Security recommends that you also copy the certificate to the Connector Framework manager server. repeat the following steps for each server in which the Connector Framework or Connector Framework Manager is installed.

Figure 102: Imprivata Certificate Download

2. Install the certificate in Local Computer "Trusted Root CA" store (on the Connector Framework Server)
 - a. Create Local Computer Certificates MMC
 - b. Type "mmc" at the command prompt
 - c. Ctrl + M
 - d. Click "Add"
 - e. Select "Certificates" Snap-In
 - f. Click "Add"
 - g. Select "Computer account"
 - h. Click "Next", "Finish", "Close", "Ok"
3. Import Certificate
 - a. Expand "Certificates" node
 - b. Expand "Trusted Root Certification Authorities" node
 - c. Right-click "Certificates" node
 - d. Select "All Tasks" > "Import"
 - e. Navigate to certificate file downloaded from OneSign
4. Install certificate in CourionService "Trusted Root CA" store (on Connector Framework Server)
 - a. Create CourionService Certificates MMC
 - i. Type "mmc" at the command prompt
 - ii. Ctrl + M
 - iii. Click "Add"
 - iv. Select "Certificates" Snap-In
 - v. Click "Add"

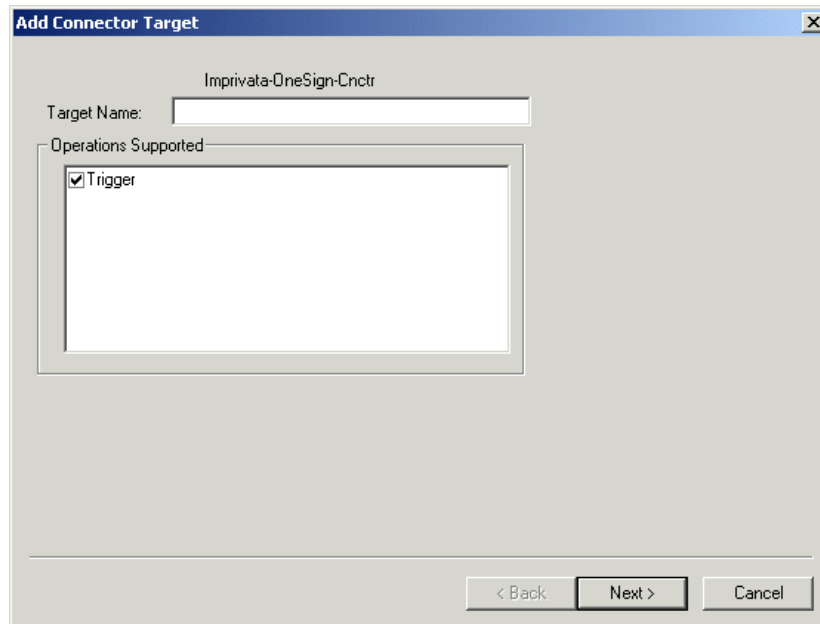
- vi. Select "Service account"
- vii. Click "Next", "Next"
- viii. Select "CourionService"
- ix. Click "Finish", "Close", "Ok"
- b. Import Certificate
 - i. Expand "Certificates" node
 - ii. Expand "Trusted Root Certification Authorities" node
 - iii. Right-click "Certificates" node
 - iv. Select "All Tasks" > "Import"
 - v. Navigate to certificate file downloaded from OneSign

Connector Configuration

Follow these steps to add the Connector for Imprivata OneSign and then add a target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **IMPRIVATA-ONESIGN-CNCTR**, and click **OK**.
3. Select **IMPRIVATA-ONESIGN-CNCTR**
4. Right click on Imprivata-OneSign-Cnctr and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 103: Add Imprivata OneSign Target



5. Enter a name (alias) for the target in the Target Name text box. This name identifies the target in the Administration Manager interface.
6. The only supported operation is Trigger, selected by default. Click **NEXT**.

The Connector Configuration Manager for Technology Connector screen appears.

Figure 104: Connector Configuration Manager for Imprivata OneSign

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **ExtSysName** — Enter the value "Courion" in a default OneSign implementation. ExtSysName is the Provisioning System Adaptor name found in the OneSign Administrator under ESSO > Provisioning.
 - **OneSignURL** — Enter the value "https://[OneSign Server Name]/sso/provision/spmlrouter" in a default OneSign implementation. The value can be tested in a web browser and should return the following message: "Error: com.imprivata.spml.SoapRouter: GET is unsupported".

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Configuring the Trigger

Configuration of a trigger is dependent on the specifics of your environment. Core Server and Imprivata can assist in determining the optimal configuration for a specific environment. The following example is broken down by objects exposed by the Connector for Imprivata OneSign:

- Use Active Directory for the Subscriber's credentials.
- Each time a new user is provisioned, they get (at minimum) an Active Directory account. These credentials are used by the Connector for Imprivata OneSign to create a Subscriber on the OneSign appliance.
- In the workflow you use to create a new account, configure a trigger to fire on Resource Success for the Create action of the account you want to link to Imprivata OneSign. This is normally the Active Directory account, but may also be an LDAP directory entry.

Note: Create a OneSign Subscriber each time a new user is provisioned through the Core Security Core Server.

Table 14 shows the attributes to be configured in this example:

Table 14: Configurable Attributes Used for Account Create Trigger to OneSign

Attribute	Description
DomainID	This is provided by the OneSign administrator and indicates to Imprivata OneSign which domain the new user is added to.
OSUsername	This is the username for the new OneSign user. You may use a Core Server macro to determine this and normally it corresponds to the username of the Active Directory account that is being provisioned by Core Server.
OSPassword	The password for the new OneSign user. This is a macro that corresponds to the password of the Active Directory account being created.
FirstName	The first name for the new OneSign user.
LastName	The last name for the new OneSign user.
EmailAddress	The email for the new OneSign user (optional).
profileUID	A unique identifier for the new OneSign user.
userDisabled	A value of "true" or "false," which indicates whether the new OneSign user is created in the disabled state or not.

Chapter 24: Kronos Workforce Central — PMM and Connector

Please contact Customer Support to get the newer connector used to integrate to Kronos Workforce Central. There is the Connector for Kronos Workforce Central WIM and the PMM for Kronos Workforce Central WIM. These should be used instead of this connector and PMM that is available in the suite installation kit.

This chapter explains how to configure the PMM and Connector for Kronos Workforce Central®:

- [*“Configuring the PMM for Kronos Workforce Central” on page 252*](#)
- [*“Configuring the Connector for Kronos Workforce Central” on page 255*](#)

Configuring the PMM for Kronos Workforce Central

The Password Management Module (PMM) for Kronos Workforce Central enables end users to automatically reset passwords on Kronos Workforce Central systems.

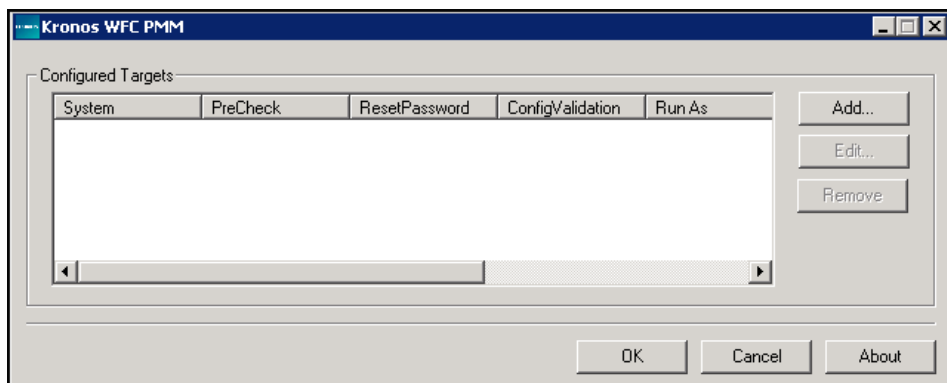
Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. For the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>Kronos Workforce Central
2. Click **YES** to start the PMM Configuration Manager.
The PMM Configuration Manager dialog box appears.

Figure 105: PMM Configuration Manager for Kronos Workforce Central



3. From this dialog box, you can:
 - Obtain the product version number. Click the **ABOUT** button.
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button or double click on the target name.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 106: Add/Edit Target Configuration for Kronos Workforce Central

Add / Edit Target Configuration

Target Name: Kronos2

PreCheck Command Line: cscript /b /nologo PMMRDK2AMMRDKRedirect.js

ResetPasswordEx Command Line: cscript /b /nologo PMMRDK2AMMRDKRedirect.js

ConfigValidation Command Line: cscript /b /nologo PMMRDK2AMMRDKRedirect.js

☐ Run Commands as User

Domain\User:

User Password:

Configure Parameters for System

Parameter: Value: Verify Value:

☐ Secure Attribute

Configured Parameters:

Name	Value
AdminPassword	XXXXXXXXXX
AdminUsername	SuperUser
RequestTypesFile	KronosRequestTypes...
ScriptName	KronosCnctr.js
URL	http://10.1.1.235/wfc/...

OK Cancel

4. **TARGET NAME** — Enter the Target name for the Kronos Workforce Central system. You need to use this same name when you configure the target in the PMM Gateway Connector configuration. Core Security recommends that you use the same name as the one used for the connector for Kronos Workforce Central.

Note: You cannot edit the name of an existing target.

5. **PRECHECK, RESETPASSWORD, and CONFIGVALIDATION COMMAND LINE** — Enter cscript /b /nologo PMMRDK2AMMRDKRedirect.js for all three parameters.
6. Leave the **RUN COMMANDS AS USER** checkbox unchecked.
7. Select the appropriate configuration parameters from the drop down menu, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the Add button. The following parameters are available:
 - **AdminUsername** — Kronos Workforce Central server administrator user name. This identifies the user whose access rights are validated for each request. For a request to succeed, the user name must have the correct access rights. The user name "Super Access" has complete access rights for all XML tags. This user name improves performance because Workforce Central does not validate the access rights for each request.
 - **AdminPassword** — The password for the administrative user.
 - **URL** — Kronos Workforce Central URL. For example, http://10.1.1.235/wfc/XmlService
 - **RequestTypesFile** — Name of the file to use to generate and parse WebService requests and responses. Unless you have a custom request types file, use KronosRequestTypes.xml

- **ScriptName** — Enter KronosCnctr.js

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("**") for security.

8. Click **OK** to save the changes and exit from the PMM Configuration Manager.

The configuration of a Kronos Workforce Central PMM target is complete.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the Connector for Kronos Workforce Central

The Connector for Kronos Workforce Central® supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

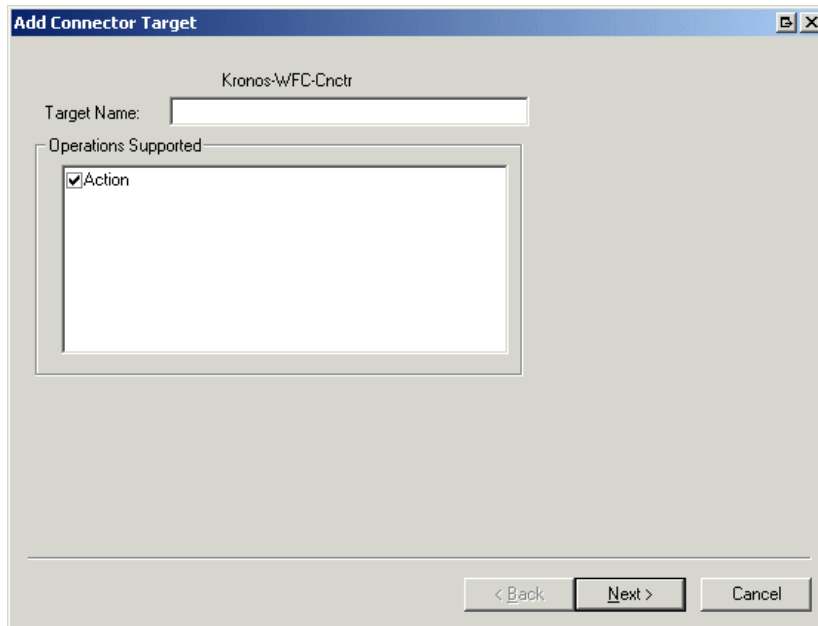
Connector Configuration

Follow these steps to add a Kronos Workforce Central target:

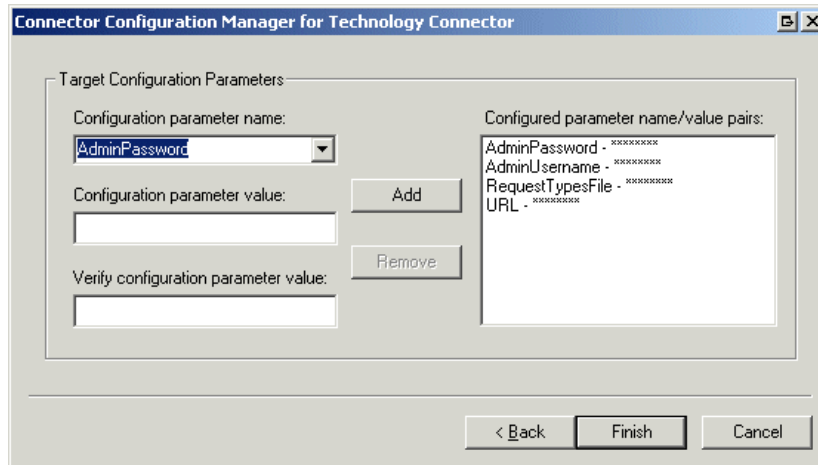
1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **KRONOS-WFC-CNCTR**, and click **OK**.
3. Select **KRONOS-WFC-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 107: Add Kronos Workforce Central Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. **ACTION** is selected by default, to enable all operations on the target. Click **NEXT**.
The Connector Configuration Manager dialog box appears.

Figure 108: Connector Configuration Manager for Kronos Workforce Central

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

- **AdminUsername** — Kronos Workforce Central server administrator user name. This identifies the user whose access rights are validated for each request. For a request to succeed, the user name must have the correct access rights. The user name "Super Access" has complete access rights for all XML tags. This user name improves performance because Workforce Central does not validate the access rights for each request.
- **AdminPassword** — The password for the administrative user.
- **URL** — Kronos Workforce Central URL. For example, `http://10.1.1.235/wfc/XmlService`
- **RequestTypesFile** — Name of the file to use to generate and parse WebService requests and responses. Unless you have a custom request types file, use `KronosRequestTypes.xml`

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 25: Microsoft Active Directory — PMM and Connector

This chapter explains how to configure the PMM and Connector for Microsoft Active Directory® directory service:

- [*“Configuring the PMM for Microsoft Active Directory” on page 258*](#)
- [*“Configuring the Connector for Microsoft Active Directory” on page 266*](#)

Configuring the PMM for Microsoft Active Directory

The Password Management Module (PMM) for Microsoft Active Directory directory service enables end users to reset passwords automatically on an Active Directory domain. You can define multiple PMM for Microsoft Active Directory targets in a password management workflow to synchronize password resets in a multiple domain or Active Directory Forest environment.

This PMM uses Active Directory Services Interfaces (ADSI) calls as an integration tool instead of LAN Manager calls which are used by the PMM for Windows NT and Windows 2000. Using ADSI enables you to specify a privileged user on the Active Directory domain with the following privileges: Change password, Reset password, Read/Write “userAccountControl,” Read/Write account restrictions, and Read group membership. Using LAN Manager calls requires the privileged user to be a member of the Account Operators group or Administrators group.

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Security.

Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Security Options for Active Directory

The Active Directory PMM supports the following security options:

[“Allow Reset of Administrative Accounts”](#)
[“Force User To Change Password at Next Logon”](#)
[“Conform to System Password History”](#)
[“Conform to System Minimum Password Age”](#)

Allow Reset of Administrative Accounts

This option enables you to specify whether or not the PMM for Active Directory resets passwords for users that are members of the following groups:

Account Operators Group
Administrators Group
Backup Operators Group
Cert Publishers Group
Domain Admins Group
Enterprise Admins Group
Group Policy Creator Owners Group
Incoming Forest Trust Builders Group
Network Configuration Operators Group

Print Operators Group
Schema Admins Group
Server Operators Group

The PMM for Active Directory does not reset passwords for disabled or expired accounts.

To select this option, see **ALLOW RESET AND UNLOCK OF ADMINISTRATIVE ACCOUNTS** on page 262.

Force User To Change Password at Next Logon

This option enables you to specify whether or not to force end users to change their passwords the next time they log into the system after performing a password reset with Core Password.

Note: **USER CANNOT CHANGE PASSWORD** must not be set on accounts when **FORCE USER TO CHANGE PASSWORD AT NEXT LOGON** is selected.

To select this option, see **FORCE USER TO CHANGE PASSWORD AT NEXT LOGON** on page 262.

Conform to System Password History

The **CONFORM TO SYSTEM PASSWORD HISTORY** option forces Core Password to check the native operating system setting for password history or password uniqueness before it resets the password.

The password history setting determines the number of unique new passwords that need to be associated with an account before the user can re-use an old password. When PasswordCourier resets a password on the native operating system, it actually performs a double password reset with a randomly generated password in addition to a user-specified password to ensure system security. Because of this, you need to specify a value that is double the number of unique password resets you want to associate with a user account when you configure the password history setting on the native operating system.

Without this option, the PMM for Active Directory does not compare a new password against the password history.

To maintain the effectiveness of the password history setting, use the Conform to Minimum Password Age option to prevent users from changing their passwords immediately after they were just changed.

To select this option, see **CONFORM TO SYSTEM PASSWORD HISTORY** on page 262.

Conform to System Minimum Password Age

The **CONFORM TO SYSTEM MINIMUM PASSWORD AGE** option forces Core Password to check the native operating system setting for minimum password age before it resets the password.

The minimum password age determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. The default value is 0. A value of a few days discourages rapid password recycling while still permitting users to change their own passwords.

Example: The minimum password age is set to one day. A user successfully changes his password to 3lmnop4 and attempts to reset it immediately. The attempt is unsuccessful and the system displays the following error:

The password on this account cannot be changed at this time. Password changed too recently.

The user can reset the password the next day as long as it complies with the rules for Conform to System Password History.

To select this option, see **CONFORM TO SYSTEM MINIMUM PASSWORD AGE** option on page 262.

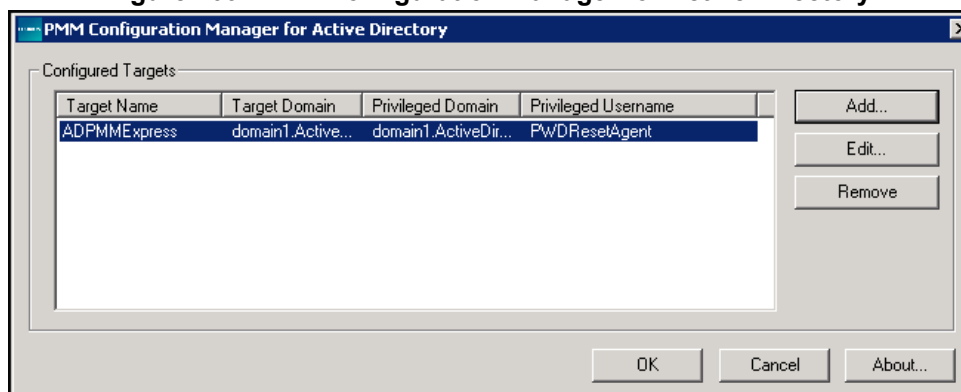
PMM Configuration

You must be logged in with the user right **LOG ON LOCALLY**.

To configure the PMM:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Password Management
Modules>Active Directory
2. Click **YES** to start the PMM Configuration Manager. The PMM Configuration Manager for Active Directory appears.

Figure 109: PMM Configuration Manager for Active Directory



3. From this dialog box, you can:
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - Obtain the product version number. Click the **ABOUT** button.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 110: Add/Edit Target Configuration for Active Directory

Add/Edit Target Configuration

Target information

Name:

Active Directory domain:

Trusted and privileged account information

Active Directory domain:

Username:

Password:

Options

☐ Allow reset and unlock of administrative accounts

☐ Unlock account only

☐ Conform to system password history

☐ Enhanced logging

☐ Conform to system minimum password age

☐ Force change password at next logon

☐ Select closest domain controller

Perform administrative logon

☒ interactively

☐ as a service

OK Cancel

The Add/Edit for Active Directory settings are used for all Active Directory password resets for the specified domain.

4. TARGET INFORMATION

- **NAME** — Enter the name of the target. (You cannot edit the name of an existing target.) You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
- **ACTIVE DIRECTORY DOMAIN** — Specify the Active Directory domain where the password resets occur. The target Active Directory domain must trust the Active Directory domain of the privileged account.

If the domain is an Active Directory domain, enter either the DNS-style name or the NetBIOS name (for example: courion.com for DNS-style domain name or courion for NetBIOS domain name).

Note: To use the DNS-style name for the Active Directory, make sure the PMM for Active Directory is running Microsoft Windows 2000 or higher.

5. TRUSTED AND PRIVILEGED ACCOUNT INFORMATION

- **ACTIVE DIRECTORY DOMAIN** — Specify the Active Directory domain of the privileged user for Active Directory password resets. The target Active Directory domain specified for Active Directory password resets must trust each of the configured password targets.

If the domain is an Active Directory domain, either enter the NetBIOS name or DNS-style name (for example: courion.com for DNS-style domain name or courion for NetBIOS domain name).

Note: To use the DNS-style name for the Active Directory, make sure the PMM for Active Directory is running on Windows 2000 or higher.

- **USERNAME** — Specify the username of the privileged user. This user must minimally have the following privileges on the target domain:

- Change password
- Reset password
- Read/Write “lockoutTime”
- Read group membership
- Read account restrictions
- Write account restrictions

Note: On Windows Server 2003, you can replace the Write account restrictions privilege with the following more specific privileges:

- Read/Write userAccountControl property of Account Restrictions
- Read/Write pwdLastSet property of Account Restrictions

Note: The privileged user you specify needs the permission to access all Organization Units (OUs) where accounts for this target may be located.

Note: The PMM configuration program does not validate that the privileged user you specify has the appropriate privileges during target creation and modification.

- **PASSWORD** — Enter the Password for the privileged user.

6. OPTIONS

- **ALLOW RESET AND UNLOCK OF ADMINISTRATIVE ACCOUNTS** — Decide whether or not to allow password resets of administrative accounts. To allow administrative resets, select this check box.
- **UNLOCK ACCOUNT ONLY** — Select this to allow the PMM to perform account unlocks alone without a password reset.
- **CONFORM TO SYSTEM PASSWORD HISTORY** — Select this enforce the native operating system user restrictions regarding password uniqueness.
- **ENHANCED LOGGING** — Select this to log the connection attempts to the ADModule.log during a password reset attempt.
- **CONFORM TO SYSTEM MINIMUM PASSWORD AGE** — Select this option to force the Access Assurance Suite application to check the native operating system setting for minimum password age before it resets the password. If you do not enable this option (or the native operating system minimum password age is set to 0), the application ignores the native operating system setting for minimum age.
- **FORCE CHANGE PASSWORD AT NEXT LOGON** — Select this to force end users to change their passwords the next time they log into the system after performing a password reset with this PMM.
- **SELECT CLOSEST DOMAIN CONTROLLER** — Select this if you want the application to unlock and reset accounts on the Domain Controller closest to the end user’s machine, rather than perform the reset on the Domain Controller that is close to the Connector Framework. (Reset on the Domain Controller close to the Connector Framework potentially requires the end user to wait until the reset is replicated to the rest of the network).

Note: The privilege “Access this computer from the network” under “User Rights Assignment” in “Local Policies” of end-user machines should be granted to the

privileged user or the Default Domain Security Settings should be enabled on the domain controllers.

7. **PERFORM ADMINISTRATIVE LOGON** — Select this to perform a password reset; the PMM must log into the Active Directory target system using the privileged account information specified.

INTERACTIVELY is the default and is intended for users who interactively use the account in the domain as well as services such as the PMM running in the background. This logon type has the additional expense of caching logon information for disconnected operations, and is therefore inappropriate.

AS A SERVICE specifies that the PMM logs into the target system as a service. This is the more secure option because only services such as the Connector Framework can access the account.

Note: If the PMM is configured on Windows Server 2008 R2, or targeted against a domain controller that is hosted on Windows Server 2008 R2, you need to select **AS A SERVICE** as the **PERFORM ADMINISTRATIVE LOGON** option.

Note: If you specify **AS A SERVICE**, the privileged account must have the “logon as a service” right assigned.

8. Click **OK** to save the changes and exit the PMM Configuration Manager.
9. If you have not identified the PMM target to the Access Assurance Suite, use the PMM Gateway connector. See [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

The configuration for the PMM for Active Directory is now complete.

Note: The PMM for Microsoft Active Directory leverages Microsoft’s ADSI programming interface. Check out this web page to learn how ADSI detects what is on the client system to determine the type of connection it makes to Active Directory. [https://msdn.microsoft.com/en-us/library/windows/desktop/aa746487\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa746487(v=vs.85).aspx)

Enabling Local Password Cache Updates on the Client Machine

Core’s ActiveX control, CourLocal, is available with this PMM. The Core ActiveX control lets an end user update the Windows domain password stored locally on the end-user’s system. This feature prevents an end-user from locking out his or her account after using the Access Assurance Suite Web Access Option to change the Active Directory or Windows NT password on the domain. For details on using CourLocal, refer to *The Core Access Assurance Suite Implementation Guide*, chapter *Web Access (ASP Page) Configuration*.

Note: Mozilla Firefox and Google Chrome may not support some Microsoft technologies such as ActiveX. If you require local password cache synchronization, Core Security recommends using one of the supported versions of Internet Explorer.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite*

Administration Manager explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Single Domain Model

When using a single domain model, the Core Access Assurance Suite is typically deployed on an Active Directory system that is a member of the domain.

1. Log on to the system as a local administrator.
2. Grant the user right **LOG ON LOCALLY** to the account. This is required so permissions and other attributes can be set.
3. Log out.
4. Log on again as the same local administrator. This activates the new rights.

Configure the PMM for Active Directory as described in [“PMM Configuration” on page 260](#).

Single or Multiple Master Domain Model

When a Master Domain model is being used, the Access Assurance Suite is typically deployed in a resource domain. The PMM for Active Directory is configured to reset passwords in the Master domain by using a delegated account from the Master domain. The example in the following section describes the steps to follow when installing in this domain model.

Note: Deploying the PMM for Active Directory in different domain models may require additional steps during installation and configuration of the Courion Server. Follow the steps for the appropriate domain model and identify a privileged account that the PMM may use when performing password resets (typically a member of the Account Operators group for the domain).

Example

Assumptions:

- Domain M is the Master domain and contains all user accounts.
- Domain R is a production domain (a resource domain) in which the Core Access Assurance Suite is installed.
- Workstation Z is a member of Domain R.
- Domain R Trusts Domain M (a one way trust).
- Admin is a local administrator of Workstation Z.
- MasterAdmin is a Domain Admin of M.
- AcctOperator is a delegated account of M. It has the right to reset passwords.

Before running the PMM Configuration Manager for Active Directory:

1. Log on to System Z as a System Z local administrator "Admin."

2. Make MasterAdmin a member of the administrator group on NT Workstation Z. The PMM for Active Directory is configured as MasterAdmin later. It is necessary to run the configuration program as a member of the Master domain (M), so account information can be verified.
3. If the Courion Server is running Windows 2000 (not Windows 2003), grant the user right **ACT AS PART OF THE OPERATING SYSTEM** for the account MasterAdmin. This right is required with Windows 2000 so the account information can be verified by the PMM configuration program.
4. Log out.
5. Log on as "MasterAdmin" to activate the new permissions.
6. Configure the Active Directory PMM.

Configuring the Connector for Microsoft Active Directory

The Connector for Microsoft Active Directory directory service supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Authentication
- Query

Connector Configuration

Follow these steps to add a Microsoft Active Directory target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **MICROSOFT-ADS-5.x**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 111: Add Active Directory Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

5. Select **ACTION** to enable these Core Provisioning actions: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

Select **AUTHENTICATION** to use the target data source for authenticating end user access to AccountCourier.

Select **QUERY** to enable Core Provisioning or Core Compliance to use queries to find data in the target data source.

6. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 112: Connector Configuration Manager for Active Directory

7. **ACTIVE DIRECTORY AUTHORIZED ACCOUNT INFORMATION** — The information in this section of the dialog box designates information about the directory server and the directory server administrator.
 - **ACTIVE DIRECTORY NAME** — Enter the name of the Active Directory server where the account management actions occur.
 - **PRIVILEGED USERNAME** — Enter the username for an account with administrator access to the Active Directory server. The username specified should be the principal name of the administrator account (username@domain.com).

The Privileged Username account needs the following permissions:

- Change Password
- Reset Password
- Read General Information
- Write General Information
- Read Group Membership
- Write Group Membership
- Read Account Restrictions
- Write Account Restrictions
- Read Logon Information
- Read all properties
- Write all properties
- Create Child Objects if adding users is part of your deployment
- Delete Child Objects if removing users is part of your deployment
- Advanced permissions, object tab:
 - Read Permissions
 - Modify Permissions

- **PASSWORD** — Enter the password for the account.
- **BIND TO SPECIFIED DOMAIN CONTROLLER** — Check this option if you want the connector to send requests to a specific domain controller in the network. If you check this box, enter the IP address or the fully-qualified domain name of the domain controller in the edit box.
- **USE ENCRYPTION** — Determines whether communication between the Connector for Microsoft Active Directory and the Active Directory target requires ADSI to use encryption for data exchange over the network.
- **SEARCH USER LOGON NAME (PRE-WINDOWS 2000)** — Select this checkbox to automatically conduct a second search on the SAMAccount field if the original search on the userPrincipalName field fails. Since accounts that existed before Windows 2000 contain a username in a different format from that contained in Active Directory, the second search captures those accounts with the earlier format for username.
- **ALLOW ACTIONS ON ADMINISTRATIVE ACCOUNTS** — Select this checkbox to allow administrator accounts to be changed, deleted, disabled, enabled, or used as a model account.
- **MAINTAIN CONNECTION** — When checked, this option pools connections to the target system for re-use, rather than opening a new connection for each operation. The option is disabled by default. Core Security recommends that you enable this option only if Server Not Operational errors occur, and you need to force the connection to stay open.
- **ALLOW FULLY QUALIFIED NAMES FOR AUTHENTICATION** — When checked, this allows a user to specify a domain name during authentication to select a domain to authenticate against.
- **HOME DIRECTORY SETTINGS** — Select the **ALLOW RETRY** checkbox to allow the connector to attempt to connect to the AD Domain controller more than once before reporting a failure. In the **NUMBER OF RETRIES** box, enter the number of retries the connector can make. In the **RETRY INTERVAL (MILLISECONDS)** box, enter the number of milliseconds to wait between retry attempts.

8. **SERVICE LOGON ACCOUNT INFORMATION** — The information in this section of the dialog box designates the user on the local workstation who is running Connector Configuration Manager and who has the following user privileges:
 - Log on as a service
 - Create and set permissions for Home Directories during provisioning.
- **DOMAIN** — Enter the name of a domain with network access.
- **USERNAME** — Enter the username for an account on the domain.
- **PASSWORD** — Enter the password for the account.
9. **SERVICE LOGON MODE:**
 - **INTERACTIVELY** — This is the default and allows users to access the account from a workstation in the domain as well as services such as the connector running in the background.
 - **AS A SERVICE** — This is the more secure option because only services such as the connector can access the account.

Note: If the connector is configured on Windows Server 2008 R2, or targeted against a domain controller that is hosted on Windows Server 2008 R2, you need to select **AS A SERVICE** as the **SERVICE LOGON MODE**.
10. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Note: The Connector for Microsoft Active Directory leverages Microsoft's ADSI programming interface. Check out this web page to learn how ADSI detects what is on the client system to determine the type of connection it makes to Active Directory. [https://msdn.microsoft.com/en-us/library/windows/desktop/aa746487\(v=vs.85\).aspx](https://msdn.microsoft.com/en-us/library/windows/desktop/aa746487(v=vs.85).aspx)

Notes and Warnings

- If a user specifies a drive letter for Home Directory Drive and fails to enter a path for Home Directory, the resource provisioning action fails.
- If the user enters a value of None for the Home Directory Drive, then the Provisioning Platform application assumes that the specified Home Directory is a local path.
- If you specify a Home Directory for the Add and Create actions, Core Provisioning creates the directory. For a Change action, if you choose to change the Home Directory attribute, Core Provisioning does not create the directory. You must create the directory manually.
- When you supply an Organizational Unit (OU) attribute in the Connector for Microsoft® Active Directory®, do not include the server suffix. For example, use ou=test rather than ou=test,dc=Courion,dc=com

- If you are using the Connector for Microsoft® Active Directory® to create a Home Directory for an Active Directory user, then the "Service Logon Account Information" user must have sufficient privileges to create the directory and assign it permissions. The privileges of the "Active Directory Authorized Account Information" user are not used for this operation.

Chapter 26: Microsoft Active Directory Application Mode (ADAM) — Connector

This chapter explains how to configure the Connector for Microsoft Active Directory® Application Mode (ADAM):

- [*“Configuring the Connector for ADAM” on page 272*](#)

Configuring the Connector for ADAM

The Connector for Microsoft Active Directory Application Mode (ADAM) supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

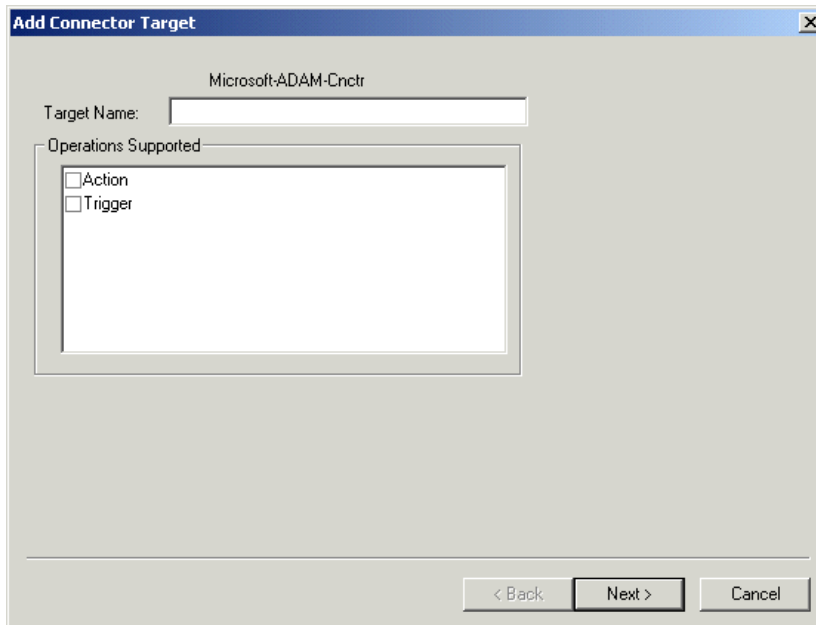
Connector Configuration

Follow these steps to add an Active Directory target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **MICROSOFT-ADAM-CNCTR**, and click **OK**.
3. Select **MICROSOFT-ADAM-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 113: Add Microsoft ADAM Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. Select **ACTION** to enable these Core Server actions: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

Select **TRIGGER** to configure event triggers that initiate functions that you associate with certain events.
7. Click **NEXT**.

The Core Server displays the following dialog box:

Figure 114: Connector Configuration Manager for Microsoft ADAM

8. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. All parameters are required.

- **Administrator Password** — The password for the administrator user
- **Administrator User** — The user name of the administrator
- **Application Directory Partition** — The name of the application directory partition to be accessed.
- **Server[:Port]** — This is the machine [and optional port] ADAM is running on. *i.e.* "machine" or "machine:389". The default port is 389.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.

9. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Chapter 27: Microsoft Active Directory Attribute Trigger — Connector

This chapter explains how to configure the Connector for Microsoft Active Directory Attribute Trigger:

- [*“Configuring the Connector for Microsoft Active Directory Attribute Trigger” on page 276.*](#)

Configuring the Connector for Microsoft Active Directory Attribute Trigger

The Connector for Microsoft Active Directory Attribute Trigger supports the following operation on a target:

- Trigger

You can manage any single-value or multi-value attribute with this trigger. Each Active Directory attribute requires an associated trigger. See [“Workflow Configuration” on page 279](#) for information about how to configure single-value or multi-value attributes within a workflow using this connector.

Prerequisites

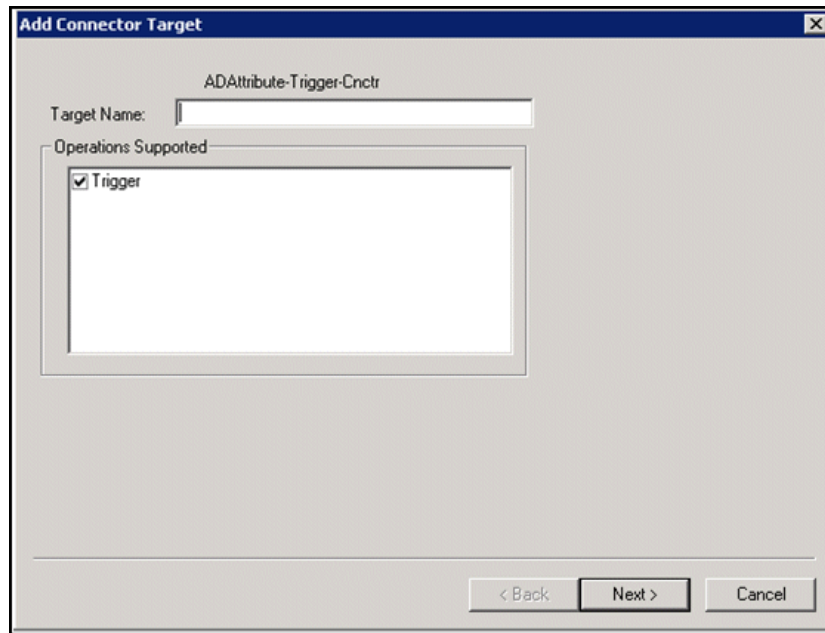
The following are prerequisites on each system where the Connector Framework or the Connector Framework manager is installed:

- Microsoft Windows Scripting Host v5.6 or higher
- Microsoft XML DOM v3.0 or higher
- Administrative access to Active Directory for Active Directory administrator that you specify during the connector configuration.

Connector Configuration

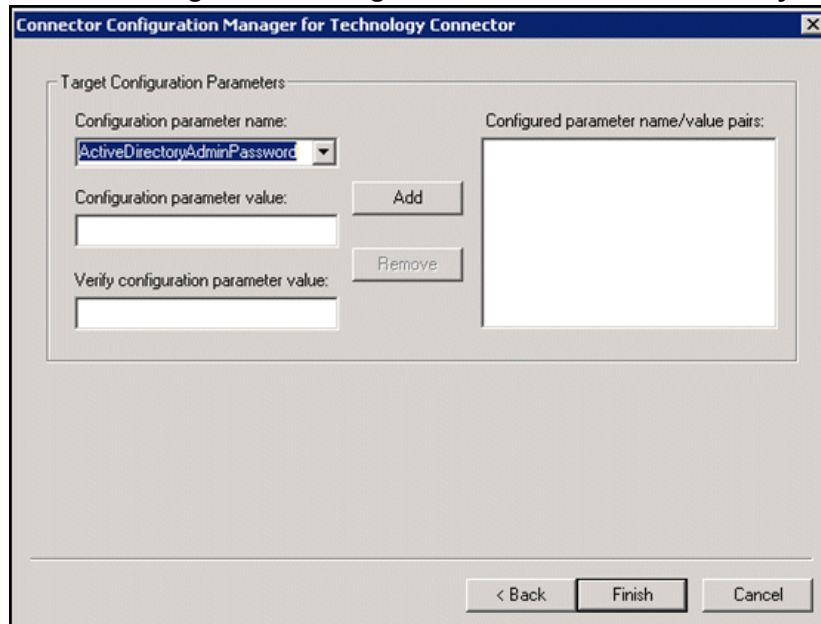
Follow these steps to add a target data source:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **ADATTRIBUTE-TRIGGER-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 115: Add Microsoft Active Directory Attribute Trigger Target

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. This connector supports the Trigger action, which enables you to configure event triggers that initiate functions that you associate with certain events.
6. Click **NEXT**.

The Connector Configuration Manager for Technology Connector dialog box appears.

Figure 116: Connector Configuration Manager for Microsoft Active Directory Attribute Trigger

7. The drop-down menu under **CONFIGURATION PARAMETER NAME** is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

ACTIVEDIRECTORYADMINUSER — The username of the Active Directory administrator with Administrative Access to the Active Directory target.

ACTIVEDIRECTORYADMINPASSWORD — The password for the Active Directory administrator.

DOMAINNAME — The Active Directory domain name on the target.

8. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for the trigger action supported by this connector.

Workflow Configuration

When configuring a workflow with the Connector for Microsoft Active Directory Attribute Trigger, use the following values for the parameters in the trigger table on the Trigger Subform, as shown in [Figure 117](#).

Figure 117: Trigger Subform

Trigger Subform

Specify the trigger configuration information. Click "Submit" when done.

Connector	Target	Object
ADAttribute-Trigger-Cntr	Target3	Trigger Object

Name:

Available:

On

Event:

Action Start

Trigger:

Active	Field Name	Value	Data Type
☐	UserDN	Control Type: Text Default Value:	TEXT
☐	AttributeName	Control Type: Text Default Value:	TEXT
☐	AttributeValue	Control Type: Text Default Value:	TEXT
☐	IsMultivalue	Control Type: List Default Value: false	ENUM

Submit Cancel

USERDN — The distinguishedName or dn value of the user whose attributes you are changing.

ATTRIBUTENAME — The name of the Active Directory attribute whose value you want to set.

ATTRIBUTE VALUE — The value of the Active Directory attribute. For single-value Active Directory attributes, this is a line of text or a macro. For multi-value Active Directory attributes, use an XML string such as the following:

```
<vals replace="true">

    <val>Value 1</val>

    <val>Value 2</val>

    <val>...</val>

    <val>Value X</val>

</vals>
```

Where the 'replace' attribute of 'vals' node specifies the operation type. For example, if 'replace' is 'true', then update new values with existing values or else append new values to existing values.

ISMULTIVALUE — A flag that indicates whether the value is a simple string or a multi-value list of strings in XML format. It is set to False by default for single-value attributes. If you are using a multi-value attribute, set it to True. The possible values for the Control type are List, Text, and Text Area.

For complete information about how to configure triggers within a workflow, refer to the chapter “Configuring Triggers, Tickets, and Notifications” in the manual *Configuring Workflows with the Core Server Administration Manager*.

Chapter 28: Microsoft Active Script — Connector

This chapter explains how to configure the Connector for Microsoft Active Script:

- [*“Configuring the Connector for Active Script” on page 282*](#)

Configuring the Connector for Active Script

The connector for Microsoft Active Script supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Audit
- Authenticating
- Notification
- Query
- Event Triggers

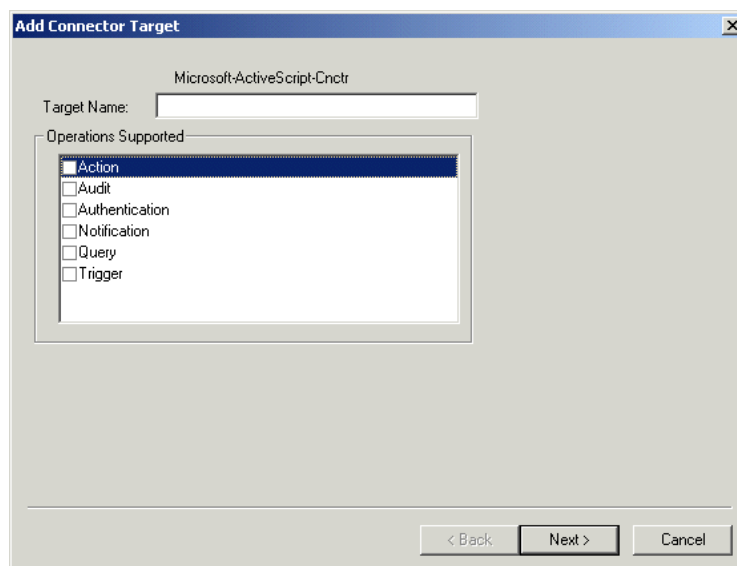
Connector Configuration

Follow these steps to add a target data source:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-ACTIVESCRIPT-CNCTR**.
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 118: Add Microsoft ActiveScript Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select **ACTION** to enable all provisioning actions on a target.
Select **AUDIT** to enable AccountCourier to create and update tickets on a target data source.

Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Server.

Select **NOTIFICATION** to enable HTML email functionality

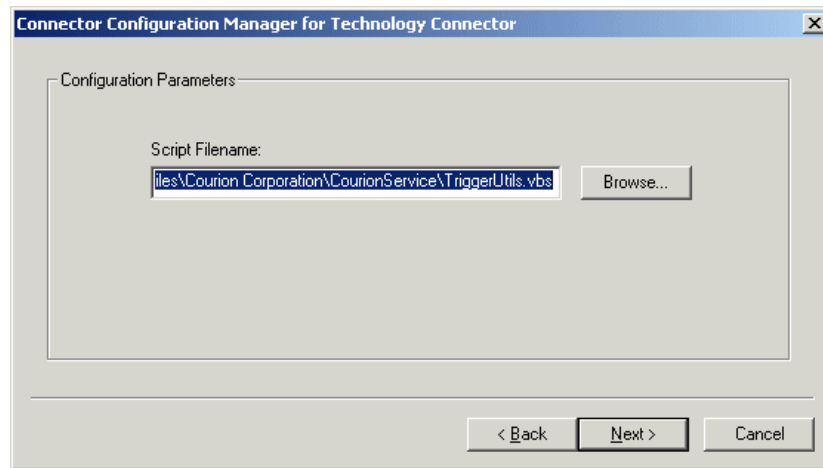
Select **QUERY** to enable Core Server or Core Server to use queries to find data in the target data source.

Select **TRIGGER** to configure event triggers that initiate functions that you associate with certain events.

6. Click **NEXT**.

The Connector Configuration Manager for Technology Connector dialog box appears.

Figure 119: Connector Configuration Manager for Microsoft ActiveScript



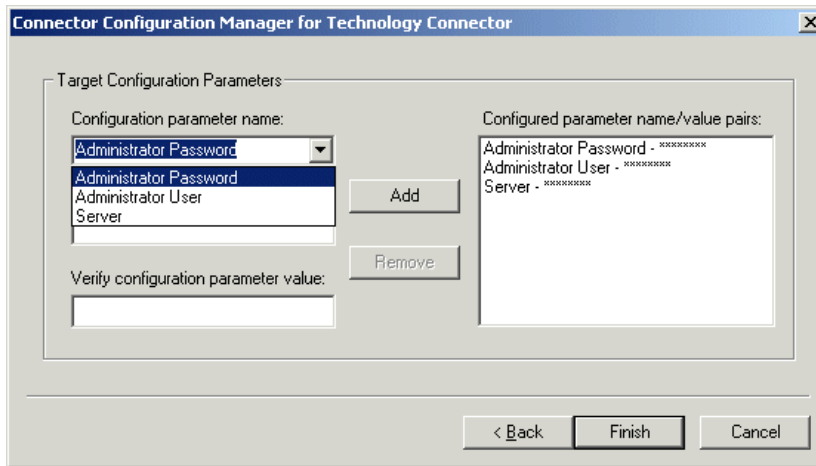
7. Enter a script name in the Script Filename box or click the **BROWSE** button and select a script name. Courion provides the following scripts:
 - `sample.js`, `sample.vbs`, and `sample.pl` are sample scripts that you can use as a guideline to write your own script. (These scripts do not actually perform any provisioning functions.)
 - `TriggerUtils.vbs`, which provides a trigger function called `CopyDir` that copies the contents of a source directory to a destination directory.
 - `ADTriggers.vbs`, which adds or removes a group to a Microsoft Active Directory account on a Resource Success event.
 - `WorkflowonlyCnctr.vbs`, also referred to as the Connector for Workflow Events. It is used to create a connector for situations in which connection to another application is not needed or not possible. This enables automation of a procedure within a workflow. For example, if you need to provision a group of users for an application in which there is no regular connector, you could use this connector to send email notification to a specific individual in charge of manually provisioning the account. Since those users might also need provisioning for other accounts in which there are regular connectors, all provisioning requests can be handled within a single workflow. Another example is a situation in which some physical action needs to be taken when an account is provisioned, such as delivery of materials. This connector could generate a ticket requesting delivery of those materials.

By default, these scripts are located in the `CourionService` directory.

8. After you select the script, click **NEXT**.

The second Connector Configuration Manager dialog box appears.

Figure 120: Connector Configuration Manager for Microsoft ActiveScript (2)



9. Each script requires different parameters to execute the function defined in the script.

The `TriggerUtils.vbs` script requires the following parameters:

- Administrator Password — The password for the Administrator User
- Administrator User — The name of a user with sufficient privileges to copy from the source directory and to write to the destination directory
- Server name — The domain for the account specified as the Administrator User

The `ADTriggers.vbs` script requires the following parameters:

- Domain — The domain for the account specified below for the Administrative User
- Domain Administrative User — The name of a user with sufficient privileges to add accounts to or remove accounts from groups
- Domain Administrative Password — The password for the Domain Administrative User
- Logon Domain — The domain for the specified Logon User
- Logon User — The name of a user with sufficient privileges on the local system to log on locally to the current server
- Logon Password — The password for the Logon User

The `WorkflowonlyCnctr.vbs` script requires the following parameters:

- Administrator Password — Any value is allowed because this parameter is not used for workflow execution
- Administrator User — Any value is allowed because this parameter is not used for workflow execution
- Server name — Any value is allowed because this parameter is not used for workflow execution

Set values for each parameter as follows:

- a. Select a parameter name from the drop-down box by highlighting it.

- b. Enter a value associated with that parameter in the **CONFIGURE PARAMETER VALUE** window and the **VERIFY CONFIGURATION PARAMETER VALUE** window.
- c. Click **ADD**. The parameter name appears in the **CONFIGURED PARAMETER NAME/VALUE PAIRS:** window. Secure information, such as user names and passwords, appear as xxxxxx.

Note: Only one parameter name/value combination can be added at a time, but multiple items may be selected together and removed from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value.

10. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 29: Microsoft ADO (ActiveX Data Objects) — Connector

This chapter explains how to configure the Connector for Microsoft ADO (ActiveX Data Objects):

- [*“Configuring the Connector for ADO” on page 288*](#)

Configuring the Connector for ADO

The connector for Microsoft ADO (ActiveX Data Objects) supports the following operations on a target:

- Authentication against an ADO-compliant data source
- Query an ADO-compliant data source
- Ticketing
- Actions:
 - Create a record in an ADO-compliant data source
 - Change a record in an ADO-compliant data source
 - Delete a record in an ADO-compliant data source
 - View a record in an ADO-compliant data source
 - Verify a record in an ADO-compliant data source
- Transaction Repository
- Trigger

This connector supports Microsoft SQL Server 2000 and higher targets.

Note: If you have access keys for Core Compliance with User Activity or Core Compliance with Sensitive Data, you can designate specific targets with the User Activity or Sensitive Data capability. SIEM (Security Information and Event Management) and DLP (Data Loss Prevention) applications can output information into a database or other file which Core Compliance can access with the Connector for Microsoft ADO. To configure a target for User Activity or Sensitive Data capability, you need to do both of the following:

- Configure a target using the Connector for Microsoft ADO.
- Edit the `feature_extensions.xml` file to add the target to the file and indicate whether it is designated for User Activity or Sensitive Data.

For details, refer to the chapter “Configuring Compliance Workflows” in the manual *Configuring Workflows with the Core Access Assurance Suite*.

Features that Require a Transaction Repository

The following Administration Manager features require that you configure a Microsoft ADO connector with a transaction repository:

- Requester/Approver functionality
- Delegation functionality
- The ability to store compliance information for use with reports using the Verify action.

See the manual *Configuring Workflows with the Core Server Administration Manager* for information about these features.

- Sharing configuration data when running the Connector Configuration Manager Configuration Repository option in Remote Mode.

See the *Core Server Implementation Guide* for information about this option.

- Role Management functionality

Using Security Options

The Connector for Microsoft ADO supports Windows Authentication as well as SQL Server Authentication. If you want to use Windows Authentication you need to use the same username and password pair to log in to the Core Server and run the Connector Configuration Manager that you use for the **PRIVILEGED USER** and **PASSWORD** in the Connector Configuration Manager for ADO dialog box (see [Figure 122](#)). The user associated with the username and password pair must have access to the SQL data source on the SQL server. Select the option **USE WINDOWS NT INTEGRATED SECURITY** in the Data Link Properties (Connection) dialog box ([Figure 124](#)) to use Windows Authentication.

Adding a Target Data Source

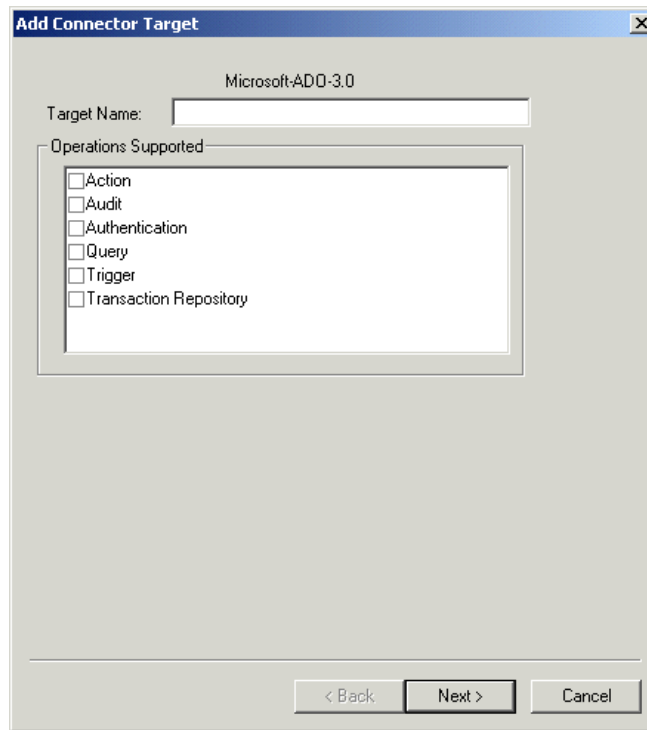
The following information is required to add a Microsoft ADO target:

- Data source Name (DSN)
- Database driver
- User and password for authentication to the DSN
- Existing database name

Follow these steps to add a target data source:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-ADO-3.0**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box for Microsoft ADO appears.

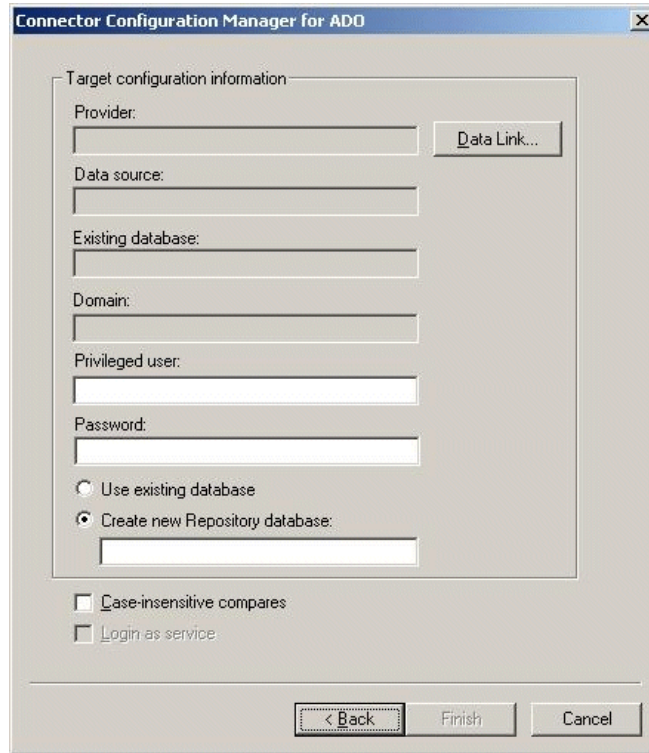
Figure 121: Add Microsoft ADO Target

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The connector supports eight operations: “Create Record,” “Delete Record,” “Create Ticket,” “Update Ticket,” “Authentication,” “Query,” “Transaction Repository,” and “Trigger”. “Create Record” and “Delete Record” are collectively called “Action” because a target cannot be added with a single action operation (for example, a target cannot be added with “Create Record” only). “Create Ticket” and “Update Ticket” are collectively called “Audit” because a target cannot be added with a single action operation (for example, a target cannot be added with “Create Ticket” only). Transaction Repository is the database where the request data is stored.

5. Select one, two, three, four, or all five operations.
 - Select **ACTION** to create and delete records on a target data source.
 - Select **AUDIT** to create and update tickets on a target data source.
 - Select **AUTHENTICATION** to use the target data source for authenticating end user access.
 - Select **QUERY** to use queries to find data in the target data source.
 - Select **TRIGGER** to trigger a script during a workflow.
 - Select **TRANSACTION REPOSITORY** to create a link to a transaction repository on the target data source.
6. Click **NEXT**.

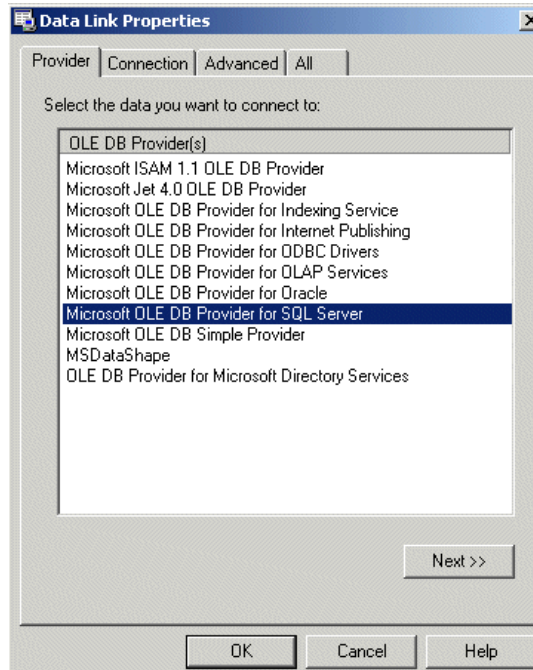
The Connector Configuration Manager for ADO dialog box appears.

Figure 122: Connector Configuration Manager for ADO

Note: The options **USE EXISTING DATABASE** and **CREATE NEW TRANSACTION REPOSITORY DATABASE:** appear active only if you have chosen to use the Transaction Repository operation. Otherwise, these options are grayed out.

7. Click the **DATA LINK** button to configure data link characteristics before you complete this dialog box.

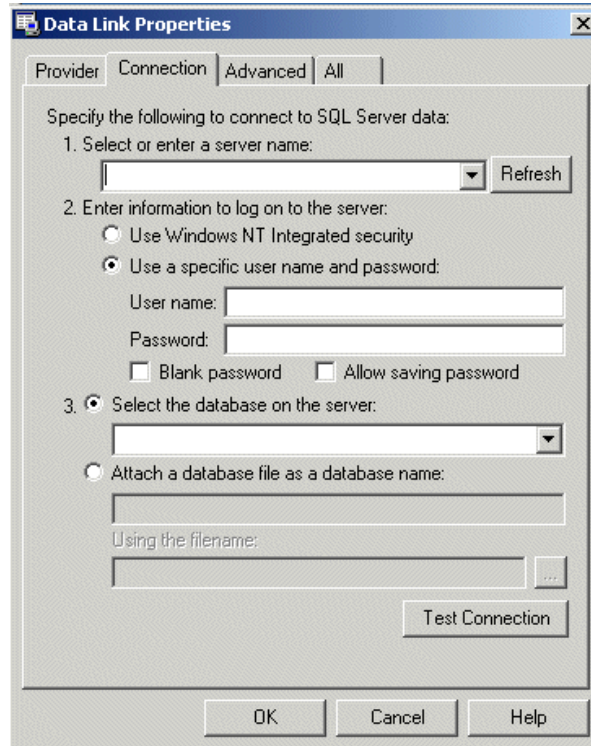
The Data Link Properties (Provider) dialog box appears.

Figure 123: Data Link Properties (Provider)

8. Select **MICROSOFT OLE DB PROVIDER FOR SQL SERVER** and click **NEXT**.

The Data Link Connection Properties (Connection) dialog box appears.

Figure 124: Data Link Properties (Connection)



9. Specify information about the SQL Server target as follows:

Enter the name of the SQL Server target machine or select one from the drop-down list.

10. Select a method to log on to the server.

- If you select **Use Windows NT integrated security**, you need to supply the domain, privileged user, and password of the privileged user on the Connector Configuration Manager for ADO dialog box (see [Figure 122](#)).

If you select **USE WINDOWS NT INTEGRATED SECURITY**, you have the option of selecting the **LOGIN AS A SERVICE** checkbox on the Connector Configuration Manager for ADO dialog box (see [Figure 122](#)). Select this option if you use Windows Authentication and require that the service user is impersonated without the use of an interactive session. (This is the more secure option as only services such as the connector can access the account.)

- If you select **USE A SPECIFIC USER NAME AND PASSWORD**, enter information about this user here. The user you specify must have the privilege to create a new database on the SQL Server target.

If the user you specify does not require a password to log on to the server, select **BLANK PASSWORD**. If the user does require a password, select **ALLOW SAVING PASSWORD**.

Note: To ensure the security of the server, Core Security recommends that the user you select to log on to the server has a password associated with the username.

- Enter the name of the database on the server or select a name from the drop-down list.

Note: If you are creating a transaction repository, you can select any database where the user has permission to log in.

- Use the **TEST CONNECTION** button to verify the data you have entered. If you choose **USE WINDOWS NT INTEGRATED SECURITY**, the user who is currently logged in to the SQL Server must have the privilege to log into the database or the test connection fails.
- Click OK when you have completed the Data Link Properties Connector dialog box. The Connector Configuration Manager for ADO dialog box appears.

Note: You do not need to enter information in the Advanced and All dialog boxes.

11. If you have not configured Transaction Repository, click **FINISH** to complete the connector configuration. If you have configured Transaction Repository, complete the remaining steps.

12. If you selected the **USE WINDOWS NT INTEGRATED SECURITY** option on the Data Link Properties (Connection) dialog box, enter the following:

- **DOMAIN** - Enter the domain name for the privileged user.
- **PRIVILEGED USER** and **PASSWORD**

The Privileged User and Password must be the same username and password you used to log in to the Core Server and run the Connector Configuration Manager. This user must have access to the SQL data source on the SQL server.

13. Select one of the following radio buttons at the bottom of the dialog box:

- **USE AN EXISTING DATABASE.** If you choose this option, the database specified in the **EXISTING DATABASE** edit box is used for the transaction repository.
- **CREATE A NEW TRANSACTION REPOSITORY DATABASE.** If you choose this option, enter the name of the new database in the edit box below this option.

14. Select the **CASE-INSENSITIVE COMPARES** checkbox if you want to allow the workflow to convert text to upper case prior to performing searches against the database.

Note: When using the Data Security Utility with the case-insensitive option enabled, hashed data is converted to upper case prior to performing the hash. Encrypted data is always case-sensitive, even with this option enabled.

15. Click **FINISH** to complete the connector configuration.

The target is now available for each action supported by this connector.

Chapter 30: Microsoft Exchange 5.5 — Connector

This chapter explains how to configure the Connector for Microsoft Exchange 5.5:

- [*“Configuring the Connector for Microsoft Exchange 5.5” on page 296*](#)

Configuring the Connector for Microsoft Exchange 5.5

The connector for Microsoft Exchange 5.5 supports the action operations on a target: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

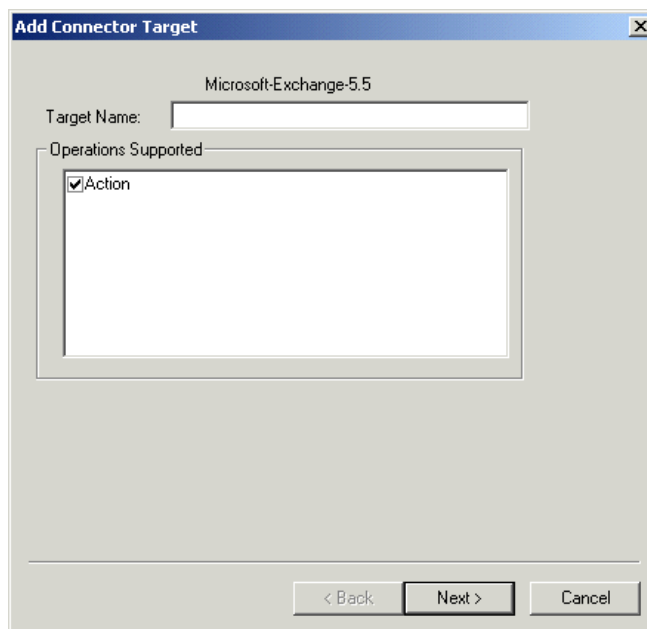
Connector Configuration

Follow these steps to add a target domain:

1. From the Start menu, select:
Programs > Core Server Core Server > Connector Configuration Manager
2. Select **MICROSOFT-EXCHANGE-5.5**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 125: Add Microsoft Exchange 5.5 Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager.

The **ACTION** check box is selected by default.

5. Click **NEXT**.

The configuration screen for Exchange 5.5 appears.

Figure 126: Connector Configuration Manager for Microsoft Exchange 5.5

6. This dialog box requires the following information.

- **EXCHANGE SERVER** — Enter the name of the Exchange server where the provisioning actions occur. Enter the name as a WINS name, which is typically the same as the hostname. IP addresses and Fully Qualified Domain Names (FQDN) are not supported.
- **PRIVILEGED DOMAIN\USERNAME** — Enter the username for the Service Account Administrator on the target Exchange Server.

Note: On Microsoft Windows 2000 or higher systems, only the username is needed. The domain defaults to the system domain. On Windows NT systems, you must qualify the username with the domain name (that is, *domainname\username*) or the domain defaults to the local machine.

- **PASSWORD** — Enter the password for the account.
- **MAILBOX ORGANIZATIONAL PATH** — enter the location of the mailbox store in the following format:

/o=organization/ou=site/cn=mailbox store

where “organization” is replaced with the organization name, “site” is replaced with the site name, and “mailbox store” is replaced with the name of the mailbox store.

Note: Each additional mailbox store requires a new target to be configured.

7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by the connector.

Chapter 31: Microsoft Exchange 2000 — Connector

This chapter explains how to configure the Connector for Microsoft Exchange 2000:

- [*“Configuring the Connector for Microsoft Exchange 2000” on page 300*](#)

Configuring the Connector for Microsoft Exchange 2000

The connector for Microsoft Exchange 2000 supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

If you want to configure this connector on a Microsoft Windows Server® 2003 server, you must install the Microsoft Exchange System Management Tools from Exchange 2003 on that server.

The Connector Framework server used to access Exchange 2000 must be a member of the Active Directory Domain where the Exchange 2000 server resides.

If the Connector Framework server is a member of a different domain than the Exchange 2000 server, you must configure the Exchange Connector so the privileged user is listed in both the Authorized Account Information and the Service Account Logon Information sections (see [Figure 128](#)). The privileged user needs to be a member of the domain where you intend to create the account.

You need to install the following tools on each server in which the Connector Framework or Connector Framework Manager is installed:

- Active Directory Users and Computers Administration Tool
- Microsoft Exchange 2000 Administration Tool

Connector Configuration

Follow these steps to configure a target domain:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-EXCHANGE-2000**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 127: Add Microsoft Exchange 2000 Target

The screenshot shows a Windows-style dialog box titled "Add Connector Target". Inside the dialog, the text "Microsoft-Exchange-2000" is displayed above a "Target Name:" label and an empty text input field. Below this is a section titled "Operations Supported" which contains a list box with a single item, "Action", that has a checked checkbox to its left. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
The **ACTION** check box is selected by default.
5. Click **NEXT**. The Connector Configuration Manager for Microsoft Exchange 2000 is displayed.

Figure 128: Connector Configuration Manager for Microsoft Exchange 2000

Connector Configuration Manager for MS Exchange 2000

Microsoft Exchange 2000 Authorized Account Information

Active Directory Domain Controller:

Active Directory Name:

Privileged user:

Password:

☐ Use Encryption
☐ Search user logon name (pre-Windows 2000)
☐ Maintain connection

Service Account Logon Information

Privileged user domain:

Privileged username:

Password:

Service Logon Mode

☒ interactively
☐ as a service

< Back Finish Cancel

6. **MICROSOFT EXCHANGE 2000 AUTHORIZED ACCOUNT INFORMATION** — The information in this section of the dialog box designates information about the directory server and the directory server administrator. This dialog box requires the following information.
- ACTIVE DIRECTORY DOMAIN CONTROLLER** — Specify the actual machine name that the Connector for Microsoft Exchange 2000 connects with to create mailboxes. It must be the machine name, not IP address or Fully Qualified Name. The machine you specify must be of a functioning Domain Controller on the named domain.
 - ACTIVE DIRECTORY NAME** — This is the name of the Active Directory Domain in which the Exchange server exists.
 - PRIVILEGED USER** — Username for an account with administrator access to both the Active Directory Domain and the Exchange 2000 server. The username specified should be the principal name of the administrator account (username@domain.com).

The privileged user for Exchange 2000 should have privileges on both the Active Directory Domain and on the Permissions object of the Exchange server. The privileges on the Active Directory Domain need to be set to allow the creation of accounts.

The privileged user account needs to be in the Exchange Administrators group, and have sufficient privileges to change attributes on any Active Directory account.

- d. **PASSWORD** — This is the password for the privileged user.
 - e. **USE ENCRYPTION** — Selecting this checkbox encrypts through an SSL connection the communication between the Exchange 2000 / Active Directory server and Core Server. To support SSL encryption, Certificate Services must be installed and enabled on Active Directory.
 - f. **SEARCH USER LOGON NAME (PRE-WINDOWS 2000)** — Select this checkbox to automatically conduct a second search on the smAMAccount field if the original search on the UserPrincipalName field fails. Since accounts that existed before Windows 2000 contain a username in a different format from that contained in Active Directory, the second search captures those accounts with the earlier format for username.
 - g. **MAINTAIN CONNECTION** — When checked, this option pools connections to the target system for re-use, rather than opening a new connection for each operation. The option is disabled by default. Core Security recommends that you enable this option only if Server Not Operational errors occur, and you need to force the connection to stay open.
7. **SERVICE ACCOUNT LOGIN INFORMATION** — The information in this section of the dialog box designates the user on the local workstation who is running Connector Configuration Manager and who has the following privileges:
- a. **PRIVILEGED USER DOMAIN** — This is the domain to which the privileged user account belongs. It need not be the same as the Active Directory domain.
 - b. **PRIVILEGED USERNAME** — This is the user whose permission is used for access to the local machine.
 - c. **PASSWORD** — This is the password for the privileged user.
8. **SERVICE LOGON MODE** This parameter designates the privileges the administrative user needs. There are two options:
- INTERACTIVELY** — This is the default and enables users to access the account from a workstation in the domain as well as services such as the connector running in the background.
 - AS A SERVICE** — This is the more secure option because only services such as the connector can access the account.
- Note:** The user you specify for the Service Logon Account must have the User Right Assignment "Log on as service" assigned to it on the system hosting the connector.
9. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 32: Microsoft Exchange 2007 and 2010 — Connector

This chapter explains how to configure the Connector for Microsoft Exchange 2007 and 2010:

- [*“Configuring the Connector for Microsoft Exchange 2007 and 2010” on page 306*](#)

Configuring the Connector for Microsoft Exchange 2007 and 2010

The Connector for Microsoft Exchange 2007 and 2010 supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Note: The Connector for Microsoft Exchange 2007 and 2010 has been qualified against Microsoft Exchange 2013. The connector supports the same capabilities against Microsoft Exchange 2013 as it does with Microsoft Exchange 2010.

Note: Please contact Customer Support to get the newer connector used to integrate to Microsoft Exchange 2013. That connector can be used to integrate with Microsoft Exchange 2013 instead of this connector available in the suite installation kit. As noted above, you can use this connector for Microsoft Exchange 2013, but it is limited to the functionality offered in this connector.

Prerequisites

- The Microsoft Exchange 2007 or 2010 server must be separate from the server hosting the Core Server components.
- The Connector Framework server used to access Exchange 2007 or 2010 must be a member of the Active Directory Domain where the Exchange 2007 or 2010 server resides.
- The privileged user must be a member of the domain in which the target resides and must be an Exchange Administrator. Add the privileged user to the Exchange Organization Administrators group.
- The privileged user must also be a local administrator on the Connector Framework server used to access Exchange 2007 or 2010. Add the privileged user to the Local Administrators group.

For Microsoft Exchange 2007 Only

- Install the 2007 client tools, which install the correct version of PowerShell 1.0.
- The privileged user must have read/write permissions to the MigrationLogs folder on the system where the connector is running (either the Courier Server or the Connector Framework server). The default location of this folder is:
C:\Program Files\Microsoft\Exchange Server\Logging\MigrationLogs

For Microsoft Exchange 2010 Only

- Install the Windows Management Framework, which includes PowerShell 2.0 and Windows Remote Management 2.0, on the Connector Framework server used to access Microsoft Exchange 2010.

Refer to <http://support.microsoft.com/kb/968929> for more information

- For Microsoft Exchange 2010, you need to alter the Connector Framework server's code execution policy to allow remoteSigned cmdlets. To do this, follow these steps:
 1. Run a PowerShell as administrator.
 2. Execute the following command:


```
Set-ExecutionPolicy RemoteSigned
```
 3. Reboot the Connector Framework server.

Prerequisites for Microsoft Windows Server 2008 and 2008 R2 and higher

- The privileged user must have full access to the \WINDOWS\TEMP directory on the Connector Framework server used to access the target system.

Note: For Windows 2012 (and probably higher) additional steps may be needed for the proper permissions to the Windows\Temp directory.

 1. Type 'Local Security Policy' in start screen/menu search and press enter
 2. Go to Local Policies > Security Options, scroll to the bottom and set 'User Account Control: Run all administrators in Admin Approval Mode' to Disabled
 3. Restart system when prompted
 4. Re-add privileged user to Temp directory permissions
 5. Re-enable the option from step 2 and do step 3
- The privileged user must have full access to the "MachineKeys" directory on the Connector Framework server used to access the target system. This directory (hidden by default) can be found at:


```
\ProgramData\Microsoft\Crypto\RSA\MachineKeys
```

Note: The permission is only on the directory and not the files in the directory.

Installing Exchange Management Tools on the Connector Framework and Connector Framework Manager Servers for Microsoft Exchange 2007

Prior to installing the Microsoft Exchange Management Tools, install .Net 2.0, Microsoft Management Console (already installed with Windows Server 2003 Service Pack 2 or higher), and Microsoft Windows PowerShell.

1. Start the Exchange 2007 Management Tools installation. From the initial window, click **STEP 4: INSTALL MICROSOFT EXCHANGE**. Click **NEXT**, accept the license agreement, and click **NEXT** again.
2. The Error Reporting screen appears. Click **No**, then click **NEXT**.
3. The Installation Type screen appears. Select **CUSTOM EXCHANGE SERVER INSTALLATION**. Leave the install path set to the default and click **NEXT**.
4. The Custom Options screen appears. Select only the **MANAGEMENT TOOLS** option and click **NEXT**.
5. On the Exchange Organization screen, enter an name and click **NEXT**.

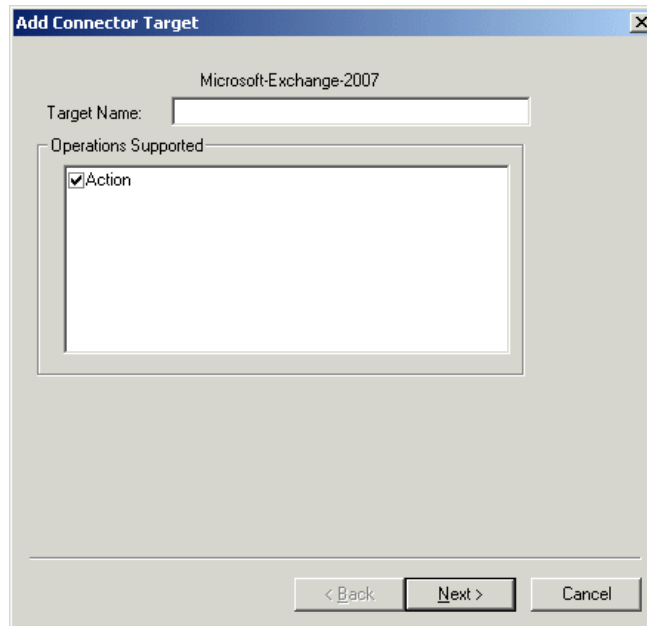
6. Exchange runs a series of readiness checks. Once they are complete, click **INSTALL**. Ignore the warning about “hostname (a) record” if it pops up
7. Exchange installs the appropriate files and then displays the Completion screen. Uncheck the **FINALIZE INSTALLATION USING THE EXCHANGE MANAGEMENT CONSOLE** check box and click **FINISH**.

Connector Configuration

Follow these steps to configure a target domain:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-EXCHANGE-2007**
3. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 129: Add Microsoft Exchange 2007 or 2010 Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
The **ACTION** check box is selected by default.
5. Click **NEXT**. The Connector Configuration Manager for Microsoft Exchange 2007 and 2010 appears.

Figure 130: Connector Configuration Manager for Microsoft Exchange 2007 and 2010

6. **MICROSOFT EXCHANGE VERSION** - Select either Microsoft Exchange 2007 or Microsoft Exchange 2010 from the drop-down list.
7. Enter the following information about the Microsoft Exchange Administrator:

EXCHANGE ADMINISTRATOR DOMAIN — Enter the name of the Active Directory Domain in which the Exchange server exists.

USER — Enter the User name for an account with administrator access to the Exchange 2007 or 2010 server. You can specify the user name in both the UPN format and sAMAccountName format. See [“Prerequisites” on page 306](#) for additional prerequisites.

PASSWORD — Enter the password for the privileged user.
8. **EXCHANGE 2007 ADMINISTRATOR TOOLS BIN FOLDER** — If you selected Microsoft Exchange 2007, enter the path name to the bin folder in the installation path of Exchange 2007. If you selected the default during the Exchange 2007 tools install, the default value appears here and you do not need to change it.
9. **EXCHANGE 2010 SERVER** — If you selected Microsoft Exchange 2010, enter the name of the Exchange 2010 server.
10. **CONNECT TO SERVER VIA HTTPS** — Check this option to connect to a Microsoft Exchange 2010 server using HTTPS (available with Exchange 2010 server only).

Note: Additionally you may need to add the Exchange server name to the “Trusted Hosts” in the WinRM configuration:

```
winrm set winrm/config/client
@{TrustedHosts="[exchange-server-name]"}
```
11. **PROVISION WITHIN THE SCOPE OF ENTIRE AD FOREST** — Check this option to enable provisioning of accounts in Microsoft Exchange 2010 across all the domains in Active Directory Forests (available with Exchange 2010 server only).
12. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Connector Framework server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 33: Microsoft Identity Integration Server (MIIS) — Connector

This chapter explains how to configure the Connector for Microsoft Identity Integration Server (MIIS):

- [*“Configuring the Connector for Microsoft Identity Integration Server \(MIIS\)” on page 312*](#)

Configuring the Connector for Microsoft Identity Integration Server (MIIS)

The connector for Microsoft Identify Integration Server (MIIS) supports the following operations on a target:

- View and Verify
- Authentication
- Query

Prerequisites

The following information is required to add an MIIS target:

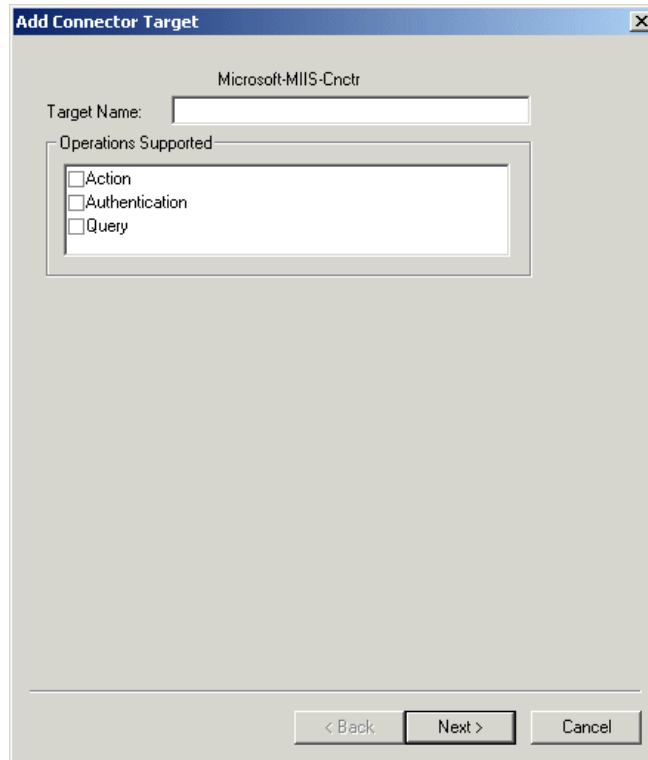
- Name or IP address of the SQL server where the MIIS metaverse data is stored
- Domain name of SQL server and privileged user (if you select Windows NT Integrated Security)
- Username and password of the privileged user who logs in to the MIIS database

The privileged user requires the privilege db_datareader. You can grant this privilege using the SQL Server Login Properties dialog box.

Connector Configuration

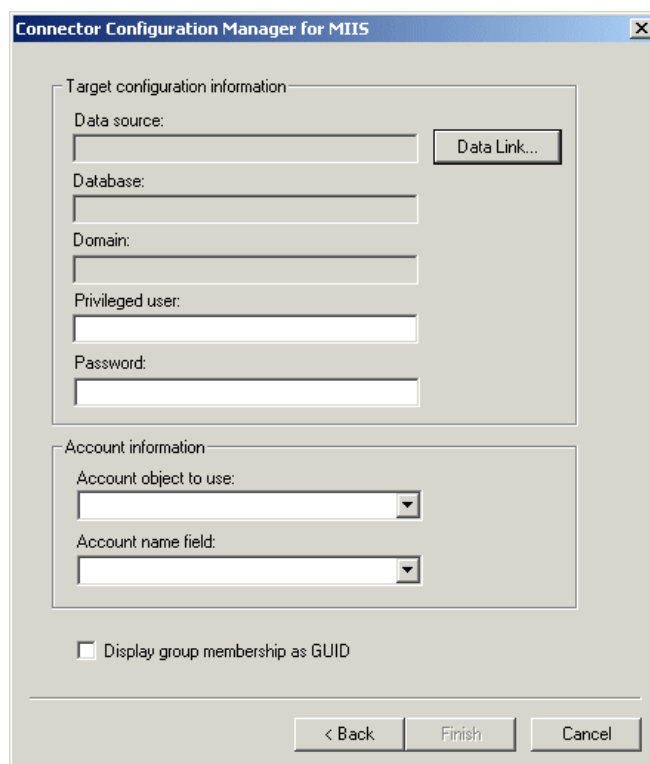
Follow these steps to configure the connector for MIIS:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **MICROSOFT-MIIS-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 131: Add MIIS Target

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select one, two, or three operations, described as follows.
 - Select **ACTION** to enable Core Server to access the MIIS database. Note that the connector does not allow you modify or delete access to an MIIS database.
 - Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Server.
 - Select **QUERY** to enable Core Server to use queries to find data in the target data source.
6. Click the **NEXT** button.

The Connector Configuration Manager dialog box appears.

Figure 132: Connector Configuration Manager for MIIS


The dialog box is titled "Connector Configuration Manager for MIIS". It contains two main sections: "Target configuration information" and "Account information".

Target configuration information:

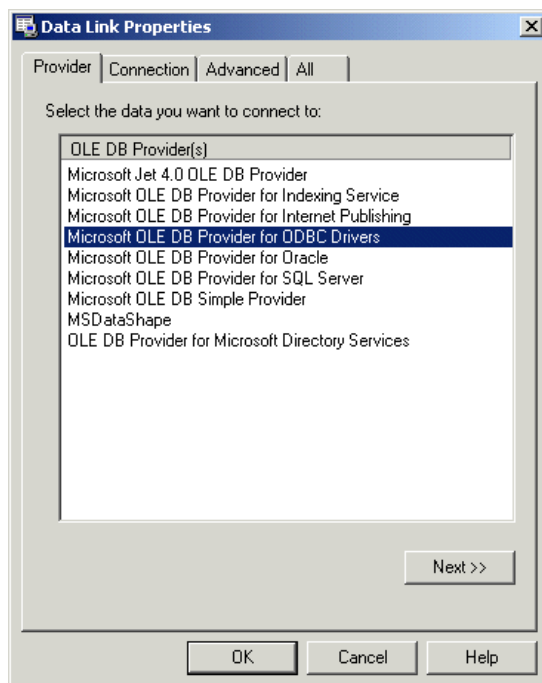
- Data source: [Text box] [Data Link... button]
- Database: [Text box]
- Domain: [Text box]
- Privileged user: [Text box]
- Password: [Text box]

Account information:

- Account object to use: [Dropdown menu]
- Account name field: [Dropdown menu]

At the bottom, there is a checkbox labeled "Display group membership as GUID" which is currently unchecked. Below the checkbox are three buttons: "< Back", "Finish", and "Cancel".

- Click the **DATA LINK** button. The Data Link Properties dialog box appears.

Figure 133: Data Link Properties 1


The dialog box is titled "Data Link Properties". It has four tabs: "Provider", "Connection", "Advanced", and "All". The "Provider" tab is selected.

Under the "Provider" tab, it says "Select the data you want to connect to:". Below this is a list box containing the following providers:

- OLE DB Provider(s)
- Microsoft Jet 4.0 OLE DB Provider
- Microsoft OLE DB Provider for Indexing Service
- Microsoft OLE DB Provider for Internet Publishing
- Microsoft OLE DB Provider for ODBC Drivers** (highlighted)
- Microsoft OLE DB Provider for Oracle
- Microsoft OLE DB Provider for SQL Server
- Microsoft OLE DB Simple Provider
- MSDataShape
- OLE DB Provider for Microsoft Directory Services

At the bottom right of the list box area is a "Next >>" button. At the very bottom of the dialog box are three buttons: "OK", "Cancel", and "Help".

- Select **MICROSOFT OLE DB PROVIDER FOR SQL SERVER** and then click the **NEXT** button.

The next Data Link Properties dialog box appears, with the **CONNECTION** tab selected.

Figure 134: Data Link Properties 2

9. Specify or select the name or IP address of the SQL server where the MIIS metaverse data is stored.
 - a. Enter the name or IP address of the SQL server target machine or select one from the drop-down list.
 - b. Select the method to log on to the server.

If you select **USE WINDOWS NT INTEGRATED SECURITY**, supply the domain name, privileged user name, and password of the privileged user on the Connector Configuration Manager for dialog box, (see [Figure 132](#)).

If you select **USE A SPECIFIC USER NAME AND PASSWORD**, enter information about this user here.

If the user you specify does not require a password to log on to the server, select **BLANK PASSWORD**. If the user does require a password, select **ALLOW SAVING PASSWORD**. You must specify an option; if you do not, the **CONNECTOR CONFIGURATION MANAGER FOR MIIS** dialog box requests a password.

Note: To ensure the security of the server, Core Security recommends that the user you select to log on to the server has a password associated with the username.
10. Enter the name of the MIIS database on the server, which is MicrosoftIdentityInformationServer, or select that name from the drop-down list.
11. Use the **TEST CONNECTION** button to verify the data you have entered. If you chose **USE WINDOWS NT INTEGRATED SECURITY**, the user who is currently logged in to the SQL server must have the privilege to log into the database or the test connection fails.

If the test fails, use the error message to correct the problem.
12. Click OK when you complete the **DATA LINK PROPERTIES CONNECTOR** dialog box.

The **CONNECTOR CONFIGURATION MANAGER FOR MIIS** dialog box returns, showing the fields you completed. A sample follows in [Figure 135](#).

Figure 135: Connector Configuration Manager Dialog Box Partially Completed

13. **ACCOUNT OBJECT TO USE** — Select an object class that contains account information. A sample object class is Person or User.
14. **ACCOUNT NAME FIELD** — Choose an attribute from the selected account object to use as the account name, such as uid.
15. **DISPLAY GROUP MEMBERSHIP AS GUID** — If you select this, the group ID is displayed instead of the group name.
16. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 34: Microsoft ODBC 3.0 — Connector

This chapter explains how to configure the Connector for Microsoft ODBC:

- [*“Configuring the Connector for Microsoft ODBC” on page 318*](#)

Configuring the Connector for Microsoft ODBC

The Connector for Microsoft ODBC-3.0 supports Microsoft Access, Microsoft SQL Server, and Oracle ODBC-compliant data sources. The connector supports the following operations on a target:

- Authentication against an ODBC-compliant data source
- Query an ODBC-compliant data source
- Ticketing - create a ticket and update a ticket in an ODBC-compliant data source
- Actions:
 - Create/Add a record in an ODBC-compliant data source
 - Change a record in an ODBC-compliant data source
 - Delete a record in an ODBC-compliant data source
 - View a record in an ODBC-compliant data source
 - Verify a record in an ODBC-compliant data source

Note: When using the ODBC connector, provisioning platform applications do not support spaces in SQL table names. If your table names contain spaces, you use the ADO connector. See [“Microsoft ADO \(ActiveX Data Objects\) — Connector” on page 287](#) for information about this connector.

Prerequisites

You need the following information to add an ODBC-enabled target:

- Data Source Name (DSN)
- Database driver
- User and password for authentication to the DSN

The DSN represents an ODBC connection to a database server. Once a driver is specified in the DSN configuration, the setup steps are driver specific.

Adding an ODBC-enabled target includes providing a Data Source Name (DSN). The Data Source Name represents an ODBC connection to a database server. Data Source Name configuration, requires specifying a database driver. After a driver is selected, the setup steps that follow are driver-specific.

The password target data source name you define in this chapter must match the name defined in the Access Assurance Suite Administration Manager.

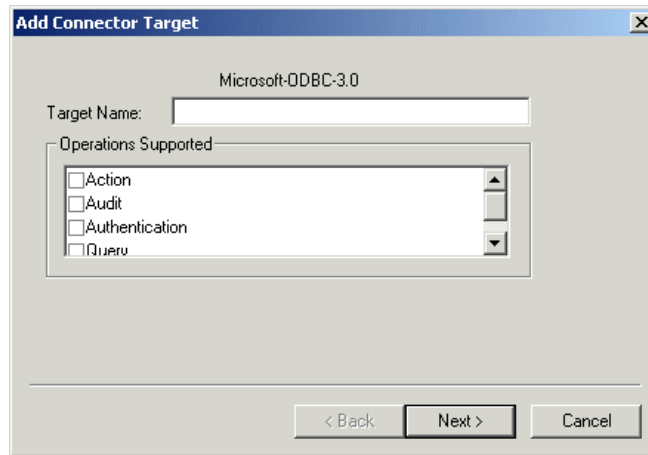
Connector Configuration

Follow these steps to add an ODBC target data source:

1. From the Start menu, select:
 - Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Click the right mouse button on “**MICROSOFT-ODBC-3.0**” and select **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 136: Add ODBC Target

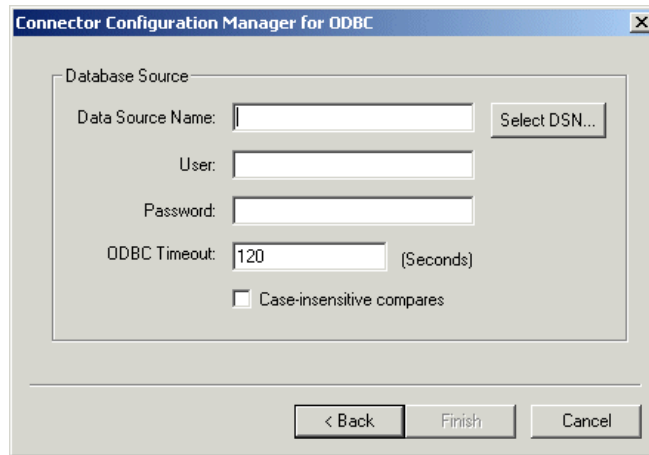


3. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The connector supports six operations: “Create Record”, “Delete Record”, “Create Ticket”, “Update Ticket”, “Authentication”, and “Query”. “Create Record” and “Delete Record” are collectively called “Action” because a target cannot be added to a single action operation (for example, a target cannot be added to “Create Record” only). “Create Ticket” and “Update Ticket” are collectively called “Audit” because a target cannot be added to a single action operation (for example, a target cannot be added to “Create Ticket” only).

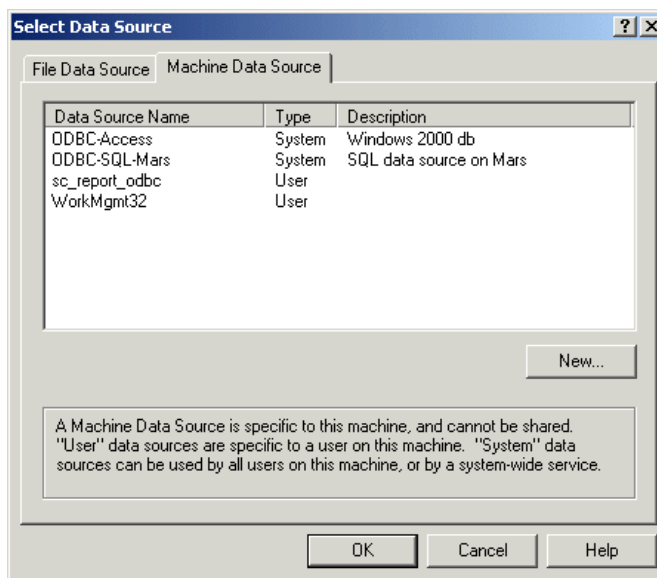
4. Select one, two, three, or all four operations.
 - Select **ACTION** to enable Core Provisioning to create and delete user profiles (records) on a target data source.
 - Select **AUDIT** to enable Core Provisioning to create and update tickets on a target data source.
 - Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Provisioning or Core Compliance.
 - Select **QUERY** to enable Core Provisioning or Core Compliance to use queries to find data in the target data source.
5. Click **NEXT**.

The Connector Configuration Manager displays the ODBC Targets dialog box.

Figure 137: Connector Configuration Manager for ODBC

6. Click **SELECT DSN...** to specify a system data source. Do not enter field information at this time.

The Select Data Source dialog box appears.

Figure 138: Select System Data Source

7. Click the **MACHINE DATA SOURCE** tab.

If the correct data source is listed, select it, click **OK** and The ODBC Targets dialog box reappears. Skip to the next step.

If the correct data source is not listed, click **NEW**. Go to one of the following sections, depending on the data source you want to add.

- [“Adding a New Microsoft Access Data Source” on page 322](#)
- [“Adding a New SQL Server Data Source” on page 325](#)
- [“Adding a New Oracle Data Source” on page 329](#)

Figure 139: Authorize ODBC Database Access

8. Enter authorization information as follows.

- Enter the **USER** and **PASSWORD** for an account with access to this data source.
- Enter a data source time-out value or accept the default (120 seconds).
- If the **CASE-INSENSITIVE COMPARES** check box is not grayed-out, decide if case sensitivity should be a factor during data source searches.

If the check box is grayed-out, the selected ODBC driver does not support case-sensitive comparisons of values supplied by the end user with values stored in the database.

If the selected ODBC driver does support case-sensitivity and the box is checked, a search on a field such as LastName for the value "smith" returns "smith" but not "Smith", "SMITH", or any other combination of upper and lower case letters in the name.

If the selected ODBC driver supports case-sensitivity and the box is not checked, then the case-sensitivity of the underlying database is used.

Microsoft Access does not support this functionality, so the check box is grayed out.

Microsoft SQL Server is case-insensitive by default. Oracle is case-sensitive regardless of the platform.

Note: Case-insensitive comparisons have significant implications when hashed data is used for authentication. If case-insensitivity is enabled and a field is marked as hashed, when a value for that field is changed, the value is forced to uppercase, hashed, and stored. When an end user authenticates, the value supplied by the end user is forced to uppercase, hashed and compared to the value in the database. If case-insensitivity is disabled after some data hashed and stored using the previous setting and the underlying database is case-sensitive, the end user must supply all uppercase information during authentication for fields that are marked as hashed.

When case-insensitivity was enabled, the data was forced to uppercase and then hashed and stored. Now that the case-insensitive check box unchecked, the connector defaults to the ability of the database. If the database is case-sensitive, then any authentication attempts are going to require an all uppercase typed entry. What the user types is hashed and compared to find a match. If what the user typed is not uppercase, a case-sensitive match does not display.

9. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The Connector Configuration Manager shows the new target data source configured for the connector and each operation.

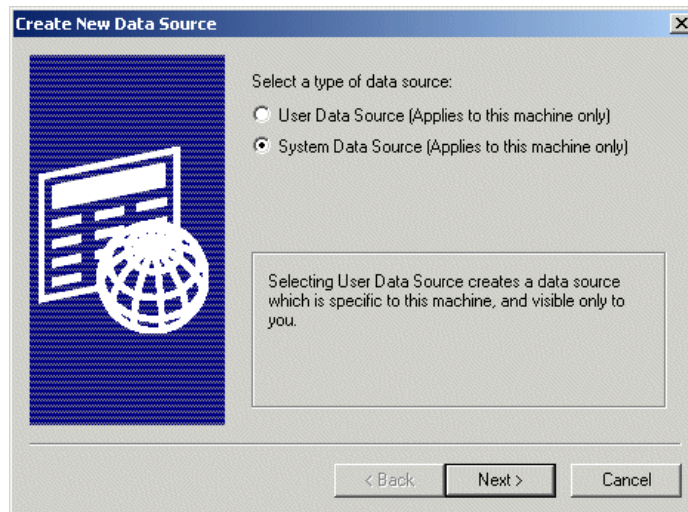
The target is now available for each provisioning action supported by this connector.

Adding a New Microsoft Access Data Source

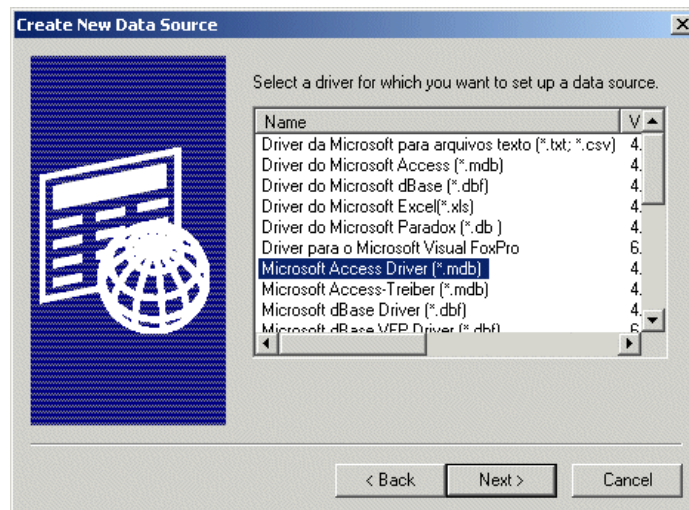
Follow steps 1 through 7 in [“Connector Configuration” on page 318](#).

1. In the Machine Data Source tab of the Select Data Source dialog box, click **NEW**.
The Create New Data Source dialog box appears.

Figure 140: Create New Microsoft Access Data Source

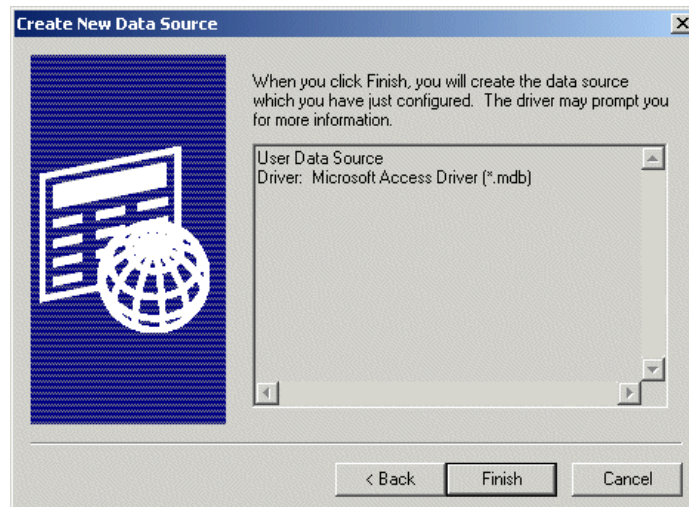


2. Select **SYSTEM DATA SOURCE** and click **NEXT**.
The driver selections dialog box appears as shown next.

Figure 141: Select Microsoft Access Driver

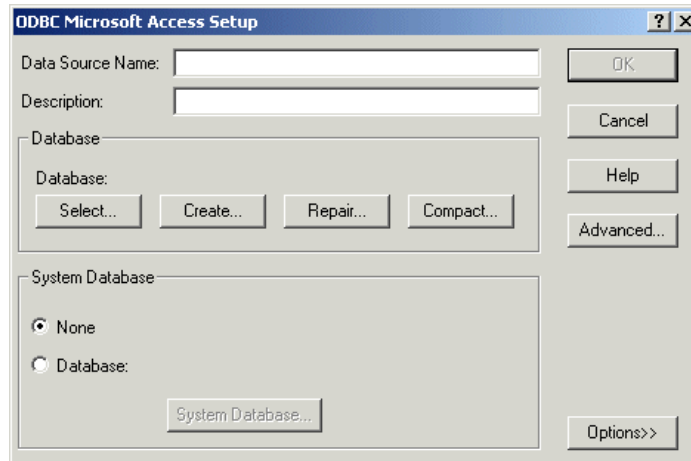
3. Select the Microsoft Access driver and click **NEXT**.

The summary dialog box appears.

Figure 142: New Microsoft Access Data Source - Summary

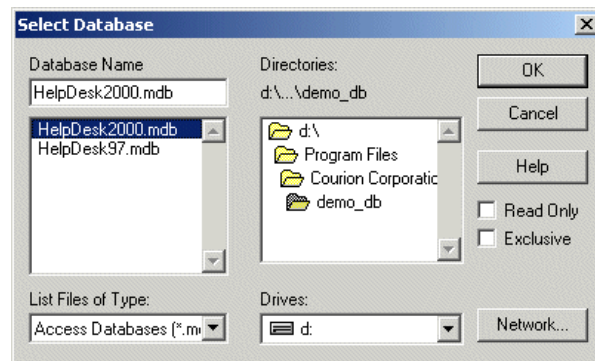
4. Review the summary of selections and click **FINISH**.

The Microsoft Access Setup dialog box appears.

Figure 143: Set Up Microsoft Access Data Source

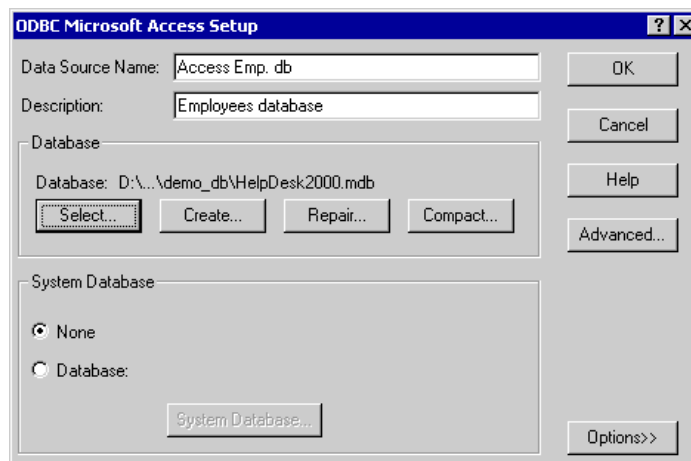
5. Enter a name for the data source and a description. This information appears in the Select Data Source dialog box ([Figure 138](#)). Click **SELECT...**.

The Select Database dialog box appears.

Figure 144: Select Microsoft Access Database

6. Locate and select the data source, then click **OK**.

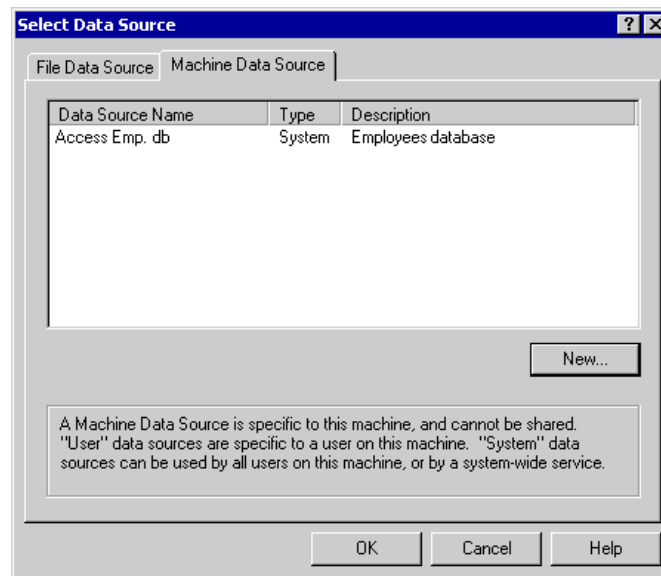
The Microsoft Access Setup dialog box reappears with the selected data source shown in the “Database:” field.

Figure 145: Setup Microsoft Access Data Source - Done

7. Click **OK**.

The Select System Data Source dialog box reappears with the new data source listed.

Figure 146: Select System for Microsoft Access Data Source - Done



The ODBC Targets dialog box reappears.

8. Return to step 8 on page 320.

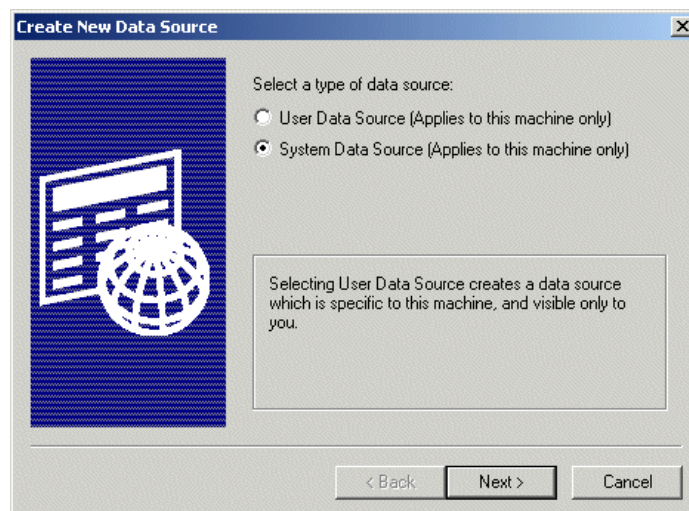
Adding a New SQL Server Data Source

Follow steps 1 through 7 in [“Connector Configuration” on page 318](#).

1. In the “Machine Data Source” tab of the “Select Data Source” dialog box, click **NEW**.

The “Create New Data Source” dialog box appears.

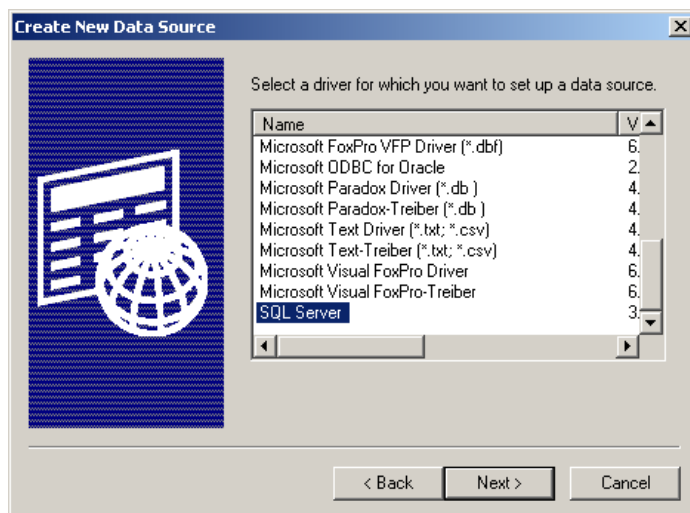
Figure 147: Create New Microsoft SQL Server Data Source



2. Select **SYSTEM DATA SOURCE** and click **NEXT**.

The driver selections dialog box appears.

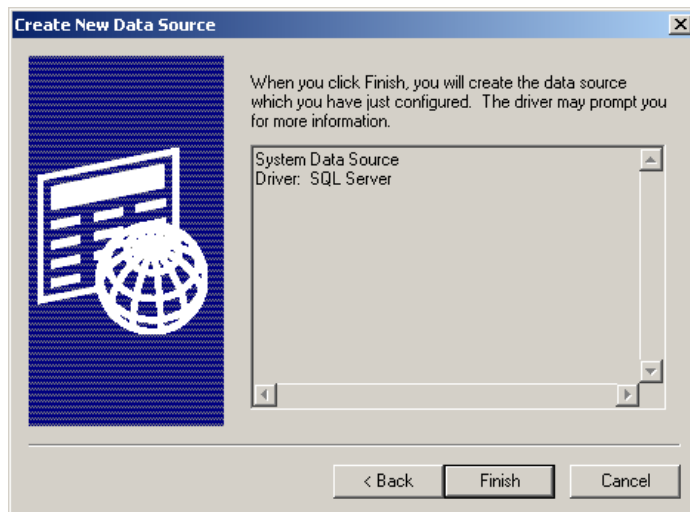
Figure 148: Select Microsoft SQL Server Driver



3. Select the SQL Server driver and click **NEXT**

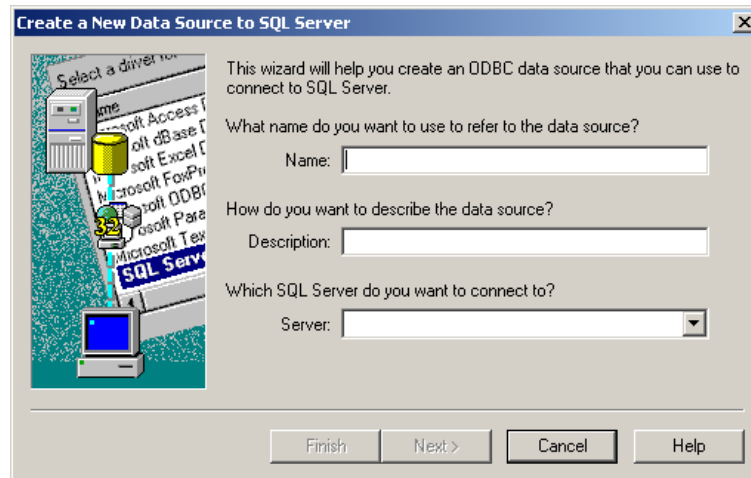
The summary dialog box appears.

Figure 149: New Microsoft SQL Server Data Source - Summary



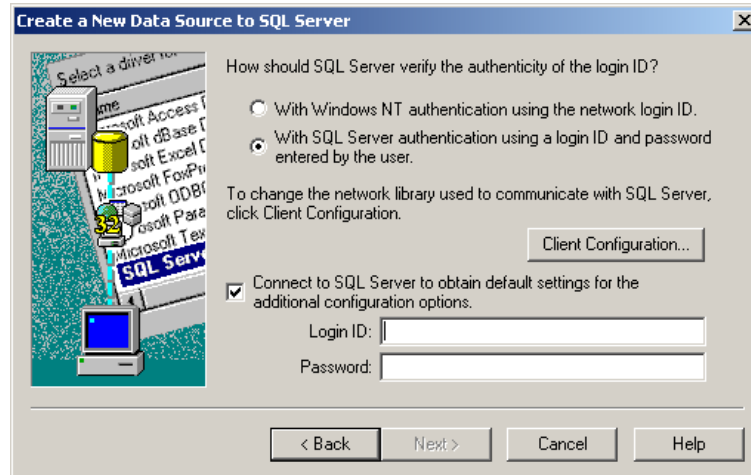
4. Review the summary of selections and click **FINISH**.

The Microsoft SQL Server setup dialog box appears as shown next.

Figure 150: Setup Microsoft SQL Server Data Source

5. Enter a name for the data source and a description in the **NAME** and **DESCRIPTION** fields. This information appears in the Select Data Source dialog box ([Figure 138](#)).
6. Click the down arrow in the “Server” text box and select the name of the server hosting the Microsoft SQL Server database.
7. Click **NEXT**.

The Microsoft SQL Server setup dialog box appears.

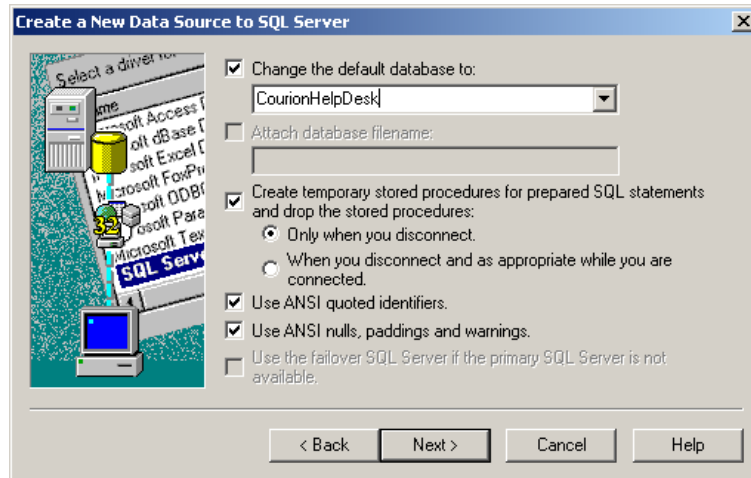
Figure 151: Setup Microsoft SQL Server Data Source - Authentication

8. Select **WITH SQL SERVER AUTHENTICATION USING A LOGIN ID AND PASSWORD ENTERED BY THE USER**.

Note: Online Help is available for all Microsoft SQL Server data source configuration dialog boxes. For detailed information on each dialog box option, click **HELP**.

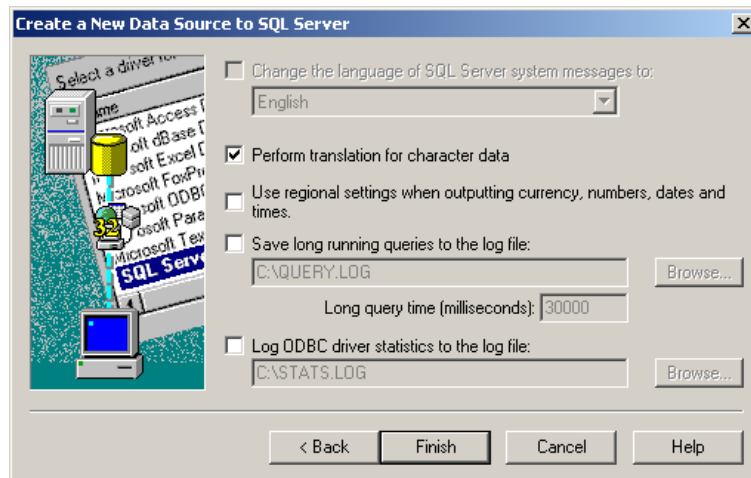
9. Enter the **LOGIN ID** and **PASSWORD** for the selected Microsoft SQL Server data source and click **NEXT**.

The Microsoft SQL Server setup dialog box appears as shown next.

Figure 152: Setup Microsoft SQL Server Data Source - Select Database

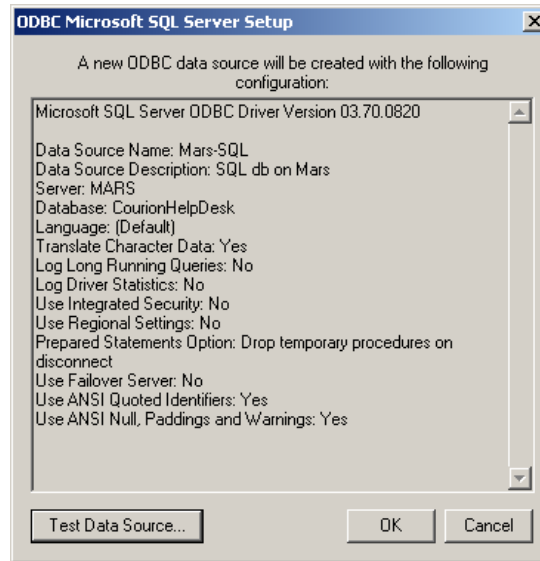
10. In the **CHANGE THE DEFAULT DATABASE TO:** text box, click the down arrow and select the appropriate database name.
11. Click **NEXT**.

The Microsoft SQL Server setup dialog box appears.

Figure 153: Setup Microsoft SQL Server Data Source - Log Files

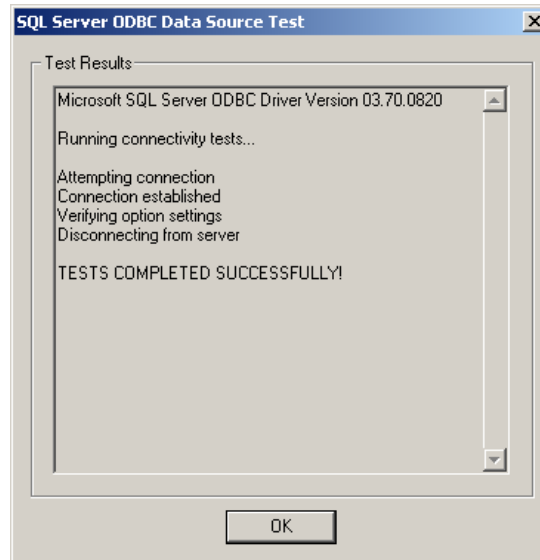
12. To change character data translation, use regional settings, or enable log files, select the appropriate check box.
13. Click **FINISH**.

A summary of selections appears.

Figure 154: Setup Microsoft SQL Server Data Source - Summary

14. To check setup selections, click **TEST DATA SOURCE...**

If the setup is configured correctly, the following window appears:

Figure 155: Setup Microsoft SQL Server Data Source - Successful Configuration

15. Click **OK**.

The ODBC Targets dialog box reappears.

16. Return to step 8 on page 320.

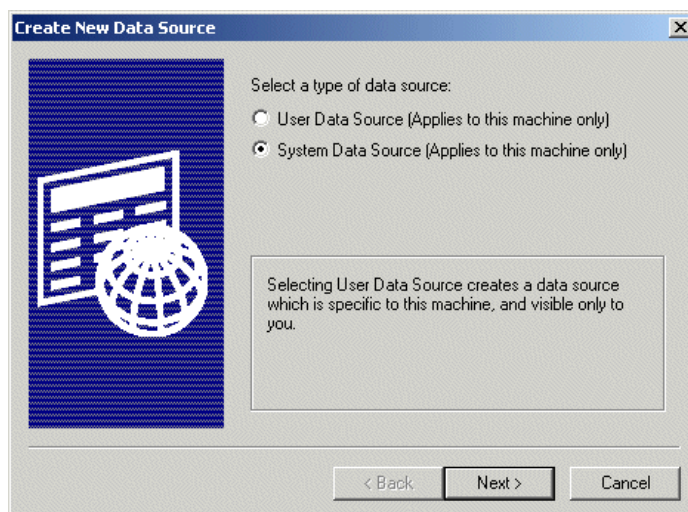
Adding a New Oracle Data Source

Follow steps 1 through 7 in [“Connector Configuration” on page 318](#).

1. In the Machine Data Source tab of the Select Data Source dialog box, click **NEW**.

The Create New Data Source dialog box appears.

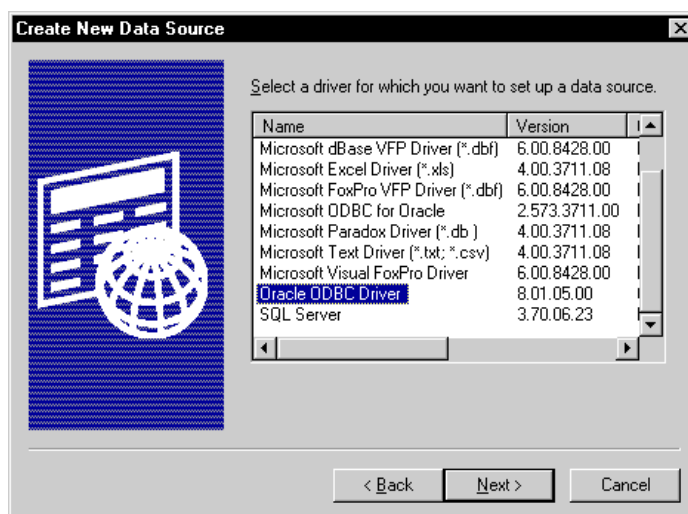
Figure 156: Create New Oracle Data Source



2. Select **SYSTEM DATA SOURCE** and click **NEXT**.

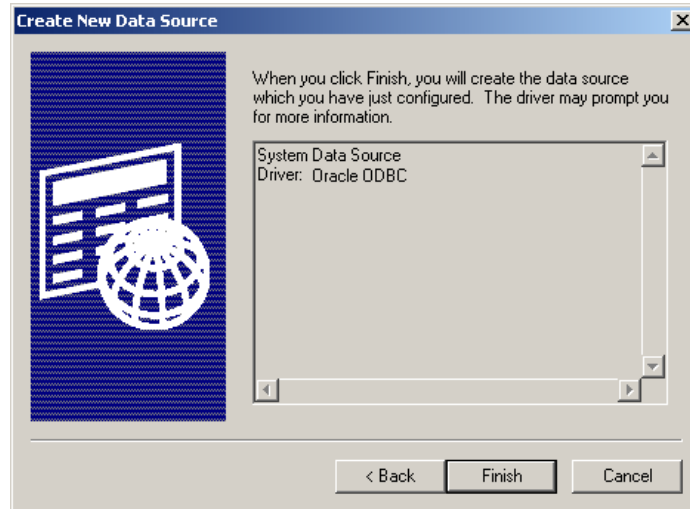
The driver selections dialog box appears.

Figure 157: Select Oracle Driver



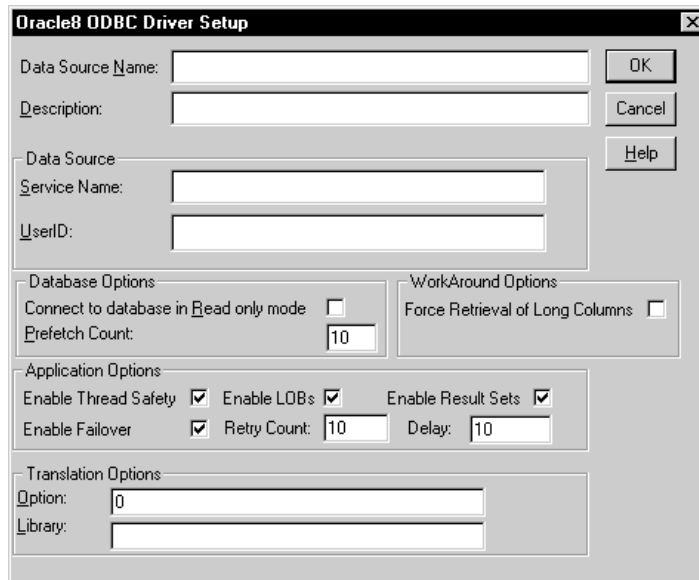
3. Select the Oracle ODBC driver and click **NEXT**.

The summary dialog box appears.

Figure 158: New Oracle Data Source - Summary

4. Review the summary of selections and click **FINISH**.

The Oracle driver setup dialog box appears.

Figure 159: Set Up Oracle Data Source

5. Enter a data source name and a description in the **DATA SOURCE NAME** and **DESCRIPTION** fields. This information appears in the Select Data Source dialog box ([Figure 138](#)).
6. Enter the name of the Oracle server in the **SERVICE NAME** text box.
7. Enter the user id for the server in the **USERID** text box.
8. Click **OK**.
The ODBC Targets dialog box reappears.
9. Return to step 8 on page 320.

Supported Data Types

Courion does not support the Nchar or Ntext data types for ODBC databases.

Notes

When you configure ticketing for the ODBC driver in the PasswordCourier Classic Customization Manager, an autonumber which is not a primary key displays as REQUIRED.

Chapter 35: Configuring the PMM for Microsoft Office365

This chapter explains how to configure the Password Management Module (PMM) for Microsoft Office365:

- [*“Configuring the PMM for Microsoft Office365”*](#)

Configuring the PMM for Microsoft Office365

The Password Management Module (PMM) for Microsoft Office365 supports password resets on a target.

Target Requirements

To configure the PMM, you need values for the following parameters on the target system:

- **ScriptName:** Set to MicrosoftOffice365PMMCnctr.js
- **AdminUserID:** Office 365 administrative account name. The user id must be an email address. This email address dictates which server the connector logs into by the domain part of the email address.
- **AdminUserPassword:** Office 365 administrative account password.
- **ServiceName:** Office 365 subscription service plan name. If the subscription were "contoso:ENTERPRISEPACK" the ServiceName would be "contoso".
- **ForcePasswordChangeAtNextLogon:** A flag displaying if the user has to change the password at next logon or not.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in ["Using the PMM Gateway Connector to Define PMM Targets" on page 61](#).

Connector Framework and Connector Framework Manager Server Requirements

This PMM is only supported on Windows Server® 2008 R2. You need to install the following tools on each server on which the Connector Framework or Connector Framework Manager is installed:

- Microsoft .Net Framework 2.0 or higher
- Windows PowerShell 2.0
- Microsoft Online Services Sign-In Assistant (IDCRL7) - 64 bit version
- Microsoft Online Services Module for Windows PowerShell (64-bit version)

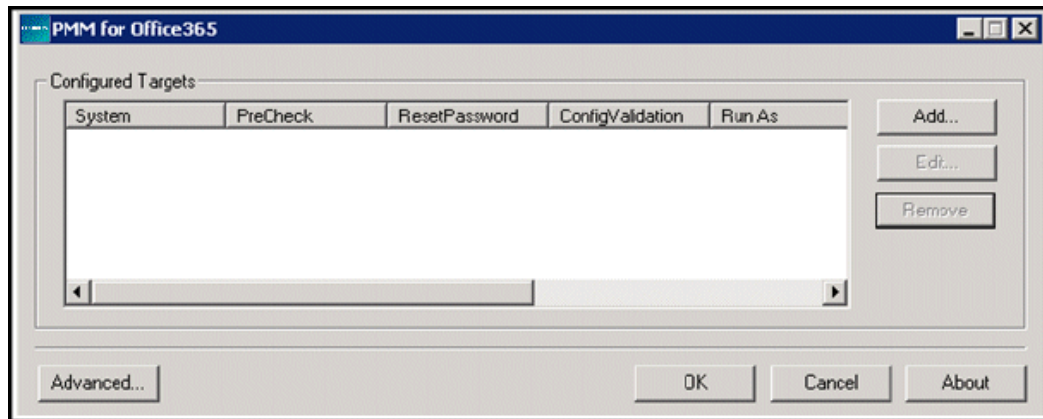
PMM Configuration

To configure the PMM:

1. From the Start menu, select:

Programs>Courion Access Assurance Suite>Password Management
Modules>Microsoft Office365

The Configuration Manager displays the Add Target dialog box. This dialog box shows any previously configured targets.

Figure 160: PMM Configuration Manager for Office365

2. From this dialog box, you can:
- Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - Obtain the product version number. Click the **ABOUT** button.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- When you select the **ADD** or **EDIT** option the Add/Edit Configuration dialog box appears.

Figure 161: Add/Edit Target Configuration

Add / Edit Target Configuration

Target Name:
0365

PreCheck Command Line:
C:\Windows\Sys\O\W64\cscript.exe /nologo /b PMMRDK2AMMRDKRedirect.js

ResetPasswordEx Command Line:
C:\Windows\Sys\O\W64\cscript.exe /nologo /b PMMRDK2AMMRDKRedirect.js

ConfigValidation Command Line:
C:\Windows\Sys\O\W64\cscript.exe /nologo /b PMMRDK2AMMRDKRedirect.js

☐ Run Commands as User

Domain\User:

User Password:

Configure Parameters for System

Parameter:
Value:
Verify Value:
☒ Secure Attribute

Add >> << Remove

Name	Value
AdminUserID	bburns@couro365.co
AdminUserPassword	XXXXXXXXXX
ForcePasswordChang...	True
ScriptName	MicrosoftOffice365PM
ServiceName	couro365ds

OK Cancel

3. **TARGET NAME** - Enter the name of the target where you want to perform the password resets. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **COMMAND LINES** - Enter the same location for all three command lines: PreCheck Command Line, ResetPassword Command Line, and ConfigValidation Command Line. The command line for the standard location is:
cscript /nologo /b PMMRDK2AMMRDKRedirect.js
5. **RUN COMMANDS AS USER** - Leave this box unchecked.
6. **CONFIGURE PARAMETERS FOR SYSTEM** - Enter in the PMM Configuration Parameters as shown in Table 15. Enter the parameter name in the Parameter text box, then enter the appropriate value in the Value text box. If the Secure Attribute checkbox is selected, you must enter the value in both the Value and Verify text boxes. Click **Add** to move the entry to the list on the right side. Do not use quotes when entering these parameters.

Table 15: PMM Configuration Parameters

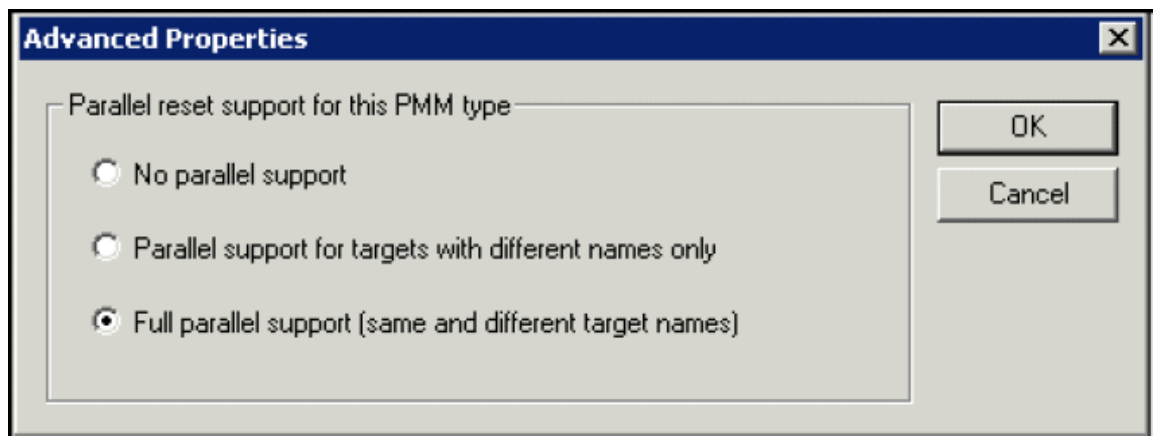
Parameter Name (parameter names are case sensitive)	Value	Check as Secure
AdminUserID	Office365 administrative account name. The user id must be an email address. This email address dictates which server the PMM logs into by the domain part of the email address. Note: This account requires the Global Administrator role.	No
AdminUserPassword	Office365 administrative account password.	Yes
ServiceName	Office365 subscription service plan name. If the subscription were "contoso:ENTERPRISEPACK" the ServiceName would be "contoso".	No
ForcePasswordChangeAtNextLogon	A flag representing whether users are forced to change their passwords at the next logon or not.	No
ScriptName	Set to MicrosoftOffice365PMMCntr.js.	No

Click **OK** when you have entered values for all parameters and checked them as secure or not.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value.

7. Select the target that you have just configured from the PMM Configuration Manager for Office365 dialog box and click the **ADVANCED** button. The Advanced Properties dialog box appears.

Figure 162: Advanced Properties

8. Select **FULL PARALLEL SUPPORT (SAME AND DIFFERENT TARGET NAMES)**. This is the default option. Click **OK**. Click **OK** on the PMM Configuration Manager for Office365 dialog box.

Chapter 36: Configuring the Connector for Microsoft Office365 Exchange Online

Please contact Customer Support to get the newer connector used to integrate to Microsoft Office 365. That connector can be used to integrate with Microsoft Office 365 instead of this connector available in the suite installation kit. It consolidates Exchange Online, Lync and SharePoint Online into one connector.

This chapter explains how to configure the Connector for Microsoft Office365 Exchange Online:

- [*“Configuring the Connector for Microsoft Office365 Exchange Online” on page 340*](#)
- [*“Licenses” on page 343*](#)
- [*“Using Triggers” on page 344*](#)
- [*“Native Query \(Macros\)” on page 345*](#)

Configuring the Connector for Microsoft Office365 Exchange Online

The Connector for Microsoft Office365 Exchange Online supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, View, Native Query, Collector, and Trigger.

Prerequisites

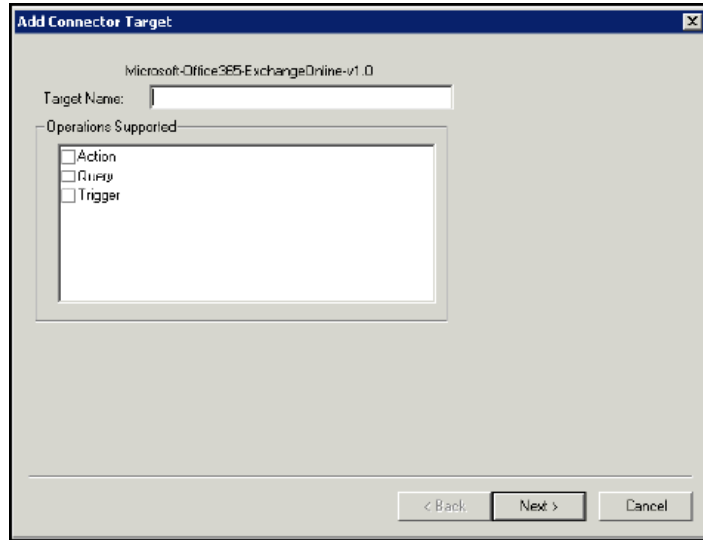
This connector is only supported on Windows Server® 2008 R2. You need to install the following tools on each server in which the Connector Framework or Connector Framework Manager is installed:

- Microsoft .Net Framework 2.0 or higher
- Windows PowerShell 2.0
- Microsoft Online Services Sign-In Assistant (IDCRL7) - 64 bit version
- Microsoft Online Services Module for Windows PowerShell (64-bit version)

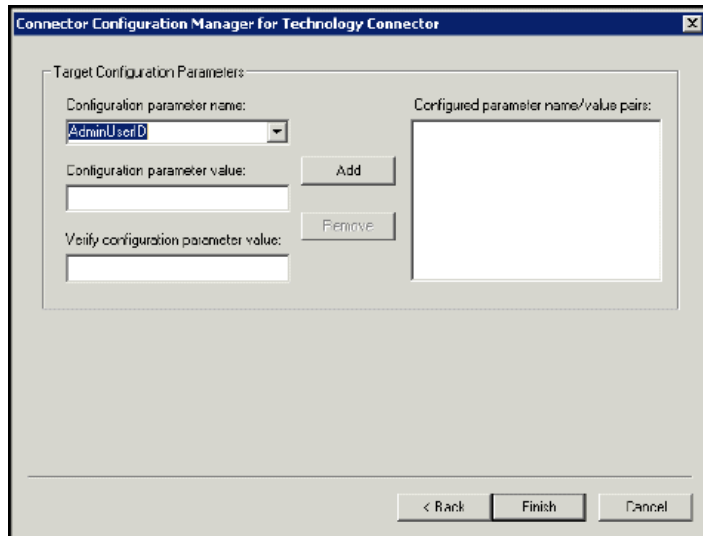
Connector Configuration

Follow these steps to configure a target domain:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Select:
File>Add Connector, select Microsoft-Office365-ExchangeOnline-V1.0
Click **OK**
3. Select **MICROSOFT-OFFICE365-EXCHANGEONLINE-V1.0**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 163: Add Microsoft Office365 Exchange Online Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface. Select the operations you want to use: Action, Query, Trigger.
6. Click **NEXT**. The Connector Configuration Manager is displayed.

Figure 164: Connector Configuration Manager

7. The drop-down list, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Values always appear as asterisks ("*") for security.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value. Table 16 lists the connector Configuration Parameters for the connector. Do not use quotes when entering these parameters.

Table 16: Connector Configuration Parameters

Parameter Name (parameter names are case sensitive)	Value
AdminUserID	Office365 administrative account name. The user id must be an email address. This email address dictates which server the connector logs into by the domain part of the email address. Note: This account requires the Global Administrator role.
AdminUserPassword	Office365 administrative account password.
ServiceName	Office365 subscription service plan name. If the subscription were "contoso:ENTERPRISEPACK" the ServiceName would be "contoso".
OnPremiseExchangeServer	Fully Qualified Domain Name (FQDN) of the on-premise Exchange 2010 SP1 server which is in hybrid configuration with Microsoft Office365 hosted in cloud.
OnPremiseExchangeUser	Admin user who has rights to connect to the on-premise Exchange 2010 SP1 server and execute the Exchange command. Note: This account requires any specific rights to successfully execute a configured trigger command.
OnPremiseExchangePwd	Admin user's password to connect to the on-premise Exchange 2010 SP1 server and execute the Exchange command.
OnPremiseExchangeAuth	Authentication method to use when connecting to the on-premise exchange. Select one of these methods: Kerberos, Basic, Digest, Negotiate. The default is Kerberos.
OnPremiseExchangeUseSSL	When set to ON , use SSL for on-premise communication. When OFF , use regular (encrypted) HTTP. The default is OFF .
MaxWaitForLicense	Maximum wait time (in minutes) to verify the assigned licenses. The default is 0 (zero) minutes.
AllowAllLicenses	When set to ON , allow the target to set licenses for all Office365 services. Note that the ID map may need to be updated manually in this case. The default is OFF .

8. Click **FINISH** when you have entered values for all parameters.

Note: Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Licenses

This connector provisions Office365 Exchange Online licenses for user accounts. This connector only supports assigning or un-assigning Exchange and general Office licenses.

When the AllowAllLicenses is set to off, the connector supports provisioning licenses as shown in Table 17.

Table 17: Support for Provisioning Licenses

Actions	User's Current State	Allowed Actions
Create	User has no license or service.	Assign services within a single pack (plan). Example: Assign Plan1:Exchange or Plan2:Exchange
Create/ Update	User has at least one service from one type of plan.	Add another service within the same pack (plan). Example: Add Plan1:OFFICESUBSCRIPTION or Plan1:Exchange Trying to add Plan1:SharePoint, Plan1:Lync or any service of other pack (plan) results in an error.
Update	User has at least one service from one type of plan. Example: User has Plan1:Exchange, Plan1:OFFICESUBSCRIPTION, Plan1:SharePoint	Remove only Exchange specific or general existing services within the same pack (plan). Example: Remove Plan1:Exchange or Remove Plan1:OFFICESUBSCRIPTION. Trying to remove Plan1:SharePoint or Plan1:Lync via the Exchange connector is ignored.

Using Triggers

This connector provides a trigger interface to execute the Exchange commands on the Active Directory user account. Example:

To Enable RemoteMailbox: This trigger can be invoked on success of the on-premise Connector for Microsoft Active Directory's provisioning action to enable the new Active Directory user as a Remote Mailbox user.

To Enable MailUser: This trigger can be invoked on success of the on-premise Connector for Microsoft Active Directory's provisioning action to mail enable the Active Directory user.

Attribute supported by this action:

Command: Exchange command to be executed on the Exchange Server specified in OnPremiseExchangeServer attribute.

Example:

```
Enable-RemoteMailBox <UserPrincipalName>
```

```
Enable-RemoteMailbox <username> -RemoteRoutingAddress  
<alias>@<tenantName>.mail.onmicrosoft.com
```

```
Enable-MailUser -Identity <UserPrincipalName> -ExternalEmailAddress  
<ExternalEmailAddressValue>
```

Note: Replace the parameter values surrounded by angle brackets with an actual value or a macro that represents the value.

Native Query (Macros)

Get Licenses

The *get licenses* script collects all the existing Office365 licenses belonging to the service plan configured in the target parameter `ServiceName`.

To use the *get licenses* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetLicenses`
3. When the macro runs, the Native Query interface returns a comma separated list of licenses belonging to the service plan configured in the target parameter `ServiceName`

Get Admin Roles

The *get admin roles* script collects all of the available administrator roles on the Office365 server.

To use the *get admin roles* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetAdminRoles`
3. When the macro runs, the Native Query interface returns a comma separated list of administrator roles.

Chapter 37:Configuring the Connector for Microsoft Office365 Lync Online

Please contact Customer Support to get the newer connector used to integrate to Microsoft Office 365. That connector can be used to integrate with Microsoft Office 365 instead of this connector available in the suite installation kit. It consolidates Exchange Online, Lync and SharePoint Online into one connector.

This chapter explains how to configure the Connector for Microsoft Office365 Lync Online:

- [*“Configuring the Connector for Microsoft Office365 Lync Online” on page 348*](#)
- [*“Licenses” on page 351*](#)
- [*“Native Query \(Macros\)” on page 352*](#)

Configuring the Connector for Microsoft Office365 Lync Online

The Connector for Microsoft Office365 Lync Online supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, View, Native Query, and Collector.

Prerequisites

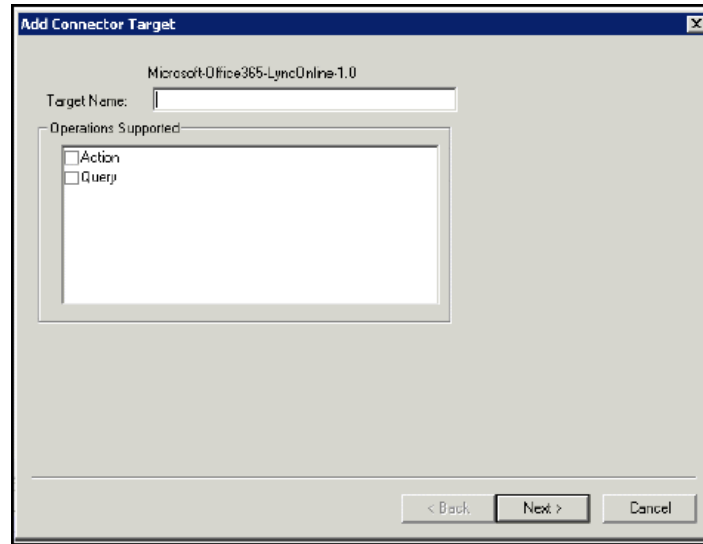
This connector is only supported on Windows Server® 2008 R2. You need to install the following tools on each server in which the Connector Framework or Connector Framework Manager is installed:

- Microsoft .Net Framework 2.0 or higher
- Windows PowerShell 2.0
- Microsoft Online Services Sign-In Assistant (IDCRL7) - 64 bit version
- Microsoft Online Services Module for Windows PowerShell (64-bit version)

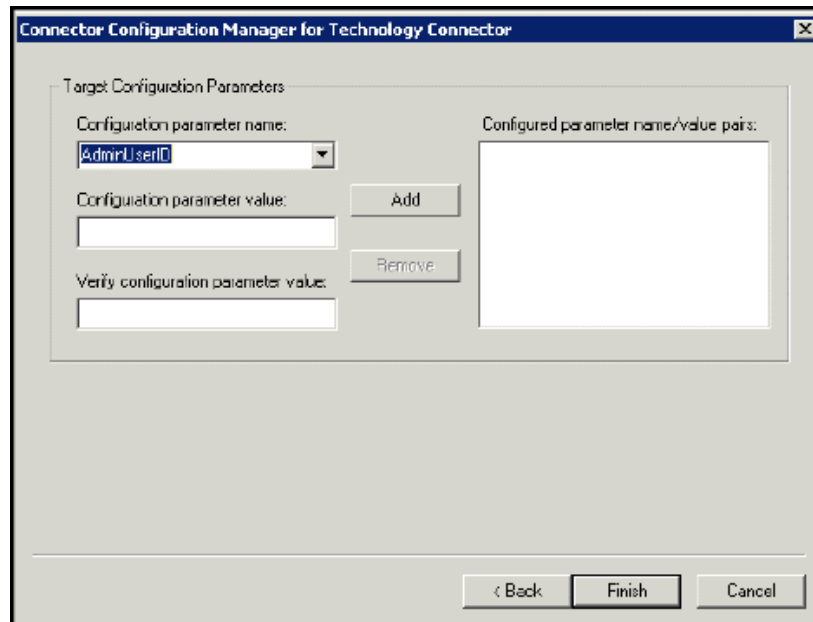
Connector Configuration

Follow these steps to configure a target domain:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Select:
File>Add Connector, select Microsoft-Office365-LyncOnline-v1.0
Click **OK**
3. Select **MICROSOFT-OFFICE365-LYNCONLINE-V1.0**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 165: Add Microsoft Office365 Lync Online Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface. Select the operations you want to use: Action, Query.
6. Click **NEXT**. The Connector Configuration Manager is displayed.

Figure 166: Connector Configuration Manager

7. The drop-down list, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Values always appear as asterisks ("*") for security.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value. Table 18 lists the connector Configuration Parameters for the connector. Do not use quotes when entering these parameters.

Table 18: Connector Configuration Parameters

Parameter Name (parameter names are case sensitive)	Value
AdminUserID	Office365 administrative account name. The user id must be an email address. This email address dictates which server the connector logs into by the domain part of the email address. Note: This account requires the Global Administrator Role.
AdminUserPassword	Office365 administrative account password.
ServiceName	Office365 subscription service plan name. If the subscription were "contoso:ENTERPRISEPACK" the ServiceName would be "contoso".
MaxWaitForLicense	Maximum wait time (in minutes) to verify the assigned licenses. The default is 0 (zero) minutes.
AllowAllLicenses	When set to ON , allow the target to set licenses for all Office365 services. Note that the ID map may need to be updated manually in this case. The default is OFF .

8. Click **FINISH** when you have entered values for all parameters.

Note: Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Licenses

This connector provisions Office365 Lync Online licenses for user accounts. This connector only supports assigning or un-assigning Lync and general Office licenses.

When the AllowAllLicenses is set to off, the connector supports provisioning licenses as shown in Table 19.

Table 19: Support for Provisioning Licenses

Actions	User's Current State	Allowed Actions
Create	User has no license or service.	Assign services within a single pack (plan). Example: Assign Plan1:Lync or Plan2:Lync
Create/ Update	User has at least one service from one type of plan. Example: User has Plan1:Exchange	Add another service within the same pack (plan). Example: Add Plan1:OFFICESUBSCRIPTION or Plan1:Lync Trying to add Plan1:Exchange, Plan1:SharePoint or any service of other pack (plan) results in an error.
Update	User has at least one service from one type of plan. Example: User has Plan1:Lync, Plan1:OFFICESUBSCRIPTION, Plan1:Exchange	Remove only Lync specific or general existing services within the same pack (plan). Example: Remove Plan1:Lync or Remove Plan1:OFFICESUBSCRIPTION. Trying to remove Plan1:Exchange or Plan1:SharePoint via the Lync connector is ignored.

Native Query (Macros)

Get Licenses

The *get licenses* script collects all the existing Office365 licenses belonging to the service plan configured in the target parameter `ServiceName`.

To use the *get licenses* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetLicenses`
3. When the macro runs, the Native Query interface returns a comma separated list of licenses belonging to the service plan configured in the target parameter `ServiceName`

Get Admin Roles

The *get admin roles* script collects all of the available administrator roles on the Office365 server.

To use the *get admin roles* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetAdminRoles`
3. When the macro runs, the Native Query interface returns a comma separated list of administrator roles.

Chapter 38: Configuring the Connector for Microsoft Office365 SharePoint Online

Please contact Customer Support to get the newer connector used to integrate to Microsoft Office 365. That connector can be used to integrate with Microsoft Office 365 instead of this connector available in the suite installation kit. It consolidates Exchange Online, Lync and SharePoint Online into one connector.

This chapter explains how to configure the Connector for Microsoft Office365 SharePoint Online:

- [*“Configuring the Connector for Microsoft Office365 SharePoint Online” on page 354*](#)
- [*“Licenses” on page 357*](#)
- [*“Native Query \(Macros\)” on page 358*](#)

Configuring the Connector for Microsoft Office365 SharePoint Online

The Connector for Microsoft Office365 SharePoint Online supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, View, Native Query, and Collector.

Prerequisites

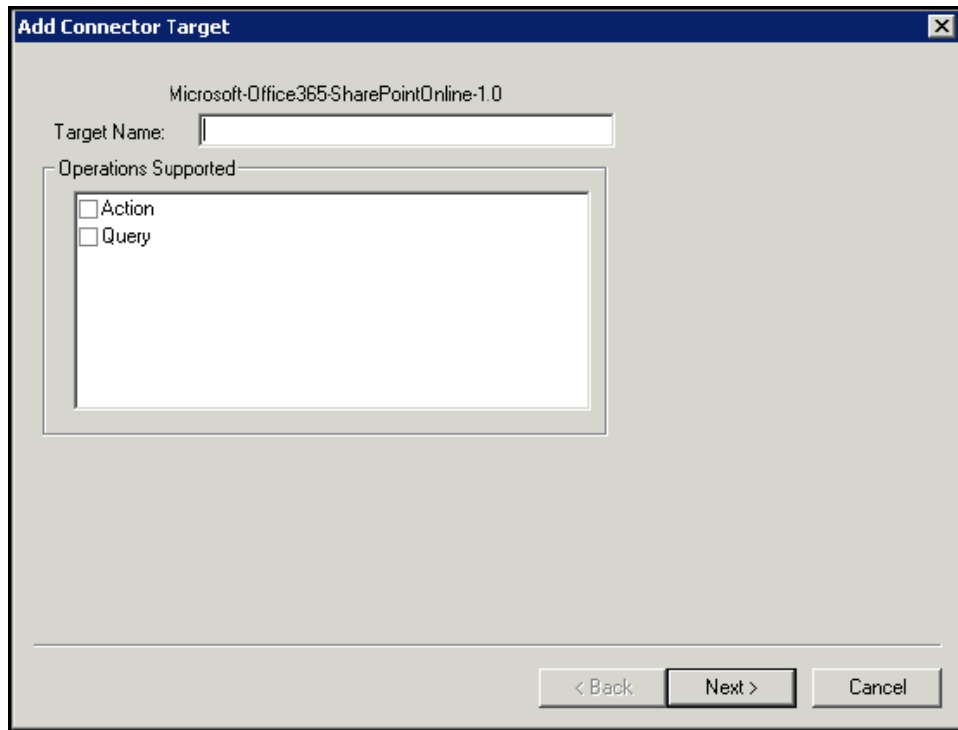
This connector is only supported on Windows Server® 2008 R2. You need to install the following tools on each server in which the Connector Framework or Connector Framework Manager is installed:

- Microsoft .Net Framework 2.0 or higher
- Windows PowerShell 2.0
- Microsoft Online Services Sign-In Assistant (IDCRL7) - 64 bit version
- Microsoft Online Services Module for Windows PowerShell (64-bit version)

Connector Configuration

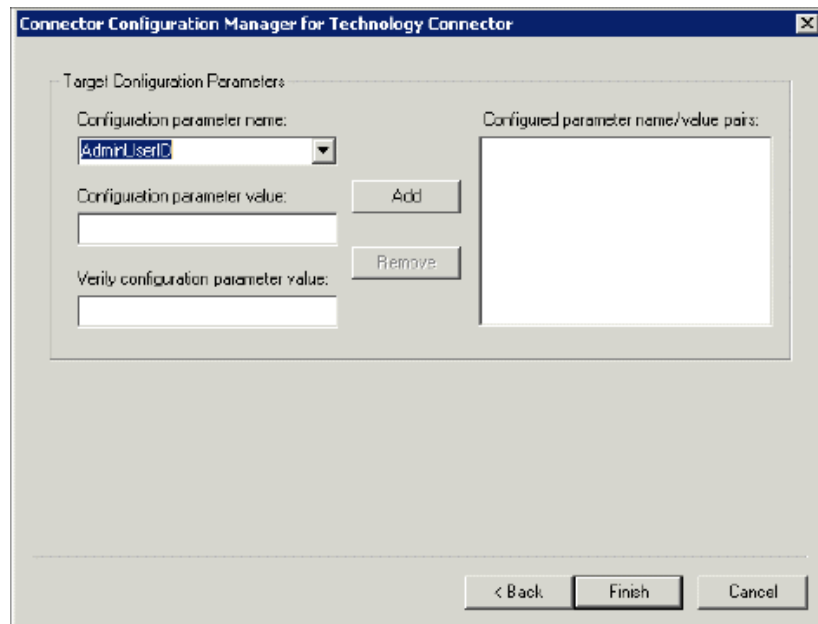
Follow these steps to configure a target domain:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Select:
File>Add Connector, select Microsoft-Office365-SharePointOnline-v1.0
Click **OK**
3. Select **MICROSOFT-OFFICE365-SHAREPOINTONLINE-V1.0**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 167: Add Microsoft Office365 SharePoint Online Target

The dialog box is titled "Add Connector Target" and has a close button (X) in the top right corner. Below the title bar, the text "Microsoft-Office365-SharePointOnline-1.0" is displayed. There is a "Target Name:" label followed by a text input field. Below this is a section titled "Operations Supported" which contains a list box with two items: "Action" and "Query", each preceded by an unchecked checkbox. At the bottom right of the dialog are three buttons: "< Back", "Next >", and "Cancel".

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface. Select the operations you want to use: Action, Query.
6. Click **NEXT**. The Connector Configuration Manager is displayed.

Figure 168: Connector Configuration Manager

The dialog box is titled "Connector Configuration Manager for Technology Connector" and has a close button (X) in the top right corner. It contains a section titled "Target Configuration Parameters". Inside this section, there are three input fields: "Configuration parameter name:" with a dropdown menu showing "AdminUser10", "Configuration parameter value:" with a text input field, and "Verify configuration parameter value:" with a text input field. To the right of these fields are two buttons: "Add" and "Remove". To the right of the "Add" and "Remove" buttons is a large empty rectangular box labeled "Configured parameter name/value pairs:". At the bottom right of the dialog are three buttons: "< Back", "Finish", and "Cancel".

7. The drop-down list, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Values always appear as asterisks ("*") for security.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value. Table 20 lists the connector Configuration Parameters for the connector. Do not use quotes when entering these parameters.

Table 20: Connector Configuration Parameters

Parameter Name (parameter names are case sensitive)	Value
AdminUserID	Office365 administrative account name. The user id must be an email address. This email address dictates which server the connector logs into by the domain part of the email address. Note: This account requires the Global Administrator Role.
AdminUserPassword	Office365 administrative account password.
ServiceName	Office365 subscription service plan name. If the subscription were "contoso:ENTERPRISEPACK" the ServiceName would be "contoso".
MaxWaitForLicense	Maximum wait time (in minutes) to verify the assigned licenses. The default is 0 (zero) minutes.
AllowAllLicenses	When set to ON , allow the target to set licenses for all Office365 services. Note that the ID map may need to be updated manually in this case. The default is OFF .

8. Click **FINISH** when you have entered values for all parameters.

Note: Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Licenses

This connector provisions Office365 Lync Online licenses for user accounts. This connector only supports assigning or un-assigning Lync and general Office licenses.

When the AllowAllLicenses is set to off, the connector supports provisioning licenses as shown in Table 21.

Table 21: Support for Provisioning Licenses

Actions	User's Current State	Allowed Actions
Create	User has no license or service.	Assign services within a single pack (plan). Example: Assign Plan1:SharePoint or Plan2:SharePoint
Create/ Update	User has at least one service from one type of plan. Example: User has Plan1:Exchange	Add another service within the same pack (plan). Example: Add Plan1:OFFICESUBSCRIPTION or Plan1:SharePoint Trying to add Plan1:Exchange, Plan1:Lync or any service of other pack (plan) results in an error.
Update	User has at least one service from one type of plan. Example: User has Plan1:Lync, Plan1:OFFICESUBSCRIPTION, Plan1:Exchange	Remove only SharePoint specific or general existing services within the same pack (plan). Example: Remove Plan1:SharePoint or Remove Plan1:OFFICESUBSCRIPTION. Trying to remove Plan1:Exchange or Plan1:Lync via the SharePoint connector is ignored.

Native Query (Macros)

Get Licenses

The *get licenses* script collects all the existing Office365 licenses belonging to the service plan configured in the target parameter `ServiceName`.

To use the *get licenses* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetLicenses`
3. When the macro runs, the Native Query interface returns a comma separated list of licenses belonging to the service plan configured in the target parameter `ServiceName`

Get Admin Roles

The *get admin roles* script collects all of the available administrator roles on the Office365 server.

To use the *get admin roles* script:

1. Create a macro through the Administration Manager using the Native Query interface of the connector.
2. Pass this string to the Native Query: `QueryType:GetAdminRoles`
3. When the macro runs, the Native Query interface returns a comma separated list of administrator roles.

Chapter 39: Microsoft SQL Server — PMM and Connector

This chapter explains how to configure the PMM and Connector for Microsoft SQL Server®:

- [*“Configuring the PMM for Microsoft SQL Server” on page 360*](#)
- [*“Configuring the Connector for Microsoft SQL Server” on page 367*](#)

Configuring the PMM for Microsoft SQL Server

The Password Management Module (PMM) for Microsoft SQL Server enables Access Assurance Suite end users to reset passwords on an SQL Server. The PMM for SQL Server is installed with the Courion Access Assurance Suite. For more information on the installation, please refer to *Installing the Access Assurance Suite*.

The PMM for SQL Server requires an access key. For information about the access key, please contact Core Security.

Prerequisites

The server must be running Microsoft Open Database Connectivity with ODBC Administrator Service enabled.

The appropriate client software for Microsoft SQL Server supported ODBC drivers must exist on every client machine where a password reset occurs.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Data Source Name Configuration

Data Source Names (DSNs) are used to identify the data source so Core Password can make connections to the database to issue password reset commands. Once the reset is complete, Core Password then closes the connection to the database. This process occurs for every database password reset for each target.

The target contains the information necessary to make an ODBC connection to a database server. During target configuration, information about database driver(s) is required, as well as specified user name(s) that have sufficient rights to execute database password reset commands. The Microsoft SQL Server driver asks for information including, but not limited to:

- DSN
- Description
- Server
- Network address
- Whether or not to use a trusted connection
- Database name
- Language name

Note: If the PMM is not configured using "Advance Mode," then the privileged user supplied in the target configuration must be able to execute the "execute sp_password" command, besides having the ability to open a connection to the database server to perform a password reset.

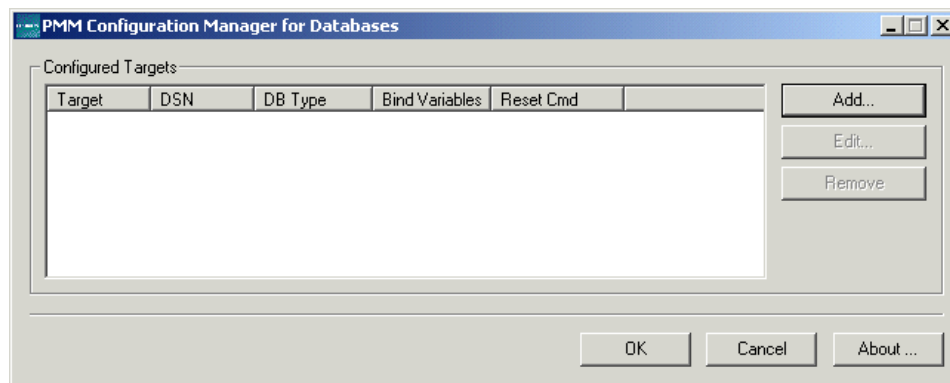
Note: Avoid using “ODBC” in the DSN as it can result in an error message.

PMM Configuration

To configure a DSN using the Microsoft SQL Server PMM:

1. From the Start menu, select:
Programs>Courion Access Assurance
Suite>Password Management Modules>Microsoft SQL Server
The PMM Configuration Manager for Databases dialog box appears.

Figure 169: PMM Configuration Manager for Microsoft SQL Server



2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box is displayed.

Figure 170: Add/Edit Target for Microsoft SQL Server

Add / Edit Target Configuration

Target information
Name:

Data Source
DSN name:
Database type:
Privileged user:
Password:

Commands
Reset password command:

Options
☐ Use bind variables

3. **TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **RESET PASSWORD COMMAND** — The default command for a reset is:
MSFT - sp_password NULL, "%pwd", "%user"
5. To set the Data Source, click the **SELECT DSN...** button.
The Data Source Name screen displays (not shown here).
6. Click the **MACHINE DATA SOURCE** tab.
The Machine Data Source screen appears.

Figure 171: Machine Data Source

Select Data Source

File Data Source Machine Data Source

Data Source Name	Type	Description
Courion_DSN	System	
demodb	System	
Employees_SQL	System	SQL db

A Machine Data Source is specific to this machine, and cannot be shared. "User" data sources are specific to a user on this machine. "System" data sources can be used by all users on this machine, or by a system-wide service.

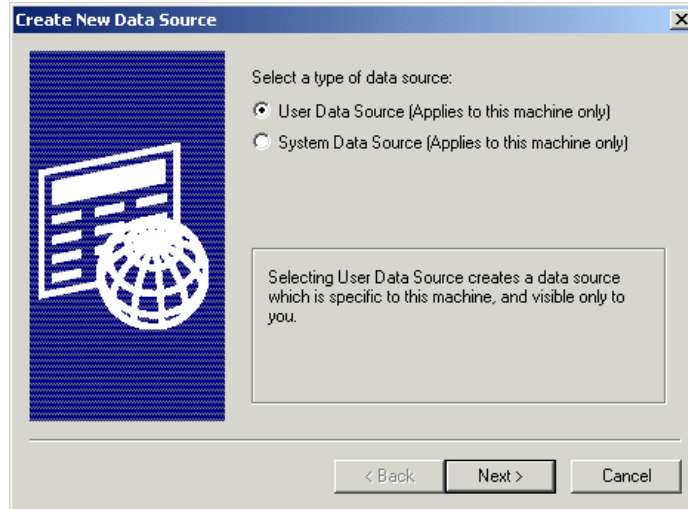
7. On the Machine Data Source screen, select a system data source from the available list or define a new data source.
 - To select an existing data source, click on the appropriate target in the **DATA SOURCE NAME** column and then click **OK**.

The Configure Database Targets tab displays the target in the **DATA SOURCE NAME** field. Skip to step 8, page 365.

- To define a new data source, click the **NEW** button.

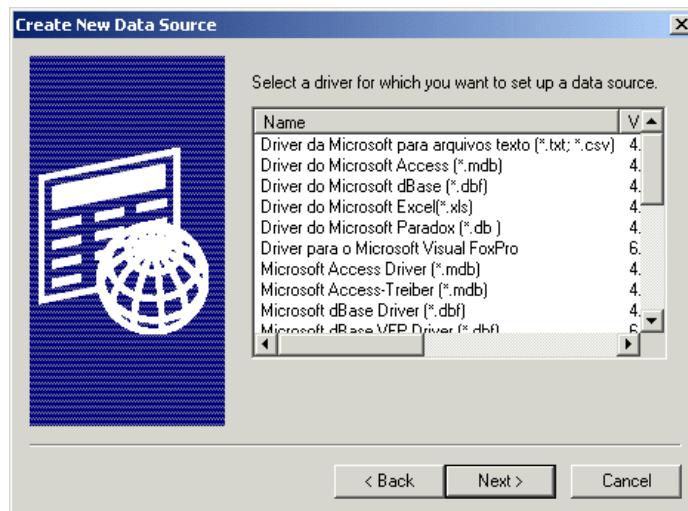
The Create New Data Source screen appears.

Figure 172: Create New Data Source Screen



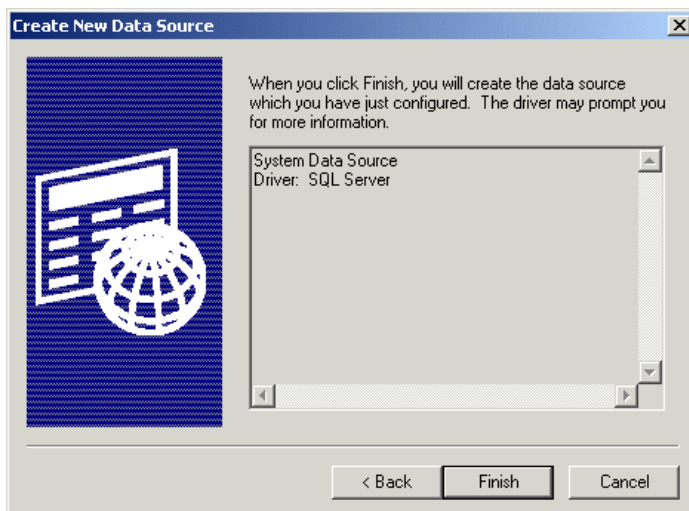
- c. Select the **SYSTEM DATA SOURCE** option and then click **NEXT**.
The Select Driver dialog box appears.

Figure 173: Data Source Driver Selection Screen



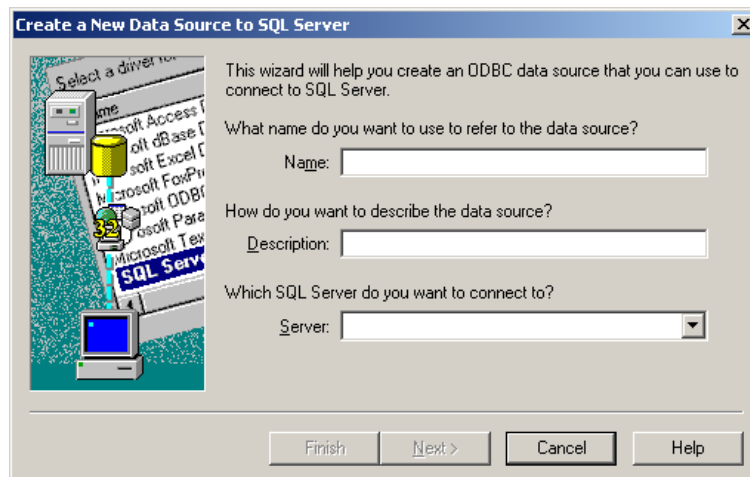
- d. Scroll through the resulting list of data source types, select the appropriate Sybase data source, and then click the **NEXT** button.

The Create New Data Source Summary screen appears.

Figure 174: Create New Data Source Summary Screen

- e. Click **FINISH**.

The Create a New Data Source to SQL dialog box appears.

Figure 175: Create a New Data Source to SQL Server Dialog Box

- f. Configure the data source on the remaining screens as needed. For information about configuring this type of data source, please refer to the database vendor's documentation.

Note: When you select the server to connect to, the dialog box **CREATE A NEW DATA SOURCE TO SQL SERVER** might not list all available servers in the **SERVER** field. You may need to enter the server name or IP address manually in this field.

After you configure the DSN and click **NEXT**, the Add/Edit Target screen returns with the newly-created DSN in the **DATA SOURCE NAME** field. The partially completed screen appears.

Figure 176: Partially Completed Add/Edit Target Databases

The screenshot shows a Windows-style dialog box titled "Add / Edit Target Configuration". It is divided into several sections:

- Target information:** A "Name:" label followed by a text box containing "SQL".
- Data Source:**
 - "DSN name:" label followed by a text box containing "Employees SQL" and a "Select DSN..." button.
 - "Database type:" label followed by a text box containing "Microsoft SQL Server".
 - "Privileged user:" label followed by a text box containing "sa".
 - "Password:" label followed by a masked text box (asterisks).
- Commands:** "Reset password command:" label followed by a text box containing the command: `execute sp_password DEFAULT, @new=\"%pwd\", @loginname=\"%`.
- Options:** A checkbox labeled "Use bind variables" which is currently unchecked.

At the bottom of the dialog are "OK" and "Cancel" buttons.

In the Add/Edit Target screen, complete these fields:

8. **PRIVILEGED USER** — Type the administrator username to authenticate the administrator for the DSN.
9. **PASSWORD** — Type the administrator password.
10. **RESET PASSWORD COMMAND** — This field shows a default reset password command. The default command you see depends of the type of database you are using. You can edit this default command for custom password resets.

In the Reset password command, the `%user` macro is the input argument for the username, and the `%pwd` macro is the input argument for the password. If you need to use an MD5 hashed password instead of the clear text version of the password you may use `%hpwd` instead of `%pwd`. If you do not include the macros, the custom command cannot use the information sent by the PMM to complete a request for password reset.

Note for Oracle only: The software modifies any existing Oracle targets that were configured using the Advanced configuration option to remove the extraneous quotes around the macros. The modification is done when the information is read from the configuration repository. No modification is made to the original entry. When the reset command is displayed in this dialog, the extraneous quotes do not display and if you save the target information, the reset command is saved in the updated format.

11. **USE BIND VARIABLES** — This Use bind variables option is available for Microsoft SQL Server and Oracle databases. (Microsoft SQL Servers use the term "parameter markers" for the same option.)

This option can improve performance on some servers. The server has a cache of recently executed statements. If you do not use bind variables, the PMM must execute a unique SQL statement for every unique password reset attempt. For example, this set of resets would enter three statements in the cache:

```
Cathy Courion resets her Oracle password to NewPwd
```

Cathy Courion resets her Oracle password to NewerPwd

Chris Courier resets his Oracle password to ChrisPwd

Using bind variables allows the PMM to prepare a single SQL statement with wild card characters. The wild card characters are replaced with specific user information at execution. The software enters the prepared wildcard SQL statement one time in the cache, and all resets are performed against that statement. See the sample password reset example below.

12. Click the **OK** button to add the DSN to the defined targets list at the bottom of the tab. When you click OK, the DSN information is validated, but the reset password command is not.

You have configured a target for this PMM.

Repeat this procedure for each data source on which you want password reset commands executed.

Sample Password Reset Example

The following is a sample Microsoft SQL Server configuration using bind variables (a stored procedure is already used by default).

1. Configure a Microsoft SQL Server target in the PMM for Databases.
2. Check the box **USE BIND VARIABLES**.
3. Enter the following in the **RESET PASSWORD COMMAND** field:

```
Execute sp_password DEFAULT, @new=%pwd, @loginname=%user
```

4. Click OK.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the Connector for Microsoft SQL Server

The Connector for Microsoft SQL Server® supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Note: Creating a new user through a workflow adds a new schema and makes the new user the owner of that schema.

To delete the user directly in the SQL server requires two steps:

- Delete the schema which the user owns.
- Delete the user.

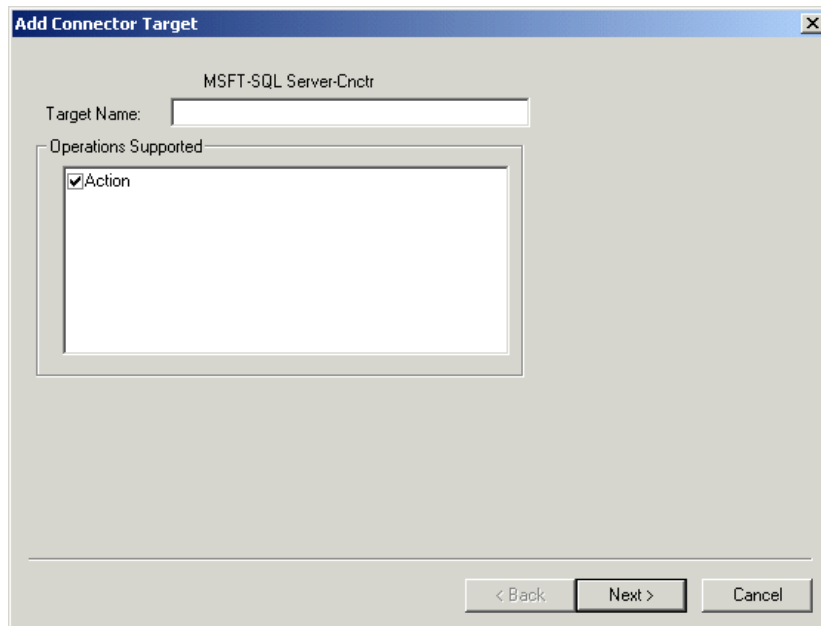
You can also delete the user through a workflow with the Delete action.

Connector Configuration

Follow these steps to add a target:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **MSFT-SQL SERVER-CNCTR**, and click **OK**.
3. Select **MSFT-SQL SERVER-CNCTR**
4. Click the right mouse button on the connector name and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 177: Add Microsoft SQL Server Target



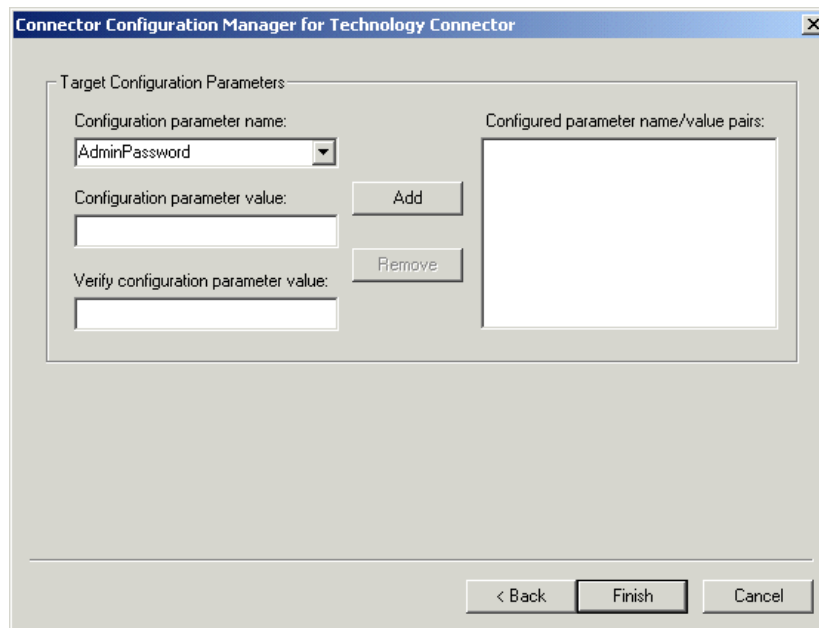
5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **ACTION** check box is selected by default.

6. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 178: Connector Configuration Manager for Microsoft SQL Server



7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **AdminPassword** — The password of the administrative user.
 - **AdminUser** — The name of the Microsoft SQL Server administrative user that can log on to the SQL server. This user must be a SQL login user, a member of the SQL Server **SECURITYADMIN** fixed server role, and the **DB_ACCESSADMIN** database role.
 - **Server** — The name of the Microsoft SQL Server.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 40: Microsoft-VBScript 5.6 — Connector

This chapter explains how to configure the Connector for Microsoft VBScript 5.6:

- [*“Configuring the Connector for Microsoft-VBScript 5.6” on page 370*](#)

Configuring the Connector for Microsoft-VBScript 5.6

The Connector for Microsoft-VBScript 5.6 supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, View
- Audit
- Authenticating
- Notification
- Query
- Event Triggers

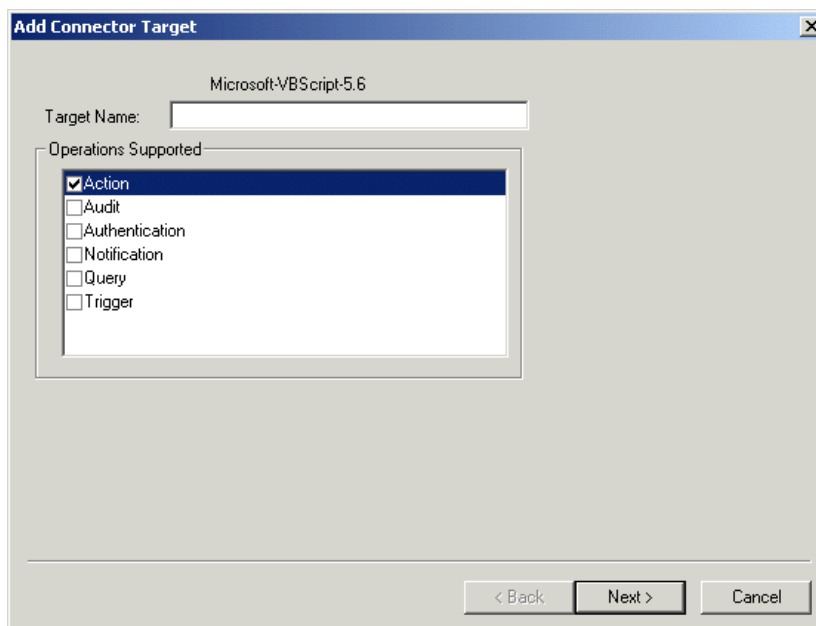
Connector Configuration

Follow these steps to add a target data source:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Select **MICROSOFT-VBSCRIPT-5.6**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 179: Add Microsoft VBScript Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select **ACTION** to enable all provisioning actions on a target.

Select **AUDIT** to enable Core Provisioning to create and update tickets on a target data source.

Select **AUTHENTICATION** to use the target data source for authenticating end user access to AccountCourier.

Select **NOTIFICATION** to enable HTML email functionality

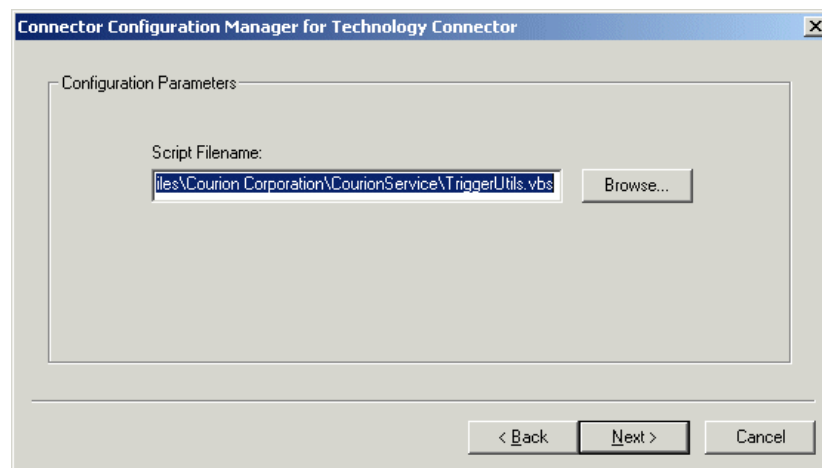
Select **QUERY** to enable Core Provisioning or Core Compliance to use queries to find data in the target data source.

Select **TRIGGER** to configure event triggers that initiate functions that you associate with certain events.

6. Click **NEXT**.

The Connector Configuration Manager for Technology Connector dialog box appears.

Figure 180: Connector Configuration Manager for Microsoft VBScript

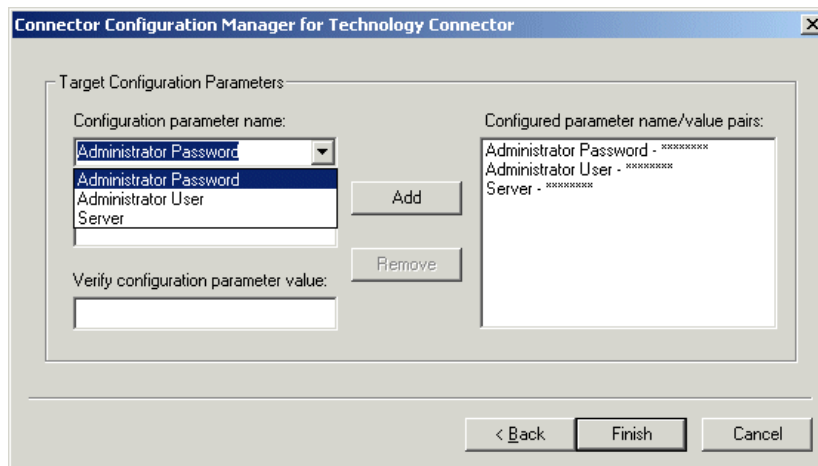


7. Enter a script name in the Script Filename box or click the **BROWSE** button and select a script name. Core Security provides the following scripts:
 - `sample.vbs`, which is a sample script that you can use as a guideline to write your own script. (This script does not actually perform any provisioning functions.)
 - `TriggerUtils.vbs`, which provides a trigger function called CopyDir that copies the contents of a source directory to a destination directory.
 - `ADTriggers.vbs`, which adds or removes a group to a Microsoft Active Directory account or Microsoft Windows NT account on a Resource Success event.

By default, these scripts are located in the `CourionService\scripts` directory.

8. After you select the script, click **NEXT**.

The target Configuration Parameters dialog box appears.

Figure 181: Connector Configuration Manager for Microsoft VBScript (2)

9. Each script requires different parameters to execute the function defined in the script. This dialog box enables you to select the parameters associated with the script you selected in the previous dialog box ([Figure 180](#)) and assign values to them.

To do this:

- g. Select a parameter name from the drop-down box by highlighting it. In this example, the `TriggerUtils.vbs` script requires the following parameters: Administrator Password, Administrator User, and Server name.
- h. Enter a value associated with that parameter in the **CONFIGURE PARAMETER VALUE** window and the **VERIFY CONFIGURATION PARAMETER VALUE** window.
- i. Click **ADD**. The parameter name appears in the **CONFIGURED PARAMETER NAME/VALUE PAIRS:** window. Secure information, such as user names and passwords, appear as xxxxxxxx.

10. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 41: Microsoft Windows 2000 and Windows NT — PMM and Connector

This chapter explains how to configure the PMM and Connector for Microsoft Windows 2000 and Windows NT Domains:

- [*“Configuring the PMM for Microsoft Windows NT and Windows 2000” on page 374*](#)
- [*“Configuring the Connector for Microsoft Windows NT Domains” on page 383*](#)

Configuring the PMM for Microsoft Windows NT and Windows 2000

The Password Management Module (PMM) for Microsoft Windows 2000 and Windows NT enables end users automatically to perform password resets and/or account unlock on Windows NT domains and workstations, Windows 2000 domains and workstations, and Windows XP Professional workstations.

Your site needs the correct access keys to run this PMM. For more information on access keys, please contact Core Server.

Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Using Security Options

This PMM provides the following options that support secure password resets on the Windows 2000 and Windows NT systems:

[“Allow Reset of Administrative Accounts”](#)
[“Conform to System Password History”](#)
[“Additional Password Settings for Admin Password Resets”](#)
[“Conform to System Minimum Password Age”](#)

Allow Reset of Administrative Accounts

This option enables you to specify whether or not the PMM for Windows NT and Windows 2000 resets passwords for users that are members of the following groups:

Administrators Group
Account Operators Group
Server Operators Group
Print Operators Group
Backup Operators Group
Communication Operators Group.

The PMM for Windows NT and Windows 2000 also does not reset passwords for disabled or expired accounts.

See the option **ALLOW RESET AND UNLOCK OF ADMINISTRATIVE ACCOUNTS** on page 379.

Conform to System Password History

The **CONFORM TO SYSTEM PASSWORD HISTORY** option forces Core Server to check the native operating system setting for password history or password uniqueness before it resets the password.

The password history setting determines the number of unique new passwords that need to be associated with an account before the user can re-use an old password. When Core Server resets a password on the native operating system, it actually performs a double password reset with a randomly generated password in addition to a user-specified password to ensure system security. Because of this, you need to specify a value that is double the number of unique password resets you want to associate with a user account when you configure the password history setting on the native operating system.

Without this option, the PMM for Windows NT and Windows 2000 does not compare a new password against the password history.

To maintain the effectiveness of the password history setting, use the Conform to Minimum Password Age option to prevent users from changing their passwords immediately after they were just changed. (See [“Conform to System Minimum Password Age” on page 376.](#))

Configuring the Password History Setting on Windows 2000

1. To configure the Password History setting on the Windows 2000 system, for the Start menu, select:
Settings > Control Panel > Administrative Tools > Local Security Policy
2. In the Local Security Settings folder, select:
Security settings > Account Policies > Password Policy > Enforce Password History
3. In the **LOCAL POLICY SETTING** window, specify a value that is double the number of unique passwords the user must enter before re-using an old password. For example, if you want to specify a password history value of 3, enter 6.

Configuring the Password History Setting on Windows NT

1. To configure the minimum password age on the Windows NT system, from the Start menu, select:
Programs > Administrative Tools (Common) > User Manager for Domains
2. From the **USER MANAGER** window, select a username.
3. From the **POLICIES** menu, select **ACCOUNT**.
4. From the **ACCOUNT POLICY** window, specify a number for the **PASSWORD UNIQUENESS** setting.

This number determines how many unique passwords a user must specify before re-using an old password. Specify a value that is double the number of unique passwords the user must enter before re-using an old password. For example, if you want to set a value of 3, enter 6.

Additional Password Settings for Admin Password Resets

You can specify additional password composition settings to control administrator password resets that are randomly generated when your site implements the “Conform to native system history” feature.

For more information about this feature, contact Core Server Customer Support.

Conform to System Minimum Password Age

The **CONFORM TO SYSTEM MINIMUM PASSWORD AGE** option forces Core Server to check the native operating system setting for minimum password age before it resets the password.

The minimum password age determines the number of days that must pass before a user can change his or her password. Defining a minimum password age prevents users from circumventing the password history policy by defining multiple passwords in rapid succession until they can use their old password again. The default value is 0. A value of a few days discourages rapid password recycling while still permitting users to change their own passwords.

Example: The minimum password age is set to one day. A user successfully changes his password to 3lmnop4 and attempts to reset it immediately. The attempt is unsuccessful and the system displays the following error:

The password on this account cannot be changed at this time. Password changed too recently.

The user can reset the password the next day as long as it complies with the rules for Conform to System Password History.

Setting the Minimum Password Age on a Windows 2000 System

1. From the Start menu, select:
Settings > Control Panel > Administrative Tools > Local Security Policy
2. In the Local Security Settings folder, select:
Security settings > Account Policies > Password Policy > Minimum Password Age
3. In the Local Security Policy Setting window, specify the minimum number of days the user must wait before changing a password.

Setting the Minimum Password Age on a Windows NT System

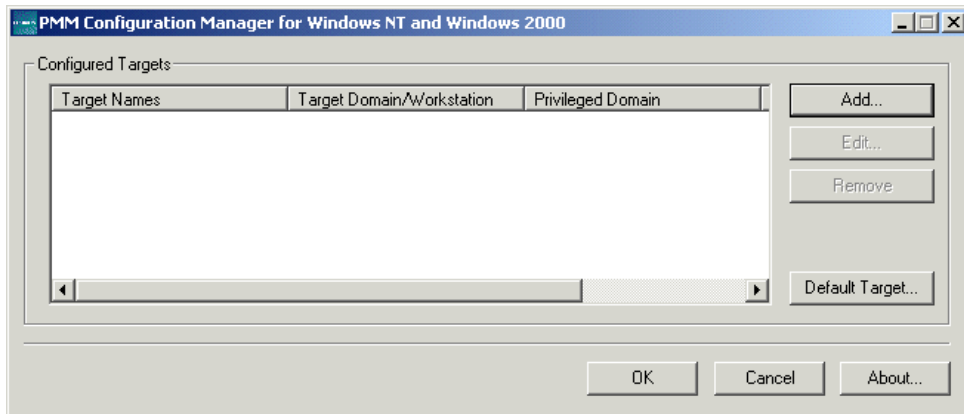
1. From the Start menu, select:
Programs > Administrative Tools (Common) > User Manager for Domains
2. From the **USER MANAGER** window, select a user name.
3. From the **POLICIES** menu, select **ACCOUNT**.
4. From the **ACCOUNT POLICY** window, you can specify the Minimum Password Age and the Maximum Password Age.

PMM Configuration

To configure this PMM, you must be logged on with the user right **LOG ON LOCALLY**.

1. From the Start menu, select:
Programs>Core Server Core Server> Password Management Modules >
Windows NT and Windows 2000
2. Click **YES** to start the PMM Configuration Manager.
The PMM Configuration Manager dialog box appears.

Figure 182: PMM Configuration Manager for Windows NT and Windows 2000



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Edit a target created with an earlier version of the PMM Configuration Manager with the **DEFAULT TARGET** button.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 183: Add/Edit Target Configuration for Windows NT and Windows 2000

Add / Edit Target Configuration

Target Information

Name:

Domain/Workstation:

Trusted and Privileged Account Information

Domain/Workstation:

Username:

Password:

Options

☐ Allow reset and unlock of administrative accounts

☐ Unlock account only

☐ Conform to system password history

☐ Use directory service DC for user verification

☐ Enhanced logging

☐ Conform to system minimum password age

Perform administrative logon :

☒ interactively

☐ as a service

OK Cancel

The Add/Edit for Windows NT and Windows 2000 settings are used for all Windows NT and Windows 2000 password resets for the specified domain/workstation.

4. TARGET INFORMATION

- a. Enter the Target name. (You cannot edit the name of an existing target.) You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
- b. Specify the domain or workstation where the password resets occur. Two backslashes “\” should precede the name of the workstation to indicate that the machine is a local workstation instead of a domain. The target domain or workstation must trust the domain or workstation of the privileged account.
If the domain is an Active Directory domain, enter either the DNS-style name or the NetBIOS name (for example: `Core Server.com` for a DNS-style domain name or `Core Server` for a NetBIOS domain name).

5. TRUSTED AND PRIVILEGED ACCOUNT INFORMATION

- a. Specify the domain or workstation of the privileged user for Windows NT and Windows 2000 password resets. Two backslashes “\” should precede the name of the workstation to indicate that the machine is a local workstation instead of a domain. The target domain or workstation specified for Windows NT password resets must trust each of the configured Windows NT password targets.
If the domain is an Active Directory domain, either enter the NetBIOS name or DNS-style name (for example: `Core Server.com` for a DNS-style domain name or `Core Server` for a NetBIOS domain name).

Note: To use the DNS-style name for the Active Directory, make sure the PMM is running on the Windows 2000 or higher operating system.

- b. Specify the privileged user. This user must be a member of the Account Operators or Administrators Group. Core Security recommends using a privileged user whose password never expires.

6. OPTIONS

- a. Decide whether or not to allow administrators to reset their passwords. To allow administrative resets, select the **ALLOW RESET AND UNLOCK OF ADMINISTRATIVE ACCOUNTS** check box.

Note: To use this functionality, the administrative user specified in the PMM Configuration Manager must be a member of the Administrators group on the domain that is being configured with the PMM.

- b. Select **UNLOCK ACCOUNT ONLY** to allow the administrative user to unlock an account without changing the password.
- c. To enforce Windows NT user restrictions regarding password uniqueness, select the **CONFORM TO SYSTEM PASSWORD HISTORY** check box.
- d. Select the **USE DIRECTORY SERVICE DC FOR USER VERIFICATION** check box to force the PMM to search a directory services (DS) domain controller (DC) first. If the PMM does not find the password on the DS DC, it searches for a non-DS DC to use. If you do not select this check box, the PMM uses the first appropriate DC that it finds whether it is a DS DC or a non-DS DC.

Note: This option applies to Windows 2000 or higher systems only. This box is greyed-out on Windows NT systems.

- e. Select the **ENHANCED LOGGING** check box to log the connection attempts to the ntmodule.log during a password reset attempt.
- f. Select the **CONFORM TO SYSTEM MINIMUM PASSWORD AGE** option to force Core Server to check the native operating system setting for minimum password age before it resets the password. If you do not enable this option (or the native operating system minimum password age is set to 0), Core Server ignores the native operating system setting for minimum age and resets the password if it is not in the password history list (and the **CONFORM TO SYSTEM PASSWORD HISTORY** option is enabled).
- g. Select the option **SELECT CLOSEST DOMAIN CONTROLLER** if you want Core Server to unlock and reset accounts on the Domain Controller closest to the end user's machine, rather than perform the reset on the Domain Controller closest to the Connector Framework. (Reset on the Domain Controller closest to the Connector Framework potentially requires the end user to wait until the reset is replicated to the rest of the network.)

Note: The privilege "Access this computer from the network" under "User Rights Assignment" in "Local Policies" of end-user machines should be granted to the privileged user, or the Default Domain Security Settings should be enabled on the domain controllers. Also, For the **SELECT CLOSEST DOMAIN CONTROLLER** option to work, the privileged user must be given the option to log on interactively (described in the next section).

7. PERFORM ADMINISTRATIVE LOGON

- a. Select the **PERFORM ADMINISTRATIVE LOGON OPTION** to perform a password reset. The PMM must log into the Windows NT or Windows 2000 target system using the privileged account information specified.

INTERACTIVELY — Interactive log on is the default and is intended for users who are interactively using the machine in the domain, as well as services such as the PMM running in the background.

Note: This logon type caches secure information for disconnected operations.

As A SERVICE — Specifies that the PMM logs into the target system as a service. This option is more secure because only services such as the PMM can access the account.

Note: If you specify **As A SERVICE**, the privileged account must have right “logon as a service.”

8. Click **OK** to save the changes and exit the PMM Configuration Manager.

The configuration for the PMM for Windows NT and Windows 2000 is now complete.

Enabling Local Password Cache Updates on the Client Machine

Core Server’s ActiveX control, CourLocal, is available with this PMM. This ActiveX control lets an end user update the Windows domain password stored locally on the end-user’s system. This feature prevents an end-user from locking out his or her account after using Core Server’s Web Access Option to change the Active Directory or Windows NT password on the domain. For details on using CourLocal, refer to *The Core Server Core Server Implementation Guide*, chapter *Web Access (ASP Page) Configuration*.

Note: Mozilla Firefox and Google Chrome may not support some Microsoft technologies such as ActiveX. If you require local password cache synchronization, Core Security recommends using one of the supported versions of Internet Explorer.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

The PMM uses a backup domain controller whenever possible; only the final reset uses primary domain controller (PDC). This is done to reduce the traffic to PDC.

If you change the password of the trusted and privileged account username that this PMM uses for Windows NT/2000 password resets, run the PMM for Windows NT/2000 configuration manager and change the password to match.

Windows NT can handle up to 2048 open netbios sessions at a time. Whenever Core Server initiates an action, it utilizes a netbios session to do so. In the event that there are more than the maximum allowed sessions open, Core Server actions fail, as there is not an available session for the action. Should this happen, no further actions are processed until these open sessions time out, which usually takes 30 to 40 minutes.

Single Domain Model

When using a single domain model, the Core Server Core Server is typically deployed on a Windows 2000 system that is a member of the domain.

1. Log on to the system as a local administrator.
2. Make sure the account has the user right **LOG ON LOCALLY**. This is required so permissions and other attributes can be set.
3. Log out.
4. Log on again as a local administrator. This activates the new permissions.

Configure the PMM for Windows NT and Windows 2000 as described in [“Using Security Options” on page 374](#).

Single or Multiple Master Domain Model

When a Master Domain model is being used, the Core Server is typically deployed in a resource domain. The PMM for Windows NT and Windows 2000 is configured to reset passwords in the Master domain by using an Account Operator from the Master domain. The example in the following section describes the steps to follow when installing in this domain model.

Note: Deploying the PMM in different domain models may require additional steps during installation and configuration of the Core Server. Follow the steps for the appropriate domain model and identify a privileged account that the PMM may use when performing password resets (typically a member of the Account Operators group for the domain).

Assumptions:

- Domain M is the Master domain and contains all user accounts.
- Domain R is a production domain (a resource domain) in which the Core Server Core Server is installed.
- NT Workstation Z is a member of Domain R.
- Domain R Trusts Domain M (a one way trust).
- Admin is a local administrator of NT Workstation Z.
- MasterAdmin is a Domain Admin of M.
- AcctOperator is an account operator of M. It has the right to reset passwords.

Before running the PMM Configuration Manager:

1. Log on to System Z as a System Z local administrator "Admin."
2. Make MasterAdmin a member of the administrator group on NT Workstation Z. The PMM for Windows NT and Windows 2000 is then configured as MasterAdmin later. It is necessary to run the configuration program as a member of the Master domain (M), so account information can be verified.
3. If the Core Server is running Windows 2000 (not Windows 2003), make sure the account being used has the user right **ACT AS PART OF THE OPERATING SYSTEM**.
4. Make sure the account has the user right **LOG ON LOCALLY**. This is required so permissions and other attributes can be set.

5. Log out.
6. Log on as MasterAdmin to activate the new permissions.
7. Configure the Windows NT and Windows 2000 PMM.

Configuring the Connector for Microsoft Windows NT Domains

The Connector for Microsoft Windows NT Domains supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Authentication
- Query

Prerequisites

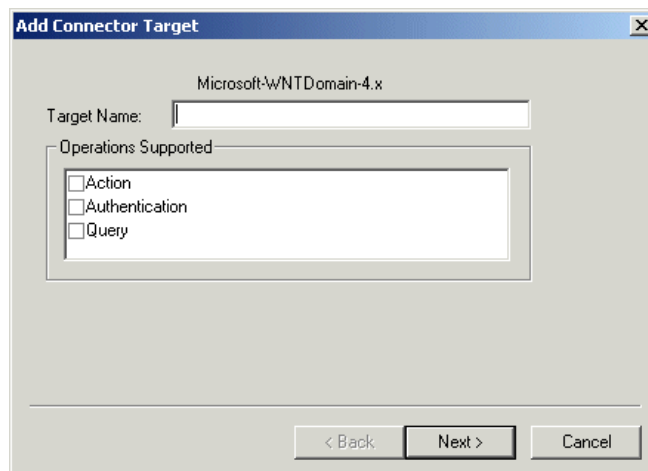
To configure the Connector for Microsoft Windows NT Domains, you must be logged on to a domain, not logged on to the local machine. If you are logged on to the local machine and attempt to configure the connector, the Connector Configuration Manager displays the error: "User *username* does not exist in Windows NT domain *domain_name*."

Connector Configuration

Follow these steps to add a target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite >Connector Configuration Manager
2. Select **MICROSOFT-WNTDOMAIN-4.X**
3. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 184: Add Windows NT Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select the **ACTION** check box to enable all provisioning actions on a target.

Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Server or Core Server.

Select **QUERY** to enable Core Provisioning or Core Compliance to use queries to find data in the target data source.

6. Click **NEXT**.

The following dialog box displays:

Figure 185: Connector Configuration Manager for Windows NT

7. This dialog box requires the following information.

- **TARGET WINDOWS NT DOMAIN** — Enter the name of the domain where the provisioning actions occur.
- **WINDOWS NT DOMAIN** — Enter the name of the domain where the user performing the provisioning actions has a privileged account.

Note: The connector is acting as the privileged user by performing the provisioning actions.

Specify the same domain for both the **TARGET WINDOWS NT DOMAIN** and the **WINDOWS NT DOMAIN**, or specify two different domains. This provides the flexibility to allow a trusted user to manage accounts on a domain other than the one on which he or she has an account.

- **PRIVILEGED USERNAME** — Enter the username for an account with administrator access to the domain.

Note: When setting up an Active Directory® domain, the privileged user must be a member of the Account Operators or the Administrators Group. Core Security recommends using a privileged user whose password never expires.

- **PASSWORD** — Enter the password for the account.
- **LOG ON AS A SERVICE** — By default, users can log on to the account interactively from a workstation in the domain as well as from services such as the Connector Framework running in the background. Check **LOG ON AS A SERVICE** to restrict access to the account only to services such as the Connector Framework.

Note: The user you specify for the Service Logon Account must have the User Right Assignment "Log on as service" assigned to it on the system hosting the connector.

8. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 42: Netscape Directory Server and iPlanet Directory Server — PMM

This chapter explains how to configure the PMM for Netscape Directory Server and iPlanet™ Directory Server:

- [*“Configuring the PMM for Netscape Directory Server” on page 388*](#)
- [*“Configuring the PMM Agent” on page 392*](#)

Configuring the PMM for Netscape Directory Server

The Password Management Module (PMM) for Netscape Directory Server and iPlanet Directory Server enables Core Server applications automatically reset user passwords on a Netscape Directory Server or iPlanet Directory Server.

The correct access keys are necessary to use this PMM. For more information on access keys, please contact Core Server.

Configuration information is the same for both the Netscape Directory Server and the iPlanet Directory Server.

Prerequisites

This PMM requires the Netscape Directory Server agent to run. For agent details, see [“Configuring the PMM Agent” on page 392](#).

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

The PMM configuration allows for the specification of a privileged user for each Netscape Directory Server or iPlanet Directory Server that can perform the reset process. The specified users must be privileged users in the Netscape or iPlanet user directory and must have write permission on at least two attributes of the user objects: `userPassword` and `passwordRetryCount`.

You can mark one privileged user entry as the default user name and password for all servers not explicitly configured.

The following information is required to configure a PMM target:

- The hostname of each Netscape Directory Server or iPlanet Directory Server
 - The Netscape Directory Server or iPlanet Directory Server TCP/IP port number
 - Whether the connection to the Netscape Directory Server or iPlanet Directory Server is made over an SSL connection
 - A username/password pair with administrative privileges that the Core Server application can use to reset users passwords for each target server
- Note:** The user must have write permission on at least two attributes: `userPassword` and `passwordRetryCount` for a successful password reset.
- The search base where the search for the Distinguished Name starts
 - Whether administrator passwords are allowed to be reset
 - The name of log file for the PMM (the default file name is `NetscapeDSAgent.log`)

The PMM for Netscape Directory Server uses privileged users to authenticate itself to the agent.

Follow these steps:

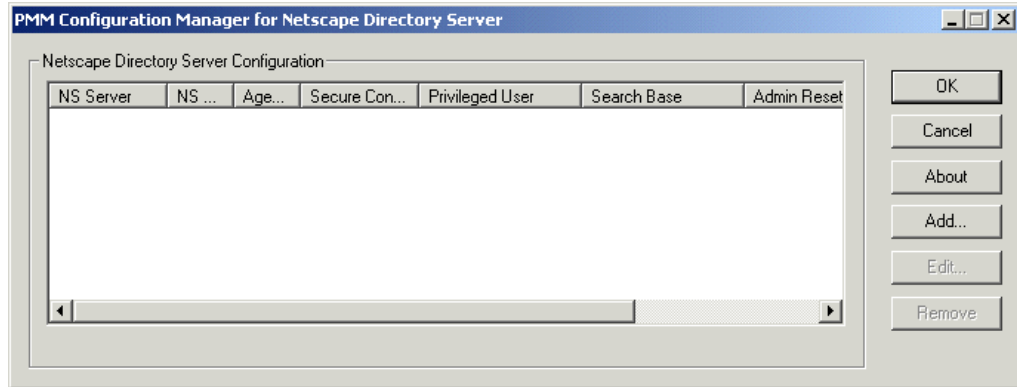
1. From the Start menu, select:

Programs>Core Server Core Server>Password Management Modules>Netscape Directory Server

Note: To navigate with the keypad, press the **ALT** button once.

The PMM Configuration Manager for Databases dialog box appears.

Figure 186: PMM Configuration Manager for Netscape Directory Server



2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Edit a target created with an earlier version of the PMM Configuration Manager with the **DEFAULT TARGET** button.
 - Obtain the product version number. Click the **ABOUT** button.
 - Enable advanced properties. Click the **ADVANCED** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 187: Add / Edit for Netscape Directory Server

Add / Edit Netscape Directory Server PMM Configuration

Netscape Directory Server Configuration

Netscape DS Server Name:

Netscape DS Port: ☒ Secure Connection

Agent Port:

* Privileged User:

Password:

* Search Base:

Certificate Database:

* Must be a distinguished name

☐ Allow reset of administrative passwords

☐ Add as the default user for unconfigured systems

3. **NETSCAPE DS SERVER NAME** — Specify the name of the Netscape Directory Server or iPlanet Directory Server on which to perform password resets. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **SECURE CONNECTION** — Select this checkbox if the connection to the Netscape Directory Server or iPlanet Directory Server is over a SSL connection.
5. **NETSCAPE DS PORT** — Specify the Netscape Directory Server or iPlanet Directory Server (TCP/IP) port. The default port for a nonsecure connection is 389, and the default port for a SSL connection is 636.

Note: If the SSL option is not activated on the Netscape or iPlanet Directory Server, the only option is to connect the server on a nonsecure port that has a default value of 389.

After the SSL option on the server activated, you can connect the server on both secure and nonsecure ports. However, with an SSL connection, specifying the nonsecure port (389 by default) causes this PMM to hang.

6. **AGENT PORT** — Specify the agent TCP/IP port number. The default port is 8193.
7. **PRIVILEGED USER** — Specify a user with a Distinguished Name that has administrative privileges.

Note: Give the user write permission on at least two attributes: userPassword and passwordRetryCount for a successful password reset.

8. **PASSWORD** — Specify the password for this user.
9. **SEARCH BASE** — Specify the search base to start searching for the Distinguished Name. It is possible to specify multiple search base trees separated by a semicolon.
10. **CERTIFICATE DATABASE** — If the connection is over SSL, specify the Certificate Database that contains the certificate of the Certificate Authority that issued the server's certificate. The PMM configuration program uses this certificate database to determine if it can trust the server's SSL certificate.

Note: This connector now uses the Microsoft WinLDAP API which leverages the Windows Certificate store. Certificates in this folder are not actually used.

11. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — Determines if the reset of administrative passwords are allowed. Core Server supports resetting the passwords of the configuration administrator, directory administrator and server administrator, but *not* the directory manager.
12. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — Determines if this privileged user is the default administrative user for all servers that are not configured through this application.
13. Click **OK**.
14. If desired, continue to configure additional servers.
15. Click **OK** in the main window to save the changes and exit the configuration program.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using Password Courier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the PMM Agent

This section describes how to register, start, and stop the PMM agent.

The PMM agent for Netscape Directory Server and iPlanet Directory Server, lets you specify the port for the agent and the log filename the agent uses for messages.

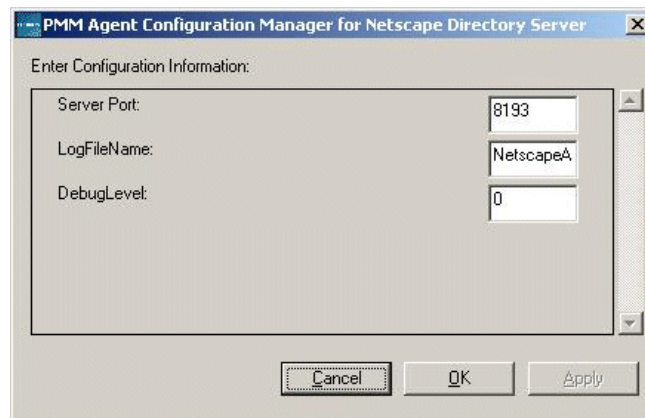
Before configuration, register the agent. Select

Start > Programs > Core Server Core Server > Password Management Modules > Netscape Directory Server > Register Agent

To configure the agent, please follow these steps:

1. From the Start menu, select:
Programs > Core Server Core Server > Password Management Modules > Netscape Directory Server > Configure Agent
The agent configuration dialog box appears.

Figure 188: PMM Agent for Netscape Directory Server and iPlanet Directory Server



2. Enter the **SERVER PORT** number. The default port is 8193.
3. Enter the **LOGFILENAME**. The default filename is `NetscapeAgent.log`. The log file is stored in the `CourionService` directory on server hosting the Connector Framework.
4. Generally, leave the **DEBUGLEVEL** at the default, 0. This is the level of log information that indicates if the password reset attempt was a success or failure. To have the agent log information for debugging, set the `DebugLevel` to `>1`.
5. Click the **OK** button.
6. Click **YES** when a dialog box asks to start/restart the PMM agent service.
7. Click **OK** to close the PMM Agent configuration.

Starting and Stopping the PMM Agent

From the Start Menu, select:

Settings > Control Panel > Administrative Tools > Services

Select the CourNSLDAPAgent, right click, and select **START** or **STOP**.

Support for SHA Hashing

The PMM for Netscape Directory Server and iPlanet Directory Server supports SHA hashing for passwords in the Password Reset action and for authentication. Follow these steps to configure SHA hashing for a password after you have configured the PMM:

1. From the Start menu, select:
Programs>Core Server Core Server>Configuration Editor
with the “Run as Administrator” privilege.
2. Navigate to the following location:
WMI>CourCnctrFrameworkMgr>CourTarget
3. Locate the connector target in the list.
4. View the AttrNameArray and find the item with the name “PasswordHash”.
5. Note the item number.
6. View the AttrValueArray, find the item number noted above and change its value to SHA (uppercase). This enables password hashing for the Password reset action and for authentication.
7. Stop the CourionService.
8. Restart the Connector Framework Manager.
9. Start the CourionService.

Note: If the PMM target is modified from within the PMM Configuration Manager, this manual setting is overridden. If this occurs, perform these steps again to enable SHA hashing.

Chapter 43: Netscape SMTP — Connector

This chapter explains how to configure the Connector for Netscape SMTP:

- [*“Configuring the Connector for Netscape SMTP” on page 396*](#)

Configuring the Connector for Netscape SMTP

The Connector for Netscape SMTP enables the Core Server to integrate with the Netscape SMTP e-mail server. This integration provides e-mail notification services for operations, such as end user authentication and provisioning actions. Adding a target to the connector identifies the server on which the Netscape SMTP application is installed.

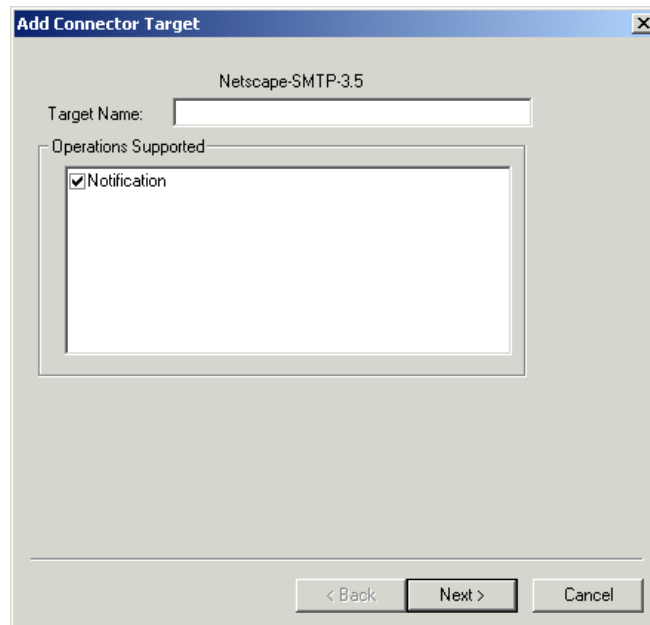
Connector Configuration

Follow these steps to add a Netscape SMTP target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **NETSCAPE-SMTP-3.5**
3. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 189: Add Netscape SMTP Target

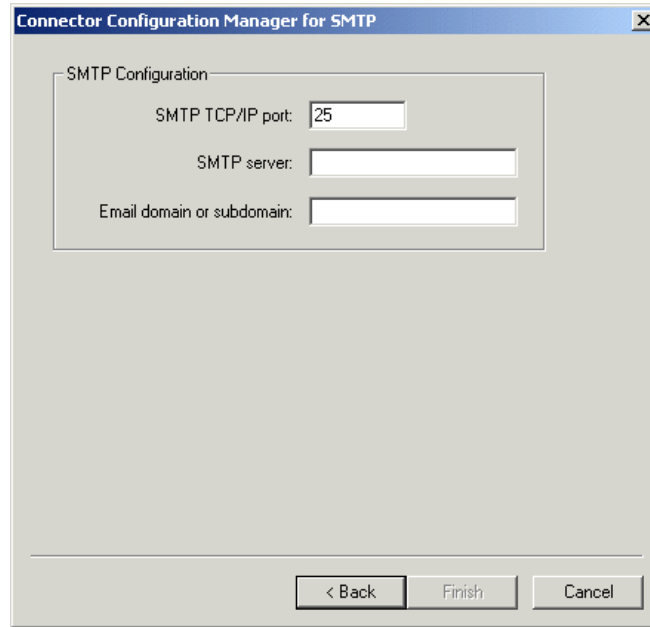


4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

The **NOTIFICATION** check box is selected by default.

5. Click **NEXT**.

The Core Server displays the following dialog box.

Figure 190: Connector Configuration Manager for Netscape SMTPThe image shows a Windows-style dialog box titled "Connector Configuration Manager for SMTP". Inside the dialog, there is a section labeled "SMTP Configuration" which contains three text input fields. The first field is labeled "SMTP TCP/IP port:" and contains the number "25". The second field is labeled "SMTP server:" and is empty. The third field is labeled "Email domain or subdomain:" and is empty. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

6. This dialog box requires the following information.
 - **SMTP TCP/IP PORT** — Specifies the SMTP TCP/IP port for the SMTP service. The default is port 25.
 - **SMTP SERVER** — Enter the name or IP address of the Netscape SMTP server that provide e-mail services.
 - **EMAIL DOMAIN OR SUBDOMAIN** — Enter the DNS domain name that identifies the e-mail system, for example, YourCompanyName.com. This step is optional and is used for verification of server availability.
7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The connector is now enabled for e-mail notification.

Chapter 44: Novell GroupWise — PMM and Connector

This chapter explains how to configure the PMM and Connector for Novell GroupWise®:

- [*“Configuring the PMM for Novell GroupWise” on page 400*](#)
- [*“Configuring the Connector for Novell GroupWise” on page 403*](#)

Configuring the PMM for Novell GroupWise

The Password Management Module (PMM) for Novell GroupWise enables end users to reset passwords automatically on Novell GroupWise systems.

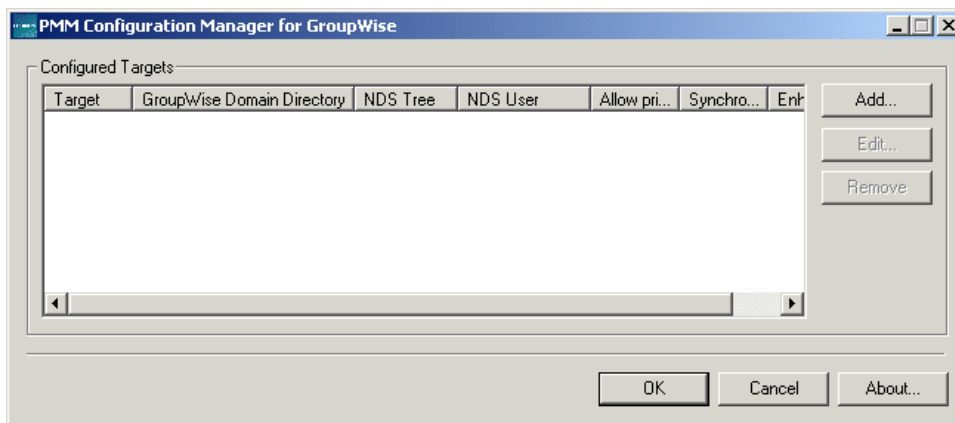
Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. For the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>Novell GroupWise
2. Click **YES** to start the PMM Configuration Manager.
The PMM Configuration Manager dialog box appears.

Figure 191: PMM Configuration Manager for Novell GroupWise



3. From this dialog box, you can:
 - Obtain the product version number. Click the **ABOUT** button.
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button or double click on the target name.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 192: Add/Edit Target Configuration for Novell GroupWise

4. TARGET

- a. **NAME** — Enter the Target name for the Novell GroupWise system. (You cannot edit the name of an existing target.) You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
- b. **ALLOW RESET OF PRIVILEGED USER ACCOUNTS** — Decide whether or not to allow resets of privileged accounts. A privileged account is one whose GroupWise account name matches the NDS common name.

If this box is not checked, the PMM rejects the reset request if the GroupWise account name matches the NDS common name.

- c. **ENABLE ENHANCED LOGGING** — This option provides you with detailed information about the Groupwise database, views, and forms accessed by the PMM, and enables you to track configuration issues. Check this option when you are setting up the PMM for the first time. Core Server recommends that you uncheck this option after all the configuration issues are resolved.

5. GROUPWISE DOMAIN

- a. **PATH TO GROUPWISE DOMAIN DIRECTORY (UNC)** — Enter the Uniform Naming Convention (UNC) path to the GroupWise domain directory.
- b. **NDS TREE** — Enter the name of the tree where the NDS user resides. The PMM uses the NDS user to access the domain directory.
- c. **NDS USER** — Enter the fully-qualified name of the user object. (CN=admin.OU=eastcoast.OU=us.0=corp or admin.eastcoast.us.corp)
- d. **PASSWORD** — Enter the password for the NDS user.

6. GROUPWISE SERVER OPERATING SYSTEM

Select **NETWARE** (the default) or **WINDOWS SERVER**. If you select Windows Server, specify a **DOMAIN NAME**, **USERNAME**, and **PASSWORD** of the privileged user on the Windows server. This user must have the following privileges:

Windows sharing permission access to the UNC domain path. At a minimum, this permission must include:

- Change
- Read

NTFS permission access to the UNC domain path. At a minimum, this permission must include:

- Read and execute
- List folder contents
- Read
- Write

7. **PERFORM ADMINISTRATIVE LOGON**

Select one of the **PERFORM ADMINISTRATIVE LOGON** options. The PMM must log into the Novell GroupWise target system using the privileged account information specified.

INTERACTIVELY is the default and is intended for users who interactively use the account in the domain as well as services such as the PMM running in the background. This logon type has the additional expense of caching logon information for disconnected operations, and is therefore not the recommended choice.

AS A SERVICE specifies that the PMM logs into the target system as a service. This is the more secure option because only services such as the Connector Framework can access the account.

Note: If you specify **As A SERVICE**, the privileged account must have the "logon as a service" right assigned.

8. Click **OK** to save the changes and exit from the PMM Configuration Manager.

The configuration of a Novell GroupWise PMM target is complete.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCouier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the Connector for Novell GroupWise

The Connector for Novell GroupWise® supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View

Prerequisites

Note: During installation of the Core Server, several files are installed that are required for communication with the Novell client software. If the Novell client software is already installed on the server when the Core Server is installed, three Novell OCX files are installed and registered. If newer OCX files are present, they are not overwritten.

The following files are installed in the "System32" folder on a 32-bit Windows system and in the "SysWoW64" folder on a 64-bit Windows system:

NWDir.ocx
Nwsess.ocx
Nwvola.ocx

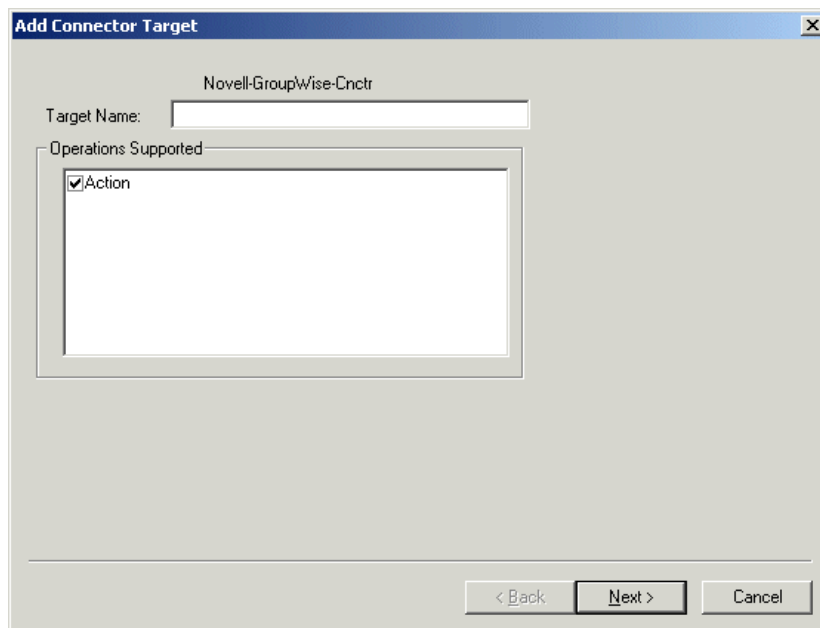
If the Novell client software is not already installed when the Core Server is installed, then the Novell OCX files are not installed and registered. In this case, there are two options for rectifying the situation:

1. Reinstall the Core Server in "Repair" mode.
2. Download and install the latest Novell NDAP ActiveX controls from:
http://developer.novell.com/wiki/index.php/ActiveX_NDAP_Controls

Connector Configuration

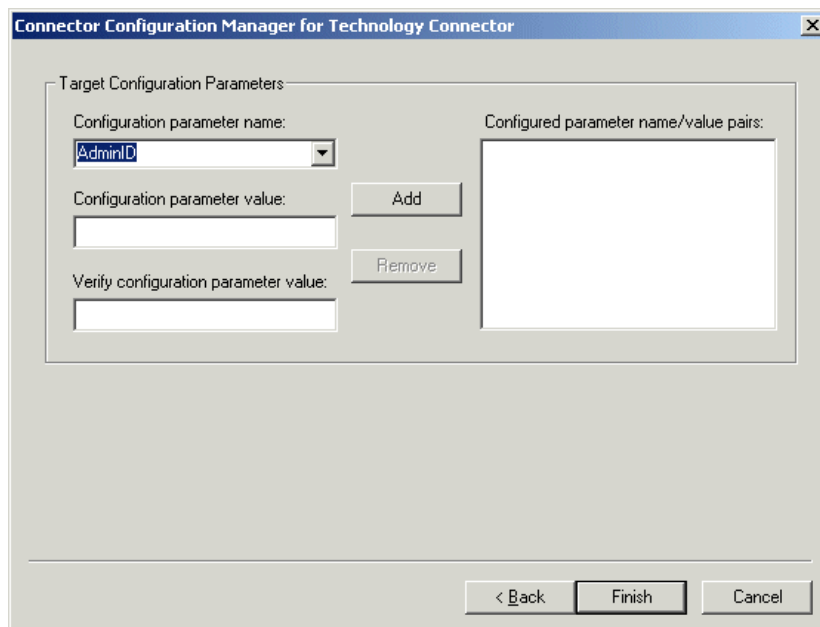
Follow these steps to add a Novell GroupWise target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **NOVELL-GROUPWISE-CNCTR**, and click **OK**.
3. Select **NOVELL-GROUPWISE-CNCTR**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 193: Add Novell GroupWise Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. Select **ACTION** to enable all operations on the target.
- Note:** Other operations that appear in this dialog box are not supported.
7. Click **NEXT**.

The Connector Configuration Manager dialog box appears.

Figure 194: Connector Configuration Manager for Novell GroupWise

8. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **AdminID** — The name of the privileged administrative user that can log in to. Specify the username only, not the context.
 - **AdminPassword** — The password for the administrative user.
 The administrative user needs to have full rights on the post office and domain where the new user is created.
 If the administrative user needs to create an NDS user, the administrative user needs to have full rights on the context where the NDS user is created. Full rights include the following:
 Supervisor
 Browse
 Create
 Rename
 Delete
 - **GroupWiseDomainPath** — The pathname indicating where the GroupWise domain is located.
 - **NDSTree** — The tree where the administrative user was defined.
Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.
9. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 45: Novell NDS eDirectory — PMM and Connector

This chapter explains how to configure the PMM and Connector for Novell NDS eDirectory:

- [*“Configuring the PMM for Novell NDS eDirectory” on page 408*](#)
- [*“Configuring the Connector for Novell NDS eDirectory” on page 411*](#)

Configuring the PMM for Novell NDS eDirectory

The Password Management Module (PMM) for Novell NDS eDirectory® enables Core Password and PasswordCourier Support Staff users to reset passwords automatically on the NDS Tree.

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Security.

Note: To configure both the Netware Bindery and Novell NDS successfully, install the Netware Bindery PMM first.

Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

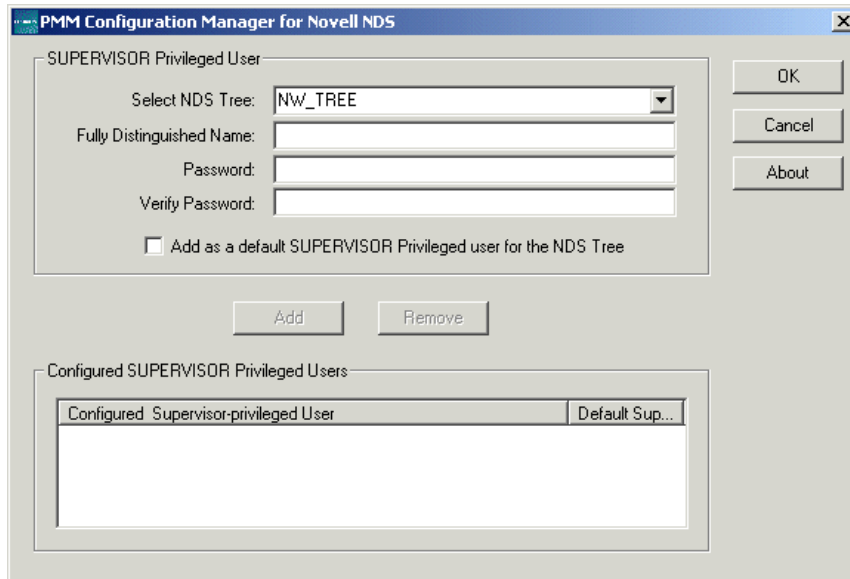
The NDS Tree and file server names must match the target name used in the PMM configuration.

This PMM supports Novell NDS eDirectory v8.8.5 with the Access Assurance Suite installed on 2008 platforms. Core Security recommends that you install the Novell Client 2 (SP2) client on any Core server with a Connector Framework configured against any Novell target.

PMM Configuration

The PMM Configuration Manager lets you specify one or more Supervisor users to execute the reset process. You can configure a separate supervisor username and password for each NDS Tree in the network. And you can mark one Supervisor entry as the default user name and password for all servers not explicitly configured.

Note: Core Password does not reset accounts with Supervisor privileges for security reasons.

Figure 195: PMM Configuration Manager for Novell NDS eDirectory

1. Select the **NDS TREE** where password resets occur. You need to use this tree name when you configure the target in the PMM Gateway Connector configuration.
2. Enter the **FULLY DISTINGUISHED NAME** of the Supervisor user.
3. Enter and verify the **PASSWORD** for the Supervisor user.
4. Click the **ADD AS A DEFAULT SUPERVISOR PRIVILEGED USER FOR THE NDS TREE** if the user is to be the default.

If an NDS Tree target is created and no Supervisor Privileged user is specifically configured, a Supervisor Privileged user marked as default during PMM configuration is used.

5. Click **ADD**.
6. Configure additional Supervisor users for other NDS Trees.
7. Click **OK** to save changes and exit the Administration Manager.

Following is a list of the minimum permissions a privileged user needs for resetting passwords:

- Locked By Intruder — Compare / Read / Write
- Login Grace Remaining — Compare / Read / Write
- Login Intruder Address — Compare / Read
- Login Intruder Attempts — Compare / Read / Write
- Login Intruder Limit — Compare / Read / Write
- Login Intruder Reset Time — Compare / Read / Write
- Password Expiration Interval — Compare / Read / Write
- Password Expiration Time — Compare / Read / Write
- Password Management — Compare / Read / Write
- [All Attributes Rights] — Compare / Read
- [Entry Rights] — Browse

To edit a Supervisor user configuration, remove it and then enter the updated information as follows:

1. Highlight the Supervisor user in the list box and click **REMOVE.**
2. Make the change(s) in the four fields (NDS Tree, name, and password) in the top half of the Configuration Manager and click **ADD.**
3. Click **OK** to save the changes and exit the Configuration Manager.

To remove a configured Supervisor user:

1. Highlight the Supervisor user in the list box and click **REMOVE.**
2. Click **OK** to save the changes and exit the Configuration Manager.

The configuration of the PMM for Novell NDS is complete.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- To configure both the Netware Bindery and Novell NDS successfully, install the Netware Bindery PMM first.
- Verify the connection to the target NDS tree before installing the Access Assurance Suite.
- Problems may occur when stopping and starting the web services on machines with the Novell intraNetWare client software version 3.5x. If this occurs, reboot the system.
- When you run the PMM Configuration Manager for Novell NDS to add a target configuration, any user already logged into NDS is automatically logged out.
- If you configure the **USER MUST CHANGE PASSWORD AT NEXT LOGIN** option with a Novell NDS PMM, the Novell® NDS® eDirectory user must also enable the “Force periodic change of password” option on the Novell® system.

Configuring the Connector for Novell NDS eDirectory

The Connector for Novell NDS eDirectory® supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Authentication

Prerequisites

ActivePerl must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. See [“Installing ActivePerl” on page 695](#) for information on how to install ActivePerl. Reboot the servers after you install ActivePerl.

Use the nds4x.pl script for provisioning on Novell NDS v. 4 systems.

Note: During installation of the Access Assurance Suite, several files are installed that are required for communication with the Novell client software. If the Novell client software is already installed on the server when the Access Assurance Suite is installed, three Novell OCX files are installed and registered. If newer OCX files are present, they are not overwritten.

The following files are installed in the "System32" folder on a 32-bit Windows system and in the "SysWoW64" folder on a 64-bit Windows system:

NWDir.ocx
Nwsess.ocx
Nwvola.ocx

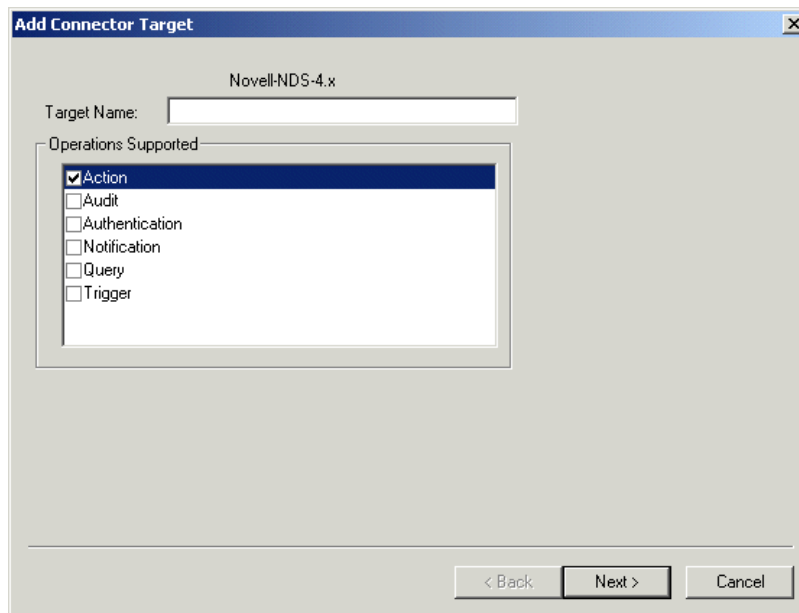
If the Novell client software is not already installed when the Access Assurance Suite is installed, then the Novell OCX files are not installed and registered. There are two ways to correct this situation:

- Reinstall the Access Assurance Suite in "Repair" mode.
or
- Download and install the latest Novell NDAP ActiveX controls from:
http://developer.novell.com/wiki/index.php/ActiveX_NDAP_Controls

Connector Configuration

Follow these steps to add a Novell NDS target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **NOVELL-NDS-4.X**, and click **OK**.
3. Select **NOVELL-NDS-4.X**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 196: Add Novell NDS eDirectory Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

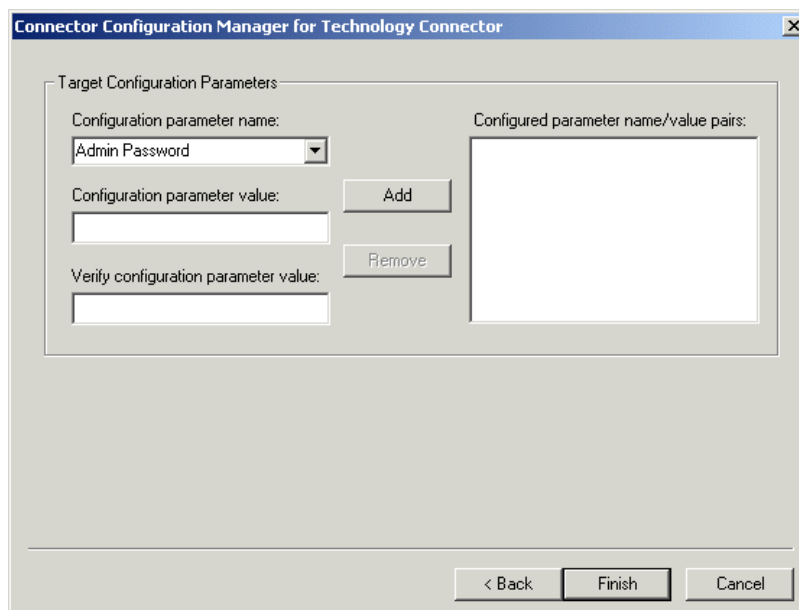
6. Select **ACTION** to enable all operations on the target.

Select **AUTHENTICATION** to use the target data source for authenticating end user access to Core Provisioning or Core Compliance.

NOTE: Other operations that appear in this dialog box are not supported.

7. Click **NEXT**.

The Connector Configuration Manager dialog box appears.

Figure 197: Connector Configuration Manager for Novell NDS eDirectory

8. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **Admin Password** — The password for the administrative user.
 The administrative user needs to have full rights on the post office and domain where the new user is created.
 If the administrative user needs to create an NDS user, the administrative user needs to have full rights on the context where the NDS user is created. Full rights include the following:
 Supervisor
 Browse
 Create
 Rename
 Delete
 - **Admin Username** — The name of the privileged administrative user that can log in. Specify the username along with the full context for the user. For example, ParentOU\Child1OU\Username.
 - **NDSTree** — The tree where the administrative user was defined.
Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.
9. Click the **FINISH** button.
 Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.
10. If you logged in as an NDS user on the Connector Framework Manager, configuring the connector logs you out of NDS. Log in to NDS again.

The target is now available for each action supported by this connector.

Configuring a Workflow to use more than one Target based on this Connector

Workflows that include two or more targets based on this connector need to configure "Target Dependency" in the workflow to have it process one Novell NDS target before it processes subsequent Novell NDS target. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform.

Chapter 46: Novell SUSE Linux Enterprise — Connector

This chapter explains how to configure the Connector for Novell SUSE[®] Linux Enterprise:

- [*“Configuring the Connector for Novell SUSE Linux Enterprise” on page 416*](#)

Configuring the Connector for Novell SUSE Linux Enterprise

The Connector for Novell SUSE supports the following actions on a target: Add, Change, Create, Enable, Disable, Delete, Verify, and View.

Prerequisites

Before you configure the connector, create a user with sudo permission and gather configuration information from the target.

1. Create a user for the connector to log in as and perform provisioning actions on. This user should be a regular user with sudo permission for the following programs:

- useradd
- grep
- usermod
- userdel
- passwd

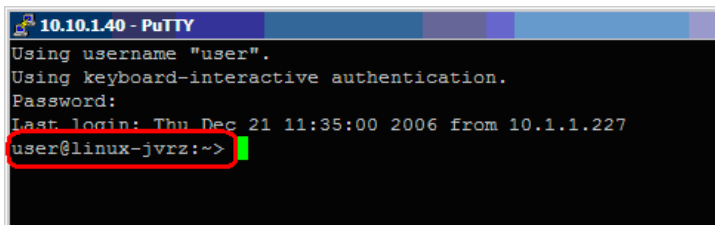
2. Gather the following information from the sudo user

SSH User

SSH Password

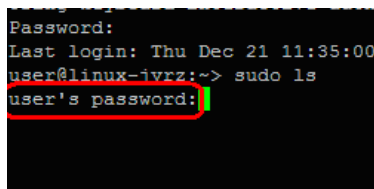
Target User Prompt — To get this information, login as the sudo user and grab the text to the left of the cursor after login is complete, as shown in [Figure 198](#).

Figure 198: Linux Target User Prompt



Sudo Password Verification Prompt — To get this information, login as the sudo user and execute a sudo ls command. Copy the text to the immediate left of the cursor when it asks you for the password, as shown in [Figure 199](#).

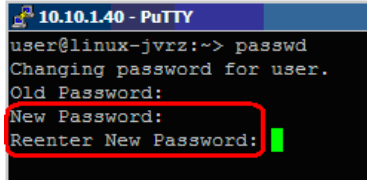
Figure 199: Linux Password Verification Prompt



SSH Server — Core Security recommends you use the IP address of the server to maximize reliability or the fully qualified domain name.

New Password Prompt / Verify New Password Prompt — To get this information, execute a `passwd` command as the `sudo` user. Enter a new password, but do not verify it. It gives you the next two settings, as shown in [Figure 200](#).

Figure 200: New and Verify New Password Prompt



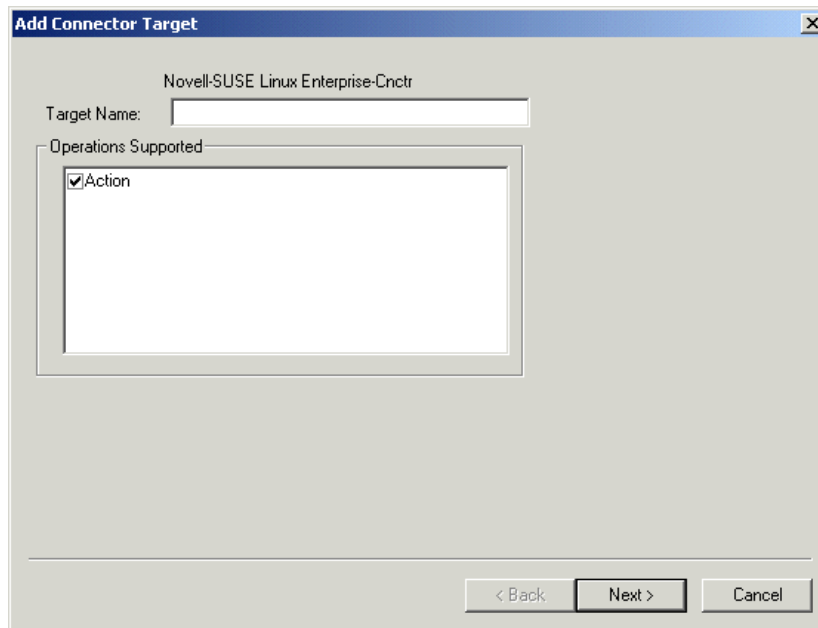
All of the information acquired in step 2 is entered when the connector is configured.

Connector Configuration

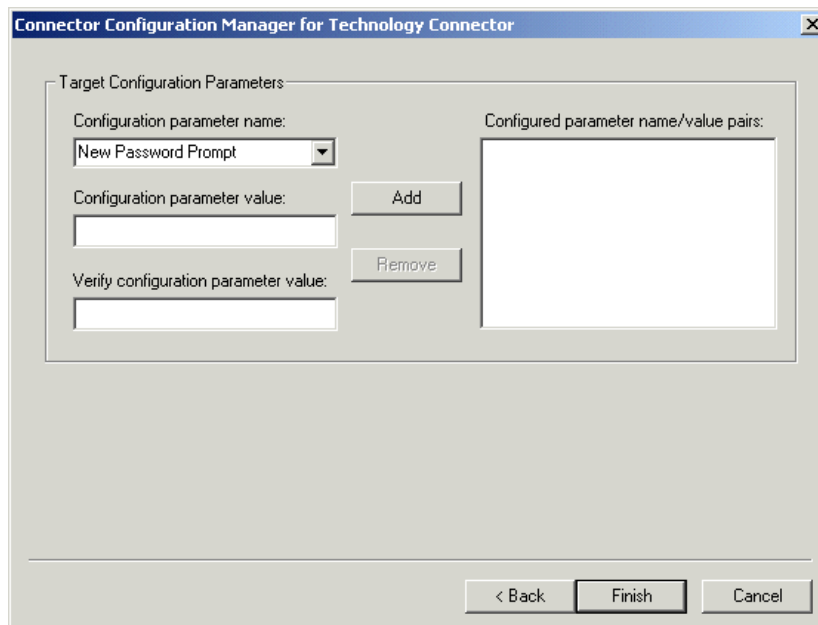
Follow these steps to add a Novell SUSE Linux Enterprise target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **NOVELL-SUSE LINUX ENTERPRISE-CNCTR**, and click **OK**.
3. Select **NOVELL-SUSE LINUX ENTERPRISE-CNCTR**
4. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 201: Add Red Hat Enterprise Linux Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. **ACTION** is selected by default, to enable all operations on the target. Click **NEXT**.
The Connector Configuration Manager dialog box appears.

Figure 202: Connector Configuration Manager for Red Hat Enterprise Linux

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Enter the values you obtained in the Prerequisites section, above.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 47: OpenVMS for VAX, Alpha, and Itanium Systems — PMM and Connector

This chapter explains how to configure the PMM and Connector for OpenVMS. The PMM and connector require the OpenVMS agent, also explained in this chapter:

- [*“Configuring the PMM for OpenVMS” on page 422*](#)
- [*“Configuring the Connector for OpenVMS” on page 425*](#)
- [*“Installing and Configuring the OpenVMS Agent” on page 427*](#)

Configuring the PMM for OpenVMS

The Password Management Module (PMM) for OpenVMS™ enables Core Server applications to reset user passwords automatically on OpenVMS systems. The PMM for OpenVMS is a component of the Core Server and is installed along with the suite.

The correct access key is necessary to run this PMM. For more information on access keys, please contact Core Server.

Prerequisites

OpenVMS must be installed and configured on the system on which you want resets performed.

Both the connector and PMM for OpenVMS™ require that you install the OpenVMS agent on the Alpha, VAX, or Itanium system. See [“Installing and Configuring the OpenVMS Agent” on page 427](#) for details.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

The PMM agent for OpenVMS requires 2.0 MBytes of free disk space on the OpenVMS system. After installation, the agent requires approximately 200 KBytes of space.

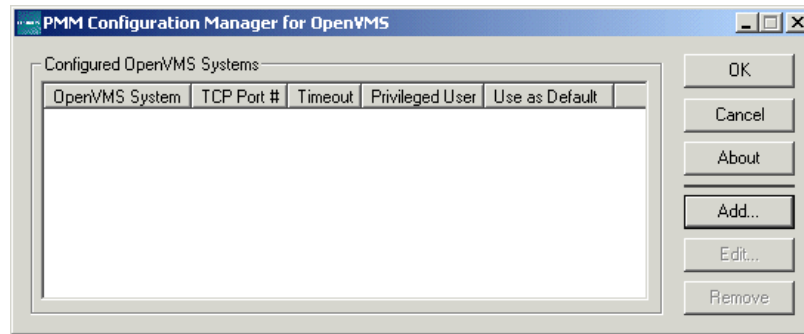
PMM Configuration

You can specify a privileged user for each OpenVMS server that performs password resets. Additionally, you can mark one user entry marked as the default username and password for all servers not explicitly configured.

To configure the PMM for OpenVMS:

1. From the Start menu, select:
Programs > Core Server Core Server > Password Management Modules > HP
OpenVMS

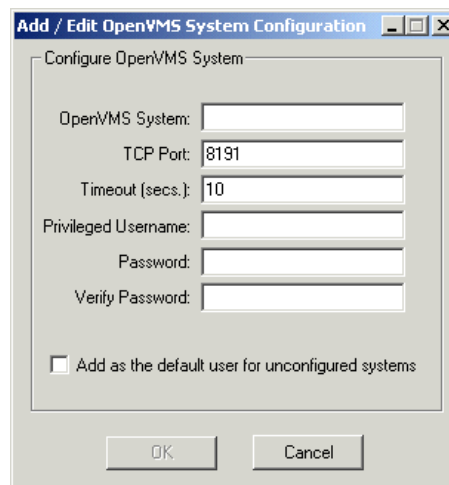
The PMM configuration manager screen appears.

Figure 203: PMM Configuration Manager for OpenVMS

Several OpenVMS systems can be supported. Each is represented by a line entry in the PMM Configuration Manager screen above.

2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 204: PMM Parameters for OpenVMS

Enter data in each text box.

3. **OPENVMS SYSTEM** — Select the OpenVMS server to perform password resets on. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **TCP/IP PORT** — Specify the TCP/IP port on which the PMM for OpenVMS agent is listening.
5. **TIMEOUT (SECS)** — Enter the amount of time (in seconds) before password reset timeout.

6. **PRIVILEGED USERNAME** — Specify the username of the privileged user created in PXY_DEF.VMS file during agent configuration.
7. **PASSWORD** and **VERIFY PASSWORD** — Specify and verify the password for the user.
8. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — Determine if this user is going to be the default user for all servers that are not configured with the PMM. If so, select the check box.
9. Click on the **OK** button to save changes.
10. Continue, if desired, to configure additional users for other servers.
11. Click the **OK** button to save any changes that are made and exit the configuration program.

You have configured a target for the PMM for OpenVMS.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Classic* explains how to do this on the classic platform.

Notes and Warnings

- You can see specific information about the cause of a password reset failure in the log file that was configured on the OpenVMS platform.
- The OpenVMS system, Port, and Privileged Username values must be the same as those specified in PXY_DEF.VMS when the PMM for OpenVMS agent was configured.
- If a user is disabled or the user's account is expired and the user attempts a password reset, the user receives a success message and the password is reset, assuming there is no other problem with the account or password. However, when the user attempts to log in with the password, the attempt fails. This is in keeping with what happens on an OpenVMS system if an administrator resets the password of an account that disabled or is expired. The password is changed, but the administrator must reset the account expiration date or enable the account before the user is able to log in with the changed password.
- For added security, the PMM for OpenVMS does not reset passwords for accounts with a UIC group less than or equal to the configured MAXSYSGROUP. Accounts with a UIC group number equal to or less than the MAXSYSGROUP value are assumed to belong to System Administrators.

Configuring the Connector for OpenVMS

The Connector for OpenVMS for VAX, Alpha, or Itanium systems supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

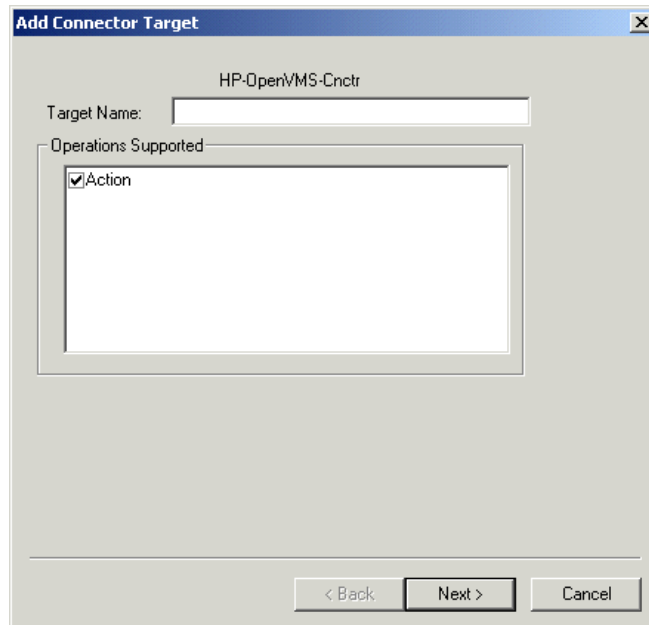
This connector requires the OpenVMS agent on the Alpha, VAX, or Itanium system. See [“Installing and Configuring the OpenVMS Agent” on page 427](#) for details.

Connector Configuration

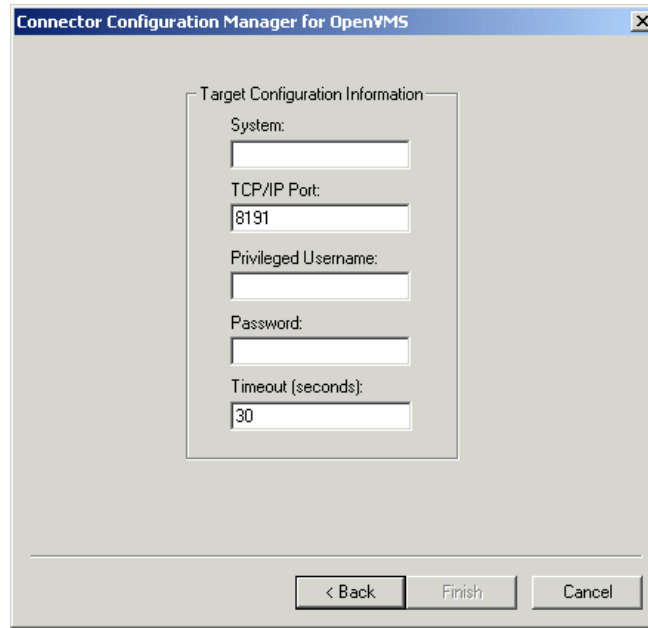
Follow these steps add a target for OpenVMS:

1. From the Start menu, select:
Programs> Core Server Core Server>Connector Configuration Manager
2. Select **HP-OPENVMS-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 205: Add OpenVMS Target



4. Enter a target name.
5. Press **NEXT**. The configuration manager dialog box for OpenVMS appears.

Figure 206: Connector Configuration Manager for OpenVMSThe image shows a Windows-style dialog box titled "Connector Configuration Manager for OpenVMS". Inside the dialog, there is a section titled "Target Configuration Information" which contains five labeled text input fields: "System:", "TCP/IP Port:", "Privileged Username:", "Password:", and "Timeout (seconds):". The "TCP/IP Port:" field contains the value "8191" and the "Timeout (seconds):" field contains the value "30". At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

6. Enter the following information about the target:

- **SYSTEM** — The DNS name or IP address for the OpenVMS system that is the target system.
- **TCP/IP PORT** — The TCP/IP port number in the agent's configuration file that the agent uses to listen for requests.
- **PRIVILEGED USERNAME** — The name of the privileged user in the configuration file of the agent. This is the user from whom the agent configured to accept connections and instructions.
- **PASSWORD** — The password on the target system for the privileged user.
- **TIMEOUT** (seconds) — This is the time limit, in seconds, for the OpenVMS agent to complete its operations.

7. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action supported by this connector.

Installing and Configuring the OpenVMS Agent

This section explains how to install, configure, start, stop, and uninstall the OpenVMS agent. Both the connector and the PMM for OpenVMS™ require that you install the OpenVMS agent on an Alpha or VAX system.

Note: This version of the Agent for OpenVMS contains OpenSSL 0.9.7c.

Installing the Agent

To install the agent for OpenVMS™, there must be 2.0 MBytes of free disk space on the OpenVMS system. Once installed, the agent requires approximately 200 KBytes of space.

[Table 22](#) shows which platforms and which versions of OpenVMS that each agent supports.

Table 22: OpenVMS Agents

Agent Filename	Support Platform	OS Version
courovmsagent.zip	Alpha	OpenVMS 7.x and above
courovmsagent-vax.zip	VAX	OpenVMS 7.x and above
courovmsagent62.zip	Alpha	OpenVMS 6.2
courovmsagent-vax62.zip	VAX	OpenVMS 6.2
courovmsagent-l64.zip	Itanium	Open VMS 8.3

The following instructions describe how to install and configure the OpenVMS™ agent. Items that are italicized are information that you need to enter manually.

Before beginning the installation process, obtain a user name/password pair that Core Server can use to reset passwords for each OpenVMS server configured.

To install the agent:

1. On the OpenVMS machine, create or designate a directory that holds the OpenVMS saveset that is used to install the agent.
2. Copy the files `unzip.exe` and `courovmsagent.zip` (for Alpha machines) or `unzip-vax.exe` and `courovmsagent-vax.zip` (for VAX machines) from the OpenVMS folder on the Core Server server to C:\.
3. Using FTP, enter the following commands from the PC where the Courovmsagent zip file and unzip utility are stored:

```
FTP my-OpenVMS-address
Login
binary
lcd C:\
```

4. `cd` to the directory established in the first step and then send the `.zip` file. For example:

```
cd SYS$SYSDEVICE:[SYSO.COMPANYNAME]
where
SYS$SYSDEVICE:[SYSO.COMPANYNAME] is the location of saveset files
COUR_AGENT060.A

put courovmsagent.zip
or
put courovmsagent-vax.zip
put unzip.exe
or
put courovmsagent-I64.zip

unzip-vax.exe
quit
```

You can check the success of the operation by making sure the files now reside in the directory established in Step 1.

5. Use `unzip` executable to restore the saveset of files used in installing and running the agent for OpenVMS. For example:

```
SET DEF SYS$SYSDEVICE:[SYSO.COMPANYNAME]
unzip==$SYS$SYSDEVICE:[SYSO.COMPANYNAME]UNZIP.EXE
or
unzip==$SYS$SYSDEVICE:[SYSO.COMPANYNAME]UNZIP-VAX.EXE
unzip courovmsagent.zip
or
unzip courovmsagent-vax.exe
```

The `unzip` operation should result in the creation of the saveset files `COUR_AGENT060.A`.

6. Use `VMSINSTAL` to install the agent's files into `SYS$STARTUP` and the system executables directory. For example:

```
@SYS$UPDATE:VMSINSTAL COUR_AGENT060 SYS$SYSDEVICE:[SYSO.COMPANYNAME]
```

7. If the backup is satisfactory, press the **ENTER** key at the prompt for the default (Yes).
8. If the files replaced by the installation are to be purged, press the **ENTER** key at the prompt to accept the default (Yes).

The installation procedure should complete from this point without error. Installation places the OpenVMS agent files as shown in [Table 23](#)

Table 23: OpenVMS Agent Files Core Server

Filename	Description	Installation Directory
COUR_AGENT060.RELEASE_NOTES	List of files in release.	SYS\$COMMON:[SYS\$HELP]
COUR_START_SCR.COM	Script to start agent, runs COUR_START_PROXY.COM as a detached process.	SYS\$COMMON:[SYS\$STARTUP]
COUR_START_PROXY.COM	Starts agent with configuration file data. Do <i>not</i> run this to start the agent.	SYS\$COMMON:[SYS\$STARTUP]
PXY_DEF.VMS	Configuration file you must modify before starting the agent.	SYS\$COMMON:[SYS\$STARTUP]
PXY.LOG	Agent log file.	SYS\$COMMON:[SYS\$STARTUP]
PXYSERVER.LOG	Agent log file.	Specified by PXY_DEF.VMS (INST_DIR)
COURION_PROXY.EXE	PMM and connector agent for OpenVMS.	SYS\$COMMON:[SYSEXEC]
COURION_ACCOUNT_DISCOVERY.COM	Performs account discovery.	SYS\$COMMON:[SYS\$STARTUP]
COURION_ACCT_DISC.EXE	Part of account discovery tool.	SYS\$COMMON:[SYSEXEC]

Warning: SYS\$STARTUP is a logical name that refers to a search path instead of one directory. If you edit SYS\$UPDATE:PXY_DEF.VMS to configure the agent, then when you save the file it is written correctly. If you copy the file PXY_DEF.VMS to SYS\$UPDATE, then the file is written in SYS\$SYSROOT:[SYS\$UPDATE] instead of SYS\$COMMON:[SYS\$UPDATE] and the agent does not act on your configuration changes. You must access the file as SYS\$COMMON:[SYS\$UPDATE]PXY_DEF.VMS or copy the file to SYS\$COMMON:[SYS\$UPDATE].

Reinstalling the Agent

To reinstall the agent, follow the directions in the section, [“Installing the Agent” on page 427](#). If `save` set COUR_AGENT_XXX has not been removed from the OpenVMS system, you can skip installation steps 1 through 4.

Configuring the OpenVMS Agent

If you configure the agent before configuring the PMM on the Connector Framework Manager, then the agent runs when the PMM for OpenVMS Configuration Manager tests the agent connection.

- TCP/IP must be running on the OpenVMS system.
- The agent must be installed as previously described.

- Before starting the agent, the file **PXY_DEF.VMS**, which the installation placed in the startup directory, must contain configuration data appropriate to the target.

SVR_PORT (default 8191) must be the same as the TCP/IP port number the agent uses.

SVR_NAME must be set equal to the host name of the system on which the agent is running. This is done by replacing “vms_system_name.”

VALIDATION_USER must refer to the name of a privileged user. Specify a user on the OpenVMS machine with the privileges of “SYSPRIV” or “BYPASS”. This is done by replacing “privileged_vms_username” with an appropriate user’s login name.

LOG_FILE defaults to pxy.log. **LOG_FILE** is the name of the log file used by the agent and can be changed by replacing the “pxy.log” value.

LOG_LEVEL is associated with log messages. A log level ranges from 0-2. Depending on the log level you specify in the **PXY_DEF.VMS** file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the **PXY_DEF.VMS** file. By default, the log level specified is 0.

INST_DIR must refer to the device directory path in which the password reset log is placed. This is done by replacing vms_device:[vms_logfile_directory] with an appropriate path. Do not use logical names that are undefined at the time when a system reboot starts the agent.

After **PXY_DEF.VMS** contains the correct configuration data, start the agent with the command:

```
@SYS$STARTUP:COUR_START_SCR.COM
```

This allows for validity checking of the configuration during configuration of the PMM.

Starting the Agent

After the PMM agent for OpenVMS installed and configured, you can issue the following command line to start it manually:

```
@SYS$STARTUP:COUR_START_SCR.COM
```

To start the PMM agent for OpenVMS automatically when the system reboots, insert the line in the system startup script, typically **SYS\$MANAGER:SYSTARTUP_VMS.COM**:

```
@SYS$STARTUP:COUR_START_SCR.COM
```

For the agent to function properly, the line must appear in the script after the TCP/IP service started and after any system logical data types used in the configuration file are established.

Stopping the Agent

There is no special stop command for the agent. The agent can be stopped like any other process by entering the command: **\$STOP /ID=process-id-for-Courion-proxy**, which can be determined using **SHOW SYSTEM** as in step 2 below.

Uninstalling the OpenVMS Agent

To uninstall the 5.50 agent:

1. Remove the line @SYS\$STARTUP:COUR_START_SCR.COM from the file SYS\$MANAGER:SYSTARTUP_VMS.COM.

2. Stop the running agent:

```
show sys/proc=Courion_Proxy
stop /id=pid-from-previous-command
```

3. Delete the installed files:

```
delete sys$system:COURION_PROXY.EXE; *
delete sys$startup:COUR_START_SCR.COM; *
delete sys$startup:COUR_START_PROXY.COM; *
```

4. Remove the configured Agent directory and log files specified in "sys\$startup:PXY_DEF.VMS" if you want to.
5. Remove log and config files if you want to:

```
delete sys$startup:PXYSERVER.LOG; *
delete sys$startup:PXY_DEF.VMS; *
delete sys$system:DHPARAMS.PEM; *
```

To uninstall the 6.00 agent:

1. Remove the line @SYS\$STARTUP:COUR_START_SCR.COM from the file SYS\$MANAGER:SYSTARTUP_VMS.COM.

2. Stop the running agent:

```
show sys/proc=Courion_Proxy
stop /id=pid-from-previous-command
```

3. Delete the installed files:

```
delete sys$system:COURION_PROXY.EXE; *
delete sys$system:COURION_ACCT_DISC.EXE; *
delete sys$startup:COUR_START_SCR.COM; *
delete sys$startup:COUR_START_PROXY.COM; *
delete sys$startup:COURION_ACCOUNT_DISCOVERY.COM; *
```

4. Remove configured Agent directory and log files that are specified in sys\$startup:PXY_DEF.VMS if you want to.
5. Remove log and config files if you want to:

```
delete sys$startup:PXYSERVER.LOG; *
delete sys$startup:PXY_DEF.VMS; *
delete sys$system:DHPARAMS.PEM; *
```

Agent Logging

The agent creates log file `PXYSERVER.LOG` in the directory where the file `COUR_START_SCR.COM` that was used to start the PMM agent resides. This log file contains information pertaining to the PMM agent for OpenVMS. It is created each time the agent is started.

The file which is configured in the `PXY_DEF.VMS` file is the log file containing entries pertaining to Password Reset attempts. The value which designates the log file name follows **LOG_FILE:**. The value which designates the log file directory path follows **INST_DIR**.

Chapter 48: Oracle Database 8*i* and 9*i* — PMM and Connector

This chapter explains how to configure the PMM and Connector for Oracle Database 8*i* and 9*i*:

- [*“Configuring the PMM for Oracle Database” on page 434*](#)
- [*“Configuring the Connector for Oracle 8*i* and 9*i*” on page 441*](#)

Configuring the PMM for Oracle Database

The Password Management Module (PMM) for Oracle enables Core Server Core Server applications to reset end user passwords automatically on Oracle version 8.1.6i.

The PMM for Oracle requires the correct access key. For details, please contact Core Server Corporation.

Prerequisites

- Microsoft Open Database Connectivity with ODBC Administrator Service enabled
- Appropriate client software for Oracle supported ODBC drivers

For information about the ODBC drivers, please refer to the database vendor's documentation.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

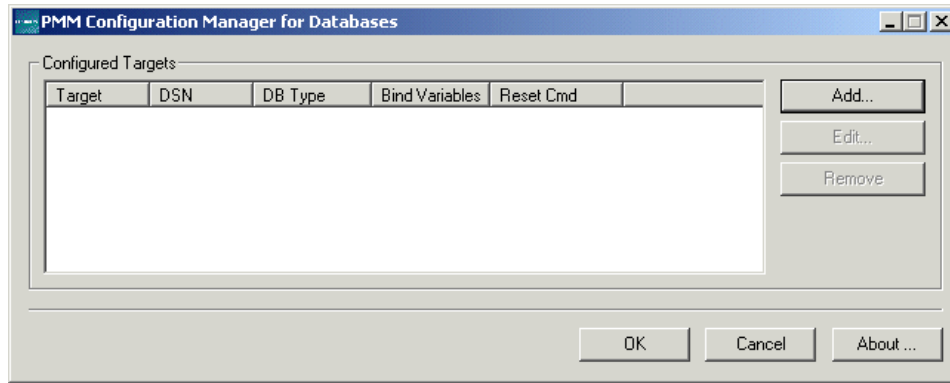
Data Source Names (DSNs) are used to identify the data source so Core Server applications can access the database to issue password reset commands. Once the reset is complete, the application then closes the connection to the database. This process occurs for every database password reset for each target data source.

Note: For the default reset command to work, the privileged user supplied in the target configuration must be able to execute the “ALTER USER” command, besides having the ability to open a connection to the database server to perform a password reset.

Note: Avoid using “ODBC” in the DSN because it can result in an error message.

To configure a DSN using the PMM for Oracle:

1. From the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>Oracle
The PMM Configuration Manager for Databases dialog box appears.

Figure 207: PMM Configuration Manager for Oracle 8i/9i

2. From this dialog box, you can

- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Edit a target created with an earlier version of the PMM Configuration Manager with the **EDIT** button.
- Obtain the product version number. Click the **ABOUT** button.

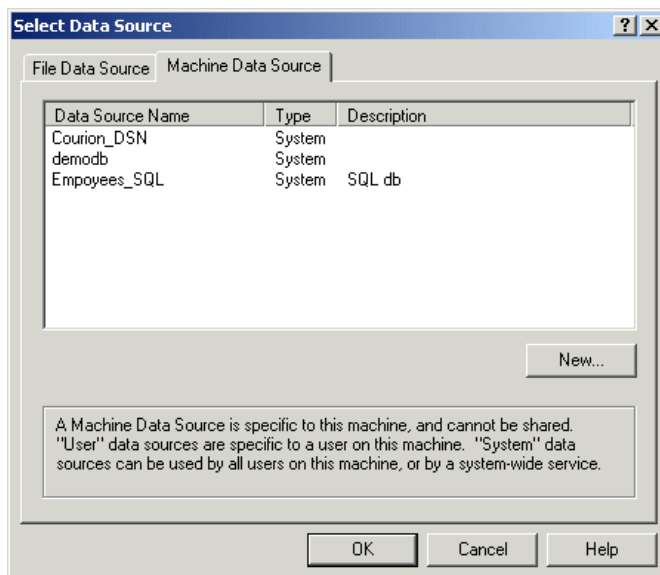
When you select the Add or Edit option, the Add / Edit Target Configuration dialog box appears.

Figure 208: Add/Edit Target for Oracle 8i/9i

Note: When entering passwords for an Oracle DSN, use all uppercase letters.

3. **TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **RESET PASSWORD COMMAND** — The default command for a reset is:
`ORACLE - ALTER USER "%user" IDENTIFIED BY "%pwd"`
5. To set the Data Source, click the **SELECT DSN...** button.
6. The Select Data source screen appears (not shown).
7. Click the **MACHINE DATA SOURCE** tab.
 The Machine Data Source screen appears.

Figure 209: Machine Data Source



8. On the Machine Data Source screen, select a system data source from the available list or define a new data source.

To select an existing data source:

- a. Click on the appropriate target in the "Data Source Name" column and then click **OK**.

The Configure Database Targets tab displays the target in the **DATA SOURCE NAME** field. Skip to step 9.

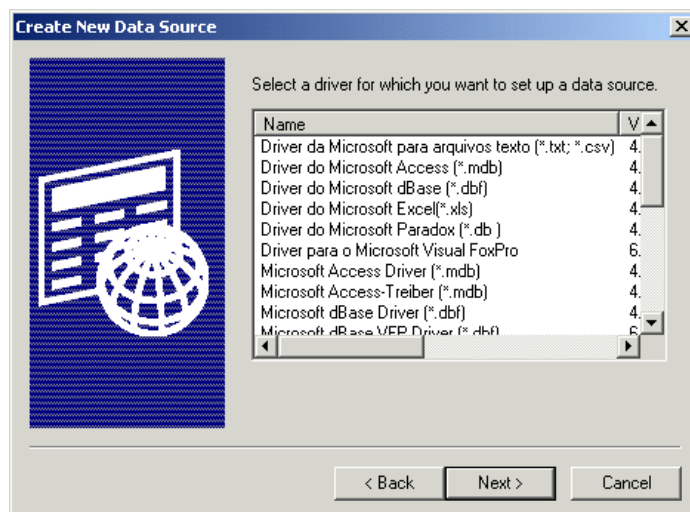
To define a new data source:

- a. Click the **NEW** button.

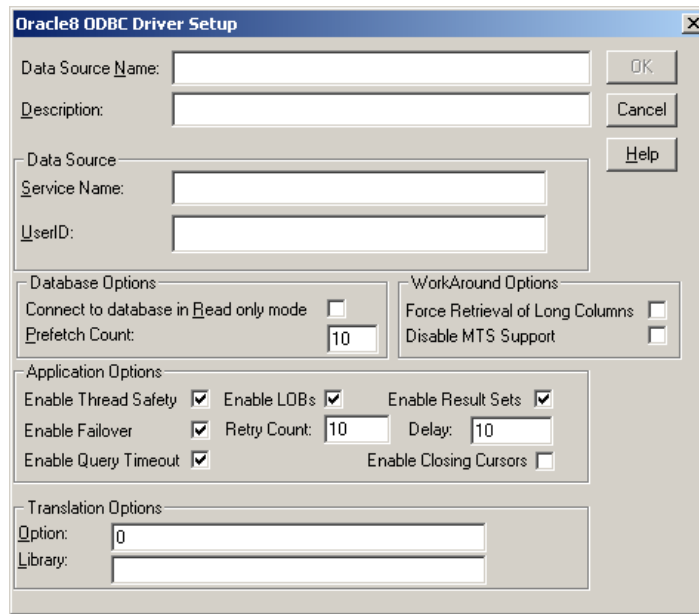
The Create New Data Source dialog box appears.

Figure 210: Create New Data Source

- b. Select **SYSTEM DATA SOURCE** and then click **NEXT**.
The Select Driver dialog box appears.

Figure 211: Driver Selection

- c. Scroll through the list of data source types and select **MICROSOFT ORACLE ODBC DRIVER**, then click the **NEXT** button.
The Oracle8 ODBC Driver Setup dialog appears.

Figure 212: Oracle ODBC Driver Setup


The Oracle8 ODBC Driver Setup dialog box contains the following sections:

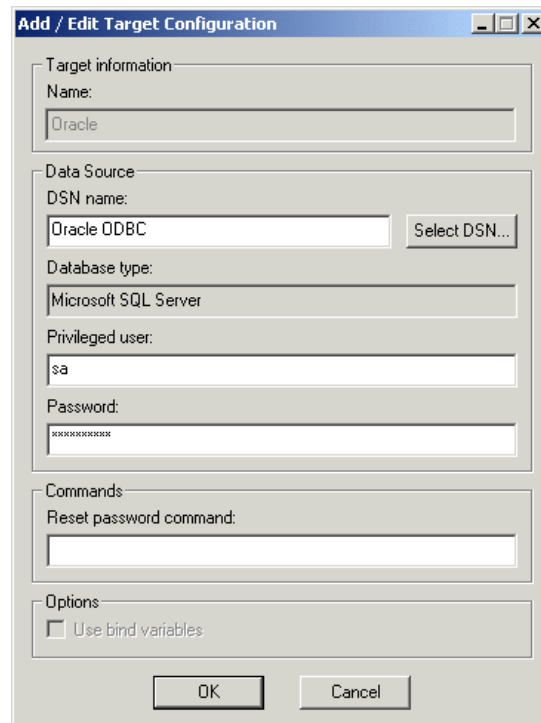
- Data Source Name:** Text field.
- Description:** Text field.
- Data Source:** Section containing:
 - Service Name:** Text field.
 - UserID:** Text field.
- Database Options:**
 - Connect to database in Read only mode: ☐
 - Prefetch Count:
- WorkAround Options:**
 - Force Retrieval of Long Columns: ☐
 - Disable MTS Support: ☐
- Application Options:**
 - Enable Thread Safety: ☒
 - Enable LOBs: ☒
 - Enable Result Sets: ☒
 - Enable Failover: ☒
 - Retry Count:
 - Delay:
 - Enable Query Timeout: ☒
 - Enable Closing Cursors: ☐
- Translation Options:**
 - Option:
 - Library:

Buttons: OK, Cancel, Help.

- d. Configure the data source as needed. For information about configuring this type of data source, please refer to the database vendor's documentation.

Note: When you select the server to connect to, the Oracle8 ODBC Driver Setup dialog may not list all available servers in the **SERVER:** field; the server name or IP address may need to be manually entered into this field.

After you configure the DSN and click **NEXT**, the Add/Edit Target screen returns with the newly-created DSN in the **DATA SOURCE NAME** field. The partially completed screen appears.

Figure 213: Partially Completed Add/Edit Target Databases


The Add / Edit Target Configuration dialog box contains the following sections:

- Target information:**
 - Name:**
- Data Source:**
 - DSN name:**
 - Database type:**
 - Privileged user:**
 - Password:**
- Commands:**
 - Reset password command:**
- Options:**
 - ☐ Use bind variables

Buttons: OK, Cancel.

In the Add/Edit Target screen, complete these fields:

9. **PRIVILEGED USER** — Type the administrator username to authenticate the administrator for the DSN.
10. **PASSWORD** — Type the administrator password.
11. **RESET PASSWORD COMMAND** — This field shows a default reset password command. The default command you see depends of the type of database you are using. You can edit this default command for custom password resets.

In the Reset password command, the `%user` macro is the input argument for the username, and the `%pwd` macro is the input argument for the password. If you need to use an MD5 hashed password instead of the clear text version of the password you may use `%hpwd` instead of `%pwd`. If you do not include the macros, the custom command cannot use the information sent by the PMM to complete a request for password reset.

Note: The software modifies any existing Oracle targets that were configured using the Advanced configuration option to remove the extraneous quotes around the macros. The modification is done when the information is read from the configuration repository. No modification is made to the original entry. When the reset command is displayed in this dialog, the extraneous quotes do not display and if you save the target information, the reset command is saved in the updated format.

12. **OPTIONS - USE BIND VARIABLES** — This Use bind variables option is available for Microsoft SQL Server and Oracle databases. (Microsoft SQL Servers use the term "parameter markers" for the same option.)

This option can improve performance on some servers. The server has a cache of recently executed statements. If you do not use bind variables, the PMM must execute a unique SQL statement for every unique password reset attempt. For example, this set of resets would enter three statements in the cache:

```
Cathy Courion resets her Oracle password to NewPwd
Cathy Courion resets her Oracle password to NewerPwd
Chris Courier resets his Oracle password to ChrisPwd
```

Using bind variables allows the PMM to prepare a single SQL statement with wild card characters. The wild card characters are replaced with specific user information at execution. The software enters the prepared wildcard SQL statement one time in the cache, and all resets are performed against that statement. Note that the default Oracle command "ALTER USER" is not compatible with bind variables. The reset command must use a stored procedure.

See the sample password reset example below.

13. Click the **OK** button to add the DSN to the defined targets list at the bottom of the tab. When you click OK, the DSN information is validated, but the reset password command is not.

You have configured a target for this PMM.

Repeat this procedure for each data source on which you want password reset commands executed.

Sample Password Reset Procedure

The following is a sample Oracle stored procedure for resetting passwords using bind variables.

1. Create a new stored procedure:

```
CREATE OR REPLACE PROCEDURE "SYSTEM"."CHANGE_PWD"
(in_username IN  varchar2,
in_password IN  varchar2)

AS
pwd_cursor integer;
sql_string varchar2(2000);
rows_processed integer;

AS
pwd_cursor integer;
sql_string varchar2(2000);
rows_processed integer;

BEGIN
sql_string := 'ALTER USER '||in_username||
IDENTIFIED BY '||in_password;
pwd_cursor := dbms_sql.open_cursor;
dbms_sql.parse(pwd_cursor, sql_string, dbms_sql.native);
rows_processed := dbms_sql.execute(pwd_cursor);
dbms_sql.close_cursor(pwd_cursor);

exception when others then
if dbms_sql.is_open(pwd_cursor) then
dbms_sql.close_cursor(pwd_cursor);
end if;
raise;
end;
```

2. Configure an Oracle target in the PMM for Databases. In the Add/Edit Target Configuration dialog box, check the box for "Use Bind Variables". For the reset password command, enter the text:

```
begin change_pwd(%user, %pwd); end;
```

3. Click OK.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the Connector for Oracle 8i and 9i

The Connector for Oracle Database 8i and 9i supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

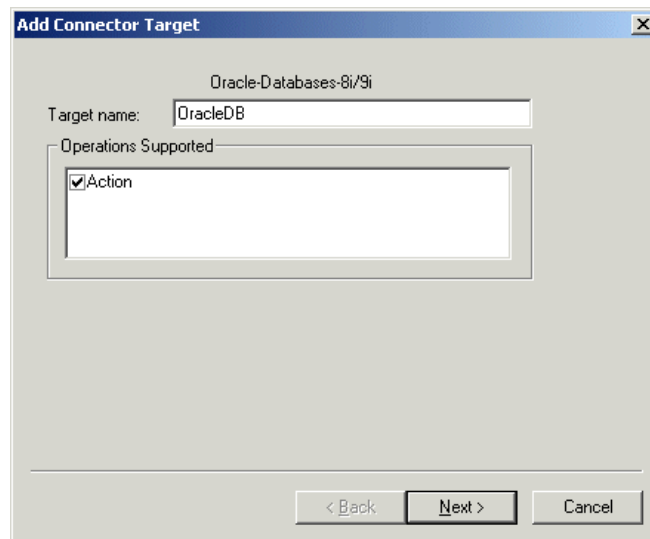
The Oracle8i or Oracle9i client must be installed on each server in which the Connector Framework or Connector Framework Manager is installed.

Connector Configuration

Follow these steps to configure the connector for Oracle8i and Oracle9i:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **ORACLE-DATABASES-8i/9i**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 214: Add Oracle 8i/9i Target



4. Enter a target name.
5. Press the **NEXT** button.
The Connector Configuration Manager dialog box appears.

Figure 215: Connector Configuration Manager for Oracle 8i/9i

6. Enter the following information about the target:

- **ORACLE SERVICE NAME** — The DNS name or IP address for the Oracle database.
- **PRIVILEGED USER NAME** — The name of the privileged user in the Oracle database. The Privileged User must have a minimum of the following rights:
 CREATE USER
 ALTER USER
 DROP USER
 GRANT ANY PRIVILEGE
 GRANT ANY OBJECT PRIVILEGE (for Oracle 9i databases only)
 GRANT ANY ROLE
 SELECT ANY DICTIONARY
 SELECT ANY TABLE
- **PASSWORD** — The password on the target system of the privileged user.
- **ALLOW PROVISIONING ON ADMINISTRATIVE ACCOUNTS** — Oracle 8i and 9i Accounts are considered Administrative accounts if they have any of the privileges mentioned in the Administrative Privileges text file.
- **ADMINISTRATIVE PRIVILEGES FILE**— Privileges to be considered as administrative privileges are mentioned in the **CourOraclePrivileges.txt** text file available in the CourionService folder. Each privilege is mentioned on a new line. Provide the full path of the text file in the text box. You can also create a text file containing the privileges and browse to that file by clicking the **BROWSE...** button.
- Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 49: Oracle E-Business Suite — PMM and Connectors

This chapter explains how to configure the PMM for Oracle E-Business Suite, the Connector for Oracle® E-Business Suite 11i, and the Connector for Oracle E-Business Suite R12:

- [*“Configuring the PMM for Oracle E-Business Suite” on page 446*](#)
- [*“Accounts Excluded From Password Reset” on page 455*](#)
- [*“Configuring the Connector for Oracle E-Business Suite 11i and the Connector for Oracle E-Business Suite R12” on page 456*](#)

Configuring the PMM for Oracle E-Business Suite

The Password Management Module (PMM) for Oracle® E-Business Suite lets an Access Assurance Suite application reset passwords automatically on the Oracle E-Business Suite of applications.

Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

The Core Password server must have access to the target Oracle database server. The install scripts access this server.

Core Password needs a privileged user account on the Oracle database server. This account must have privileges at a level that allow it to access the objects required to execute the PMM. Among these objects is the `fnd_user_pkg` package. Enter the username and password for this account in the configuration program.

Note: If the target is an Oracle 8.1.7 database, do not use privileges inherited from roles to grant access to objects required for PL/SQL execution. Privileges must be granted directly to the user without the use of a role.

PMM Configuration

This section describes how to:

- Run the install scripts: `pmmsetup1` and `pwdpmm_install.sql`
- Add or edit an Oracle ODBC Driver as a target data source
- Add or edit a Microsoft ODBC for Oracle driver as a target data source

Running the Install Scripts

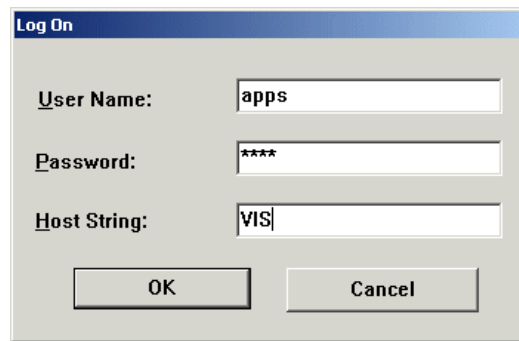
The install scripts (`pmmsetup1` and `pwdpmm_install.sql`) are located in the folder `Oracle E-Business` under the installation directory you specified when you installed the Core Access Assurance Suite. By default this is `C:\Program Files (x86)\Courion Corporation\Oracle E-Business`.

Note: The `pmmsetup1` script creates a new table called `xx_courion_restrict`. When running the script, you are prompted for the name of a tablespace to create the new table in. If you have not already created a tablespace, refer to the Oracle documentation for information about how to create a tablespace.

To run the install scripts:

1. Start SQL*Plus on the Core Server. The Log On dialog box appears:

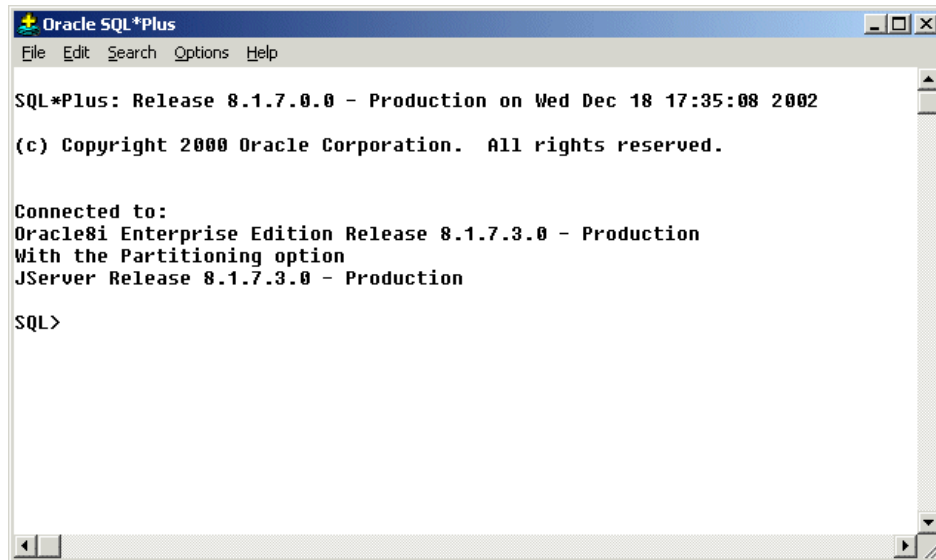
Figure 216: SQL PLus Logon



2. Log on with the User Name of the privileged account on the Oracle database server, the password for this account, and the Oracle database server name as the Host String (for example, VIS). This is the Net*8 service name for the database. You use this information when you configure the driver later.

A message similar to the following appears with the SQL> prompt when you successfully log on.

Figure 217: Logon Successful Message



3. Start the pmmsetup1 install script. For example:

```
SQL> @"D:\Program Files (x86)\Courion Corporation\Oracle E-Business\pmmsetup1"
```

The install script creates a minimally privileged user for the PMM to use and a new table named `xx_courion_restrict`. It prompts you for the following information:

- The username and password of the APPS user
- The username and password of the new minimally privileged PMM user
- The name of the tablespace where the `xx_courion_restrict` table is created

4. Start the `pwdpmm_install.sql` install script. For example:

```
SQL> @"D:\Program Files (x86)\Courion Corporation\Oracle E-
Business\pwdpmm_install"
```

As the script runs, a number of messages appear on the screen.

5. After a successful installation, enter the `exit` command at the `SQL>` prompt to quit `SQL*Plus`.

Now you can decide on the target data source. There are two choices:

- Oracle ODBC driver (next) and
- Microsoft ODBC driver ([“Adding a Microsoft ODBC for Oracle Driver as a Target Data Source” on page 453](#)).

Identify the desired ODBC driver and follow the corresponding instructions. Note that you can specify only one driver type for each target.

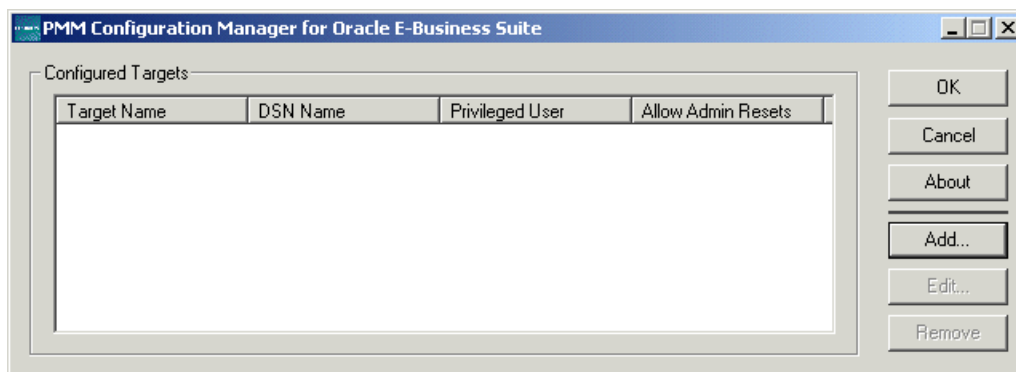
Adding an Oracle ODBC Driver as a Target Data Source

1. From the Start menu, select:

Programs>Courion Access Assurance Suite>Password Management
Modules>Oracle E-Business Suite

The Configuration Manager displays its the main dialog box. This dialog box shows any previously configured targets.

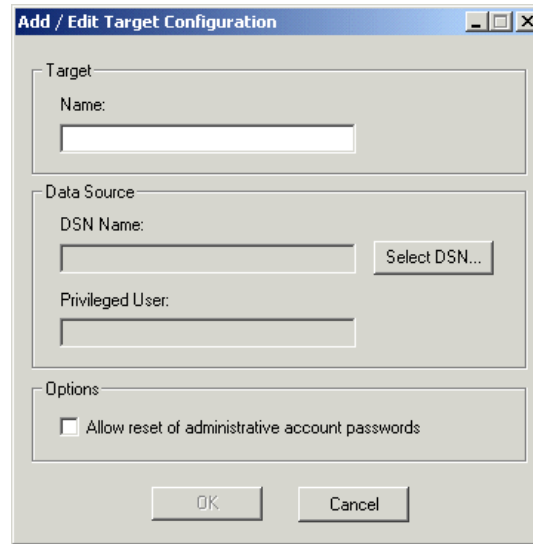
Figure 218: PMM Configuration Manager for Oracle E-Business



2. From this dialog box, you can

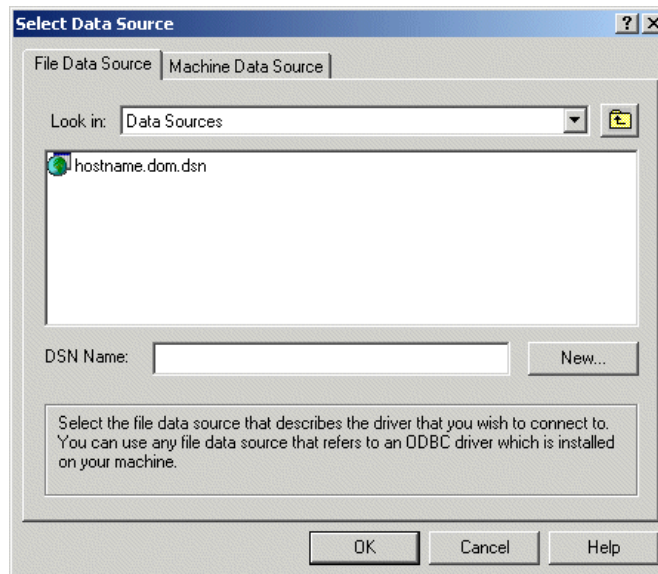
- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

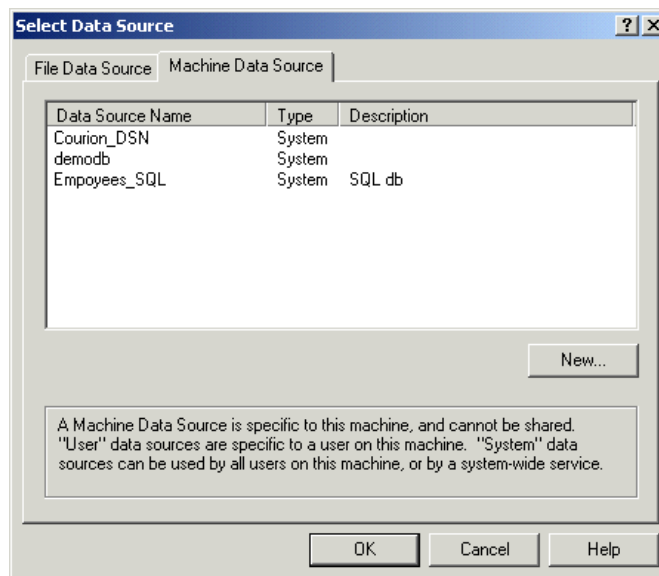
Figure 219: Add/Edit Target Configuration Dialog Box for Oracle E-BusinessThe dialog box is titled "Add / Edit Target Configuration". It contains three main sections: "Target", "Data Source", and "Options". The "Target" section has a "Name:" label and a text input field. The "Data Source" section has a "DSN Name:" label, a text input field, and a "Select DSN..." button. Below this is a "Privileged User:" label and a text input field. The "Options" section has a checkbox labeled "Allow reset of administrative account passwords". At the bottom are "OK" and "Cancel" buttons.

3. Enter a target in the Target Name field. (You cannot edit the name of an existing target.) You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. Click **SELECT DSN**.

The Select Data Source dialog box appears.

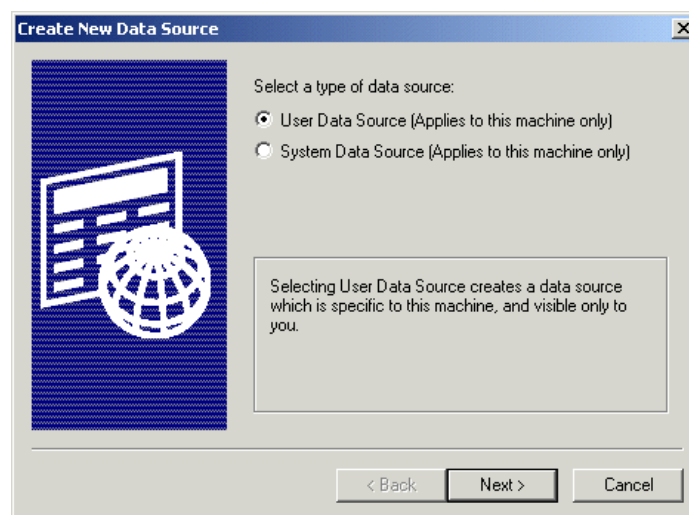
Figure 220: Select Data SourceThe dialog box is titled "Select Data Source". It has two tabs: "File Data Source" and "Machine Data Source". The "File Data Source" tab is selected. It has a "Look in:" dropdown menu showing "Data Sources" and a folder icon button. Below this is a list box containing "hostname.dom.dsn". At the bottom is a "DSN Name:" label, a text input field, and a "New..." button. A text box at the bottom contains the instruction: "Select the file data source that describes the driver that you wish to connect to. You can use any file data source that refers to an ODBC driver which is installed on your machine." At the very bottom are "OK", "Cancel", and "Help" buttons.

5. Click the **MACHINE DATA SOURCE** tab.
- The dialog box in [Figure 221](#) appears.

Figure 221: Machine Data Source List

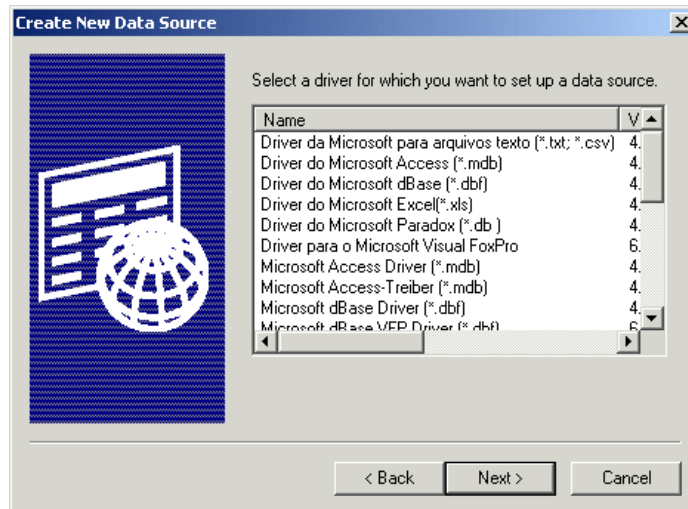
6. Click **NEW**.

The **CREATE A NEW DATA SOURCE** dialog box appears.

Figure 222: Create a New Data Source

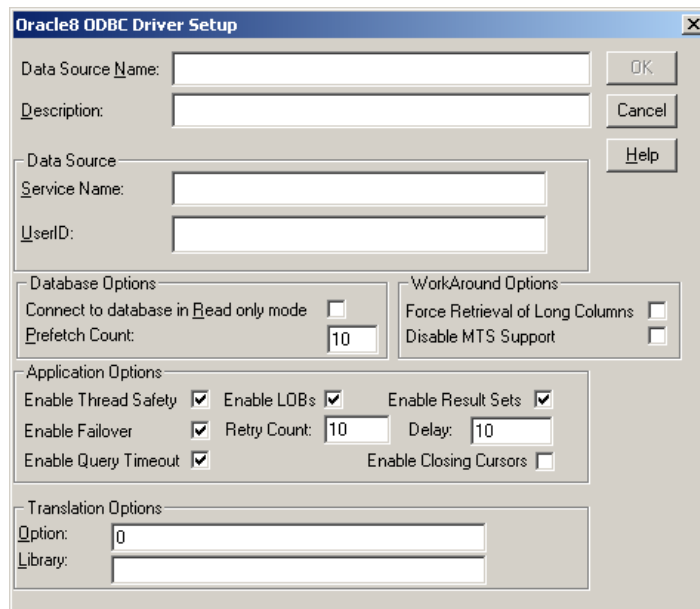
7. Select **SYSTEM DATA SOURCE (APPLIES TO THIS MACHINE ONLY)** and click the **NEXT** button.

The list of data sources appears.

Figure 223: List of Drives in Create New Data Source

8. Select the Oracle ODBC Driver and click the **NEXT** button.

The Oracle8 ODBC Driver Setup dialog box appears.

Figure 224: Oracle8 ODBC Driver Setup

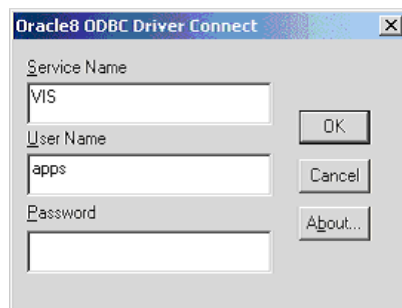
9. To set up the Oracle8 ODBC driver:
 - a. **DATA SOURCE NAME** — Enter a unique data source name.
 - b. **DESCRIPTION** — Enter a brief description of the data source.
 - c. **SERVICE NAME** — Enter the service name. This is the “Host String” name you used to connect to the Oracle database server when you ran the install script (the Net*8 service name for the database). For example, VIS.
 - d. **USERID** — Enter the UserID. This is the privileged account name you used to connect to the Oracle database server when you ran the install script.
 - e. **DATABASE OPTIONS, WORKAROUND OPTIONS, APPLICATION OPTIONS, TRANSLATION OPTIONS**

These options are specific to features of Oracle8 ODBC Drivers. In the **WORKAROUND OPTIONS** section, select **Disable MTS Support** (Multi-Threaded Server). Otherwise, you can accept the default selections that appear in these sections. Refer to the Oracle8 ODBC driver documentation for more information about these features.

10. After completing the options, click the **OK** button.

The Oracle8 ODBC Driver Connect dialog box appears.

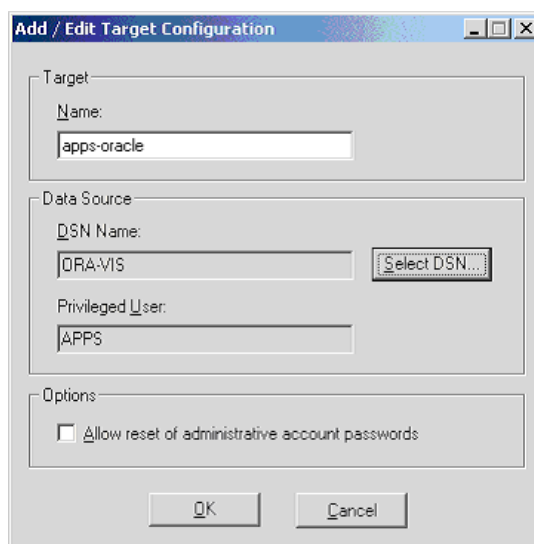
Figure 225: Oracle8 ODBC Driver Connect



11. Enter your password into the Password box and click the **OK** button.

The Add/Edit Target Configuration dialog box appears with the new target in the Name window.

Figure 226: Add/Edit Configuration Target with Oracle Target



12. If you want to allow password resets of the Administrative account on the Oracle database server, select **ALLOW RESET OF ADMINISTRATIVE ACCOUNT PASSWORDS** in the Options section.

Note: To use this option, the user account should be assigned System Administrator responsibility.

13. Click the **OK** button.

The PMM Configuration Manager for Oracle E-Business Suite main dialog box appears with the new target in the list of target names.

14. Click the **OK** button to save the newly configured target.

You have configured an Oracle ODBC driver as a target data source. Skip to [“Creating a Workflow for a Target” on page 454](#).

Adding a Microsoft ODBC for Oracle Driver as a Target Data Source

1. Follow steps 1 through 6 from the previous section - [“Adding an Oracle ODBC Driver as a Target Data Source”](#).
2. From the Create New Data Source screen, select **MICROSOFT ODBC FOR ORACLE**.
The Microsoft ODBC for Oracle Setup dialog box appears.

Figure 227: Microsoft ODBC for Oracle Setup

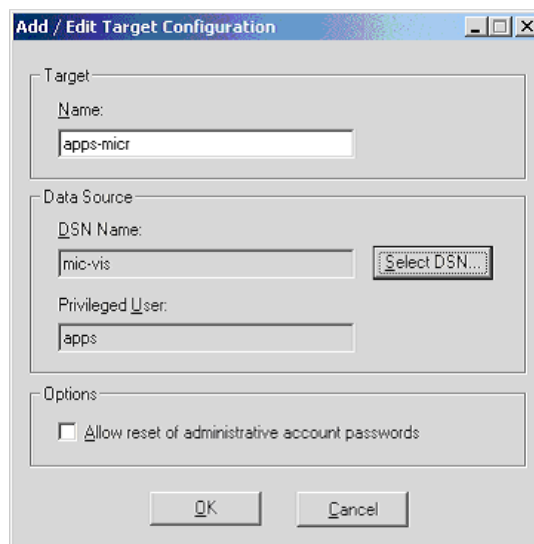
3. To set up the Microsoft ODBC for Oracle driver:
 - a. Enter a unique data source name.
 - b. Enter a brief description of the data source.
 - c. Enter the User Name. This is the privileged account name you used to connect to the Oracle database server when you ran the installation script.
 - d. Enter the server name. This is the “Host String” name you used to connect to the Oracle database server when you ran the install script (the Net*8 service name for the database). For example, VIS.
 - e. Click the **OK** button.

The Microsoft ODBC for Oracle Connect dialog box appears.

Figure 228: Microsoft ODBC for Oracle Connect

4. Enter your password in the Password box and click **OK**.

The Add/Edit Target Configuration dialog box appears with the new target in the Name window.

Figure 229: Add/Edit Target ConfigurationThe image shows a Windows-style dialog box titled "Add / Edit Target Configuration". It has three main sections: "Target", "Data Source", and "Options". In the "Target" section, the "Name:" field contains "apps-micr". In the "Data Source" section, the "DSN Name:" field contains "mic-vis", and there is a "Select DSN..." button to its right. The "Privileged User:" field contains "apps". In the "Options" section, there is a checkbox labeled "Allow reset of administrative account passwords" which is currently unchecked. At the bottom of the dialog are "OK" and "Cancel" buttons.

5. If you want to allow password resets of the Administrative account on the Oracle database server, select **ALLOW RESET OF ADMINISTRATIVE ACCOUNT PASSWORDS** in the Options section.

Note: To use this option, the user account should be assigned System Administrator responsibility.

6. Click the **OK** button.

The PMM Configuration Manager for Oracle E-Business Suite main dialog box appears with the new target in the list of target names.

7. Click the **OK** button to save the newly configured target.

You have configured a target for this PMM.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Accounts Excluded From Password Reset

Oracle E-Business Suite uses some accounts on the Oracle database server for maintenance only. Users cannot perform password resets on these accounts. By default, the accounts excluded from password resets are:

ANONYMOUS
APPSMGR
AUTOINSTALL
CONCURRENT MANAGER
DATAMERGE
FEEDER SYSTEM
GUEST
INITIAL SETUP
STANDALONE BATCH PROCESS
SYSADMIN

Note: You can modify the list of accounts that are excluded from password resets. Contact Core Security Customer Support for more information.

Configuring the Connector for Oracle E-Business Suite 11i and the Connector for Oracle E-Business Suite R12

The Connector for Oracle E-Business Suite 11i and the Connector for Oracle E-Business Suite R12 support the following actions on a target: Add, Change, Create, Disable, Enable, View, and Verify. There is no Delete action in Oracle E-Business.

Upgrading from Oracle E-Business Suite 11i to Oracle E-Business Suite R12:

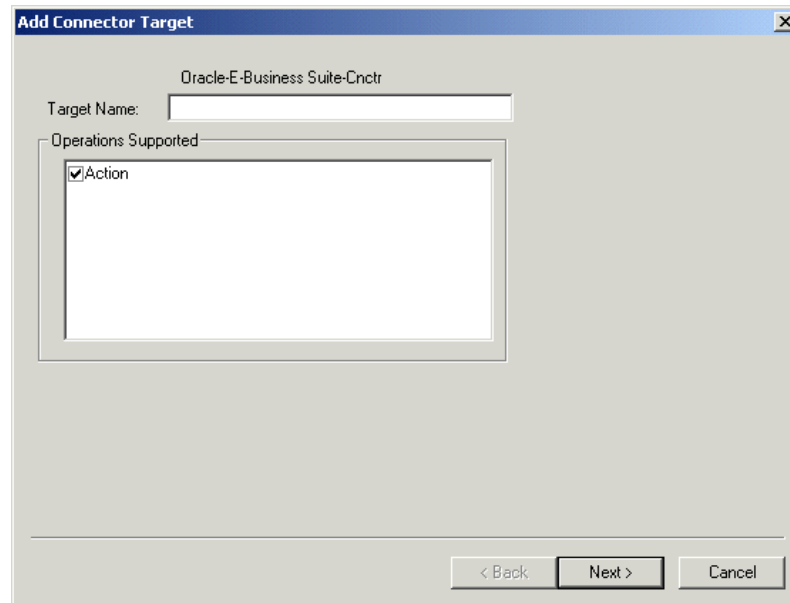
In Oracle E-Business Suite 11i, Responsibility Keys are sent through workflows delimited with a comma (','). Example: SYSTEM_ADMINISTRATOR,APPLICATION_DIAGNOSTICS. In Oracle E-Business Suite R12, Responsibility Keys are sent through workflows delimited with a pipe ('|'). Example: SYSTEM_ADMINISTRATOR|APPLICATION_DIAGNOSTICS.

If you are upgrading from Oracle E-Business Suite 11i to R12, you need to update these attributes in all existing workflows. You also need to update any custom macros that read these values and process them, along with any other customizations that process them.

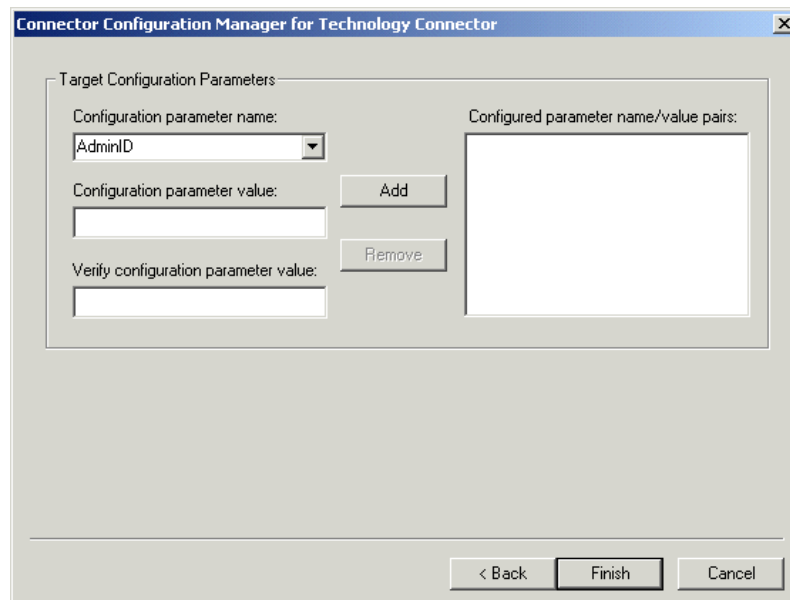
Connector Configuration

Follow these steps to configure the connector for Oracle E-Business:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select
ORACLE-E-BUSINESS SUITE-CNCTR
or
ORACLE-E-BUSINESS SUITE R12-CNCTR
and click **OK**.
Select **ORACLE-E-BUSINESS SUITE-CNCTR**
or
ORACLE-E-BUSINESS SUITE R12-CNCTR
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 230: Add Oracle E-Business Target

4. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**.
The configuration screen for Oracle E-Business appears.

Figure 231: Connector Configuration Manager for Oracle E-Business

5. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **AdminID** — If the value is set to “APPS”; then you only need to configure the other required parameters and click **FINISH**. If you want to use a different value, additional configuration is required. See [“Configuring the AdminID for a value other than APPS”](#).
 - **AdminPassword** — Password for the AdminID account

- **DSNName** — Name of the ODBC target
- **OracleApplication** — Unique ID that specifies the application ID. This parameter is required, but is not used.
- **UseGroupMembership** — Values for this parameter are Yes (the workflow uses the Membership Control on the User Responsibilities) or No (the workflow does not use the Membership Control).

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

6. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by the connector.

Configuring the AdminID for a value other than APPS

To create a privileged user that is not an APPS user, you need to copy a set of the supplied scripts to the Oracle database server and then run them.

1. Copy the scripts to the Oracle database server

for Oracle E-Business Suite 11i from the directory <install drive>:\<install folder>\Courion Corporation\Oracle E-Business\Cnctrs.

for Oracle E-Business Suite 12r from the directory <install drive>:\<install folder>\Courion Corporation\Oracle E-Business\Cnctrs-R12.

All files must be placed in the same directory. The files include:

```
COUR_USER_EMP_PKG.pkb
COUR_USER_EMP_PKG.pks
create_cour_sys.sql
create_synonyms_cour.sql
grants_cour_apps.sql
```

2. Run SQLPLUS from the installation directory and connect to the E-Business Suite Database as SYSTEM (or any user with DBA role). Run the create_cour_sys.sql script:

Figure 232: Run create_cour_sys.sql

```

C:\WINDOWS\system32\cmd.exe - sqlplus system@vis11

J:\Courion\scripts>sqlplus system@vis11

SQL*Plus: Release 9.2.0.1.0 - Production on Thu Mar 15 23:16:39 2007
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> @create_cour_sys.sql

```

You are prompted for the following parameters:

Table 24: Parameters for the create_cour_sys.sql script

Parameter	Means
new_tablespace_name	The new tablespace for Connector user
new_datafile	The 10 Mb datafile for this tablespace
new_user_name	The Connector User name
new_user_password	The password for this user

Figure 233: Parameters for the create_cour_sys.sql script

```

C:\WINDOWS\system32\cmd.exe
J:\Courion\scripts>sqlplus system@vis11
SQL*Plus: Release 9.2.0.1.0 - Production on Thu Mar 15 23:16:39 2007
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.
Enter password:
Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production
SQL> @create_cour_sys.sql
Enter value for new_tablespace_name: TS_COURION_02
old 1: CREATE TABLESPACE &&new_tablespace_name
new 1: CREATE TABLESPACE TS_COURION_02
Enter value for new_datafile: E:\ORACLE\VISDATA\TS_COURION02.dbf
old 2: DATAFILE '&new_datafile' SIZE 10M
new 2: DATAFILE 'E:\ORACLE\VISDATA\TS_COURION02.dbf' SIZE 10M
Tablespace created.
Enter value for new_user_name: COUR01
Enter value for new_user_password: COUR123
old 1: CREATE USER &&new_user_name IDENTIFIED BY &new_user_password
new 1: CREATE USER COUR01 IDENTIFIED BY COUR123
old 2: DEFAULT TABLESPACE &&new_tablespace_name
new 2: DEFAULT TABLESPACE TS_COURION_02
User created.
old 1: GRANT CONNECT, RESOURCE TO &&new_user_name
new 1: GRANT CONNECT, RESOURCE TO COUR01
Grant succeeded.
Disconnected from Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production
J:\Courion\scripts>_

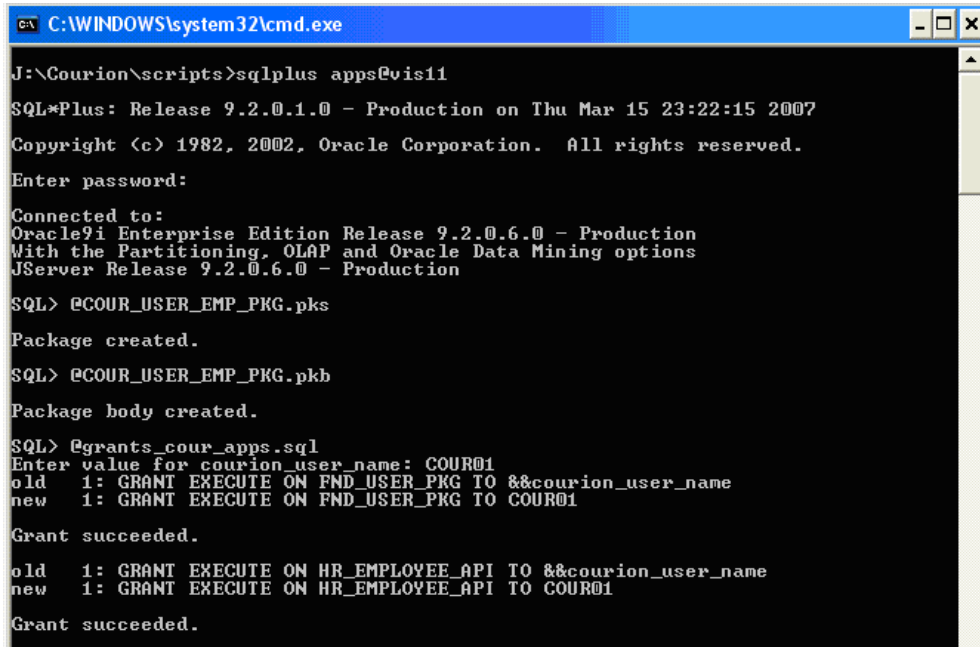
```

- Run SQLPLUS and connect as APPS. Run the following scripts as APPS:

Table 25: Parameters for APPS connection

Script	Purpose
COUR_USER_EMP_PKG.pks	Creates the package specification
COUR_USER_EMP_PKG.pkb	Creates the package body
grants_cour_apps.sql	Grants for Connector User

You are prompted for the Connector User name with the courion_user_name parameter:

Figure 234: Prompt for the Connector User Name


```

C:\WINDOWS\system32\cmd.exe

J:\Courion\scripts>sqlplus apps@vis11

SQL*Plus: Release 9.2.0.1.0 - Production on Thu Mar 15 23:22:15 2007
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> @COUR_USER_EMP_PKG.pks

Package created.

SQL> @COUR_USER_EMP_PKG.pkb

Package body created.

SQL> @grants_cour_apps.sql
Enter value for courion_user_name: COUR01
old 1: GRANT EXECUTE ON FND_USER_PKG TO &&courion_user_name
new 1: GRANT EXECUTE ON FND_USER_PKG TO COUR01

Grant succeeded.

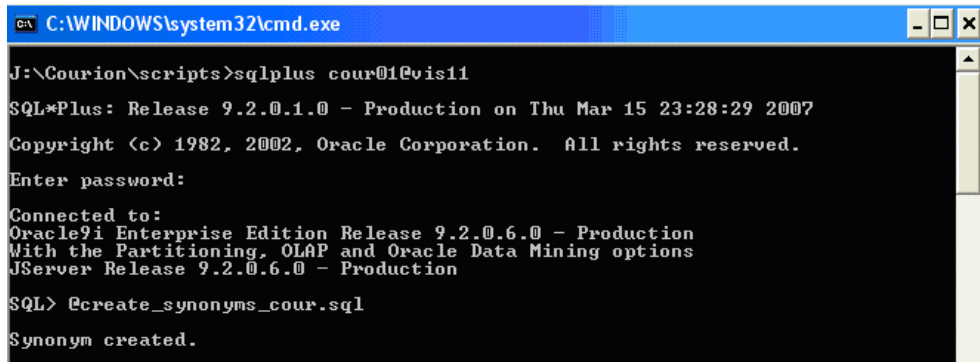
old 1: GRANT EXECUTE ON HR_EMPLOYEE_API TO &&courion_user_name
new 1: GRANT EXECUTE ON HR_EMPLOYEE_API TO COUR01

Grant succeeded.

```

You should see 35 "Grant succeeded" messages.

4. Run SQLPLUS and connect as Connector user. Run create_synonyms_cour.sql. No parameters are required to do this:

Figure 235: Run create_synonyms_cour.sql


```

C:\WINDOWS\system32\cmd.exe

J:\Courion\scripts>sqlplus cour01@vis11

SQL*Plus: Release 9.2.0.1.0 - Production on Thu Mar 15 23:28:29 2007
Copyright (c) 1982, 2002, Oracle Corporation. All rights reserved.

Enter password:

Connected to:
Oracle9i Enterprise Edition Release 9.2.0.6.0 - Production
With the Partitioning, OLAP and Oracle Data Mining options
JServer Release 9.2.0.6.0 - Production

SQL> @create_synonyms_cour.sql

Synonym created.

```


Chapter 50: Oracle Internet Directory — Connector

This chapter explains how to configure the Connector for Oracle Internet Directory (shown in the connector as Oracle Internet Directory Server) and the Connector for Oracle Directory Server Enterprise.

- [*“Configuring the Connector for Oracle Internet Directory” on page 464*](#)

Configuring the Connector for Oracle Internet Directory

The Connector for Oracle Internet Directory supports the following operations on a target:

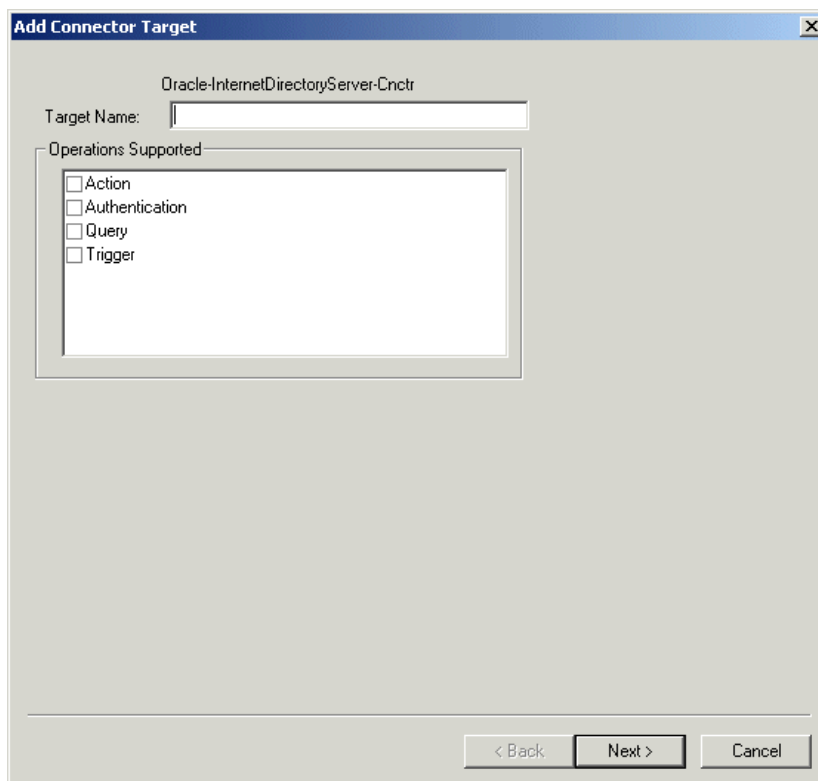
- Authentication and query against a Oracle Internet Directory server
- Create and delete an entry in a Oracle Internet Directory server directory
- Add, Change, Create, Enable, Disable, Delete, Verify, and View actions in a Oracle Internet Directory server directory.

Follow these steps to add a Oracle Internet Directory target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **ORACLE-INTERNETDIRECTORYSERVER-CNCTR**
3. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears

Figure 236: Add Oracle Internet Directory Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
5. Select one or more operations:
 - Select **ACTION** to enable the Add, Change, Create, Delete, Disable, Enable, Verify, and View actions on a target data source.
 - Select **AUTHENTICATION** to use the target data source for authenticating end user access to the provisioning application.

- Select **QUERY** to enable the provisioning application to use queries to find data in the target data source.
 - Select **TRIGGER** to allow access to two groups of triggers. These triggers (MVAddValue - objectClass and MVRemoveValue – objectClass) add or remove a value from a multi-valued attribute in an object. There are three parameters for each trigger (CN, Attribute and Value). CN is the object(s) to modify. Commas are used to separate entries, so they must be escaped in each individual entry with “^2C”. Attribute is the attribute to change. Value is the value to set or remove. Values must match exactly. Triggers are configured on the Trigger Subform in the Administration Manager. See the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for details.
6. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 237: Connector Configuration Manager for Oracle Internet Directory

Connector Configuration Manager for Oracle Internet Directory Server

Target Configuration

Directory server:

Directory server port: ☐ Use secure connection

Certificate database:

*Privileged username:

Password:

Search Container Configuration

*Topmost container for performing searches:

* Entries must contain a fully distinguished name

7. Enter **TARGET CONFIGURATION** information:
- **DIRECTORY SERVER** — Enter the name (or IP address) of the LDAP server on which the provisioning actions are performed.
 - **DIRECTORY SERVER PORT** — Enter the TCP/IP port number used by the LDAP server to communicate with the connector. The default is 389 for a nonsecure connection or 636 for an SSL connection.
 - If the SSL option is not enabled on the Oracle Internet Directory server, connection to the server must use a nonsecure port with port number 389.
 - **USE SECURE CONNECTION** — Check this if SSL is used to secure the traffic.

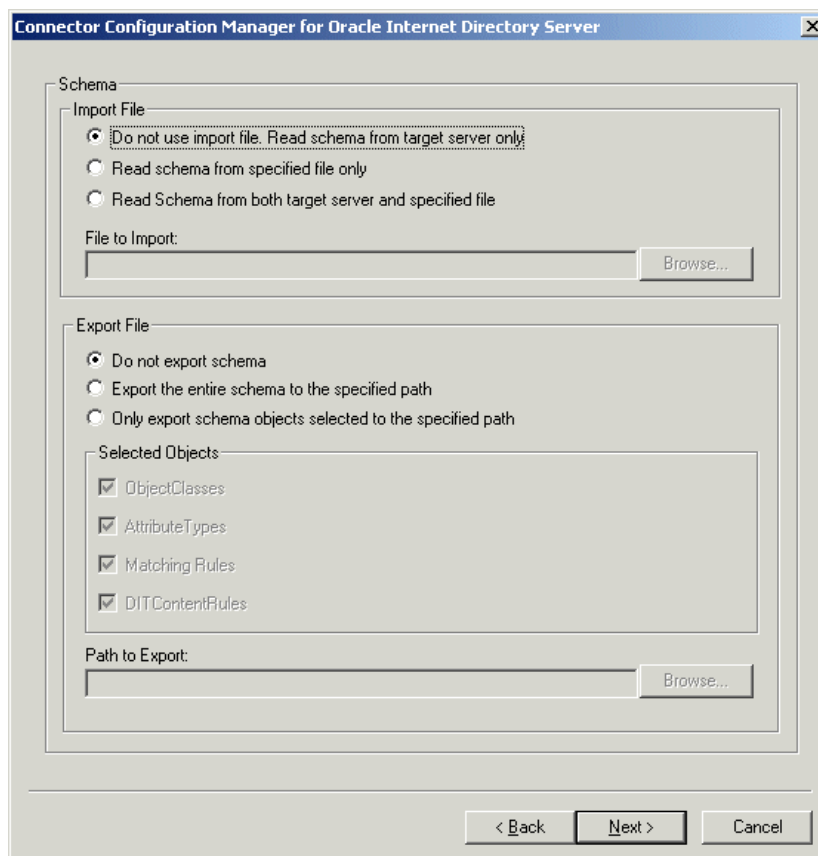
- **CERTIFICATE DATABASE** — If the connection to the Oracle Internet Directory server uses SSL, specify the filename of a p7b file, such as `cert7.db`, that contains certificates used by the LDAP server and trusted by Core Security software. The Connector Configuration Manager uses this certificate file to determine if it can trust the server's SSL certificate.

Note: This connector now uses the Microsoft WinLDAP API which leverages the Windows Certificate store. Certificates in this folder are not actually used.

- **PRIVILEGED USERNAME** — Enter the name that identifies the user who has sufficient rights to add, delete, modify and search the sub-tree of the directory.
 - **PASSWORD** — Enter the privileged user's password.
8. **TOPMOST CONTAINER FOR PERFORMING SEARCHES** — Enter the base Distinguished Name (search base) of the container from which queries, such as those made by a custom macro, begin. You can specify multiple search base trees by using a semicolon to separate the Distinguished Names. Use the format "o=name", for example, o=corp.courion.com.
 9. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 238: Connector Configuration Manager for Oracle Internet Directory Server (2)



10. Enter **SCHEMA** information:

Note: For most configurations, the default settings of **DO NOT USE IMPORT FILE** and **DO NOT EXPORT SCHEMA** are the appropriate settings.

- **Import File** — Select how to control how external schema information is provided to the connector:
 - A. **DO NOT USE IMPORT FILE. READ SCHEMA FROM TARGET SERVER ONLY**
 - B. **READ SCHEMA FROM SPECIFIED FILE ONLY**
 - C. **READ SCHEMA FROM BOTH TARGET SERVER AND SPECIFIED XML FILE**
 - **FILE TO IMPORT** — The location of the XML file to be imported that contains the additional schema information. See [“Import File Example” on page 468](#) for an example of this file.
11. **Export File** — Select how to control how to export existing schema information for the connector:
- A. **DO NOT EXPORT SCHEMA**
 - B. **EXPORT THE ENTIRE SCHEMA TO THE SPECIFIED PATH**
 - C. **ONLY EXPORT SCHEMA OBJECTS SELECTED TO SPECIFIED PATH**
 - d. **PATH TO EXPORT** — The folder directory entry to export the schema information to file.

Note: This feature is not implemented yet.

12. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 239: Connector Configuration Manager for Oracle Internet Directory Server (3)

The screenshot shows a dialog box titled "Connector Configuration Manager for Oracle Internet Directory Server". Inside, there is a tab labeled "Create Object Configuration". Below the tab, there is a text field labeled "*Container for directory entry creation:". Below this field is a button labeled "Retrieve Objects". Below the button are three dropdown menus labeled "Object class for account actions:", "Password field for account object:", and "Profile UID field for account object:". Below these dropdowns is a checkbox labeled "Enforce case-insensitive comparison". At the bottom of the dialog box, there is a note: "* Entries must contain a fully distinguished name". At the very bottom of the dialog box are three buttons: "< Back", "Finish", and "Cancel".

13. Enter **CREATE OBJECT CONFIGURATION** information:

- **CONTAINER FOR DIRECTORY ENTRY CREATION** — Enter the Distinguished Name of the container which the provisioning application uses for all actions, including creating and deleting entries and authentication.

Enter only one container here.

- **RETRIEVE OBJECTS** — Click this button to retrieve the list of objects which can be used for account actions, object class, and account passwords. This list lets you specify the password field to ensure that the provisioning application does not copy it from the Model Account.

The differences between a Profile and an Account are determined by the workflow. Generally a user only has one profile and may have many accounts.

- **OBJECT CLASS FOR ACCOUNT ACTIONS** — Select the name of the object class that defines the attributes for the resource entries to be managed by the provisioning application. Typically, the object class is “inetOrgPerson”.
- **PASSWORD FIELD FOR ACCOUNT OBJECT** — Select the attribute to be used as the account password. For example, userPassword.
- **PROFILE UID FIELD FOR ACCOUNT OBJECT** — Select the attribute to be used as the profile UID. For example, uid (user identifier) or cn (common name). The current setting is active only when the Oracle Internet Directory is used for the IdentityMap.

Note: If you want to store the IdentityMap on the Oracle Internet Directory (in the LDAP directory), extend the LDAP schema to store the IdentityMap. See the manual *Configuring Workflows with the Access Assurance Suite Administration Manager* for information about how to do this.

- **ENFORCE CASE-INSENSITIVE COMPARISON** — If you leave this box unchecked, the LDAP server applies its own matching rules when searching. Otherwise the connector retrieves all related entries (and values) and perform case-insensitive comparison.

14. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services. The target is now available for each action supported by this connector.

Import File Example

The import file is used to provide additional DITContentRules to the schema information to associate object classes with auxiliary objects. To create a DITContentRule the object class OID or Name must be provided along with the auxiliary object name(s) that contain that auxiliary attributes of an object.

The following XML syntax is used to provide this information:

```
<?xml version="1.0" encoding="UTF-8"?>
<ditcontentrules>
  <ditcontentrule>
    <oid></oid>
    <name></name>
    <auxobjects>
      <auxobject></auxobject>
      <auxobject></auxobject>
      <auxobject></auxobject>
    </auxobjects>
  </ditcontentrule>
</ditcontentrules>
```

```
        </auxobjects>  
    </ditcontentrule>  
</ditcontentrules>
```

To discover the correct auxiliary objects that contains the needed auxiliary attributes, you can use any LDAP browser to export the schema to research the information.

Chapter 51: PeopleSoft — PMM and Connector

This chapter explains how to configure the PMM and Connectors for PeopleSoft®:

- [*“Configuring the PMM for PeopleSoft” on page 472*](#)
- [*“Configuring the Connector for PeopleSoft” on page 479*](#)
- [*“Configuring the Web Services Connector for PeopleSoft Enterprise Applications” on page 483*](#)

Configuring the PMM for PeopleSoft

The Password Management Module (PMM) for PeopleSoft lets Access Assurance Suite applications reset passwords automatically on PeopleSoft systems.

The correct access key is necessary to run this PMM. For more information on access keys, please contact Core Security.

Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

All of the following requirements, through [“Configuring PeopleSoft Applications” on page 473](#), pertain to PeopleSoft PMM installation.

Using PeopleSoft External APIs

The PeopleSoft PMM lets you configure multiple PeopleSoft targets. Each target can connect to a PeopleSoft server running a different version of PeopleSoft software. For example, you can configure one target to connect with a PeopleSoft version 8.21 server and another target to connect with a version 8.4 server. To configure different targets, install versions of PeopleSoft External APIs that correspond with the versions on the target PeopleSoft Servers.

Note: PeopleSoft 8.4 does not provide external API setup. Before configuring targets for PeopleSoft 8.4 or later, follow the steps in PeopleBooks “Setting Up a Client Machine to Access a C++ API.” Ensure that you apply the same level of software patches to the Connector Framework and Connector Framework Manager as are applied to the PeopleSoft server. Then copy file `psjoa.jar` to directory `winx86` as in the example below.

Installing the PeopleSoft External APIs on the Connector Framework or Connector Framework Manager Servers

Each version of PeopleSoft server has a unique set of PeopleSoft external APIs associated with it. Install each version of the PeopleSoft external APIs into a different directory on each server where a Connector Framework or Connector Framework Manager is installed. When you configure the PMM for PeopleSoft, enter one of these directory paths into the “PMM Configuration Manager for PeopleSoft” dialog box.

Path of an 8.21 Directory

The following is a sample path to a directory on the Connector Framework and Connector Framework Manager for PeopleSoft external APIs for PeopleSoft server version 8.21.


```
C:\Pt821\bin\Client\winx86_extapi
```

Note: The default installation directory name is Pt810. Create separate directories for each version of PeopleSoft External APIs.

Path of an 8.4 Directory

The following are sample paths to directories on the Connector Framework and Connector Framework Manager for PeopleSoft external APIs for PeopleSoft server version 8.4. The actual path depends on the location of the PeopleSoft API. The path must include both the PeopleSoft and Java client directories.

```
PATH
C:\Program Files\Java\jre1.5.0_06\bin\client
C:\PT847\bin\client\winx86
```

For the last line in this example, you would copy the `psjoa.jar` file into this directory using the following command:

```
C:\> copy c:\PT84\class\psjoa.jar c:\pt84\bin\client\winx86
```

Then create a new variable called `CLASSPATH` that points directly to the `psjoa.jar` file. Here, based on the examples above, is the value for `CLASSPATH` variable:

```
CLASSPATH=C:\PT847\bin\client\winx86\psjoa.jar
```

For more information about installing PeopleSoft external APIs, refer to the section on *External API Integration* in the PeopleSoft PeopleTools Installation document for the appropriate version of PeopleSoft API software.

Installing Java Virtual Machine Versions

The Connector Framework and Connector Framework Manager require specific Java Virtual Machine versions to use the PeopleSoft external API to connect to a PeopleSoft server.

For more information about which Java Virtual Machine versions you need to install on the Connector Framework and Connector Framework Manager, refer to the section on *External API integration* in the PeopleSoft PeopleTools Installation document for the appropriate version of PeopleSoft API software.

Configuring PeopleSoft Applications

Before you configure the PMM for PeopleSoft, ensure that you have configured these PeopleSoft applications appropriately as described below.

PMM for PeopleSoft Privileged User Permissions

Ensure that the privileged user that the PMM for PeopleSoft uses to reset PeopleSoft passwords has permission to read and write the `USER_PROFILE` Component Interface.

Note: The privileged user requires a minimum set of access to the USER_PROFILE Component Interface. To obtain minimal access, set the following USER_PROFILE methods to Full Access: Get, ResetPassword, ResetPassword_AlphaNum, Save, and SetPassword. The USER_PROFILE methods Create, Cancel and SetUserDescription are optional. See [Figure 240](#).

Figure 240: Component Interface Permissions

Home > PeopleTools > Maintain Security > Use > Permission Lists [New Window](#)

Component Interface Permissions

USER_PROFILE

First 1-8 of 8 Last

Method	*Method Access
Get	Full Access
ResetPassword	Full Access
ResetPassword_AlphaNum	Full Access
Save	Full Access
SetPassword	Full Access
Create	No Access
Cancel	No Access
SetUserDescription	No Access

Full Access (All)

No Access (All)

OK Cancel

PSWDEXPIRED Property in the USER_PROFILE Component Interface

The USER_PROFILE Component Interface requires a property named "PSWDEXPIRED" pointing to the Password Expired field of the user component. This property is not provided by default. To add this property to the USER_PROFILE Component Interface, follow these steps:

1. Log in to the PeopleTools development environment on your PeopleSoft server system.
2. Open the USER_PROFILE Component Interface in the PeopleTools Application Designer utility.
3. Select the PSWDEXPIRED field from the PSUSRPRFL_WRK record definition.
4. Drag and drop the PSWDEXPIRED field from the Component window to the Component Interface window.
5. Save the changes.

Forcing a Password Change on Next Logon

This procedure is optional. Use it only to configure the “Force Password Change on Next Logon” feature for a PMM for PeopleSoft target. To use this feature, complete the following steps on each PeopleSoft target system that the PMM for PeopleSoft uses to reset PeopleSoft passwords:

1. Log in to the target PeopleSoft server using the Administrative username.
2. Open the Password Controls page.
3. Select **PASSWORD EXPIRES IN XXX DAYS** and set it to a value from 1 and 365 days. This attribute applies to all the PeopleSoft application users and specifies the maximum number of days after which users must change their passwords. To use the **FORCE PASSWORD CHANGE ON NEXT LOGON** feature, check the box in the PMM Configuration Manager for PeopleSoft dialog box (see page 476).

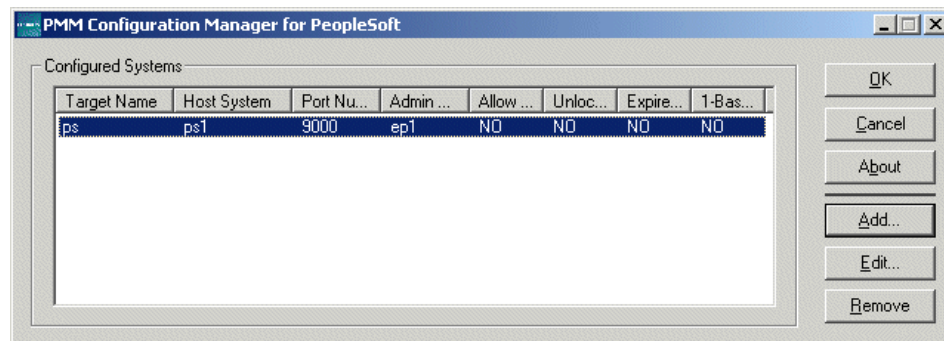
The USER_PROFILE Component Interface requires a property named “LASTPSWDCHANGE” pointing to the LASTPSWDCHANGE field of the user component. This property is not provided by default. To add this property to the USER_PROFILE Component Interface, follow these steps:

1. Log in to the PeopleTools development environment on your PeopleSoft server system.
2. Open the USER_PROFILE Component Interface in the PeopleTools Application Designer utility.
3. Select the LASTPSWDCHANGE field from the PSOPRDEFN record definition.
4. Drag and drop the LASTPSWDCHANGE field from the Component window to the Component Interface window.
5. Save the changes.

PMM Configuration

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Password Management
Modules>PeopleSoft
The PMM Configuration Manager dialog box appears.

Figure 241: PMM Configuration Manager for PeopleSoft



2. From this dialog box, you can:

- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, another PMM Configuration Manager for PeopleSoft dialog box appears.

Figure 242: PMM Configuration Manager for PeopleSoft- Add Target

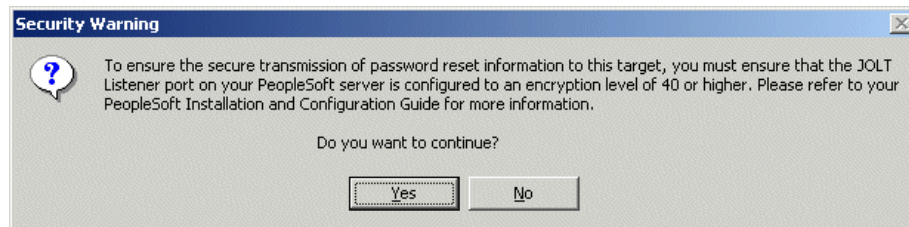
3. **TARGET NAME** — Enter a target alias in the Target Name field. (You cannot edit the name of an existing target.) The target alias enables you to have multiple targets configured against the same PeopleSoft server. For example, you can configure different targets for PasswordCourier end-user Web Access and PasswordCourier Support Staff access. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
4. **PEOPLESOFT SERVER** information
 - a. **HOST** — Enter the PeopleSoft server domain name or IP address for the PeopleSoft server that performs password resets.
 - b. **PORT** — Enter the JOLT port number on the PeopleSoft server where the PeopleSoft application server's JOLT Listener process is listening.
This port number resides in a file named as in the following format:

```
PeopleSoft-Install
Directory\appserv\domainname\psappsrv.cfg
```

The number is listed as the Port attribute of Jolt Listener. By default, this value is 9000.

5. **PRIVILEGED USER** information
 - a. **NAME** — Enter the Privileged Username that the target uses to reset PeopleSoft passwords. This privileged user must have permissions to read and write the USER_PROFILE Component Interface.
 - b. **PASSWORD** — Enter the Password associated with the specified privileged user.
6. **PATH FOR EXTERNAL API** — Enter the path to the PeopleSoft external API files on the Connector Framework and Connector Framework Manager. These APIs correspond to the version of the PeopleSoft server software associated with this target. See [“Using PeopleSoft External APIs” on page 472](#).
7. **USE ONE-BASED INDEX FOR COLLECTIONS** — This value depends on the version of PeopleSoft server associated with this target. The default value is determined by the API files referenced in the “Path for external APIs.” In general, use the default value determined by the PMM.
8. **ALLOW RESET FOR ADMINISTRATIVE PASSWORDS** — Select this checkbox if you allow passwords resets for PeopleSoft users with either the “PeopleSoft Administrator” or “System Administrator” role.
9. **UNLOCK DISABLED ACCOUNT** — Select this checkbox if password resets should unlock accounts that are locked out.
10. **FORCE PASSWORD CHANGE ON NEXT LOGON** — Select this checkbox if you require PeopleSoft users to change their password on their next logon after a password reset has occurred. See [“PSWDEXPIRED Property in the USER_PROFILE Component Interface” on page 474](#).
11. Click **OK** to accept your entries in the dialog box.

The following message appears.



The security of password reset information between the PMM for PeopleSoft and the target PeopleSoft server depends on the encryption level on the Jolt Listener port.

12. If the Jolt listener port on the PeopleSoft server is configured to an encryption level of 40 or above, click **YES**.

If the encryption level is below 40, click **No** to return to the PMM Configuration Manager dialog box. Then click **CANCEL** to cancel the configuration of the target. You can reconfigure the target after the encryption level on the PeopleSoft server set to a higher value.

You have configured a PMM target.

Note: You need to re-start the PMM Configuration Manager for each different PeopleSoft® target you want to edit. If you edit a PeopleSoft® target, do not attempt to edit a second PeopleSoft® target in the same instance of running the PMM Configuration Manager.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Configuring the Connector for PeopleSoft

The Connector for PeopleSoft supports the following actions on a target: Add, Change, Create, Disable, Delete, Enable, Verify, and View.

Note: PeopleSoft, and Core provisioning applications use different definitions for Action and Profile. The Connector for PeopleSoft supports both profile management and action. Profile Management supports Create, Update, and Delete account.

Prerequisites

The Connector for PeopleSoft requires the 32 bit PeopleTools External API files. If your version of PeopleSoft/PeopleTools only offers 64 bit version of the External API files, please contact Customer Support and request the Connector for Oracle PeopleSoft.

The Connector for PeopleSoft requires an Access Key. For more information about the Access Key, please contact Core Security.

Privileges Required

The privileged user on the Connector Framework and Connector Framework Manager requires full access to certain Component Interfaces on the PeopleSoft server. These are:

.USER_PROFILE

.DELETE_USER_PROFILE

To allow access to a Component Interface in a PeopleSoft PeopleTools application, create a Permission List by navigating to:

Home>PeopleTools>Security>Permissions & Roles>Permission Lists

To add a Component Interface, click on (+), type the Component Interface name or search for it. Click on Edit to grant all method access. For more details on setting Component Interface security, see the sections on “Setting Security Options” in the following PeopleSoft PeopleBooks documentation: “Security Administration” and “PeopleSoft CompInterfaces.”

Creating a Role for This Connector

Additionally, you need to create a role specific for this connector. After creating the role, add the permission list to it and assign the role to the privileged user.

Configuring the Connector Framework and Connector Framework Manager to Support the PeopleSoft Target

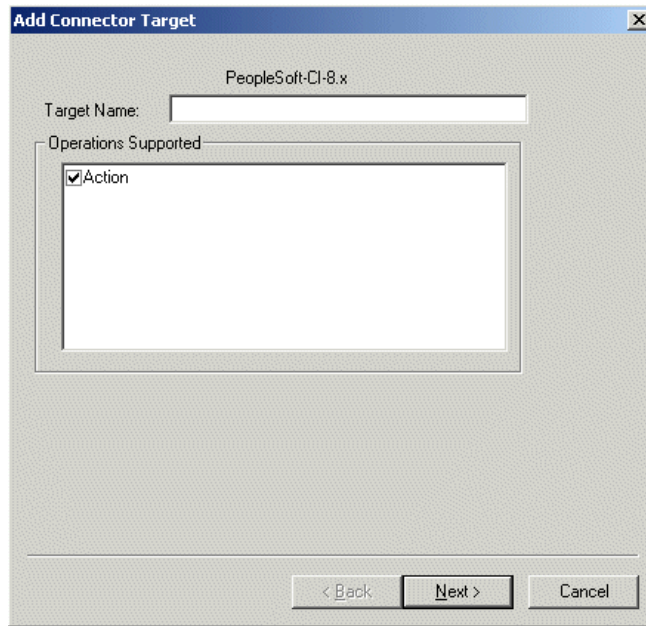
On each server in which the Connector Framework or Connector Framework Manager is installed, complete the following steps to configure the web service to support the PeopleSoft target.

1. Install the PeopleSoft File Server. Refer to the section on “Using the PeopleSoft Installer” in the PeopleSoft Installation Guide for detailed information about how to do this.
2. Set the environment variable PS_HOME to point to the installed PeopleSoft PeopleTools directory. Example: `c:\PT848`
3. Install the Java Virtual Machine (JVM) supplied with Sun Microsystems Java Development Kit (JDK). You can find this in the `%PS_HOME%\JRE` directory or download it from:
www.java.com.
4. Set the environment variable CLASSPATH to include the `psjoa.jar` file.
Example: `<PS_HOME>\class\psjoa.jar`
5. Set the environment variable PATH to include the directory containing `jvm.dll`.
Example: `<JAVA_HOME>\jre1.6.0_03\bin\client`
6. Set the environment variable PATH to include the directory containing the 32 bit version of the `psapiadapter.dll`. Example:
`<PS_HOME>\bin\client\winx86`
7. Install the patch level of PeopleTools to match the version-patch level of the PeopleSoft server. You can obtain patches from:
support.peoplesoft.com

For more information about installing PeopleSoft external APIs, refer to the section on “External API Integration” in the PeopleSoft PeopleTools Installation Guide for the appropriate version of PeopleSoft API software.

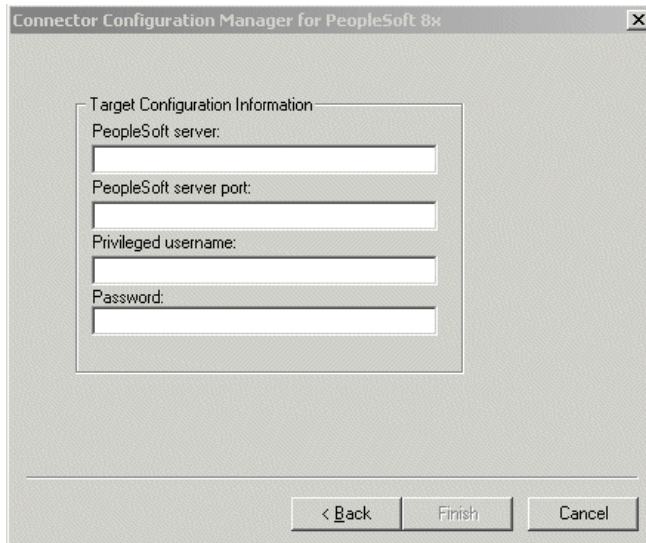
Connector Configuration

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **PEOPLESOFT-CI-8.X**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 243: Add PeopleSoft Target


The dialog box is titled "Add Connector Target". It has a text field for "Target Name:" with the placeholder text "PeopleSoft-CI-8.x". Below this is a section titled "Operations Supported" containing a list box with a single checked item, "Action". At the bottom are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target to the Administration Manager.
5. Select **ACTION** to enable the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.
6. Click **NEXT**. The Connector Configuration Manager for PeopleSoft 8.x appears.

Figure 244: Connector Configuration Manager for PeopleSoft


The dialog box is titled "Connector Configuration Manager for PeopleSoft 8x". It contains a section titled "Target Configuration Information" with four text input fields labeled: "PeopleSoft server:", "PeopleSoft server port:", "Privileged username:", and "Password:". At the bottom are three buttons: "< Back", "Finish", and "Cancel".

7. Enter the following **TARGET CONFIGURATION INFORMATION**:
 - **PEOPLESOFT SERVER** — Enter the DNS name for the PeopleSoft server.
 - **PEOPLESOFT SERVER PORT** — The port on which the PeopleSoft server listens. For the server port number, check with your PeopleSoft administrator.
 - **PRIVILEGED USERNAME** — The administrative ID that the connector uses to authenticate to the PeopleSoft server.

- **PASSWORD** — The password for the privileged username.
8. Click **FINISH** to complete the configuration.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Courion Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each of the provisioning actions for the selected connector.

Configuring the Web Services Connector for PeopleSoft Enterprise Applications

Please contact Customer Support to get the newer connector used to integrate to PeopleSoft over web services called the Connector for Oracle PeopleSoft. That connector should be used to integrate with PeopleSoft over web services instead of this connector available in the suite installation kit.

The Web Services Connector for PeopleSoft Enterprise Applications supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, and View.

Configuring PeopleSoft Web Services

Web Services integration is provided by exposing the component interface for USER_PROFILE and DELETE_USER_PROFILE.

For PeopleTools 8.44 to 8.46

Consult the PeopleSoft PeopleBooks specific to your version, for information on configuring WSDL Binding for Component Interfaces.

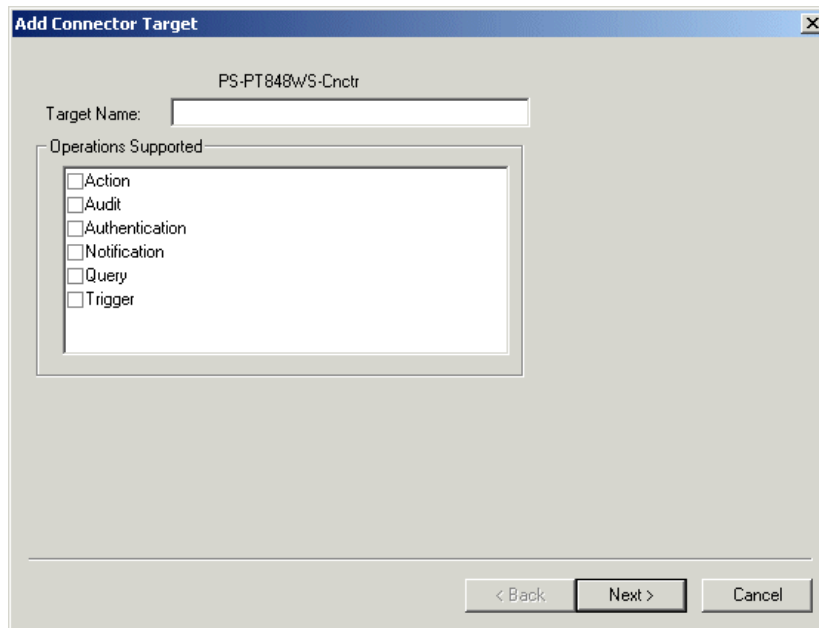
For PeopleTools 8.47 and higher

Consult the PeopleSoft PeopleBooks specific to your version, for information on Providing Web Services.

Connector Configuration

Follow these steps to add a Peoplesoft target:

1. From the Start menu, select:
Programs>Courion Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **PS-PT848WS-CNCTR**, and click **OK**.
3. Select **PS-PT848WS-CNCTR**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

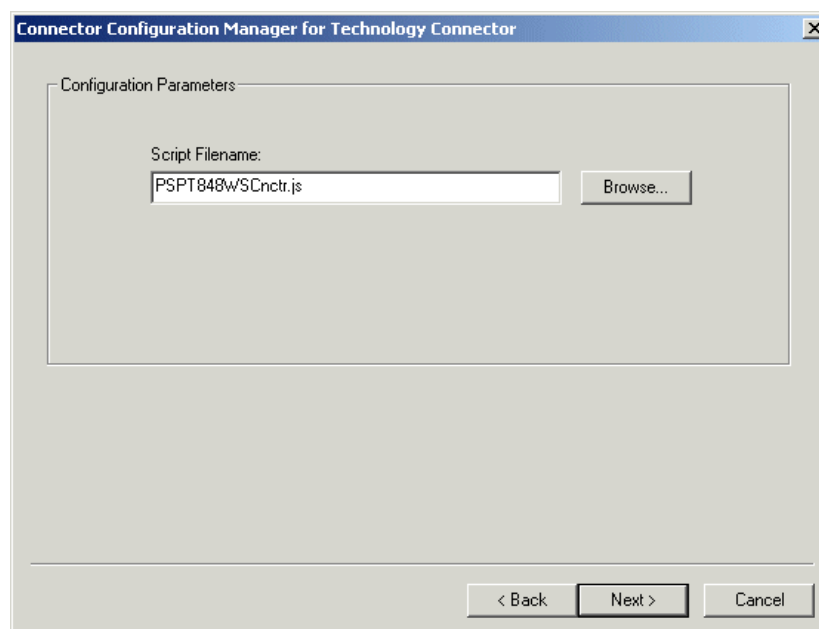
Figure 245: Add PeopleSoft PeopleTools 8.48 Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. Select **ACTION** to enable the following actions on the target: Add, Change, Create, Delete, Disable, Enable, and View.

Note: Other operations that appear in this dialog box are not supported.

7. Click **NEXT**.

The Connector Configuration Manager dialog box appears.

Figure 246: Connector Configuration Manager for PeopleSoft PeopleTools 8.48

8. The default `PSPT848WSCnctr.js` script providing the functionality for performing connector operations is entered for the **SCRIPT FILENAME**. If you want to use a different script, browse to the location and name of that script. Click the **NEXT** button.

The second configuration window for Peoplesoft appears.

Figure 247: Connector Configuration Manager for PeopleSoft PeopleTools 8.48

9. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **WSDL URL** — URL path to the location of User Profile WSDL.
 - **DeleteWSDL URL** — URL path to the location of Delete User Profile WSDL.
 - **WS User Name** — User with rights to access location where WSDLs are stored.
 - **WS User Password** — User password to use to access WSDLs.
 - **WS-Security** — Flag to indicate that the target system uses WS-Security SOAP Header. Values are “True” or “False”.
 - **Disable Namespaces** — Flag to disable usage of namespacing within SOAP messages. Values are “True” or “False”.
 - **Privileged User** — User with rights to execute actions against target system.
 - **Privileged User Password** — Password for the privileged user.
 - **Operation Create Name** — Create operation name if an alias is being used.
 - **Operation Get Name** — Get operation name if an alias is being used.
 - **Operation Update Name** — Update operation name if an alias is being used.
 - **Operation UpdateData Name** — UpdateData operation name if an alias is being used.
 - **Operation Delete Name** — Delete operation name if an alias is being used.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

10. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Notes and Warnings

- The Web Service Connector for PeopleSoft Enterprise Applications requires that Disabling Namespace be set to “True” and WS-Security be set to “False”, when using PeopleSoft PeopleTools 8.46 and below.
- The Web Service Connector for PeopleSoft PeopleTools Enterprise Applications does not support the "copy" operation on Email Addresses, IDType and Role attributes on the Create, Add, Change, Enable, and Disable actions.
- Changes or upgrades to the PeopleSoft CRM and Financials application may require changes to this connector.

Chapter 52: Red Hat Enterprise Linux — PMM and Connector

This chapter explains how to configure the PMM and Connector for Red Hat® Enterprise Linux®. It also explains how to install and use the Linux PMM agent:

- [*“Configuring the PMM for Red Hat Enterprise Linux” on page 488*](#)
- [*“Writing Password Management Scripts” on page 491*](#)
- [*“Installing and Configuring the Linux PMM Agent” on page 492*](#)
- [*“Configuring the Connector for Red Hat Enterprise Linux” on page 497*](#)

Configuring the PMM for Red Hat Enterprise Linux

The Password Management Module (PMM) for Red Hat® Enterprise Linux® enables Core Access Assurance Suite applications to reset passwords automatically on Linux systems. The PMM is a component of the Core Access Assurance Suite and is installed when the suite is installed.

You can specify the user and password pair that is appropriate for the server on which a reset is requested. Additionally, you can mark one privileged user entry as the default username and password pair for all servers not explicitly configured.

The correct access key is needed for this PMM. For details on access keys, please contact Core Security.

Prerequisites

This PMM requires the Linux PMM agent to run. See [“Installing and Configuring the Linux PMM Agent” on page 492](#) for details on the agent.

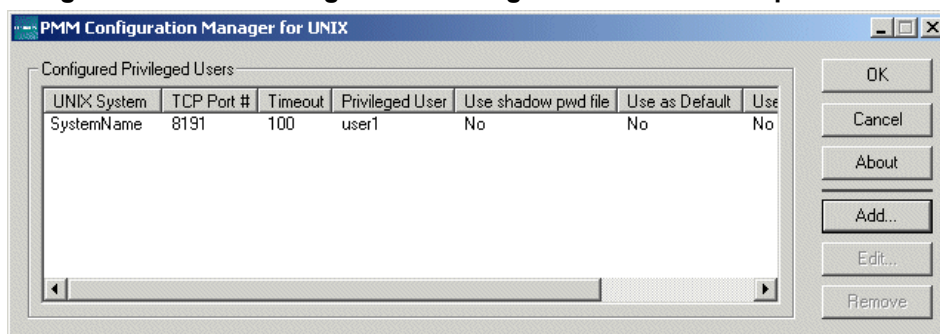
The PMM also requires the Linux Pluggable Authentication Modules (libpam.so{X.YY}) on the machine where the PMM agent for Linux is installed.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Programs> Core Access Assurance Suite>Password Management Modules>Linux
2. Click on Linux and, when prompted, click **YES** to begin the configuration.
The PMM Configuration Manager for Unix appears.

Figure 248: PMM Configuration Manager for Red Hat Enterprise Linux



3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 249: Add / Edit UNIX System PMM Configuration for Red Hat Enterprise Linux

To configure a privileged user for the PMM for Linux, perform the following steps:

4. Enter the name of the Linux server on which password resets are performed. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
5. Enter the TCP/IP port on which the Linux agent is listening. The default is 8191.
6. Enter the amount of time (in seconds) before password reset timeout in the **TIMEOUT (SECS)** field. The default value for this field is 10 seconds.
7. Enter the name of the privileged user.

Note: The privileged user configured requires no special privileges; the account is only used to activate the password reset executed by the agent software.

8. Enter the password for the privileged user.
9. **RESET TYPE**

Determine the reset type to be performed and select “Local Workstation” or “NIS” as appropriate.

- If you select **LOCAL WORKSTATION** and the Linux system uses a shadow password file to authenticate users, check the **USE SHADOW PASSWORD FILE** check box.
 - If you select **NIS** and the privileged user exists in the local database and not in the NIS map, check the **USE LOCAL PASSWORD FILE FOR VERIFYING THIS PRIVILEGED USER** check box. Additionally, if the local database where the privileged user's password file uses a shadow file, check the **USE SHADOW PASSWORD FILE** check box.
10. **USE SHADOW PASSWORD FILE** — If the password file is stored in a shadow file, check this box.
 11. **USE LOCAL PASSWORD FILE FOR VERIFYING THIS ADMINISTRATIVE USER** — If you want this user's password to be authenticated using the local system password file, check the box.
 12. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — If you want this username to be the default username for all servers not specifically configured in the PMM Configuration Manager, check the box.
 13. **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** — If you want to allow password resets of users with a UID or GID of zero, check this box.
 14. Click the **OK** button to save the configuration.
 15. If desired, continue to configure additional users for other servers.
 16. You have finish configuring the PMM. Click the **OK** button to save the changes and exit the configuration program.

You have configured a target for this PMM.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Writing Password Management Scripts

The PMM for Linux has the ability to run a sequence of Linux shell commands to perform a password reset. This allows the PMM for Linux to reset any password which has an administrative password reset available via the Linux shell.

The Linux agent reads a specialized script language. The syntax of the language is as follows:

- **S N send-string** - Send 'send-string' to a pseudo terminal (pty) and pause for N number of seconds before continuing. The send string can contain any of the following substitution macros:
 %u - The user name to be reset
 %p - the plain text password
 %e - the encrypted password
- **V N verify-string** - Verify that 'verify-string' is found in the output from the pty after waiting N number of seconds for a response and continue when a response is received. The verify string can contain any of the substitution macros described in the send command. It is necessary to have a verify string at the end. If the final verify command isn't received, the end user receives a failure message.
- **;** comment-string - A comment string. Comments must be alone on a line. Commands cannot have trailing comments.

Use a scripting language such as Perl or shell script to write a script that performs a password reset.

The following is an example of a script that uses a custom Perl script to reset a user's password:

```
; Send to launch custom reset script
s 2 perl password_reset_cmd %u %p
; Verify successful message
v 2 "Password reset was successful"
```

Note: Arguments to the “s” and “v” commands must be enclosed with quotation marks.

To tell the PMM for Linux agent to use the script for performing resets, go to the directory where the agent was installed and locate the pxy_def.txt file. Open the file with a text editor and add the following line:

- `SCRIPT_NAME:pwd.scr`

where pwd.scr is the name of the created script file.

For the change to take effect, start and stop the agent ([“Configuring the PMM Agent” on page 493](#))

Installing and Configuring the Linux PMM Agent

This section explains how to install, configure, start, stop, and uninstall the Linux PMM agent.

Installing the Agent

The PMM agent runs as a daemon on the Linux machine. Table 26 describes the agent installation components included with the PMM for Linux.

Table 26: PMM Agent for Linux Components

Agent Files	Installation Components
PMM for Linux agent files	configure pwdcour_start_scr pwdcour_unixpxy pxy_def.txt install uninstall
PMM for Linux agent tar files	unixlinux.tar (supports Red Hat Enterprise Linux versions 2.1 to 3.x) unixlinux-b.tar (supports Red Hat Enterprise Linux 4.0)

Copy the tar file for the Linux system from the Unix folder located in the directory where the Core Access Assurance Suite is installed to a temporary directory on the Linux machine on which the agent is being installed. Log on to the machine as a superuser and proceed to the directory where the tar file was placed.

Note: You must have superuser privilege to install the agent.

Note: If NIS is being used, install the agent on the same machine as the NIS master.

Extract the installation files for the platform using the following command:

```
tar -xvf unixlinux.tar
```

This creates and places all of the install files inside of a subdirectory named courion.

1. Change to that directory and then execute the installation shell script by typing `./install`.

Follow the prompts and answer the questions. The following information is required:

2. The install directory for the agent (the default is `/usr/local/courion`)
3. The password filename (the default is `/etc/passwd`)
4. Whether the system uses NIS.

5. If NIS is being used, the default path to yp database directory for the make command (/var/yp).
6. The TCP/IP port available to the agent (default is 8191)

Note: The agent installation is complete when the steps are performed. If any changes need to be made, make them before finishing step 6.

After installing the agent, launch it by rebooting or by executing the following command:

```
/etc/rc3.d/S99pwdcour_unixpxy start
```

Configuring the PMM Agent

Installation places a configuration file named `pxy_def.txt` in the agent's installation directory on the Linux host. (The default installation directory is `/usr/local/courion.`) This file has several parameters that control the agent's actions and configuration. You can use a text editor, such as `vi`, to change the `pxy_def.txt` file. Table 27 provides a description of the various parameters.

Table 27: PMM agent for Linux Configuration Parameters

Parameter Syntax	Description
<code>INST_DIR:install_dir</code>	This is the directory in which the agent is installed. By default, the agent is installed in <code>/usr/local/courion.</code>
<code>LOG_FILE:log_file</code>	This is the name of the file to which the agent logs all messages. If the directory is omitted, the <code>log_file</code> is automatically created in the directory specified by <code>INST_DIR</code> . If this parameter is omitted, the default value is <code>pxy.log</code> .
<code>LOG_LEVEL:n</code>	Log messages have a log level 'n' associated with them. The log level ranges from 0-2. Depending on the log level you specify in the <code>pxy_def.txt</code> file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the <code>pxy_def.txt</code> file. By default, the log level specified is 0.
<code>MAKE_DIR:make_directory</code>	This is the directory in which the make command can be found. It is used to rebuild the NIS password map. If the directory is omitted, the default is <code>/var/yp</code> . Note: This argument is only relevant when the PMM is configured for native NIS reset support.

Table 27: PMM agent for Linux Configuration Parameters (Continued)

Parameter Syntax	Description
NIS_YPMAKE_CMD: <i>make_cmd</i>	This the command line used to rebuild and/or push the NIS password map. If it is omitted, the default command is: <pre>cd%s;%s/make passwd NOPUSH=TRUE.</pre> The first “%s” is a substitution macro for the value specified by Y_DIR. The second “%s” is a substitution macro for the value specified by MAKE_DIR. Note: This argument is only relevant when the PMM is configured for native NIS reset support.
NIS_YPMAKE_RESP: <i>response</i>	This is the expected response from the command used to rebuild and/or push the NIS password map. If this value is omitted, the default response is “updated passwd.” Note: This argument is only relevant when configured for native NIS reset support.
NIS_PASSWORD_FILE	This parameter is used to specify the path to the NIS password file on the local machine. It is necessary to use this file when NIS password files that are not /etc/passwd are being used.
PASSWORD_FILE: <i>passwd_file</i>	This represents the fully qualified file name of the password file against which users are validated and native workstation and/or NIS resets are performed. If the file is omitted, the default is /etc/passwd.
PWD_ERR_MSG: <i>err_msg</i>	This is a custom error message displayed to the user when an error occurs during a password reset. If it is omitted, a technical error description is displayed.
SCRIPT_NAME: <i>script_file</i>	This is the name of the script file to run for resets. For more information on scripts, see “Creating a Workflow for the Target” on page 490. If this parameter is omitted, a native password reset (either workstation or NIS) is performed.
SHDW_FILE: <i>shadow_file</i>	This is the fully qualified file name of the shadow file against which users are validated and native workstation resets are performed. This value is consulted if the PMM Configuration Manager is configured with the USE SHADOW PASSWORD FILE check box checked. If it is omitted, the default is /etc/security/shadow.
SVR_NAME: <i>server</i>	This represents the host name of the server on which the agent is installed. There is no default value. This value must be valid.
SVR_PORT: <i>port_number</i>	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value and the port number specified here must be the same as the one used during PMM configuration. This value must be present.

Table 27: PMM agent for Linux Configuration Parameters (Continued)

Parameter Syntax	Description
VALIDATION_USER: <i>username</i>	This user name must match the user configured for this server on the machine running on the Connector Framework Manager. If this parameter is omitted, the default value is root. Note: The privileged user configured requires no special privileges, the account is only used to activate the password reset executed by the agent software.
YP_DIR: <i>yp_dir</i>	This is the directory where the NIS password file exists. If it is omitted, the default value is /var/yp. Note: This argument is only relevant when the PMM is configured for native NIS password reset support.

Starting and Stopping the Agent

For any changes to take effect, stop and then start the agent using the startup script. To start the PMM agent, run the startup script with the argument **START**. Run the script with the **STOP** argument to stop the agent.

- To start: `/etc/pwdcour_unixpxy start`
- To stop: `/etc/pwdcour_unixpxy stop`

Displaying the Version Information

To output the version of the proxy, execute the following command from the UNIX prompt: `/usr/local/courion/pwdcour_unixpxy -v`

This outputs the version information to the command window, e.g. 7.50.00.113

There is not an option in the `/etc/pwdcour_unixpxy` file to output the version information; you have to run it directly from the install directory (default for AIX is `/usr/local/courion`).

The default install directory is the same for each platform the proxy is installed on (`/usr/local/courion`).

Uninstalling the Agent for Upgrading

To upgrade the PMM agent for Linux, uninstall the previous agent and then install the new agent.

Note: Before beginning the uninstall process, back up the directory `install-dir/pxy_def.txt` to another directory, where *install-dir* is the installation directory, typically `/usr/local/courion`. Also back up the reset script file to another directory if scripted resets are being used.

Note: The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

To uninstall the PMM agent for Linux, execute the uninstall script by typing a command of the form

```
installdir/uninstall
```

- Follow the prompts and answer the questions. You must know the install path.
- After using tar to extract the distribution files for the new PMM agent for Linux, install the new agent by following the steps outlined in [*“Installing the Agent” on page 492*](#).
- Merge custom entries from the backed up `pxy_def.txt` file into the new `install-dir/pxy_def.txt` file.
- Restore the backed-up reset script to the desired directory. Make sure the new `pxy_def.txt` file refers to that script.

Configuring the Connector for Red Hat Enterprise Linux

The Connector for Red Hat Enterprise Linux supports the following actions on a target: Add, Change, Create, Enable, Disable, Delete, Verify, and View.

Prerequisites

Before you configure the connector, create a user with sudo permission and gather configuration information from the target.

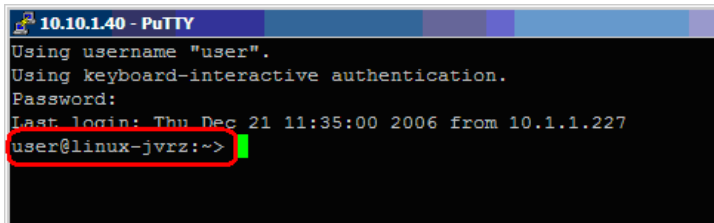
1. Create a user for the connector to log in as and perform provisioning actions on. This user should be a regular user with sudo permission for the following programs:
 - useradd
 - grep
 - usermod
 - userdel
 - passwd
2. Gather the following information from the sudo user

SSH User

SSH Password

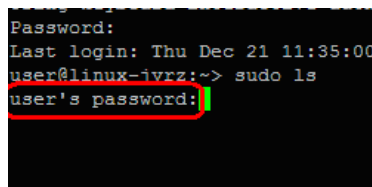
Target User Prompt — To get this information, login as the sudo user and grab the text to the left of the cursor after login is complete, as shown in [Figure 250](#).

Figure 250: Linux Target User Prompt



Sudo Password Verification Prompt — To get this information, login as the sudo user and execute a sudo ls command. Copy the text to the immediate left of the cursor when it asks you for the password, as shown in [Figure 251](#).

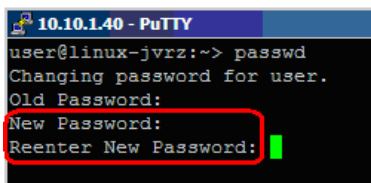
Figure 251: Linux Password Verification Prompt



SSH Server — Core Security recommends you use the IP address of the server to maximize reliability or the fully qualified domain name.

New Password Prompt / Verify New Password Prompt — To get this information, execute a `passwd` command as the `sudo` user. Enter a new password, but do not verify it. It gives you the next two settings, as shown in [Figure 252](#).

Figure 252: New and Verify New Password Prompt



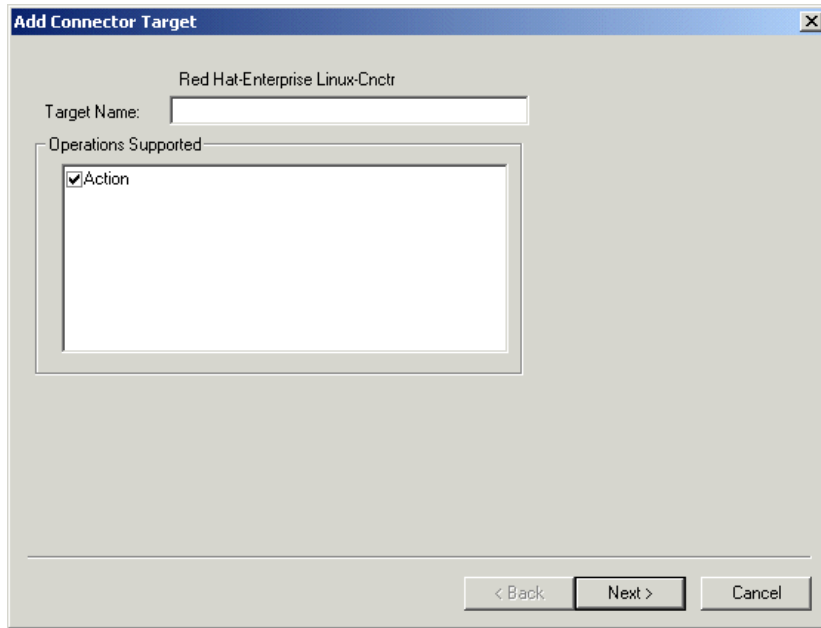
You enter all of the information acquired in step 2 when you configure the connector.

Connector Configuration

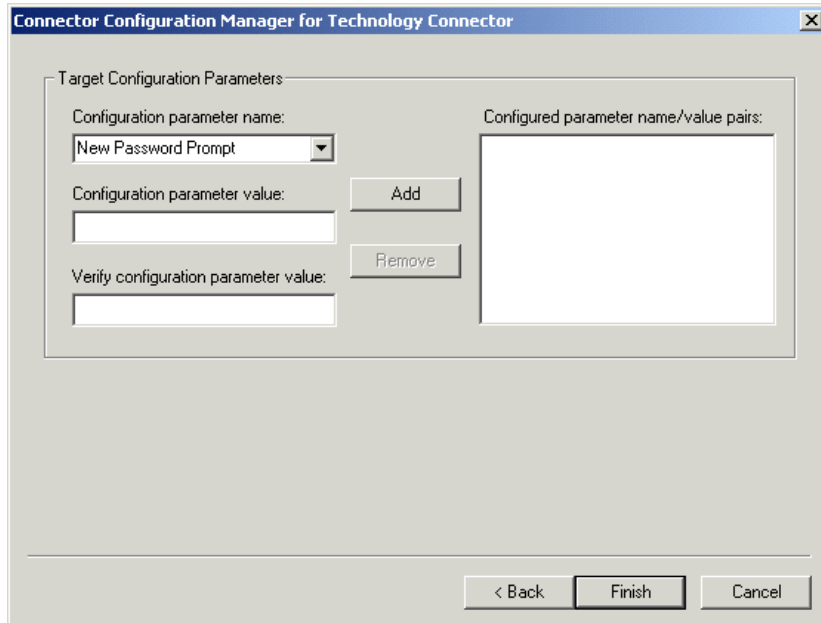
Follow these steps to add a Red Hat Enterprise Linux target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **RED HAT-ENTERPRISE LINUX-CNCTR**, and click **OK**.
3. Select **RED HAT-ENTERPRISE LINUX-CNCTR**
4. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears.

Figure 253: Add Red Hat Enterprise Linux Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. **ACTION** is selected by default, to enable all operations on the target. Click **NEXT**.
The Connector Configuration Manager dialog box appears.

Figure 254: Connector Configuration Manager for Red Hat Enterprise Linux

7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second

time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 53: Research In Motion BlackBerry 4.x — Connector

This chapter explains how to configure the Connector for Research In Motion® (RIM®) BlackBerry®:

- [*“Configuring the Connector for RIM BlackBerry” on page 502*](#)

Configuring the Connector for RIM BlackBerry

The connector for RIM BlackBerry supports the following actions on a target: Add, Change, Create, Delete, Disable, Verify, and View.

Configure targets using:

- The BlackBerry User Administration tool password or SQL Username/Password pair (if so configured).
- The name of the target BlackBerry "service" to provision for.
- The path to the BlackBerry User Administration tool.
- The host name or address of the BlackBerry server if the BlackBerry Administration tool is not installed on the BlackBerry server itself.

The resource being managed is the BlackBerry server user. The BlackBerry server uniquely identifies users dependent upon which mail system is configured.

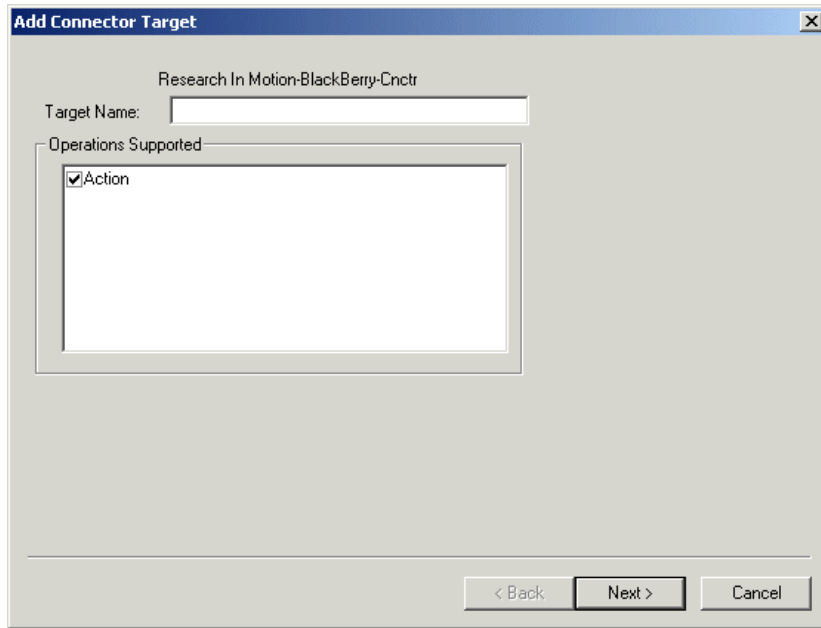
- For Microsoft Exchange, this is the mailbox name (jdoe@domain.ext).
- For IBM Lotus Domino, this is the canonical name (CN=John Doe/O=Server01).
- For Novell GroupWise, this is the user ID (jsmith).

When configuring the unique identifier in the IdentityMap, use the unique identifier respective to the configured mail system.

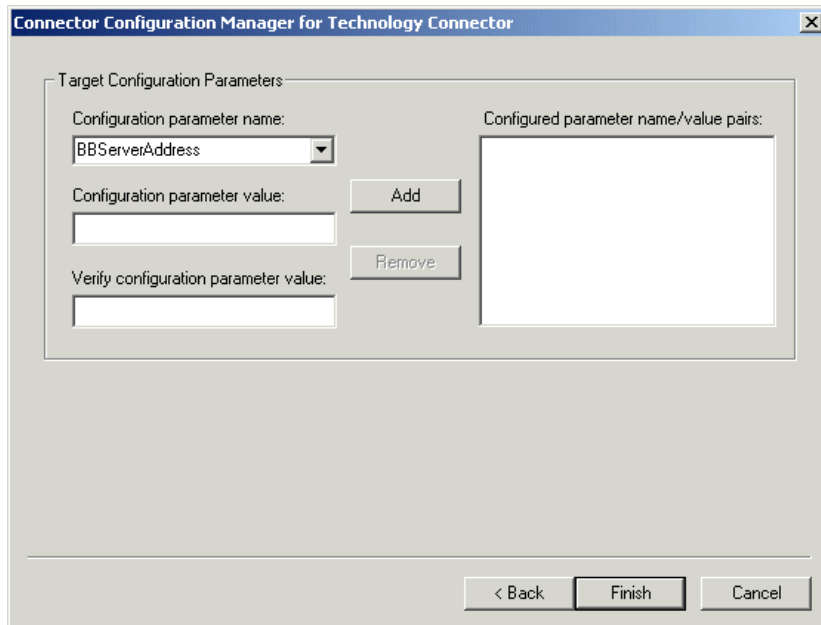
Connector Configuration

Follow these steps to add a target domain:

1. From the Start menu, select:
Programs > Core Access Assurance Suite > Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **RESEARCH IN MOTION-BLACKBERRY-CNCTR**, and click **OK**.
3. Select **RESEARCH IN MOTION-BLACKBERRY-CNCTR**.
4. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 255: Add RIM BlackBerry Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**. The configuration screen for RIM BlackBerry appears.

Figure 256: Connector Configuration Manager for RIM BlackBerry

6. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **BBSERVERADDRESS** — The host name or address of the BlackBerry server. This is only required if the BlackBerry User Administration tool is not installed on the same server as the BlackBerry server.

- **BBSERVICE**NAME — The name of the specific BlackBerry service on the BlackBerry server to manage.
- **TOOLPASSWORD** — The password to access the BlackBerry User Administration client tool. This password is set during installation BlackBerry User Administration tool.
- **TOOLPATH** — The complete path to the BlackBerry User Administration client tool (e.g. C:\path\to\BESUserAdminClient.exe).

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.

7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by the connector.

Notes and Warnings

- A BlackBerry user can only be provisioned after the user's mail account is completely created. For example, a Microsoft Exchange user's mailbox is not created until the user has logged into his or her mail account.
- The connector cannot perform Change or Disable actions on a BlackBerry user until the user has activated his or her BlackBerry.
- The Disable action does not disable a BlackBerry user. Instead, the action disables a user's BlackBerry by issuing a "kill BlackBerry" command to the device.
- The BlackBerry Enterprise Server system does not have the capability to enable or disable specific users. Therefore, there is no Enable action available and the Disable action is instead implemented to disable a user's BlackBerry device.
- The activation password expiration time is limited by the BlackBerry Enterprise server to between 1 and 720 hours. The default value is 48 hours.
- The activation password expiration time may not be changed without specifying a new activation password.
- To clear a user's BlackBerry software configuration, submit "CLEARCONFIG" as the user's new software configuration in a Change action.
- To clear a user's BlackBerry group assignment, submit "CLEARGROUP" as the user's new group in a Change action.

Chapter 54: Research In Motion (RIM) BlackBerry 5.x — Connector

This chapter explains how to install the BlackBerry Administration certificate and configure the Connector for Research In Motion® (RIM®) BlackBerry® 5.x:

- [*“Installing the BlackBerry Administration Certificate” on page 506*](#)
- [*“Configuring the Connector for RIM BlackBerry” on page 510*](#)

Note: Install the BlackBerry Administration Certificate before you configure the connector.

Installing the BlackBerry Administration Certificate

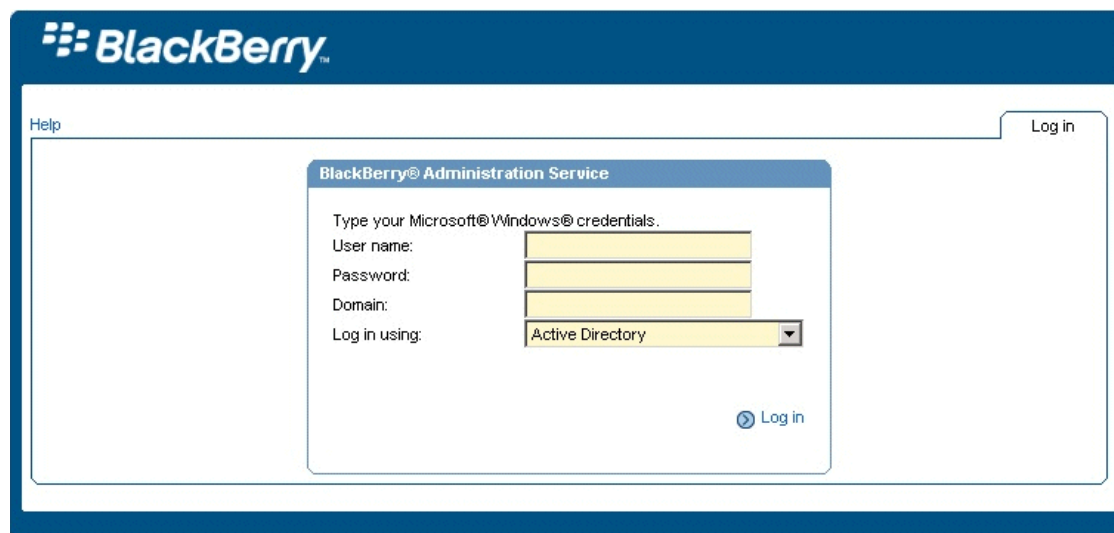
Follow these steps to install the BlackBerry administration certificate as a trusted certificate on the server where the Connector for BlackBerry 5.x is running:

1. Use Microsoft Internet Explorer® to browse to the BlackBerry Administration Service. Example: <https://BlackBerryServer.companyname.com/webconsole/app>

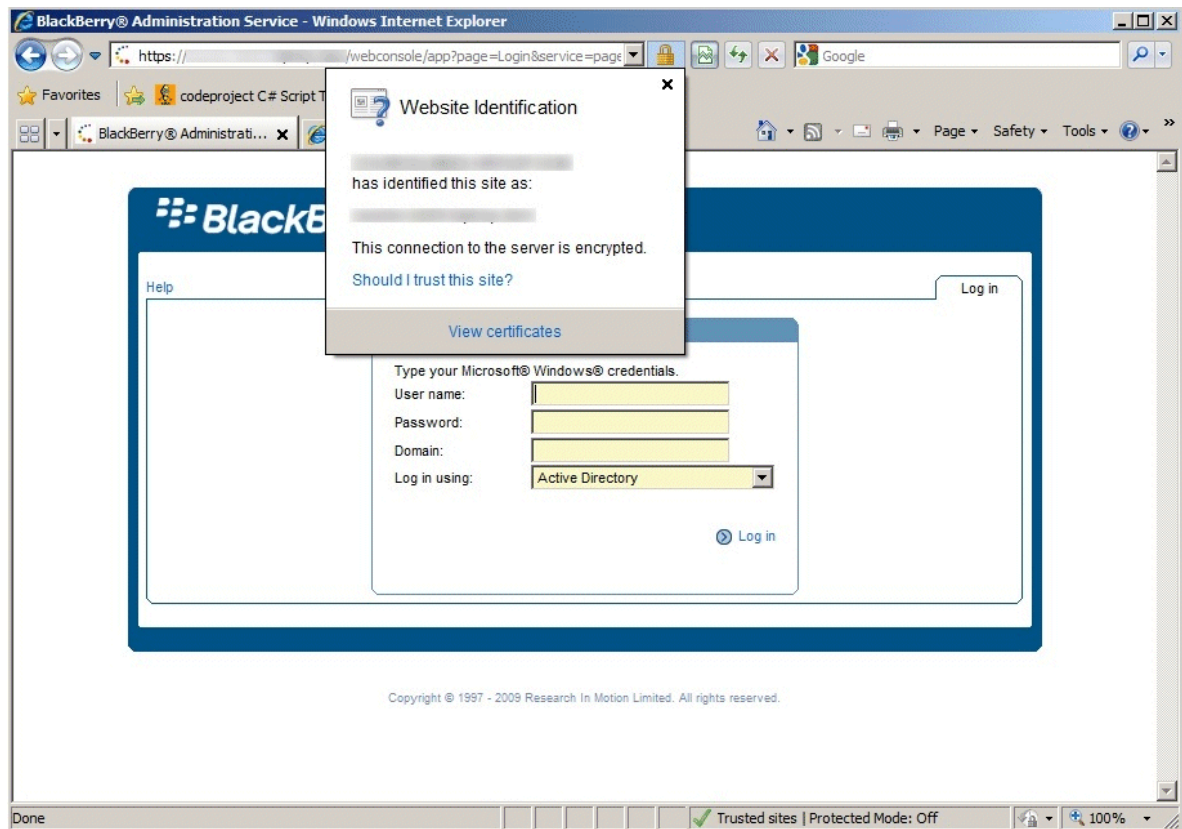
Note: The hostname of the server where the BlackBerry Administration Service resides is the Administration Web Service Hostname that you specify during connector configuration.

[Figure 257](#) shows the BlackBerry Administration Service.

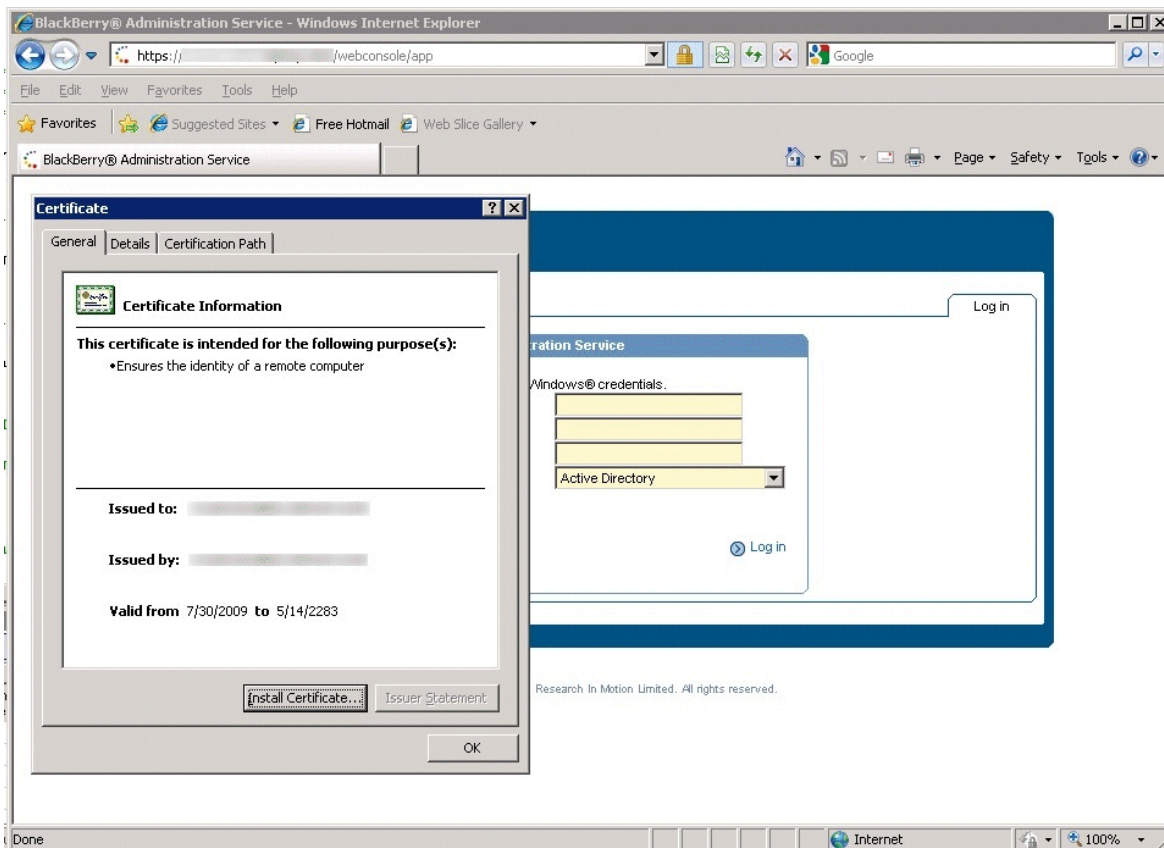
Figure 257: BlackBerry Administration Service



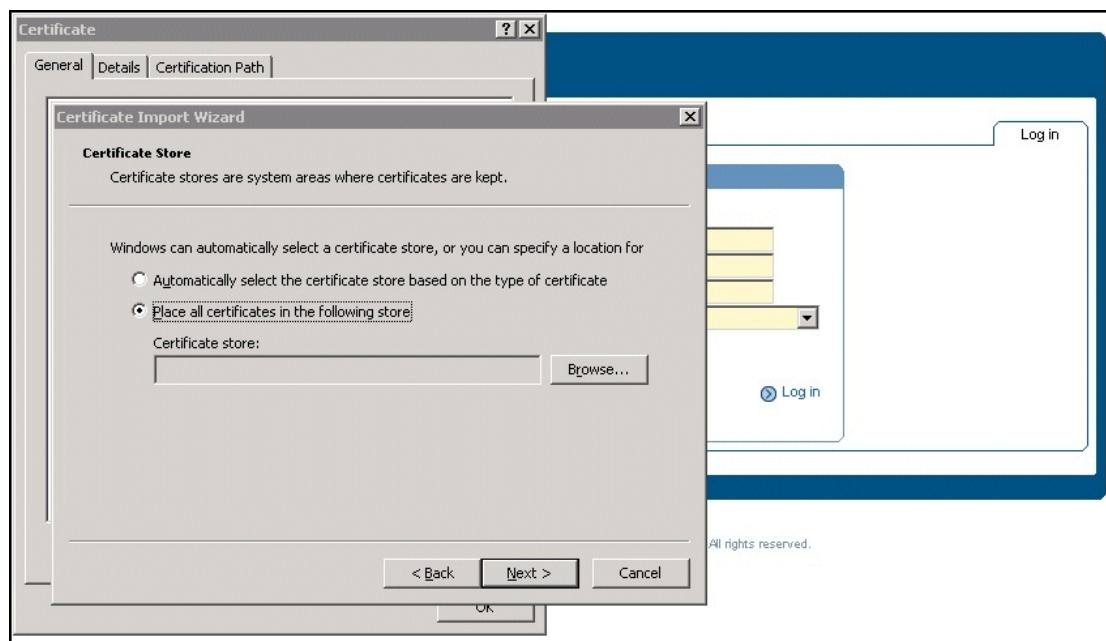
2. View the certificate. The method you use to do this depends on the version of Internet Explorer that you use. For Internet Explorer version 8, for example, you click on the lock icon in the tool bar, as shown in [Figure 258](#), then click on **VIEW CERTIFICATES**.

Figure 258: Viewing the Administration Certificate

3. Click the **INSTALL CERTIFICATE...** button to start the installation wizard, as shown in [Figure 259](#).

Figure 259: Install Certificate

4. On the Certificate Import Wizard dialog box, select the **PLACE ALL CERTIFICATES IN THE FOLLOWING STORE** option, and click **BROWSE...**, as shown in [Figure 260](#).

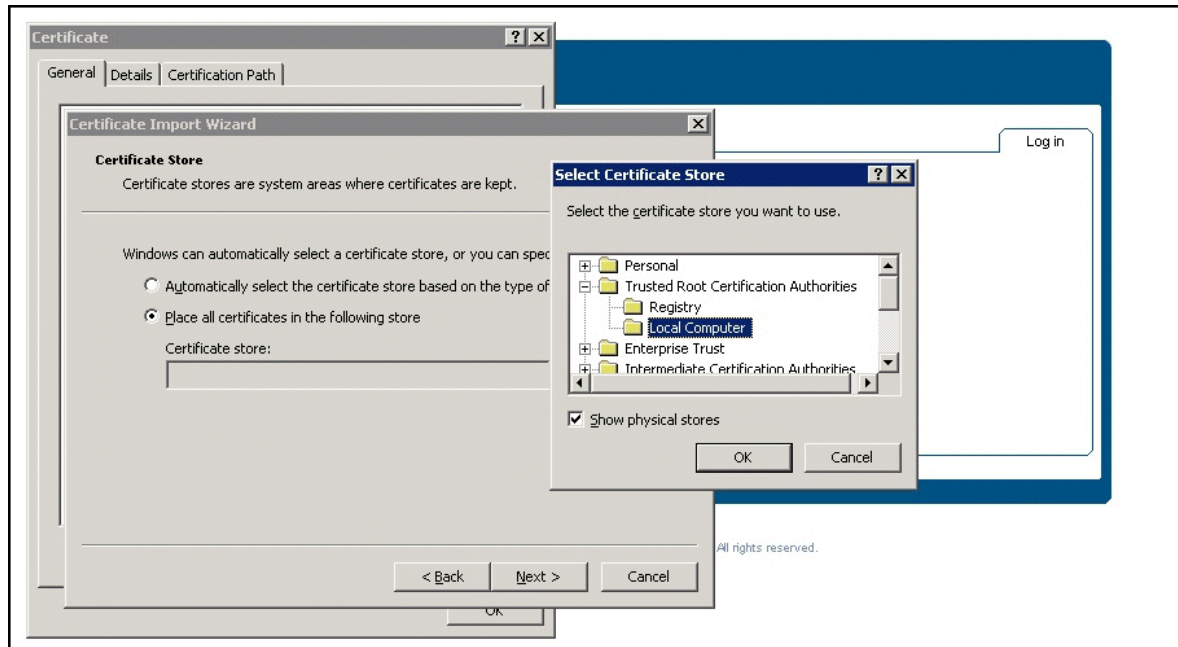
Figure 260: Certificate Import Wizard

5. In the Select Certificate Store dialog box, select the **SHOW PHYSICAL STORES** check box, and select the following folder:

Trusted Root Certification Authorities\Local Computer

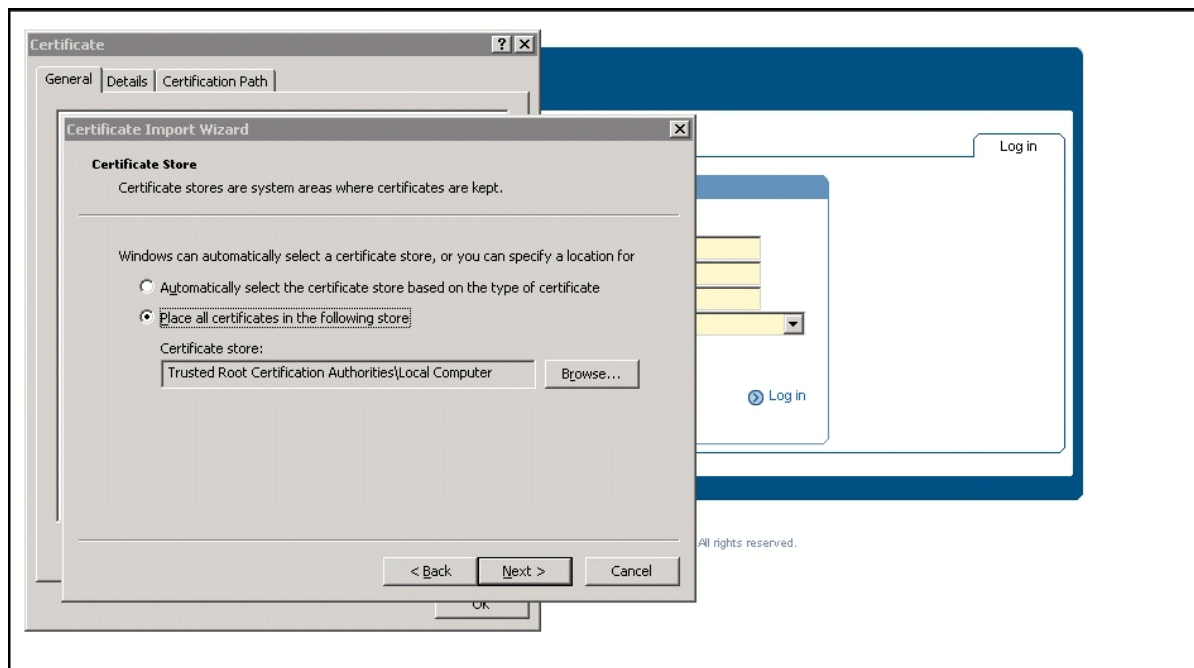
See [Figure 261](#).

Figure 261: Select Certificate Store



6. Select **OK**. The Certificate Import Wizard dialog box appears, with the **CERTIFICATE STORE** field populated with the folder you specified in the Select Certificate Store dialog: Trusted Root Certification Authorities\Local Computer. See [Figure 262](#).

Figure 262: Certificate Import Wizard with Certificate Store Populated



7. Click **NEXT**, then click **FINISH**.

Configuring the Connector for RIM BlackBerry

The connector for RIM BlackBerry supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Configure targets using:

- Administrator username
- Administrator password
- Administrator domain
Example: companyname.com
- The hostname or address of the server where the BlackBerry Administration Service resides. This is the hostname in the path you specified when browsing to the BlackBerry Administration Service to install the BlackBerry Administration Certificate (see [“Installing the BlackBerry Administration Certificate” on page 506](#)).
Example: BlackBerryServer.companyname.com

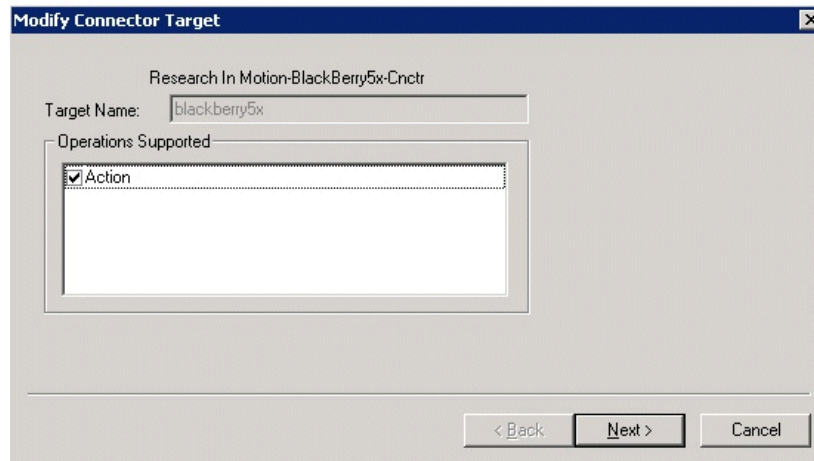
The BlackBerry server uniquely identifies users by email address. For Microsoft Exchange, this is the mailbox name (jdoe@domain.ext).

When configuring the unique identifier in the IdentityMap, use the unique identifier that corresponds to the configured mail system.

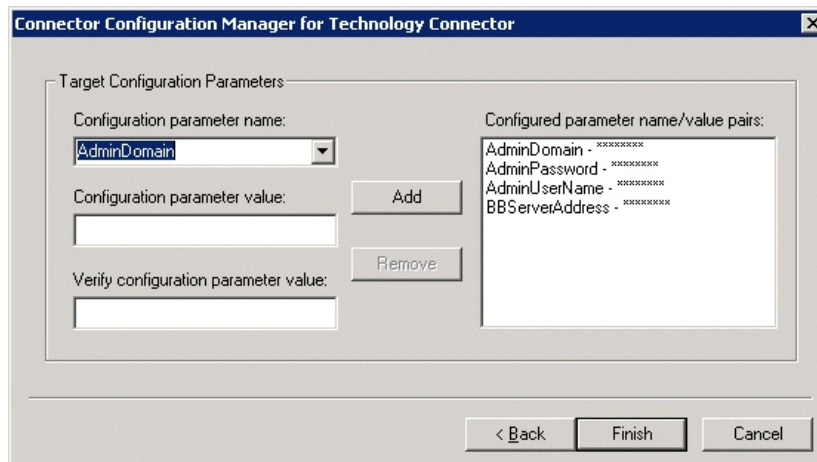
Connector Configuration

Follow these steps to add a target domain:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **RESEARCH IN MOTION-BLACKBERRY5X-CNCTR**, and click **OK**.
3. Select **RESEARCH IN MOTION-BLACKBERRY5X-CNCTR**.
4. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 263: Add RIM BlackBerry Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**.
The connector configuration manager for RIM BlackBerry appears.

Figure 264: Connector Configuration Manager for RIM BlackBerry

6. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **BBSERVERADDRESS** — The hostname or address of the server where the BlackBerry Administration Service resides.
 - **ADMINUSERNAME** — The name of the BlackBerry administrator user.
 - **ADMINPASSWORD** — The password of the BlackBerry administrator user.
 - **ADMINDOMAIN** — The Active Directory domain where the administrator user resides. If you leave this blank, the connector uses the BlackBerry Administrator Service as its authentication provider instead of Active Directory.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

7. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services. Restart the services to activate the connector.

The target is now available for each action supported by the connector.

Notes and Warnings

- A BlackBerry user can only be provisioned after the user's mail account is completely created. For example, a Microsoft Exchange user's mailbox is not created until the user has logged into his or her mail account.
- The connector cannot perform Change, Disable, or Enable actions on a BlackBerry user until the user has activated his or her BlackBerry.
- The Disable action generates a random password for the user's BlackBerry device and locks the device immediately. The user cannot access the device's software, email, or make outgoing phone calls until the password is reset using the Enable action. The user can still answer incoming phone calls.
- The activation password expiration time is limited by the BlackBerry Enterprise server to be between 1 and 720 hours. The default value is 48 hours.
- The activation password expiration time may not be changed without specifying a new activation password.
- When using the Enable action, ensure that any password entered meets the minimum password strength requirements of the ITPolicy that governs the user's BlackBerry device.

Because the API provided by the Blackberry Server returns no indication of an error when a password fails to meet the password strength requirements, workflows cannot report password-strength failures to the end user. When this occurs, the end user cannot use the Blackberry device following a successful Enable action. To prevent this occurrence, assure that the Core Security workflow includes password-strength rules that meet the Blackberry Server password-strength requirements.

- The Disable action has an optional Boolean attribute called "DisableBlackBerryUser." When set to "true," the BlackBerry user account becomes disassociated with its Microsoft Exchange mailbox when it is disabled. As a result, you can no longer specify the user's email address to access the Blackberry user account.

When a user is disabled in this manner, delete the user's BlackBerry account information from the IdentityMap. You can do this through periodic maintenance, or by configuring the workflow to either perform the deletion in a Trigger or to send a notification to an administrator requesting the deletion. This prevents future workflow errors that would result from passing an unknown email address to the BlackBerry server.

Chapter 55: RSA Access Manager — PMM

This chapter explains how to configure the PMM for RSA Access Manager:

- [*“Configuring the PMM for RSA Access Manager” on page 514*](#)

Configuring the PMM for RSA Access Manager

The Password Management Module (PMM) for RSA Access Manager is built using Core Security's RDK technology to automate the password reset for RSA Access Manager accounts by using the native Java packages shipped with Access Manager.

This PMM supports Anonymous SSL connections to the Access Manager server. It does not support Clear connections and has no support for Authenticated SSL connections.

Prerequisites

To configure the PMM, you need values for the following parameters on the target system:

- ServerName
- ServerPort
- SSLMode
- AdminUserName
- AdminPassword
- Group
- Role

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. See [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

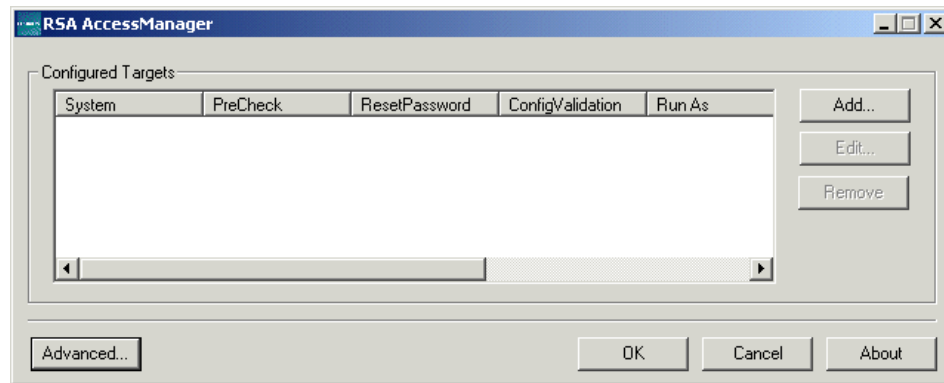
Note: *ExtensionPMM4RSAct.log* is the debug log file name for this PMM.

Installation

Take the `ct_admin_api.jar` file from the Access Manager server (in the `\lib` directory) and copy it to the `CourionService\ctreset` directory. Obtain the jar file from the actual server you intend to perform resets against due to compatibility and version issues.

PMM Configuration

1. From the Start menu, select:
Programs> Core Access Assurance Suite>Password Management Modules>RSA Access Manager
The Configuration Manager displays the Add Target dialog box. This dialog box shows any previously configured targets.

Figure 265: Add Target Dialog Box

2. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 266: The Add/Edit Target Configuration Dialog Box for RSA Access Manager

Add / Edit Target Configuration

Target Name:

PreCheck Command Line:

ResetPasswordEx Command Line:

ConfigValidation Command Line:

☐ Run Commands as User

Domain\User:

User Password:

Configure Parameters for System

Parameter:

Value:

Verify Value:

☒ Secure Attribute

Configured Parameters:	
Name	Value

- Enter values for the following parameters:

TARGET NAME — Enter the name of the target where you want to perform the password resets. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

COMMAND LINES — Enter the same location for all three command lines: PreCheck Command Line, ResetPassword Command Line, and ConfigValidation Command Line. If you installed AAS in the default location, the command line to specify is:

```
java -cp "c:\program files (x86)\courion
corporation\courionservice\ctReset;c:\program files (x86)\courion
corporation\courionservice\ctReset\ct_admin_api.jar" ExtensionPMM4RSACT
```

RUN COMMANDS AS USER — Leave this box unchecked.

CONFIGURE PARAMETERS FOR SYSTEM — Enter in the Configuration Parameters as shown in Table 28. Enter the parameter name in the Parameter text box, then enter the appropriate value in the Value text box. If the Secure Attribute checkbox is selected, you must enter the value in both the Value and Verify text boxes. Click Add to move the entry to the list on the right side.

All parameters are required. Do not use quotes when entering these parameters.

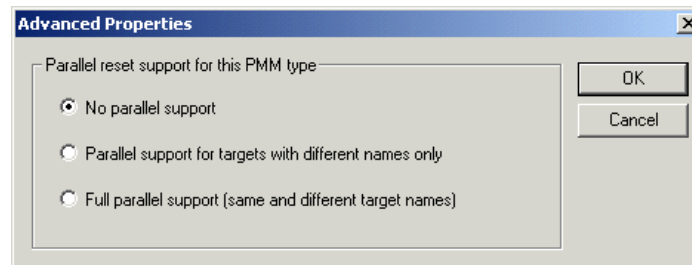
Table 28: System Parameters

Parameter Name (parameters are case-sensitive)	Value	Check as Secure?
ServerName	The hostname of the Access Manager server	No
ServerPort	The port number of the Access Manager server.	No
SSLMode	The mode of SSL communication to the Access Manager server. Enter Anon (case-sensitive).	No
AdminUserName	The username of the administrative user you want the PMM for RSA Access Manager to log in as, to perform password resets.	No
AdminPassword	The Access Manager password for the administrative user. Mark this field as secure.	Yes
Group	The Access Manager Administrative group. Usually, this is Default Administrative Group.	No
Role	The Access Manager Administrative role. Usually, this is Default Administrative Role.	No

Click OK when you have entered values for all parameters.

4. Select the target you have just configured from the Add Target Dialog box, and click the **ADVANCED** button. The Advanced Properties dialog box appears.

Figure 267: Advanced Properties Dialog Box



5. Select the **NO PARALLEL SUPPORT** (the default) option. Click **OK**.
6. From the Add Target dialog box, click **OK**.

Chapter 56: RSA Authentication Manager — PMM and Connector

Please contact Customer Support to get the newer PMM and connector used to integrate to RSA Authentication Manager version 8.1.

This chapter explains how to configure the PMM and Connector for RSA Authentication Manager:

- [*“Configuring the PMM for RSA Authentication Manager” on page 520*](#)
- [*“Configuring the Connector for RSA Authentication Manager” on page 525*](#)
- [*“Obtaining the Command Client User Name and Password” on page 529*](#)
- [*“Obtaining the rsaws.dll File” on page 530*](#)

Configuring the PMM for RSA Authentication Manager

The Password Management Module (PMM) for RSA Authentication Manager is built using Core Security's RDK technology to automate the password reset for RSA Authentication Manager's user accounts and tokens by integrating with the product's C# API.

The PMM resets both the user and token resources on the target system. The identifier that is used in the IdentityMap™ for the user resource is the Login UID. For the token resource, the identifier is the Token Serial Number.

Prerequisites

To configure the PMM, you need values for the following parameters on the target system:

- RSAServerURL
- CommandUser (See [“Obtaining the Command Client User Name and Password” on page 529](#) to obtain this value.)
- CommandUserPwd (See [“Obtaining the Command Client User Name and Password” on page 529](#) to obtain this value.)
- PrivilegedUser (must have SuperAdminRole assigned to it)
- PrivilegedUserPwd
- RealmName
- IdentitySource
- WeakValidation
- ForceChangeMode
- ResourceType
- ScriptName

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. See [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

You need to copy the rsaws.dll file from the RSA Authentication Manager server to the connector framework or the connector framework manager. See [“Obtaining the rsaws.dll File” on page 530](#) for information on how to do this.

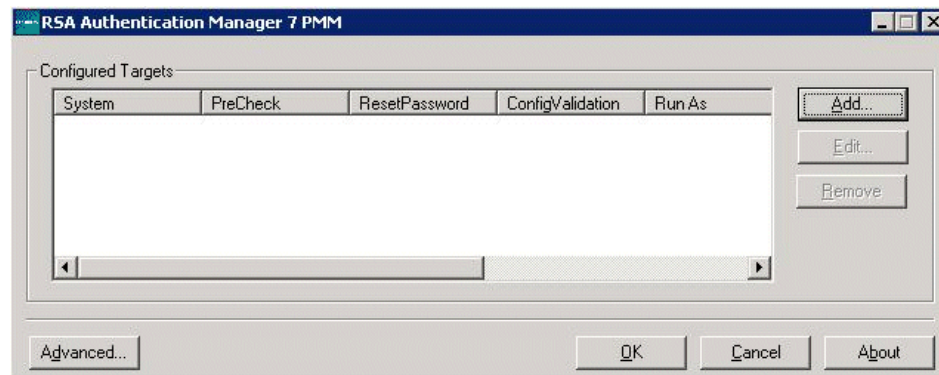
PMM Configuration

To configure the PMM:

1. From the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>RSA Authentication Manager

The Configuration Manager displays the Add Target dialog box. This dialog box shows any previously configured targets.

Figure 268: PMM Configuration Manager for RSA Authentication Manager 7



2. From this dialog box, you can:
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - Obtain the product version number. Click the **ABOUT** button.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 269: Add/Edit Target Configuration for RSA Authentication Manager

3. **TARGET NAME** — Enter the name of the target where you want to perform the password resets. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

COMMAND LINES — Enter the same location for all three command lines: PreCheck Command Line, ResetPassword Command Line, and ConfigValidation Command Line. The command line for the standard location is:

```
cscript /nologo /b PMMRDK2AMMRDKRedirect.js
```

RUN COMMANDS AS USER — Leave this box unchecked.

CONFIGURE PARAMETERS FOR SYSTEM — Enter in the PMM Configuration Parameters as shown in Table 29. Enter the parameter name in the Parameter text box, then enter the appropriate value in the Value text box. If the Secure Attribute checkbox is selected, you must enter the value in both the Value and Verify text boxes. Click Add to move the entry to the list on the right side. Do not use quotes when entering these parameters.

Table 29: PMM Configuration Parameters

Parameter Name (parameters are case sensitive)	Value	Check as Secure?
RSASERVERURL	RSA service command server URL. For example: https://rsaam:7002/ims-ws/services/CommandServer	No

Table 29: PMM Configuration Parameters

Parameter Name (parameters are case sensitive)	Value	Check as Secure?
COMMANDUSER (See “Obtaining the Command Client User Name and Password” on page 529 to obtain this value.)	Command Client account to access command server.	No
COMMANDUSERPWD (See “Obtaining the Command Client User Name and Password” on page 529 to obtain this value.)	Command Client account password.	Yes
PRIVILEGEDUSER	Privileged account used to provision. Must have SuperAdminRole assigned to it.	No
PRIVILEGEDUSERPWD	Privileged account password	Yes
REALMNAME	Administrative realm name.	No
IDENTITYSOURCE	Identity Source associated with the realm. Example: Internal Database	No
WEAKVALIDATION (optional)	True (the default) <i>or</i> False When set to False, you need to install an RSA Authentication Manager certificate on the Core Server. Note: If using HTTPS in the RSAServerURL and using the RSA Authentication Manager certificate on the Core Server, set this to True.	No
FORCECHANGEMODE (optional)	True <i>or</i> False (the default) When set to True, it forces users to change their PIN when logging in after the PIN for the user reset.	No
RESOURCE TYPE	Principal (user accounts) <i>or</i> Token	No
SCRIPTNAME	RSAAuthMgr71Cnctr.js	No

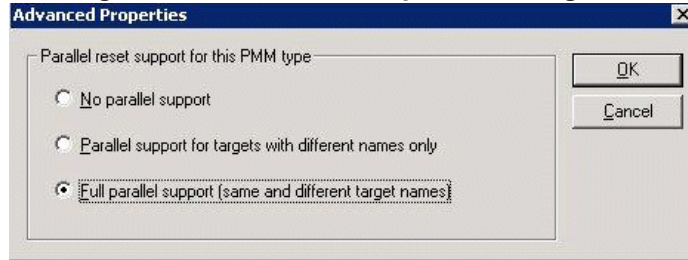
Click **OK** when you have entered values for all parameters and checked them as secure or not.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value.

4. Select the target you have just configured from the Add Target Dialog box, and click the **ADVANCED** button. The Advanced Properties dialog box appears.

Figure 270: Advanced Properties Dialog Box



5. Select the **FULL PARALLEL SUPPORT (SAME AND DIFFERENT TARGET NAMES)** (the default) option. Click **OK**.
6. From the Add target dialog box, click **OK**.

Notes and Warnings

Account names are not case sensitive within the RSA Authentication Manager. However, the target preserves the case when displaying a list of accounts. Case must be preserved in the IdentityMap.

If the password policy "Minimum Lifetime" in the RSA Security Console is set to a value that is easily violated the user may see the error, "Password policy not satisfied", when trying to reset their password. For example, if this is set to 1 day and the user tries to reset their password twice in one day, they see this error with the generic message of "Password policy not satisfied."

Password Reset actions are only supported for users from the Internal Database identity source.

Configuring the Connector for RSA Authentication Manager

The Connector for RSA Authentication Manager is built using Core Security's RDK technology to automate provisioning of RSA Authentication Manager's user accounts and tokens by integrating with the product's C# API. This connector supports the Account ID Generation engine capability to check if the proposed account name already exists in the target for user accounts.

The Connector for RSA Authentication Manager supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, View, Authentication, and Query.

Prerequisites

Parameters

To configure the connector, you need values for the following parameters on the target system:

- RSAServerURL
- CommandUser (See [“Obtaining the Command Client User Name and Password” on page 529](#) to obtain this value.)
- CommandUserPwd — (See [“Obtaining the Command Client User Name and Password” on page 529](#) to obtain this value.)
- PrivilegedUser (must have SuperAdminRole assigned to it)
- PrivilegedUserPwd
- RealmName
- IdentitySource
- EmergencyAccessMode
- WeakValidation
- ExpirationTimerInHours
- NumberOfOneTimePins

Copying the rsaws.dll file

You need to copy the rsaws.dll file from the RSA Authentication Manager server to the connector framework or the connector framework manager. See [“Obtaining the rsaws.dll File” on page 530](#) for information on how to do this.

Connector Configuration

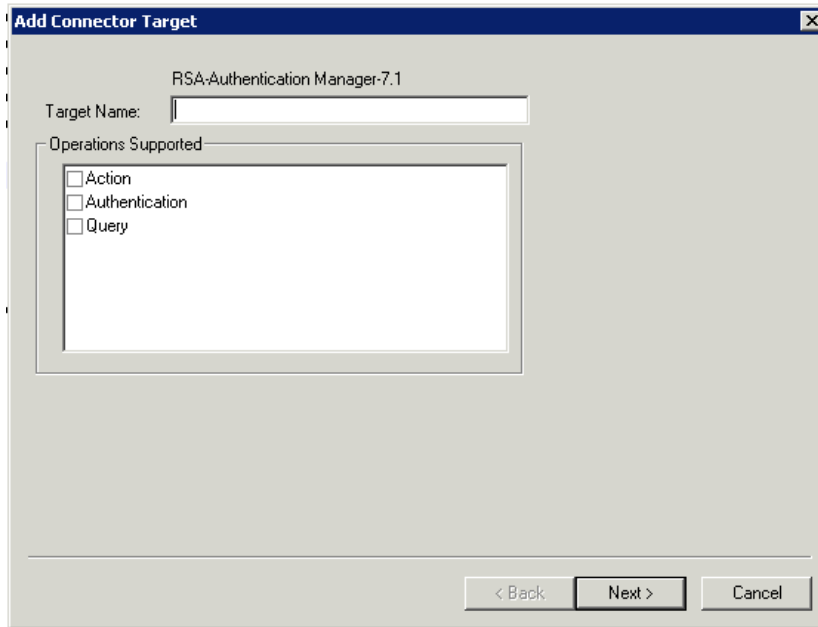
Follow these steps to add a target:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager

2. Choose **File>ADD CONNECTOR**, select **RSA-AUTHENTICATION MANAGER-71**, and click **OK**
3. Select **RSA-AUTHENTICATION MANAGER-71**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears, as in [Figure 271](#).

Figure 271: Add RSA Authentication Manager Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**. The target configuration dialog box appears as in [Figure 272](#).

Select **ACTION** to enable these provisioning actions: Add, Change, Create, Enable, Delete, Disable, Verify, and View.

Select **AUTHENTICATION** to use the target data source for Resource Claiming.

Select **QUERY** to enable the use of queries for Resource Claiming.

Figure 272: Connector Configuration Manager for RSA Authentication Manager

6. The drop-down list, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button. Values always appear as asterisks (“**”) for security.

Note: You can add only one parameter name/value combination at a time, but you can select multiple items together and remove them from the list of configured name/value pairs at the same time.

Note: Adding a value for the same parameter a second time overwrites the previous value. Table 30 lists the connector Configuration Parameters for the connector. Do not use quotes when entering these parameters.

Table 30: Connector Configuration Parameters

Parameter Name (parameters are case sensitive)	Value
RSASERVERURL	RSA service command server URL. For example: https://rsaam:7002/ims-ws/services/CommandServer
COMMANDUSER (See “Obtaining the Command Client User Name and Password” on page 529 to obtain this value.)	Command Client account to access command server.
COMMANDUSERPWD (See “Obtaining the Command Client User Name and Password” on page 529 to obtain this value.)	Command Client account password.

Table 30: Connector Configuration Parameters

Parameter Name (parameters are case sensitive)	Value
PRIVILEGEDUSER	Privileged account used to provision. Must have SuperAdminRole assigned to it.
PRIVILEGEDUSERPWD	Privileged Account Password
REALMNAME	Administrative realm name.
IDENTITYSOURCE	Identity Source associated with the realm. Example: Internal Database
EMERGENCYACCESSMODE (optional)	True <i>or</i> False (default) When set to true, this enables emergency access code generation.
WEAKVALIDATION (optional)	True (the default) <i>or</i> False When set to False, you need to install an RSA Authentication Manager certificate on the Core Server.
EXPIRATIONTIMERINHOURS (optional)	Number of hours a temporary passcode or one-time-use passcode lasts before it expires.
NUMBEROFONETIMEPINS (optional)	Number of one-time-use passcodes to generate. When this parameter is set to 0 or not specified, a temporary fixed passcode is generated.

- Click **FINISH** when you have entered values for all parameters.

Notes and Warnings

Create actions are only supported for users from the Internal Database identity source.

Obtaining the Command Client User Name and Password

When you install the RSA Authentication Manager, the system creates a command client user name and password for secure connections to the command server. The user name and password are randomly generated on creation, and are unique to each deployment.

You need to set command client and user name values for each connection to the command server. Use the Manage Secrets utility to obtain these values from the RSA Authentication Manager.

To obtain the command client user name and password from the RSA Authentication Manager:

1. From a command prompt on the RSA Authentication Manager host, change directories to RSA_AM_HOME/Utils.
2. Enter the following command:

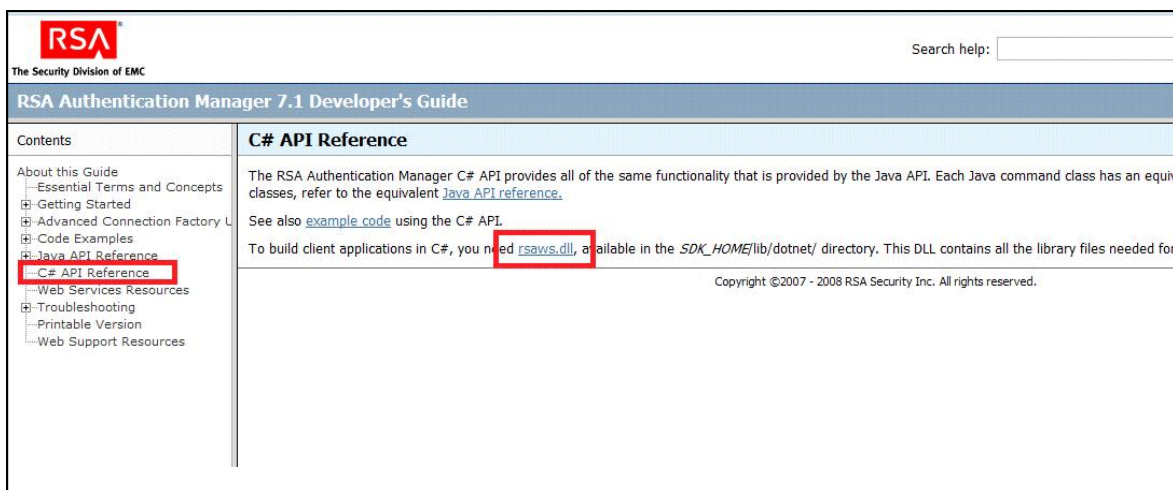
```
rsautil manage-secrets --action list
```
3. When prompted, type in your master password. The system displays the list of your internal system passwords.
4. Locate the values for your command client user name and password. For example:
Command Client User Name: CmdClient_vKr9aLK9
Command Client User Password: e9SHbK0W4i

Obtaining the rsaws.dll File

To obtain the rsaws.dll file, follow these steps:

1. Browse to the SDK folder on the RSA Authentication Manager full installation media.
2. Go to the following folder: docs\guide\
3. Open this file in Internet Explorer:
auth_manager_developer_guide.html
4. Click on **C# API REFERENCE** in the left panel as highlighted in [Figure 273](#).

Figure 273: C# API Reference Guide



5. Click on **RSAWS.DLL** as highlighted in [Figure 273](#) to save it on the Connector Framework and the Connector Framework Manager server.
6. Copy this file into the CourierService directory.

Chapter 57: RSA SecurID — PMM and Connector

This chapter explains how to configure the PMM and Connector for RSA SecurID. The PMM and connector require the RSA SecurID agent, also explained in this chapter: RSA re-branded SecurID to RSA Authentication Manager, so please check that chapter if looking for RSA Authentication Manager.

- [*“Configuring the PMM for RSA SecurID” on page 532*](#)
- [*“Configuring the Connector for RSA SecurID” on page 538*](#)
- [*“Installing and Configuring the Agent on a UNIX System” on page 540*](#)
- [*“Installing and Configuring the Agent on a Windows System” on page 544*](#)

Configuring the PMM for RSA SecurID

The Password Management Module (PMM) for RSA SecurID enables PasswordCourier and PasswordCourier Support Staff to:

- Automatically reset RSA SecurID PINs
- Allow an end user to request to have the SecurID token re-synchronized with the ACE/Server (ACE/Server 5.1 and later)
- Allow an end user to request to have emergency access codes generated for use while that user's token is lost (ACE/Server 5.1 and later)

The PMM for RSA SecurID can reset PINs for the following RSA SecurID tokens:

- RSA SecurID Software Token (formerly SoftID®)
- RSA SecurID Standard Card
- RSA SecurID Key Fob
- RSA SecurID PinPad Card

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Server.

Prerequisites

An agent for RSA SecurID must be installed on the same machine(s) as the ACE/Server®. The agent must be installed and configured before you install and configure the PMM. For a UNIX system, see [“Installing and Configuring the Agent on a UNIX System” on page 540](#). For a Windows systems, see [“Installing and Configuring the Agent on a Windows System” on page 544](#).

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

You cannot use targets configured with the token re-synchronization action or the generate emergency one-time passcode(s) action with the Core Security Telephone Access option or the Transparent Synchronization feature.

Core Security recommends that you do not include targets configured to use RSA SecurID token management capabilities (token re-synchronization and emergency one-time access codes) in the same workflow with targets configured to automatically reset RSA SecurID PINs. The token management capabilities do not function well when sharing a password management workflow configuration.

PMM Configuration

The PMM configuration manager lets you create privileged user accounts that can establish a connection to the PMM for RSA SecurID Agent on the system hosting the RSA ACE/Server. The specified users must be valid local users or have a valid domain account in the domain in which the RSA ACE/Server is installed.

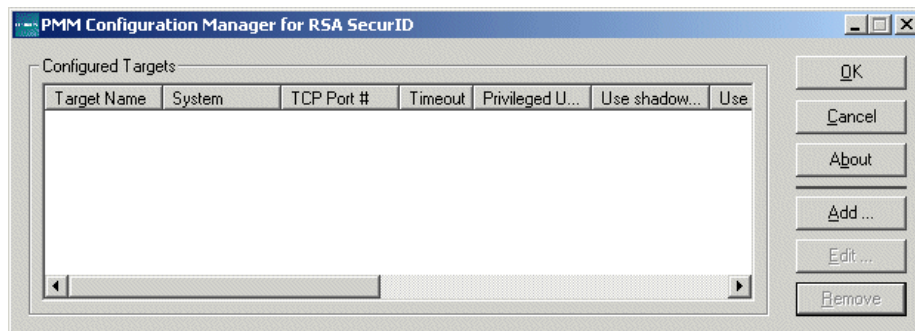
Additionally, by checking the **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** check box ([Figure 275](#)), you can specify one configuration as the default configuration for all servers not explicitly configured.

Note: Before configuring the PMM for RSA SecurID, copy the file `apideamon.exe` from the RSA SecurID server to the CourionService folder.

1. From the Start Menu, select:
Programs>Core Access Assurance Suite>Password Management Modules>RSA SecurID
2. Click **YES** when prompted to begin the configuration.

The PMM Configuration Manager for RSA SecurID appears.

Figure 274: PMM Configuration Manager for RSA SecurID



3. From this dialog box, you can:
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 275: Add/Edit RSA SecurID System PMM Configuration

Here, the **GENERATE EMERGENCY ONE-TIME PASSCODE(S)** action is selected. If this option is not available, the **GENERATE** section is grayed out.

4. TARGET PROPERTIES

- a. **NAME** — Enter the name of the target on the ACE/Server. You cannot edit the name of an existing target. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

- b. **ACTION** — Select an action to associate with this target:

RESET PERSONAL IDENTIFICATION NUMBER (PIN) — This action allows an end user automatically to reset RSA SecurID PINs. This is the default.

TOKEN RE-SYNCHRONIZATION — This action allows an end user to request to have the SecurID token re-synchronized with the ACE/Server.

GENERATE EMERGENCY ONE-TIME PASSCODE(S) — This action allows an end user to request to have emergency access codes generated for use while that user's token is lost.

EMERGENCY ONE-TIME PASSCODE PROPERTIES — If you selected this in the Target properties section, complete this section.

NUMBER OF PASSCODES TO GENERATE — Enter a value from 1–50. Default is 2.

PASSCODE LENGTH — This value specifies the number of characters required in the passcode. Enter a value from 4–8. The default is 6.

HOURS UNTIL EXPIRATION — This value indicates the number of hours that the newly generated passcode is valid. Enter a value from 1–210, 240 (24 years). The default is 24.

CHARACTERS TO INCLUDE — Select the types of characters you want to allow in the passcode returned from the ACE/Server. The selections you make indicate your request for the passcodes; the actual composition of the passcodes that the ACE/Server returns depends on its configuration.

5. ACE/SERVER PROPERTIES

- a. **CS TYPE** — Select the operating system where the RSA ACE/Server is installed from the drop-down menu. The options are Solaris/AIX/HP-UX or Windows NT/2000.
- b. **HOST** — Specify the RSA ACE/Server Host where RSA SecurID PIN resets are to be performed.
- c. **TCP PORT** — Specify the TCP port on which the RSA SecurID agent is listening.
- d. **TIMEOUT** — Specify the time out if it is different from the default (10 seconds).

6. PRIVILEGED USER INFORMATION

- a. **PRIVILEGED USERNAME** — The username must be in the form `domain\username` when the target system (agent) is configured on a Microsoft Windows-based system. The username must match the validation user specified in the agent configuration. If a domain is not provided, the PMM for RSA SecurID configuration program looks at the specified ACE/Server host system and see if this user has an account on that system. It is also possible to specify a local account using the form `\\machinename\username`.

The privileged user requires no special privileges. The account is only used to activate the password reset executed by the agent software.
- b. **PASSWORD** — Specify the password for the user.
- c. **USE SHADOW PASSWORD FILE** — Specify whether or not the UNIX server uses a shadow password file for the local user authentication if the SecurID agent runs on UNIX systems.
- d. **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** — Determine if this user is to be the default user for unconfigured systems.

7. Click the **OK** button.

PMM configuration for one target is now complete.

If you specified Token Re-Synchronization or Generate Emergency One-Time Passcodes, see the appropriate section under [“Configuring Targets Using the Token Re-Synchronization Action” on page 536](#) or [“Configuring Targets using the Generate Emergency One-Time Passcodes Action” on page 536](#).

For information on defining a PIN target, please see [“TARGET PROPERTIES” on page 534](#).

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Note: The SecurID "Username" is the user's SecurID token serial number and not the login username. In addition, the serial number is the full serial number as it exists in the ACE/Server or Authentication Manager Server (for example, 000012345678) and not the serial number as is printed on the back of the token (for example, 12345678).

Notes and Warnings

If the Core Access Assurance Suite and this PMM are installed and configured on the same machine and then the Core Access Assurance Suite is uninstalled, you need to rerun the agent install and select the **REPAIR** option.

Configuring Targets Using the Token Re-Synchronization Action

Complete the following steps if you configured a target for the PMM for RSA SecurID with the token re-synchronization action to ensure optimal performance.

- If you specify a target that matches the name of the PMM for RSA SecurID target that is configured to use the token re-synchronization action, change the file `password.asp` to display only one input field. The configured label/prompt and help text should provide direction for entering input into this field. Consider making the input box wider to display all user input. Also, do not make the `<input type="password">`, as end users need to see the values they are entering.
- Set the password strength/composition settings for the token re-synchronization target in the PasswordCourier or PasswordCourier Support Staff customization manager on the classic platform or the Administration Manager on the provisioning platform to two times the passcode length for the minimum and the maximum length. This length entered is checked and the end user is given additional tries to enter the proper number of characters that are equivalent to two different passcodes.
- Depending on how long it takes for a new passcode to appear, you may need to increase the Web Access Configuration timeout and/or the IIS ASP timeout to allow the end user enough time to view and enter the needed passcodes.
- After selecting the target for token resynchronization, the end user is prompted to wait until the token code changes values, enter the current value into the input field, wait for the token code to change again, and enter the new current value. Core Security recommends that you include information describing this process in the help text for the form.

Configuring Targets using the Generate Emergency One-Time Passcodes Action

Note: This feature is available on the Core Password and PasswordCourier Support Staff Classic Platform only.

The following macro is available only to support the Generate emergency one-time passcodes action: `%PWD_SUCCESS_WITH_INFO%`

This macro is not exposed in the customization manager. Use this macro in the Success message for the target configured to use the Generate emergency one-time passcode(s) action.

Note: No other PMM target or any email or ticket should use this macro, since it is not meaningful for any other PMM or any other action other than the Generate emergency one-time passcode(s) action in the PMM for RSA SecurID.

Complete the following steps if you have configured a target for the PMM for RSA SecurID with the Generate emergency one-time passcode(s) action to ensure optimal performance.

- When you configure a PMM for RSA SecurID target in the PasswordCourier or PasswordCourier Support Staff customization manager that is configured with this action, set the "use escrow password" feature in the Advanced properties (button) in the Add/Edit target dialog box. This prevents the end user page from displaying the input fields for the password, as that input is not needed for this action.
- The Success message for the target configured with this action should include the new macro %PWD_SUCCESS_WITH_INFO% so that the message can display the emergency access codes that were generated.

Configuring the Connector for RSA SecurID

The Connector for RSA SecurID supports the following actions a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Prerequisites

You must install the agent for RSA SecurID on the same machine(s) as the ACE/Server. Install and configure the agent before you install and configure the connector. See [“Installing and Configuring the Agent on a UNIX System” on page 540](#) or [“Installing and Configuring the Agent on a Windows System” on page 544](#).

Note: If you are currently running the PMM for RSA SecurID and you install the Connector for RSA SecurID, you must reconfigure the PMM.

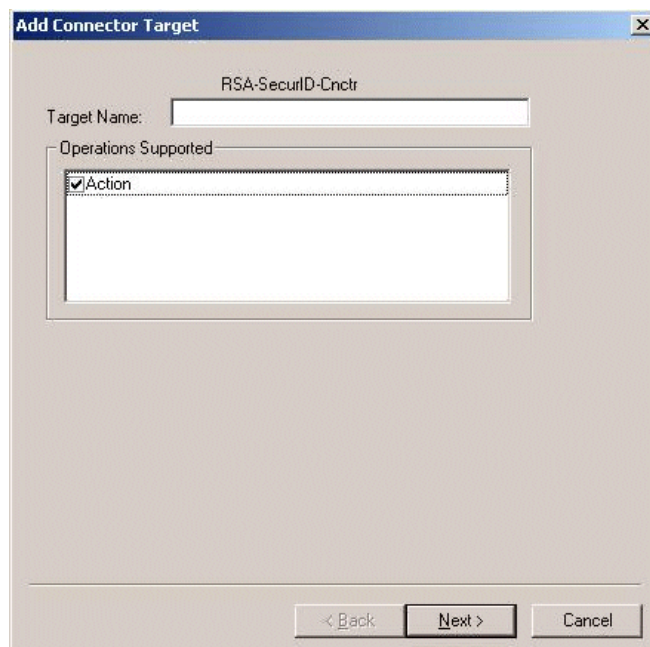
Connector Configuration

Follow these steps to add a target:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose File>**ADD CONNECTOR**, select **RSA-SECURID-CNCTR**, and click **OK**
3. Select **RSA-SECURID-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears, as in [Figure 276](#).

Figure 276: Add RSA SecurID Target



5. Enter a name (alias) for the target in the **TARGET NAME** text box and click **NEXT**. The target configuration dialog box appears as in

Figure 277: Connector Configuration Manager for RSA SecurID

6. **ACE/SERVER OPERATING SYSTEM** — Select the operating system where the RSA ACE/Server is installed from the drop-down menu. The available values are Windows and AIX/HPUX/Solaris.
7. **AGENT HOST** - Specify the RSA ACE/Server Host for provisioning actions.
8. **AGENT PORT** — Specify the TCP port on which the RSA SecurID agent is listening.
9. **TIMEOUT** — Specify the time out if it is different from the default (10 seconds).
10. **PRIVILEGED USER** — Use the format domain\username when the target system (agent) is configured on Windows NT or Windows 2000. The username must match the validation user specified in the agent configuration. If a domain is not provided, the Connector for RSA SecurID configuration program looks at the specified ACE/Server host system to determine if this user has an account on that system. It is also possible to specify a local account using the form:

`\\machinename\username`
 The privileged user requires no special privileges. The account is only used to activate the actions executed by the agent software.
11. **PASSWORD** — Specify the password for the privileged user.
12. Click **FINISH**.

Note: Adding, modifying, or removing a target at the time the Courion Server is configured requires stopping and restarting the Courion Server. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if the Courion Server should be restarted.

13. Select **YES** to implement the new selections.

The target is now available for each action supported by the connector

Installing and Configuring the Agent on a UNIX System

The following information is required to configure the PMM agent:

- The hostname of the ACE/Server where the PMM for RSA SecurID agent is being installed.
- Whether the UNIX machine on which the ACE/Server is installed uses a shadow password file to authenticate end users.
- A configured user name/password pair that Core Server may use to authenticate itself to each ACE/Server.

Installing the Agent on a UNIX System

1. Locate the SecurID folder in the Core Server folder on the local host (`local host/Program Files (x86)/Core Server/SecurID`).
2. Open the folder and select the appropriate `.tar` file.
3. Copy the `.tar` file to a temporary directory on the UNIX machine where the agent is being installed.
4. Log on to the UNIX machine as a superuser and proceed to the directory where the file was placed. Extract the installation files using one of the following commands:

For a RSA ACE/Server version 4.1:

```
tar-xvf Securidxxx41.tar
```

For a RSA ACE/Server version 5.1:

```
tar-xvf Securidxxx51.tar
```

where `xxx` is `sol` for an ACE/Server running Solaris UNIX, `aix` for an ACE/Server running AIX, or `hp` for an ACE/Server running HP-UX.

Extracting the files creates a subdirectory named `SecurID41` or `SecurID51` that holds the install files.

5. Change to the directory `SecurID41` or `SecurID51` and execute the installation script by typing `./install`. The system prompts:

```
Please enter the ACE/Server directory (i.e.
/usr/local/ACEServ)
```

6. Specify the directory name; this must already exist. The system prompts:

```
Enter the directory you wish to install the daemon in
(/usr/local/CourSecurID).
```

7. Specify the directory name. If the directory does not exist, the system creates it. The system prompts:

```
Enter your password file (/etc/passwd)
```

8. Specify the password directory name. The system prompts:

```
Enter path to make (/usr/bin)
```

9. Specify the directory where the `make` command resides. The system prompts:

Enter TCP port for daemon to listen on (8192)

10. Specify the TCP port. The system prompts:

Do you want to allow resetting the SecurID PIN on disabled Tokens? (y/n, y)

Specify `y` or `n`. The following text provides background for this.

- In the system startup script, add the name of the SecurID agent startup script:
For AIX: `/etc/pwdcour_SecurIDpxy start`
For HP-UX: `/sbin/rc3.d/S99pwdcour_SecurIDpxy start`
For Solaris: `/etc/rc3.d/S99pwdcour_SecurIDpxy start`

Continue to the section below [*“Configuring the Agent on a UNIX System”*](#)

Allowing Resets of Disabled Tokens

A SecurID token may be in a disabled state because:

- The RSA ACE/Server administrator manually disabled the token to block the end user from entering the system.
- The token was disabled because the end user failed multiple times to log into the system.

Resetting a PIN on a disabled token reenables the token regardless of the action that disabled it. If you do not allow resetting the PINs on disabled tokens, end users who accidentally lock themselves out must contact the Help Desk to reenables their tokens.

If you allow reset of RSA SecurID PINs on disabled tokens, then the PMM for RSA SecurID always allows end users to reset their SecurID PINs. To prevent end users from resetting their SecurID PINs on manually disabled tokens (administratively locked out tokens), set the token to both the “Disabled” and the “Lost” status.

Configuring the Agent on a UNIX System

Installing the PMM for RSA SecurID Agent also installs the configuration file `SecurIDpxy_def` in the agent's installation directory (default `/usr/local/CourSecurID`). The configuration file has several parameters that control agent operation. You can use a text editor, such as `vi`, to change the `SecurIDpxy_def` file. Table 31 provides the configuration information the RSA SecurID agent requires.

Before beginning the configuration process on a UNIX system, add `root` to the list of ACE/Server database administrators. This step is necessary because the PMM for RSA SecurID agent runs as `root` by default.

Table 31: PMM Agent Configuration Information, RSA SecurID on UNIX Systems Core Server

Parameter	Syntax	Description
ALLOW_RESET_DISABLED	y/n	Decide whether or not to reset the PIN on disabled tokens. The valid values are Y (reset disabled tokens) and N (do not reset disabled tokens). For details, see “Allowing Resets of Disabled Tokens” on page 541
INST_DIR	install_dir	This directory is where the PMM is installed. By default, the agent is installed in <code>/usr/local/CourSecurID</code> .
LOG_FILE	log_file	This is the name of the file where the PMM logs all messages. If it does not already exist, the <code>log_file</code> is automatically created. If you omit a path, the file is created in the directory specified by <code>INST_DIR</code> . If you omit this parameter, the default is <code>SecurIDpxy.log</code> .
LOG_LEVEL	<i>n</i>	Log messages have a log level <i>n</i> associated with them. The log level ranges from 0-2. Depending on the log level you specify in the <code>SecurIDpxy_def</code> file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the <code>SecurIDpxy_def</code> file. By default, the log level is 0.
MAKE_DIR:make_directory	make_dir	This is the directory in which the make command can be found. It is used to rebuild the NIS password map. If the directory is omitted, the default is <code>/var/yp</code> .
PASSWORD_FILE	passwd_file	This is the fully qualified filename of the passwd file that a Core Server end user is validated against. If it is omitted, the default is <code>/etc/passwd</code> .
PWD_ERR_MSG	err_msg	This is a custom error message displayed to the end user when an error occurs during a PIN reset. If this message is omitted a technical error description is displayed.
SHDW_FILE	shadow_file	This is the fully qualified filename of the shadow password file against which a Core Server end user is validated. If the filename is omitted the default is <code>/etc/shadow</code> .
SVR_NAME	server	This is the name of the server where the agent is installed. There is no default value. This value must be valid.
SVR_PORT	port_number	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value. This value must be valid.
VALIDATION_USER	username	You must add this manually if the privileged username is not <code>root</code> ; for <code>root</code> , you can omit it. The username must match the username configured for this server on the machine running on the Connector Framework Manager. Note: The privileged user requires no special privileges. The account is used only to authenticate the password reset request that the agent software tries to execute.

To apply any changes to the configuration, stop and then start the agent as described next.

Starting and Stopping the Agent on a UNIX System

Should it become necessary to start the agent, run the startup script with the argument `start`. To stop the agent, run the script with the argument `stop`. The commands are

- For AIX:
To start: `/etc/pwdcour_SecurIDpxy start`
To stop: `/etc/pwdcour_SecurIDpxy stop`
- For HP-UX:
To start: `/sbin/rc3.d/S99pwdcour_SecurIDpxy start`
To stop: `/sbin/rc3.d/S99pwdcour_SecurIDpxy stop`
- For Solaris:
To start: `/etc/rc3.d/S99pwdcour_SecurIDpxy start`
To stop: `/etc/rc3.d/S99pwdcour_SecurIDpxy stop`

Uninstalling the Agent for Upgrading on a UNIX System

To upgrade the agent for the PMM for RSA SecurID, you need to uninstall the previous agent and then install the new agent. You must know the install directory path (default `/usr/local/CourSecurID`). The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

Note: Before beginning the uninstall process, back up the `installdir/SecurIDpxy_def` to another directory, where `installdir` is the installation directory, typically `/usr/local/CourSecurID`.

1. To uninstall the PMM for RSA SecurID agent, execute the uninstall script by typing `installdir/uninstall`.
2. Follow the prompts and answer the questions.
3. After extracting the distribution files for the new PMM for RSA SecurID agent, install the new agent by following the steps under [“Installing the Agent on a UNIX System” on page 540](#) or [“Installing the Agent on a Windows System” on page 544](#).
4. Merge custom entries from your backed up `SecurIDpxy_def` file into the new `installdir/SecurIDpxy_def` file.
5. Restore the backup reset script to the desired directory. Make sure the new `SecurIDpxy_def` file refers to that script.

Installing and Configuring the Agent on a Windows System

Installing the Agent on a Windows System

Note: To install the agent, you must be a member of the local administrator group.

Note: The agent can only connect to the RSA ACE/Server if it runs as the administrator.

The ACE/Server administrator username and password is required information. The administrator must be a user with administrative rights on the ACE/Server.

Make sure the RSA ACE/Server username being used granted the user right **LOG ON AS SERVICE**. If the user does not have the needed rights, an error is returned during the installation. The username must be in the form of *domain\user* name. If a domain is not provided, it is assumed that this user is a local user.

1. Locate the SecurID folder in the Core Server folder on the local host (local host/Program Files (x86)/Core Server/SecurID).
2. Open the folder and select the `SecurIDInstall.exe` file.
3. Copy the `SecurIDInstall.exe` file to a temporary directory on the Microsoft Windows-based system where the agent is being installed.
4. Log on to the machine as a privileged user and proceed to the directory where the `.exe` file was placed. Double click on the `SecurIDInstall.exe` to begin the InstallShield Wizard.
5. Follow the Wizard's instructions.

After you install the SecurID agent on a Windows 2000 system running ACE/Server 4.1 where the validation user matches the user name on the ACE/Server, you might receive an error message that states that the agent was not able to contact the PMM. If this error occurs, make sure that all services are running properly. If they are, then cancel out and run the configuration again.

Configuring the Agent on a Windows System

After you install the agent, the Installshield launches the agent service configuration for SecurID. Table 32 provides the configuration information that the RSA SecurID agent uses.

Table 32: Agent Configuration Information for RSA SecurID on Windows

Fields	Description
SecurIDpxyPort	This is the port number that the RSA SecurID agent service is listening to. If the number is omitted, the default value is 8192.

Table 32: Agent Configuration Information for RSA SecurID on Windows

Fields	Description
ValidationUser	This is the account used to authenticate the user performing the reset from the server to the agent on the ACE/Server. This user name must match the privileged user on the Windows system running the PMM or connector for RSA SecurID. The format must be <code>username</code>, not <code>domain\username</code>. If the user name is omitted, the default value is Admin. Note: The privileged user requires no special privileges. The account is used only to activate the password reset executed by the agent software.
AllowResetDisabledToken	If this value is omitted, the default value is No. A SecurID token may be in a disabled state because: • The RSA ACE/Server administrator manually disabled the token to block the end user from entering the system. • The token was disabled because the end user failed multiple times to log into the system. Resetting a PIN on a disabled token reenables the token regardless of the action that disabled it. If the PMM is not configured to reset the PINs on disabled tokens, end users who accidentally lock themselves out must contact the Help Desk to reenables their tokens. If you allow reset of RSA SecurID PINs on disabled tokens during configuration, then the PMM for RSA SecurID always allows end users to reset their SecurID PINs. To prevent end users from resetting their SecurID PINs on manually disabled tokens (administratively locked out tokens), you must set the token to both the "Disabled" and the "Lost" status.
LogFile	This is the log filename for RSA SecurID agent service. If it is omitted, the default value is <code>SecurIDpxy.log</code>.
ValidateAceServerUser	If this value is omitted the default value is No. If the value is set to YES, it signifies that the ACE/Server authentication is enabled. The ValidationUser you provide must be a valid ACE/Server administrative user and should be able to connect using the ACE/Server credentials only. If the value is set to No, it signifies that the Windows native authentication is enabled. The ValidationUser you provide must be a valid Windows domain administrative user and should be able to connect using the Windows native credentials only.

When you click the **APPLY** button, the configuration information is saved in the registry. The install shield then asks if it should start the RSA SecurID agent service. Click **"YES"** to start the service.

Reconfiguring the Agent on a Windows System

After the agent is installed, you can reconfigure the agent by executing:

Start > Programs > Core Access Assurance Suite > Password Management Module Agent for RSA SecurID > Configure Password Management Module for RSA SecurID

After editing the configuration, click **FINISH**.

The software prompts you to start the agent. Click **YES** to start the service and change the configuration.

Starting and Stopping the Agent on a Windows System

To start and stop agent in a Windows 2000 environment, go to Start > Settings > Control Panel > Administrative Tools > Services. Select the CourSecurIDAgent, right click and select **START** or **STOP**.

To start and stop the agent in a Windows NT environment, go to Start > Settings > Control Panel > Services. Select the CourSecurIDAgent, right click and select **START** or **STOP**.

Uninstalling the Agent for Upgrading on a Windows System

To upgrade the agent, you need to uninstall the previous agent and then install the new agent.

Remove the agent by using the Windows Add/Remove Control Panel applet or by running the SecurIDInstall.exe file and selecting the **REMOVE** option.

Chapter 58: SAP Server — PMMs and Connectors

This chapter explains how to configure the PMMs and Connectors for SAP Server:

- [*“Configuring the PMM for SAP” on page 548*](#)
- [*“Configuring the Connector for SAP” on page 556*](#)
- [*“Configuring the PMM for SAP Logon” on page 563*](#)
- [*“Configuring the Connector for SAP Logon” on page 567*](#)
- [*“Using the SAP Account Discovery Tool” on page 570*](#)

The Connector for SAP Logon and PMM for SAP Logon are intended for use with versions before 4.6c. For version 4.6c or higher of SAP, use the regular Connector for SAP and PMM for SAP.

Use of the SAP Account Discovery Tool requires versions 4.7 or higher.

For information on the PMM for mySAP.com, see [*“mySAP.com — PMM” on page 573*](#).

Configuring the PMM for SAP

The PMM for SAP enables end users to reset their passwords on a SAP application server. The PMM for SAP is installed with the Core Access Assurance Suite. For information on installation, see the manual *Installing the Core Access Assurance Suite*.

The PMM for SAP requires an access key. For more on access keys, please contact Core Security.

Note: The SAP Logon prerequisites and configuration, and the PMM prerequisites described next are the same as those required for the Connector for SAP. Therefore if you have configured the connector, your site has already met them.

SAP Logon Requirements and Configuration

Before you configure the PMM for SAP, install and configure the SAP Logon software on each server in which the Connector Framework or Connector Framework Manager is installed. The prerequisites and configuration of SAP Logon for the PMM for SAP are the same as for the SAP Connector. Please refer to [page 556](#) for details.

PMM Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Prerequisites on the Connector Framework and Connector Framework Manager Servers

To use the PMM for SAP systems, install the following pre-requisite software on the each server in which the Connector Framework or Connector Framework Manager is installed:

- SAP Logon 6.20 or higher

This software includes the required file `librfc32.dll`

Using the Custom Remote Function Call

By default, the PMM for SAP makes a series of Remote Function Calls (RFCs) into BAPI methods during a password reset. Each password reset results in up to four methods being called. The PMM performs significant processing to interpret the results of each call. Also, each target represents a single client.

The PMM for SAP includes a configuration option (**REMOTE FUNCTION CALL** on the Add/Edit Target Dialog Box) that enables you to specify a single, customized RFC (Y_COUR_MOD2). This function consolidates all of the operations performed by default. This method has a number of advantages:

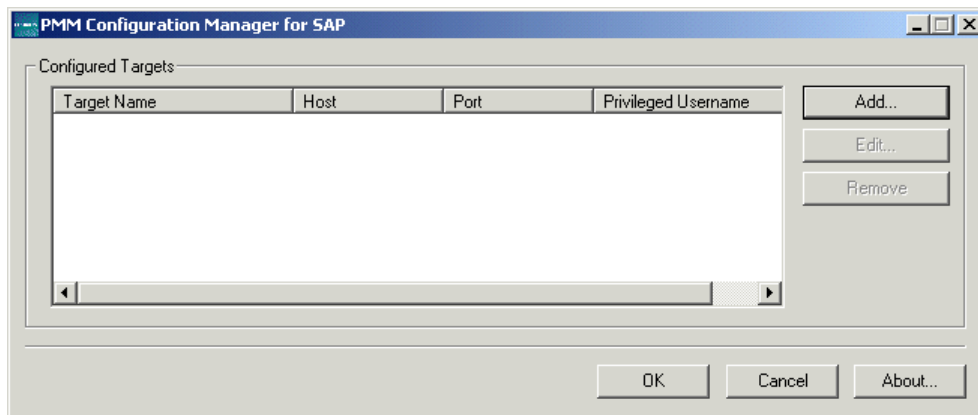
- It moves the majority of the workload onto the SAP server, allowing for greater parallelism in Core Security components.
- It enables the PMM to issue a single RFC per server (which is conveyed to all of the clients on that server).
- It reduces the number of calls that must be made to the server.

To specify this RFC in the PMM configuration, you need to install it. See [“Installing the Remote Function Call \(RFC\)” on page 554](#)

PMM Configuration

1. From the Start menu, select:
Programs > Core Access Assurance Suite > Password Management Modules > SAP
The PMM Configuration Manager for SAP appears.

Figure 278: PMM Configuration Manager for SAP



2. From this dialog box, you can:
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.

When you select the **ADD** or **EDIT** option, the Add/Edit Target Configuration dialog box appears.

Figure 279: Add/Edit Target Configuration for SAP

Add / Edit Target Configuration

Target information
SAP system:

Logon Information
SAP application server:

Client:

User:

Password:

Language: System number/Gateway instance: 00

Remote Function Call:

☒ Force User to Change Password at Next Logon
☐ Unlock user before a password reset

OK Cancel

3. Enter the following target information:

- a. **SAP SYSTEM** — Enter the name for the target configuration. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
- b. **SAP APPLICATION SERVER** — This is the SAP application server description name in the SAP Logon configuration.
- c. **CLIENT** — This value represents the company ID and is specific to the SAP installation. The default client numbers are 000,001 and 066, although using these numbers is not recommended. If you do use these numbers, the system displays a warning message.
- d. **USER** — This is the name of a privileged user that already exists on the SAP system. The username must be the SAP user type **SYSTEM**.

The privileged user must be a role that provides the following authorizations:

- S_RFC — access to function modules for lock/unlock and password change/reset.
 - S_USER_GRP with the following values "User group = *" and "Activity = 05,02", where "05" is for lock/unlock and "02" is for password change.
- e. **PASSWORD** — This is the password of the Privileged User, masked for security.

- f. **LANGUAGE** — This optional field enables you to specify a two-character language code that specifies the language interface on the SAP application server. The default is EN (English). The language code you enter must match the language code in the SAP Logon configuration. Other language codes include:

CS Czech	NO Norwegian
DE German	PT Portuguese
FR French	RU Russian
JA Japanese	ES Spanish
NL Netherlands Dutch	SV Swedish

Your SAP application server may have other language codes available. Refer to the Language Management Transaction on the SAP application server for a complete list of language codes.

- g. **SYSTEM NUMBER/GATEWAY INSTANCE** — This is a required field. Acceptable values are "00" to "99".

If the SAP Application Server string is specified **WITHOUT** the port indicator value (*i.e.*, /S/33XX), then the value entered in the "System Number" field is used for both the SYSNR and GWSERV.

If the SAP Application Server String is specified **WITH** the port indicator value (*i.e.*, /S/33XX), then the XX is used as the SYSNR and the GWSERV is the value placed into the "System Number" field.

If you need the two values to be different from one another, then use the /S/33XX value in the "SAP Application server:" field for the System Number, and the value entered into the "System/Gateway Number:" for the Gateway Number.

4. **REMOTE FUNCTION CALL** — Enter the name of a custom Remote Function Call in this text box if you are using one. The default name is Y_COUR_MOD2.
5. **FORCE USER TO CHANGE PASSWORD AT NEXT LOGIN** — This option forces end users to change their passwords the next time they log in after performing a password reset.
6. **UNLOCK USER BEFORE A PASSWORD RESET** — This option only applies to an SAP system in which the patch described in SAP Note 826050 has **not** been applied. If a user is locked, the user is not unlocked unless this option is checked. This option unlocks all lock types when doing a password reset.

SAP provides three lock types:

- too many failed logon attempts
- local administrative lock, and
- global administrative lock.

Note: On an SAP system in which the patch described in SAP Note 826050 has been applied, this option has no functionality. Instead the following behavior applies:

If the lock is caused by too many failed logon attempts, the account is unlocked before a password reset.

If the lock is an administrative lock, the account remains locked.

7. Click **OK** when the configuration is complete.

Mapping the SAP Servers and Clients Using the Custom Remote Function Call

Each SAP server has one or more clients. If you are using the custom remote function call, it is possible to issue remote function calls between clients on the same server given the appropriate configuration.

The following steps describe how to implement this configuration:

1. Select a "master" client for each SAP Server.

Password resets are conveyed to the clients on a given SAP server by a single master client. For each server, identify a single client as the master.

2. Create RFC Destination (RFCDES) entries for each child client from the master client.

This allows RFCs to run remotely on other clients on the server from the selected master client. You need to map between target IDs and the RFCDES entry IDs. To facilitate this, consider these guidelines:

- Use a naming convention that is consistent with your target naming
 - Create a database table with a mapping between target ID and RFCDES entry ID
3. Install the Core Security RFC on each of the master clients.

The Core Security-supplied RFC needs to be installed and accessible remotely on each of the master clients. This is how the PMM for SAP interfaces with the SAP systems. See [“Installing the Remote Function Call \(RFC\)” on page 554](#) for information about how to do this.

4. Store Information in a DB repository representing the topology.

Construct a custom macro that can determine all of the additional clients on a server given a single client. To do this, create a separate table containing a mapping which represents each client and associates it with a server ID.

5. Modify the IdentityMap.

Each user needs to have entries in the IdentityMap for each server on which they have at least one client account. The targetID needs to correspond to the master client for that server.

6. Configure One SAP PMM target per master client.

Ensure that the **REMOTE FUNCTION CALL** text box in the Add/Edit Target Configuration dialog box is populated with the name of the custom RFC that installed on the master clients (see [Figure 279](#)).

7. Add the master client targets to a workflow.

Use the Target Configuration form in the Core Server Administration Manager. See the chapter “Configure Global Actions and Settings” in the manual *Configuring Workflows with the Core Server Administration Manager* for information on how to do this.

8. Configure a custom macro that returns the set of clients for a given target.

The result of the macro should be a string which has the name of all of the clients except for the current target delimited by commas

For example, assume that server S1 has clients C1, C2, and C3. C1 is the master client. Then, the macro should take as input the name of the current target (which is C1) and return "C2,C3". C2 and C3 should correspond to entries in the RFCDES SAP table for client C1. The special value "NONE" represents the master client so the string "NONE,C2,C3" performs resets on the master client and the child clients C2 and C3.

"NONE" must be capitalized.

9. Configure the "Additional Clients" attribute.

On the Resource Overrides Administration Manager form (see [Figure 280](#)), set the default value for the "Additional Clients" attribute to the macro that was created in the last step. It should be hidden.

Updated Resource Overrides Administration Manager Form

The Resource Overrides form for PMM Gateway Connector (PMM-Gateway-Cnctr) targets pointing at the SAP PMM appears as in [Figure 280](#).

Figure 280: Resource Overrides Administration Manager Form

Choose Resource Attributes to Override: ?

Operation	Resource Attribute	Presentation	Label	Help Text	Obtain Value From	Attribute Display Options
Override	Additional Clients	☐ Required ☐ Secure ☐ Verify ☐ Visible ☐ Read Only ☐ Global	Additional Clients:	A pipe delimited list of additio	Default Value	Control Type: ? Text Default Value: Macro.ClientsForSAPTarget
Override	Password	☒ Required ☒ Secure ☒ Verify ☒ Visible ☐ Read Only ☐ Global	Password:	New password for the provid	Default Value	Control Type: ? Text Default Value:
Override	User Must Change Password at Next Logon	☐ Required ☐ Secure ☐ Verify ☒ Visible ☐ Read Only ☐ Global	Force change at next login?:	Should the user's password t	Default Value	Control Type: ? Boolean Default Value: ☐

The updated form has the new attribute, **ADDITIONAL CLIENTS**. Enter a comma-delimited list of SAP clients here. The client names are specific to the server that the target references. Ensure that the client names you supply reference names that you supply in the RFC Destination Table (RFCDES) on the SAP server.

Notes

If you are using the customized remote function call, you cannot create a workflow that uses the RFC optimization and allows the user to select a subset of clients per server to reset.

A single native status is returned per server. A single event is fired on success/non-success per server. Only a single ticket is created per server. If you do not use the customized remote function call, each of these operations is fired per client.

Installing the Remote Function Call (RFC)

Installing the RFC requires that you complete the three procedures described in this section: create a package, create a function group, and create a function module (the RFC).

Creating the Package

Use the SAP Package Builder application (SE21) to create a “package” that contains the function group. You can use an existing package.

Creating the Function Group

Use the SAP Function Builder application (SE37) to create a “function group” using the menu item:

Goto>Function Groups>Create Group

This function group must belong to the package you created in the previous step. You can use an existing function group.

Creating the Function Module

Use the SAP Function Builder application (SE37) to create a “function module” (RFC) that belongs to the function group you created in the previous step.

Then, follow these steps:

- From the Source Code tab, upload the source code contained in the PW_RESET_RFC.TXT file provided by Core Security into the RFC using the menu option:
Utilities>More Utilities>Upload/Download>Upload
- Edit the function name in the source code to match the name of the function module you created previously.
- Define the following import arguments using the Import tab:
 1. Parameter Name: USERNAME, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 2. Parameter Name: LOCKUSER, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 3. Parameter Name: FORCECHANGE, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 4. Parameter Name: PWD, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 5. Parameter Name: TMPPWD, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 6. Parameter Name: CLIENTS, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES

7. Parameter Name: RUNLOCAL, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 - Define the following export arguments using the Export tab:
 1. Parameter Name: OUTPUT, Type Spec: TYPE, Associated Type: STRING, Pass Value: YES
 2. Parameter Name: SUCCESS, Type Spec: TYPE, Associated Type: I, Pass Value: YES
 - Set the "Process Type" to "Remote Enabled Module" using the Attributes tab.
 - Activate the RFC with the menu option:
Function Module>Activate
 - Release the RFC into the environment with the menu option:
Function Module>Release>Release

Configuring the Connector for SAP

The Connector for SAP on SAP systems supports the following actions on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Note: The SAP Logon requirements and configuration, and the connector requirements and prerequisites described next are the same as those required for the SAP PMM. Therefore if you have configured the PMM, your site has already met them.

SAP Logon Requirements

Before you configure the connector for SAP, install and configure the SAP Logon software on each server in which the Connector Framework or Connector Framework Manager is installed. The SAP Logon software is included with the SAP software distribution kit. See the SAP documentation for more information about SAP Logon.

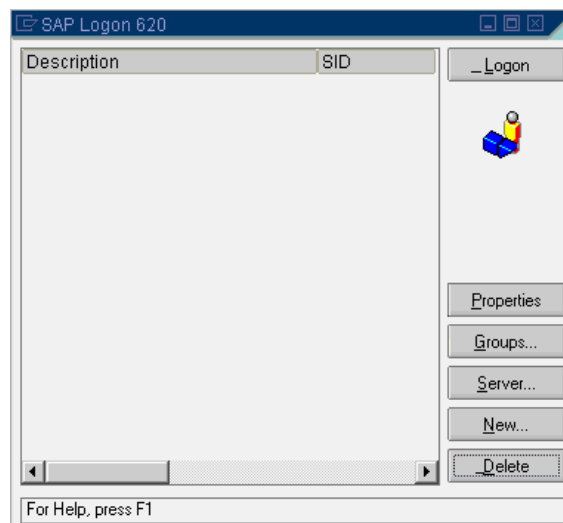
SAP Logon Configuration - Specifying the SAP Server Name

During the SAP Logon configuration, you enter a system description for the SAP server and a language code for the SAP server. Both the server description and the language code that you enter during the SAP Logon configuration must match the server description and the language code that you enter in the Connector Configuration Manager for SAP dialog box (see [Figure 284](#)).

The following is an example of how to enter the SAP server name during the SAP Logon configuration. The version of the SAP Logon that you are using may differ from this one.

1. Select "All Programs -> SAP Front End -> SAPlogon". To specify a target if none currently exists, select **NEW** from the SAP Logon configuration dialog box. If a target currently exists, click **PROPERTIES**.

Figure 281: SAP Logon Configuration



The New Entry dialog box appears.

Figure 282: SAP Logon Properties Dialog Box

2. Enter a name for the SAP server in the **DESCRIPTION** field. The name you enter here is also used to configure the connector.
3. Enter the appropriate server and routing information. Click **OK**.
4. If you clicked **PROPERTIES** instead of **NEW**, the Properties screen opens instead of the New Entry screen. Enter a name for the SAP server in the **DESCRIPTION** field here.

Prerequisites

Each SAP server must meet one of these SAP BASIS and Support Package levels for provisioning actions with the Connector for SAP:

- For Component: SAP_BASIS Release: 46C Package Name: SAPKB46C59
- For Component: SAP_BASIS Release: 620 Package Name: SAPKB62067
- For Component: SAP_BASIS Release: 640 Package Name: SAPKB64025
- For Component: SAP_BASIS Release: 700 Package Name SAPKB70021

Setting the Correct Trust Level

Follow these steps to trust the assemblies for the appropriate executable file used by the Connector for SAP systems:

1. List the SAP.NET PMM with the .NET Framework Global Assembly Cache Tool.

*directory-path-to-exe*gacutil.exe -I SAP.connector.dll

For example,

C:\WINNT\Microsoft.NET\Framework\v1.0.3705\gacutil.exe

Execute the following steps to trust the assemblies for the appropriate executable file used by the PMM for SAP systems, depending on whether you are configuring a target against a SAP R/3 4.6c, SAP 4.7, or SAP ECC 5.0 system. If you are configuring targets against two or three different systems, complete the steps for each revision.

2. Select Start > Settings > Control Panel
3. Open Administrative tools.

4. Open Microsoft.NET Framework Wizards.
5. Double Click **TRUST AN ASSEMBLY**.
6. Select the option "Make changes to this computer" and click the **NEXT** button.
7. Browse and select the appropriate actuator for your SAP revision:
 - For connecting to an SAP server with basis level 46C, select SAPActuator.exe and click **NEXT**.
 - For connecting to an SAP server with basis level 620, select SAPActuator47.exe and click **NEXT**.
 - For connecting to an SAP server with basis level 640, select SAPActuatorECC.exe and click **NEXT**.
 - For connecting to an SAP server with basis level 700 select SAPActuatorECC60.exe and click **NEXT**.
8. Raise the assembly level from "None" to "Full Trust" and click **NEXT**.
9. Click **FINISH**.

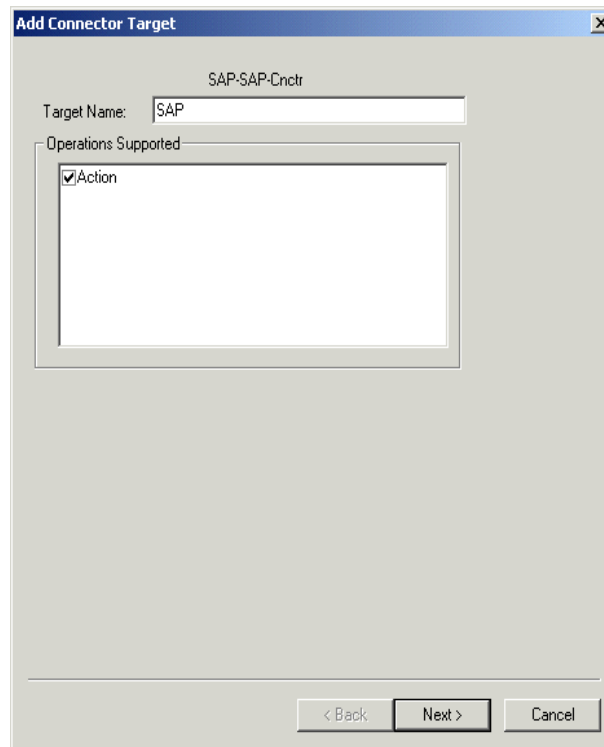
SAP Role Support

- The User Roles attribute is deprecated.
- The new Roles attribute supports both the Copy and Override behavior.
 - When you select the Copy behavior for the "Roles" attribute, the From and To attributes of the roles are copied from the model to the new account.
 - When you select the Override behavior for the "Roles" attribute, the From attribute is set to the current date, and the To attribute is set to 12/31/9999.
- When the Roles attribute is assigned, the SAP system automatically assigns the role description for each role to the new/changed account.
- Composite roles are supported. Assignment of a composite role to a user results in the assignment of all roles contained in the composite.

Connector Configuration

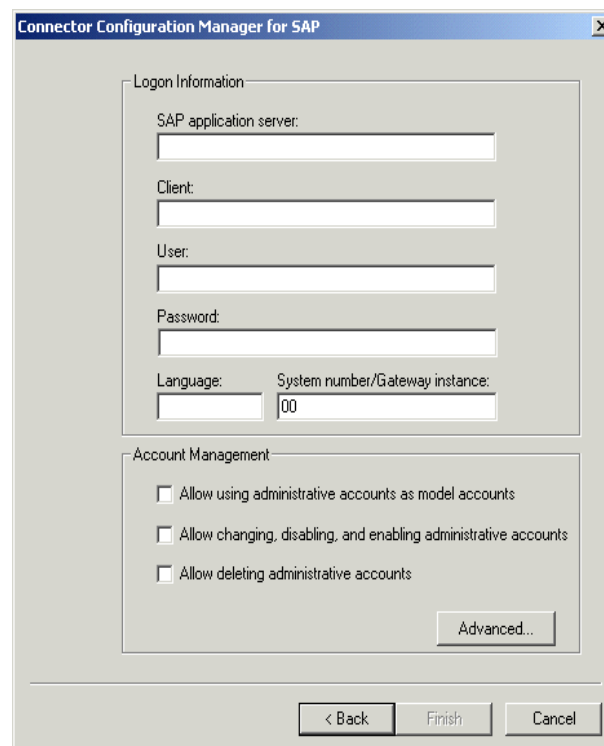
Follow these steps to configure the connector for SAP:

1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Select **SAP-SAP-CNCTR**
3. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 283: Add SAP Target


The dialog box titled "Add Connector Target" has a title bar with a close button. Inside, the text "SAP-SAP-Cnctr" is displayed. Below it, the "Target Name:" label is followed by a text box containing "SAP". Under the "Operations Supported" section, there is a list box with "Action" checked. At the bottom, there are three buttons: "< Back", "Next >", and "Cancel".

4. Enter a target name and press the **NEXT** button.
The Connector Configuration Manager dialog box appears.

Figure 284: Connector Configuration Manager for SAP


The dialog box titled "Connector Configuration Manager for SAP" has a title bar with a close button. It contains two main sections: "Logon Information" and "Account Management".
 The "Logon Information" section includes fields for:
 - SAP application server:
 - Client:
 - User:
 - Password:
 - Language: (with a dropdown arrow)
 - System number/Gateway instance: (with a text box containing "00")
 The "Account Management" section includes three checkboxes:
 - ☐ Allow using administrative accounts as model accounts
 - ☐ Allow changing, disabling, and enabling administrative accounts
 - ☐ Allow deleting administrative accounts
 An "Advanced..." button is located at the bottom right of the "Account Management" section. At the bottom of the dialog, there are three buttons: "< Back", "Finish", and "Cancel".

5. Enter the **LOGIN INFORMATION** for the target:

- a. **SAP APPLICATION SERVER** — This is the SAP server description name as specified in SAP Logon Properties dialog box (see [Figure 282](#)).
- b. **CLIENT** — This value represents the company ID and is specific to the SAP installation. The default client numbers are 000,001 and 066, although using these numbers is not recommended. If you do use these numbers, the system displays a warning message.
- c. **USER** — This is the name of a privileged user that already exists on the SAP system. The username must be the SAP user type **SYSTEM**.

The privileged user must be in a role that provides the following authorizations:

- S_RFC - access to function modules:
 - 1) Create, clone user in all groups
 - 2) Assign Roles or delete roles from the user
 - 3) Lock/unlock user
 - 4) Change or reset the user password
 - 5) Change the validity date for user logon
 - 6) Change the validity date for Roles
- S_USER_GRP with the following values "User group = *" and "Activity = 05,02", where "05" is for lock/unlock and "02" is for password change.
- S_USER_AGR
- S_USER_PRO
- S_USER_SAS
- d. **PASSWORD** — This is the password of the privileged User, masked for security.
- e. **LANGUAGE** — This optional field enables you to specify a two-character language code that specifies the language interface on the SAP server. The default is EN (English). The language code you enter must match the language code in the SAP Logon configuration. Other language codes include:

CS Czech	NO Norwegian
DE German	PT Portuguese
FR French	RU Russian
JA Japanese	ES Spanish
NL Netherlands Dutch	SV Swedish

Your SAP server may have other language codes available. Refer to the Language Management Transaction on the SAP server for a complete list of language codes.

- f. **SYSTEM NUMBER/GATEWAY INSTANCE** — This is a required field. Acceptable values are "00" to "99".

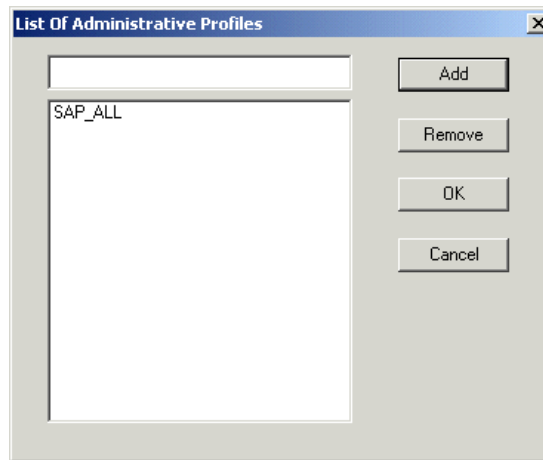
If the SAP Application Server string is specified WITHOUT the port indicator value (*i.e.*, /S/33XX), then the value entered in the "System Number" field is used for both the SYSNR and GWSERV.

If the SAP Application Server String is specified WITH the port indicator value (*i.e.*, /S/33XX), then the XX is used as the SYSNR and the GWSERV is the value placed into the "System Number" field.

If you need the two values to be different from one another, then use the /S/33XX value in the "SAP Application server:" field for the System Number, and the value entered into the "System/Gateway Number:" for the Gateway Number.

6. Enter the account management Information for the target:
 - a. **ALLOW USING ADMINISTRATIVE ACCOUNTS AS MODEL ACCOUNTS** — Check this box to indicate that administrative user accounts can be modeled for account creation. By default, this box is unchecked (do not allow modeling of administrative accounts). An administrative user has the authorizations defined in the Advanced Properties dialog box.
 - b. **ALLOW CHANGING, DISABLING, AND ENABLING ADMINISTRATIVE ACCOUNTS** — Check this box to allow users to change, disable, and enable administrative accounts.
 - c. **ALLOW DELETING ADMINISTRATIVE ACCOUNTS** — Check this box to allow users to disable administrative accounts.
7. Click **ADVANCED**. The Advanced properties dialog box appears.

Figure 285: Connector for SAP Advanced Properties



The advanced dialog box lists authorizations on the SAP server. Users having any of these authorizations qualify as administrative users.

8. To add an authorization, enter it in the top box and click **ADD**. To remove an authorization, highlight it and click **REMOVE**. Click **Cancel** to remove an authorization before you add it to the list.
9. Click **OK** when you have completed the Advanced dialog box.

The Connector Configuration Manager for SAP ([Figure 284](#) on page 559) appears.

10. Click **FINISH** to complete the configuration.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Notes

The Connector for SAP uses the SAP.NET connector (published by SAP) to interact with the back-end system at the BASIS level via RFC calls into BAPI code. The SAP.NET connector handles all the RFC transactions including communications security between the Core Server and the back-end system.

Configuring the PMM for SAP Logon

The PMM for SAP Logon enables end users to reset their passwords on a SAP application server. The PMM for SAP Logon is installed with the Core Server Core Server. For information on installation, see to the manual *Installing the Core Server*.

Note: The PMM for SAP Logon is intended for use with versions R/3 3.x to 4.5b. For version 4.6c or higher of SAP, use the PMM for SAP.

The SAP Logon requirements and configuration, and the PMM requirements described next are the same as those required for the SAP Logon connector. Therefore if you have configured the connector, your site has already met them.

SAP Logon Prerequisites and Configuration

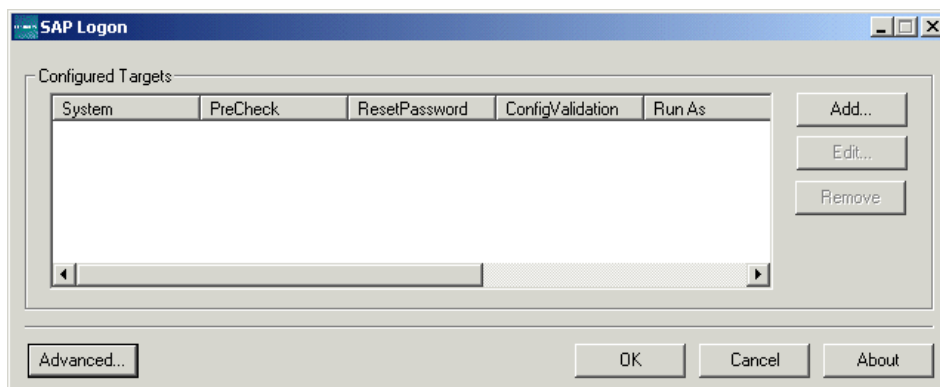
Before you configure the PMM for SAP Logon, install and configure the SAP Logon software on each server in which the Connector Framework or Connector Framework Manager is installed. The requirements and configuration of SAP Logon for the PMM for SAP Logon are the same as the Connector for SAP. Please refer to [page 556](#) for details. Please note that this refers specifically to the SAP Logon requirements and configuration. The requirements and configuration for the PMM for SAP Logon is different from the PMM for SAP, and is shown below.

PMM Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Programs > Core Server Core Server > Password Management Modules > SAP Logon
The PMM Configuration Manager for SAP Logon appears.

Figure 286: PMM Configuration Manager for SAP Logon

2. From this dialog box, you can:

- View the targets already configured in the **CONFIGURED TARGETS** list.
- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.
- Enable advanced properties. Click the **ADVANCED** button.

When you select the **ADD** or **EDIT** option, the Add/Edit Target Configuration dialog box appears.

Figure 287: Add/Edit Target Configuration for SAP Logon

Target Name:
SAP Logon

PreCheck Command Line:
cscript.exe /nologo /b "PMMForSAPLogon.vbs"

ResetPasswordEx Command Line:
cscript.exe /nologo /b "PMMForSAPLogon.vbs"

ConfigValidation Command Line:
cscript.exe /nologo /b "PMMForSAPLogon.vbs"

☐ Run Commands as User

Domain\User:

User Password:

Configure Parameters for System

Parameter:

Value:

Verify Value:

☒ Secure Attribute

Add >>

<< Remove

Configured Parameters:

Name	Value

OK Cancel

3. Enter the following target configuration information:
 - a. **TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
 - b. For all three **COMMAND LINE** fields, enter the following text, as shown in [Figure 287](#):
cscript.exe /nologo /b "PMMForSAPLogon.vbs"
4. Leave the **RUN COMMANDS AS USER** checkbox unchecked.
5. Fill in the Configuration Parameters as shown in the table below. Enter the parameter name in the **PARAMETER** text box, then enter the appropriate value in the **VALUE** text box. If the **SECURE ATTRIBUTE** checkbox is selected, you must enter the value in both the **VALUE** and **VERIFY** text boxes. Click **ADD** to move the entry to the list on the right side.

Table 33: Configuration parameters for SAP Logon PMM

Parameter Name	Value	Secure Attribute?	Required?
PrivUserID	A valid SAP R/3 admin userid	No	Yes
PrivUserPWD	The password for the user specified	Yes	Yes

Table 33: Configuration parameters for SAP Logon PMM

Parameter Name	Value	Secure Attribute?	Required?
Target	R/3 SAP System Target that you are logging on to	No	Yes
SAPPath	The Directory of the Sap Logon Gui	No	No Default = "C:\Program Files\SAP\FrontEnd\SAP Logon"
SAPExe	Executable name for the SAP logon 620 Client application	No	NO Default = Saplogon.exe
ForcePasswordReset	A value of "true" or "false". This flag indicates whether to force the user to need to change their password on their next login after the password is reset. If not configured, the value currently set of the user account is maintained.	No	No Default = true
blsWelcomeDialog	A value of "true" or "false". This flag indicates whether there is a welcome dialog box when Login into the SAPlogon 620 client app.	No	No Default = false
ReuseSAPLOGON	A value of "true" or "false". This flag indicates whether to reuse the application.	No	No Default = false A value of true is not advised. It is extremely unstable due to memory leaks in the sap UI.

6. Click **OK** to configure the PMM.

Notes Regarding the PMMForSAPLogon.vbs Script

The script supports a detailed logging mode for debugging. To engage this capability, set the variable "SAPLOG", on line 77, to the value "2".

The script supports a stand-alone debugging mode. To engage this capability, set your argument values in the statements starting on line 1250, and set the variable "bLocalDebug" on line 215 to the value "True".

The script does currently support the capability to leave the SAP Logon 620 UI application running between resets to improve performance, but it is extremely unstable due to memory leaks in the sap UI.

Configuring the Connector for SAP Logon

The Connector for SAP Logon on SAP systems supports the following actions on a target: Add, Change, Create, Delete, Disable, and Enable.

Note: The Connector for SAP Logon is intended for use with versions before 4.6c. For version 4.6c or higher of SAP, use the Connector for SAP.

The SAP Logon requirements and configuration, and the connector requirements described next are the same as those required for the PMM for SAP Logon. Therefore if you have configured the PMM, your site has already met them.

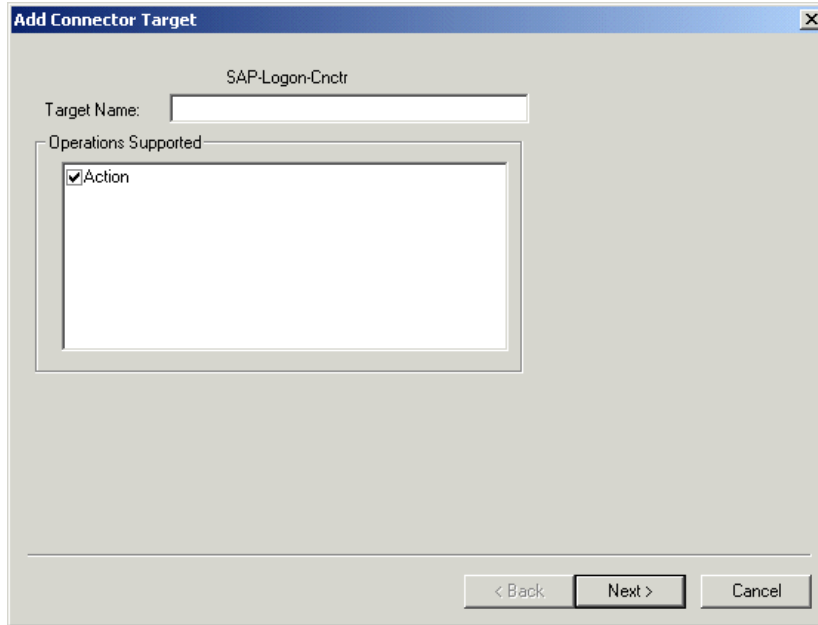
SAP Logon Requirements and Configuration

The requirements and configuration of SAP Logon for the Connector for SAP Logon are the same as for the Connector for SAP. Refer to [page 556](#) for details. Note that this refers specifically to the SAP Logon requirements and configuration. The requirements and configuration for the Connector for SAP Logon is different from the Connector for SAP, and is shown below.

Connector Configuration

Follow these steps to configure the connector for SAP Logon:

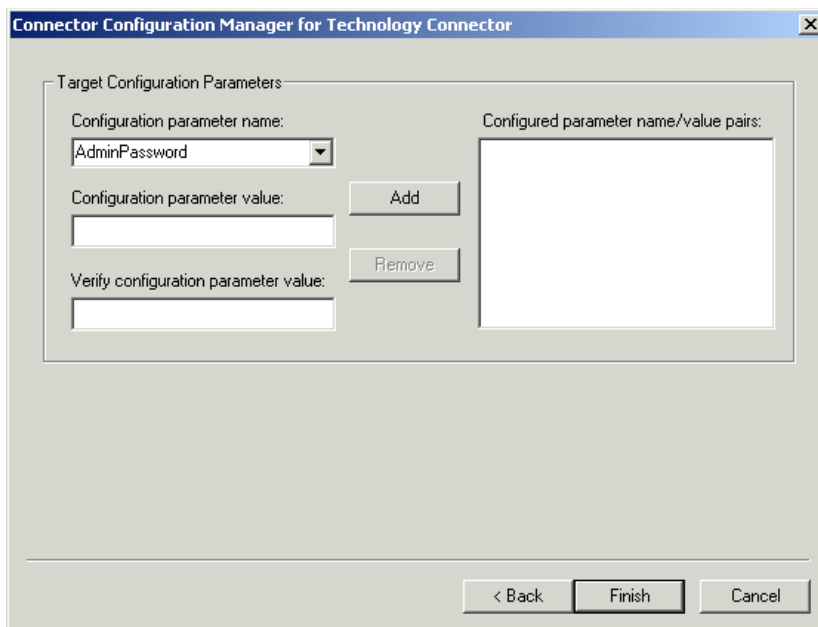
1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **SAP-LOGON-CNCTR**, and click **OK**.
3. Select **SAP-LOGON-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**
The Add Connector Target dialog box appears.

Figure 288: Add SAP Logon Target


The dialog box is titled "Add Connector Target". It has a text field for "Target Name:" with the value "SAP-Logon-Cnctr" entered. Below this is a section titled "Operations Supported" containing a list box with a single checked item, "Action". At the bottom right are three buttons: "< Back", "Next >", and "Cancel".

5. Enter a target name and press the **NEXT** button.

The Connector Configuration Manager dialog box appears.

Figure 289: Connector Configuration Manager for SAP Logon


The dialog box is titled "Connector Configuration Manager for Technology Connector". It features a section titled "Target Configuration Parameters" on the left. This section includes a "Configuration parameter name:" dropdown menu with "AdminPassword" selected, a "Configuration parameter value:" text field, and a "Verify configuration parameter value:" text field. To the right of these fields are "Add" and "Remove" buttons. On the right side of the dialog is a large list box titled "Configured parameter name/value pairs:". At the bottom right are three buttons: "< Back", "Finish", and "Cancel".

6. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **AdminPassword** — A valid SAP R/3 admin password
 - **Client** — The client ID, typically a 3 digit number

- **Description** — The description of the system that you defined in the SAPLogon 6.20 application
- **Domain** — The domain of the Domain User
- **DomainPassword** — The password of the Domain User
- **DomainUser** — This is a user that has access to the network. It is used so the Courion Service can access the network using these credentials
- **Language** — Two letter code for the language used by the SAP system (see below for details)
- **SAPAdmin** — The SAP user with sufficient privileges to create and delete users

The Language parameter enables you to specify a two-character language code that specifies the language interface on the SAP application server. The default is EN (English). The language code you enter must match the language code in the SAP Logon configuration. Other language codes include:

CS Czech	NO Norwegian
DE German	PT Portuguese
FR French	RU Russian
JA Japanese	ES Spanish
NL Netherlands Dutch	SV Swedish

Your SAP application server may have other language codes available. Refer to the Language Management Transaction on the SAP application server for a complete list of language codes.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

7. Click **FINISH**. A message displays showing the SAP system being contacted to verify the information supplied.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each provisioning action for the selected connector.

Using the SAP Account Discovery Tool

The SAP Account Discovery Tool extracts the First name, Last name, Full name, and Username for each user account on a specific SAP server to build the Core Server for existing SAP accounts on a SAP server. This tool requires the Microsoft .NET framework. Use of the SAP Account Discovery Tool requires versions 4.7 or higher.

To run the SAP Account Discovery tool, follow these steps:

1. Create an XML request document containing the configuration information for the applicable target. This document is referred to later as SAPDiscoveryInput.xml. The contents should be as follows:

```
<?xml version="1.0" ?>
<CourRoot version="1.0">
  <CourTechEngineRequest requestType="accountList"
    transactionID="1">
    <CourDataPass>
      <CourParam paramName="1">
        <CourValue>Place SAP Router String Here</
        CourValue>
      </CourParam>
      <CourParam paramName="2">
        <CourValue>Place Client Here</CourValue>
      </CourParam>
      <CourParam paramName="3">
        <CourValue>Place Administrator Username
        Here</CourValue>
      </CourParam>
      <CourParam paramName="4">
        <CourValue>Place Administrator Password
        Here</CourValue>
      </CourParam>
      <CourParam paramName="5">
        <CourValue>Place Language Code Here (i.e.
        EN)</CourValue>
      </CourParam>
      <CourParam paramName="78">
        <CourValue>Place System Number Here (i.e.
        00)</CourValue>
      </CourParam>
    </CourDataPass>
  </CourTechEngineRequest>
</CourRoot>
```

2. Call the applicable SAP Actuator with the following command line:
 SAPActuatorECC SAPDiscoveryInput.xml >SAPDiscoveryOutput.xml
 - SAPActuator47.exe for SAP R/3 4.7
 - SAPActuatorECC.exe for SAP ECC 5.0
 - SAPActuatorECC60.exe for SAP ECC 6.0
3. Wait for the Actuator to complete its execution.

4. Check the results in the SAPDiscoveryOutput.xml file. They should be formatted as follows:

```
<?xml version="1.0" ?>
<CourRoot version="1.0">
  <CourTechEngineResponse requestType="accountList"
    transactionID="1" logLevel="success"
    logMessage="EMPTY">
    <CourStatus logLevel="success" logMessage="EMPTY" /
  >
  <CourDataPass>
    <CourParam paramName="1010"
      paramType="stringList">
      <CourValue>Username | First Name | Last Name
      | Full Name</CourValue>
      <CourValue>Username | First Name | Last Name
      | Full Name</CourValue>
      <CourValue>Username | First Name | Last Name
      | Full Name</CourValue>
      <CourValue>Username | First Name | Last Name
      | Full Name</CourValue>
    </CourParam>
  </CourDataPass>
</CourTechEngineResponse>
</CourRoot>
```


Chapter 59: mySAP.com — PMM

This chapter explains how to configure the PMM for mySAP:

- [*“Configuring the PMM for mySAP.com” on page 574*](#)

Configuring the PMM for mySAP.com

The Password Management Module (PMM) for mySAP.com™ enables end users to reset their passwords on a SAP® R/3® server. The PMM for mySAP.com is installed with the Core Access Assurance Suite.

The PMM for mySAP.com requires a specific access key. For information about access keys, please contact Core Security.

Prerequisites

Internet Explorer must be used with this PMM.

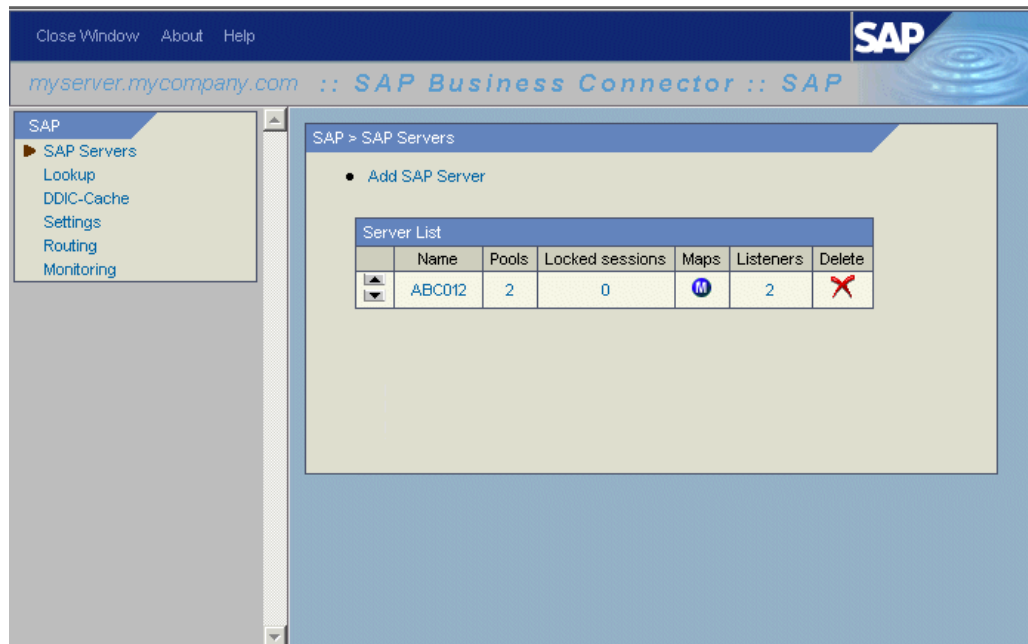
You must have version 4.5b, 4.5c, or 4.6c of mySAP.com. The SAP must include SAP R/3, SAP's Business Connector, and an SSL Certificate (see [“Using Multiple R/3 Servers with a Single Business Connector” on page 578](#)).

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

Business Connector SAP Configuration

Please refer to SAP documentation. The following information and screens are examples only. These operations must be completed by a mySAP.com administrator.

Under the SAP Servers tab, there is a list of available SAP servers ([Figure 290](#)). (**Note:** the SAP specific illustrations all appear via a web browser.)

Figure 290: SAP Servers Defined in the Business Connector

Make sure this list includes the single SAP R/3 on which passwords are being reset. If not, this server must be defined.

To direct a request to the appropriate SAP R/3 server, the Business Connector contains a series of routing rules. Existing rules are listed under the Routing Rules tab ([Figure 291](#)).

Figure 291: Routing Rules in the Business Connector

Routing Rule List							
Edit	Enabled?	Status	Sender	Receiver	Msg Type	Transport	St
▶	✓ Yes	✓	EXTERNAL	SAP-BAPI	BAPI_USER_UNLOCK	RFC	wm.PartnerMgr.flows.EXTERN
▶	✓ Yes	✓	EXTERNAL	SAP-BAPI	BAPI_USER_EXISTENCE_CHECK	RFC	wm.PartnerMgr.flows.EXTERNAL.SA
▶	✓ Yes	✓	EXTERNAL	SAP-BAPI	SUSR_USER_CHANGE_PASSWORD_RFC	RFC	wm.PartnerMgr.flows.EXTERNAL.SAP-B
▶	✓ Yes	✓	EXTERNAL	SAP-BAPI	BAPI_TRANSACTION_COMMIT	RFC	wm.PartnerMgr.flows.EXTERNAL.S

Configure the five routing rules required for the PMM for mySAP.com according to the following screens. This step should be completed before configuring the PMM for mySAP.com ([Figure 292](#) and [Figure 293](#)).

Figure 292: SAP Routing Rule Defined 1

Close Window Help

myserver.mycompany.com :: SAP Business Connector :: Routing

Routing

- Routing Rules
- Transactions
- Transports

Routing > Routing Rules > Edit Routing Rule

- Return to Routing Rules

Routing Rule Flow

Sender **EXTERNAL**

Receiver **SAP-BAPI**

Message Type **BAPI_USER_EXISTENCE_CHECK**

ACL Group <None>

Package Default

Pre-Processing Service

Main flow service **wm.PartnerMgr.flows.EXTERNAL.SA**

Post-Processing Service

Transport

RFC

Configure RFC Transport

Specify SAP Destination **ABC012**

Name of Outbound Service **pub.sap.transport.RFC.OutboundProcess**

Save Cancel

Figure 293: SAP Routing Rule Defined 2

Close Window Help

myserver.mycompany.com :: SAP Business Connector :: Routing

Routing

- Routing Rules
- Transactions
- Transports

Routing > Routing Rules > Edit Routing Rule

- Return to Routing Rules

Routing Rule Flow

Sender **EXTERNAL**

Receiver **SAP-BAPI**

Message Type **BAPI_USER_CHANGE**

ACL Group <None>

Package Default

Pre-Processing Service

Main flow service **wm.PartnerMgr.flows.EXTERNAL.SA**

Post-Processing Service

Transport

RFC

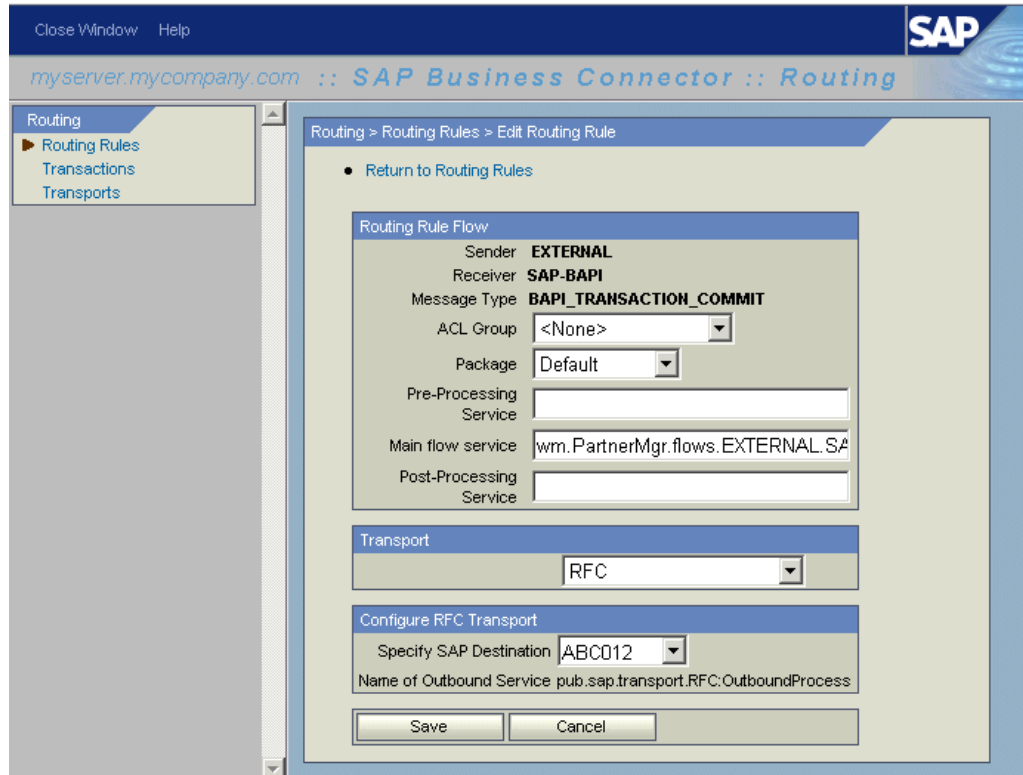
Configure RFC Transport

Specify SAP Destination **ABC012**

Name of Outbound Service **pub.sap.transport.RFC.OutboundProcess**

Save Cancel

Figure 294: SAP Routing Rule Defined 3



Close Window Help

myserver.mycompany.com :: SAP Business Connector :: Routing

Routing

- Routing Rules
- Transactions
- Transports

Routing > Routing Rules > Edit Routing Rule

- Return to Routing Rules

Routing Rule Flow

Sender: **EXTERNAL**

Receiver: **SAP-BAPI**

Message Type: **BAPI_TRANSACTION_COMMIT**

ACL Group: <None>

Package: Default

Pre-Processing Service:

Main flow service: **wm.PartnerMgr.flows.EXTERNAL.SA**

Post-Processing Service:

Transport: RFC

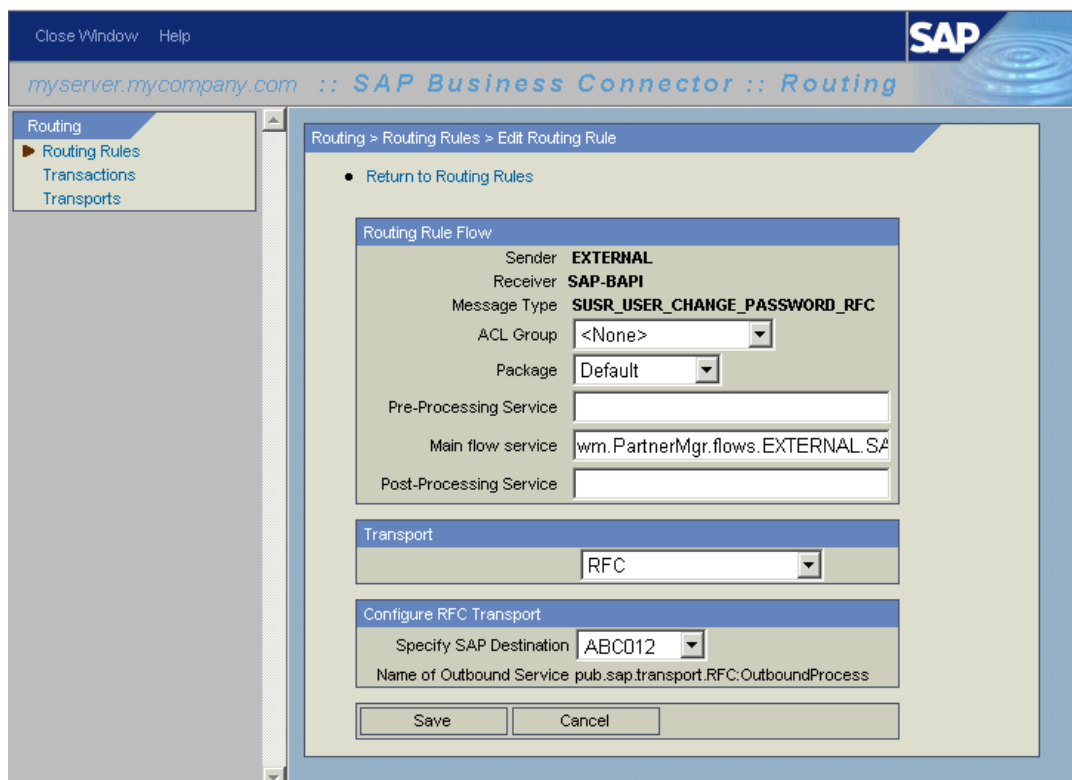
Configure RFC Transport

Specify SAP Destination: ABC012

Name of Outbound Service: **pub.sap.transport.RFC.OutboundProcess**

Save Cancel

Figure 295: SAP Routing Rule Defined 4



Close Window Help

myserver.mycompany.com :: SAP Business Connector :: Routing

Routing

- Routing Rules
- Transactions
- Transports

Routing > Routing Rules > Edit Routing Rule

- Return to Routing Rules

Routing Rule Flow

Sender: **EXTERNAL**

Receiver: **SAP-BAPI**

Message Type: **SUSR_USER_CHANGE_PASSWORD_RFC**

ACL Group: <None>

Package: Default

Pre-Processing Service:

Main flow service: **wm.PartnerMgr.flows.EXTERNAL.SA**

Post-Processing Service:

Transport: RFC

Configure RFC Transport

Specify SAP Destination: ABC012

Name of Outbound Service: **pub.sap.transport.RFC.OutboundProcess**

Save Cancel

Figure 296: SAP Routing Rule Defined 5

When completed, these templates provide routing rules for the password reset request.

Using Multiple R/3 Servers with a Single Business Connector

The PMM for mySAP supports for multiple R/3 servers from a single Business Connector. To do this, the PMM automatically replaces the value for the Receiver with the R/3 system name defined as a target for the PMM. For example, if the Business Connector defines two R/3 systems (HR_SVR and FI_SVR), you would create eight routing rules as follows:

Sender	Receiver	Msg Type
EXTERNAL	HR_SVR	BAPI_USER_CHANGE
EXTERNAL	HR_SVR	BAPI_USER_EXISTENCE_CHECK
EXTERNAL	HR_SVR	BAPI_TRANSACTION_COMMIT
EXTERNAL	HR_SVR	SUSR_USER_CHANGE_PASSWORD_RFC
EXTERNAL	FI_SVR	BAPI_USER_CHANGE
EXTERNAL	FI_SVR	BAPI_USER_EXISTENCE_CHECK
EXTERNAL	FI_SVR	BAPI_TRANSACTION_COMMIT
EXTERNAL	FI_SVR	SUSR_USER_CHANGE_PASSWORD_RFC

If the routing rules do not already exist, the PMM creates the routing rule "stubs" automatically.

Configuring a target creates the "stub" for BAPI_USER_EXISTENCE_CHECK, and returns the error: Unknown Partner and Message Type. Routing Rule created. Sender: EXTERNAL Receiver: HR_SVR MsgType: BAPI_USER_EXISTENCE_CHECK

After the "stub" is created, log into the Business Connector and perform the following actions to complete the routing rule configuration (["SAP Routing Rule Defined 1" on page 576](#)):

1. Fill in the Transport (RFC).
2. Specify SAP Destination (HR_SVR).
3. Click Save.
4. Click the entry "No" in the "Enabled?" column to toggle the state to enabled (see ["Routing Rules in the Business Connector" on page 575](#)).

During a reset attempt, the PMM creates the remaining routing rule "stubs" if they do not exist. Each attempt returns an error:

Unknown Partner and Message Type. Routing Rule created. Sender: EXTERNAL Receiver: HR_SVR MsgType: BAPI_USER_CHANGE

Unknown Partner and Message Type. Routing Rule created. Sender: EXTERNAL Receiver: HR_SVR MsgType: BAPI_TRANSACTION_COMMIT

Unknown Partner and Message Type. Routing Rule created. Sender: EXTERNAL Receiver: HR_SVR MsgType: SUSR_USER_CHANGE_PASSWORD_RFC

After each error, and before the next reset attempt, follow the steps above to complete the routing rule configuration.

To add the FI_SVR, repeat the process to configure the routing rules.

SSL Certificate

For the PMM for mySAP.com to reset passwords, the system must trust the certificate authority (CA) that signed the mySAP.com Business Connector's SSL certificate. To verify that the CA is a trusted authority, compare its name with the certificate authority list included with Internet Explorer.

For Internet Explorer version 4.x, path View > Internet Options > Content Tab > Authorities button > Network Server authentication drop-down selection. For Explorer version 5.x, use path Tools > Internet Options... > Content tab > Certificates button > Trust Root Certification Authorities tab.

If the system does not trust the CA:

1. Get the CA's certificate from the Business Connector administrator or the CA administrator.
2. Double click on the certificate file and select **INSTALL CERTIFICATE** and the certificate is installed by a wizard.
3. In the Certificate Store wizard dialog, select **PLACE ALL CERTIFICATES IN THE FOLLOWING STORE** then click the **BROWSE** button.
4. In the Select Certificate Store dialog, click the **SHOW PHYSICAL STORES** check box, expand **TRUSTED ROOT CERTIFICATION AUTHORITIES** and select **LOCAL COMPUTER**.
5. Click **OK**.
6. Finish the remainder of the wizard.

If this is the first time a certificate is installed on the system, a dialog appears with information about the certificate. This should be verified to ensure that the correct certificate is being installed. The dialog also asks if the certificate should be added to the root directory. Click **YES**.

The certificate is now installed.

Privileges Required by the Privileged User

The PMM for mySAP.com requires the following sets of user credentials to perform password resets:

On the Business Connector:

1. Ensure that the privileged user credentials you enter in the PMM Configuration ([Figure 305](#)), exist on the Business Connector. Also, the privileged user must be able to execute the following services on the Business Connector:

pub.sap.transport.RFC:InboundProcess

pub.sap.client:createTID

pub.sap.client:lockSession

pub.sap.client:releaseSession

To execute the above services, the user must belong to a group that is associated with both the Internal ACL and the SAPUsers ACL. By default, the Administrators and the Developers groups are associated with the SAPUsers ACL and Internal ACL.

You may use a privileged user that already exists on the Business Connector to configure the PMM for mySAP.com. However, it is important that the existing user you use belongs to a group that is associated with both the SAPUsers and the Internal ACL. By default, the existing users that you may use are the 'Administrator' and 'Developer' users, which belong to the Administrators and Developers group, respectively.

The following sample instructions illustrate how to create a new user, "CourAdmin" and new group "Courion," and associate the new group with the required ACLs.

Note: The following information and screens are examples only. For more details, please refer to SAP documentation.

To create a new user on the Business Connector:

- a. Navigate to **SECURITY > USERS AND GROUPS > ADD AND REMOVE USERS** ([Figure 297](#)). Enter the user name "CourAdmin," in the text box and the password in the password field.

Figure 297: Create New User

Security > Users and Groups > Add and Remove Users

- Return to Users and Groups

Create Users

User Names: One "username" or "username;password" per line.

CourAdmin

The password below will apply to all new users that do not have a password specified above.

Password: *****

Re-Enter Password: *****

Create Users

Remove Users

Select Users

- Administrator (not removable)
- Default (not removable)
- Developer (not removable)
- Replicator (not removable)
- SAPUser (not removable)

Remove Users

b. Click **CREATE USERS**.

To create a new group:

a. Navigate to **SECURITY > USERS AND GROUPS > ADD AND REMOVE GROUPS** ([Figure 298](#)). Enter the group name "Courion" in the text box.

Figure 298: Create New Group

Security > Users and Groups > Add and Remove Groups

- Return to Users and Groups

Create Groups

Group Names: One group name per line

Courion

Create Groups

Remove Groups

Select Groups

- Administrators (not removable)
- Anonymous (not removable)
- Developers (not removable)
- Everybody (not removable)
- Replicators (not removable)
- SAPUsers (not removable)
- ☐ WmPartnersUsers

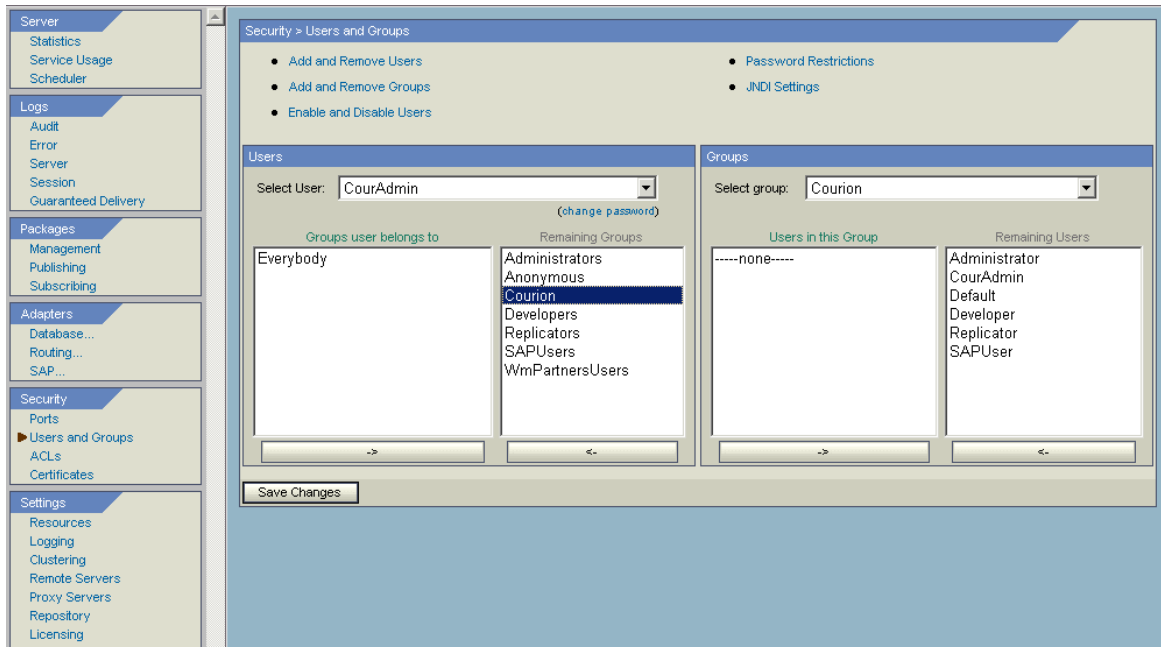
Remove Groups

b. Click **CREATE GROUPS**.

To add the new user to the new group:

- a. Navigate to **SECURITY > USERS AND GROUPS**. Select **COURADMIN** from the Select User drop down ([Figure 299](#)). Select **COURION** from the Select Groups drop down, and click the <- button.

Figure 299: Add New User to New Group

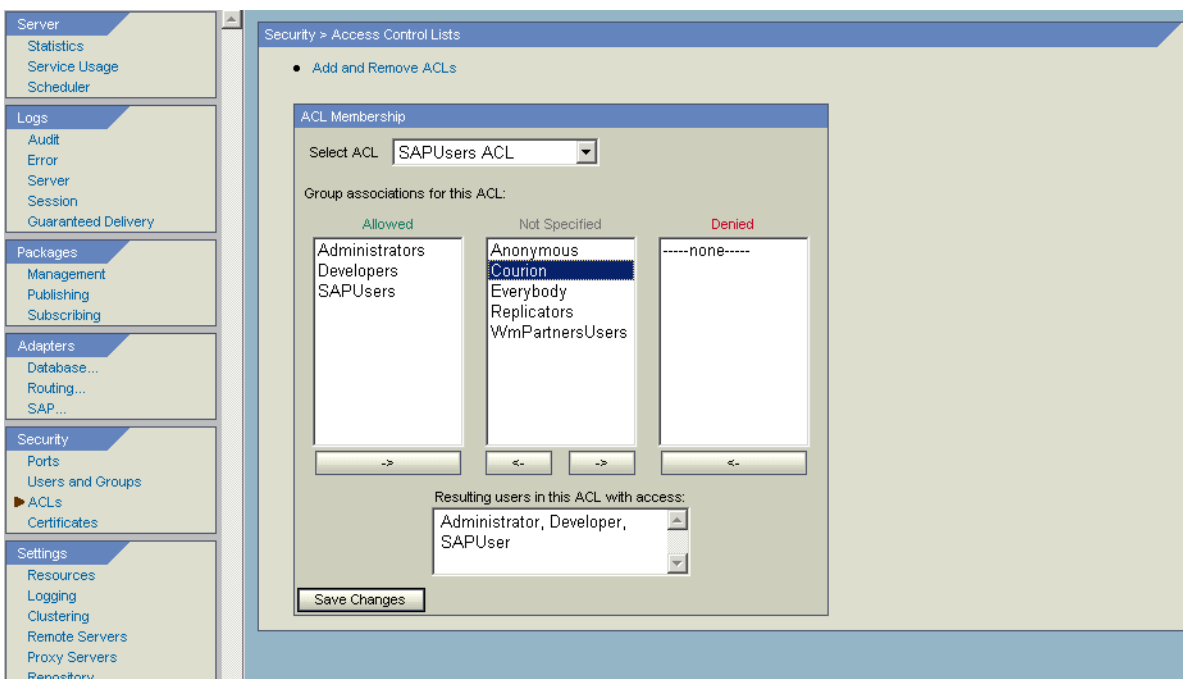


- b. Click **SAVE CHANGES**.

To associate the new Group with the required ACLs:

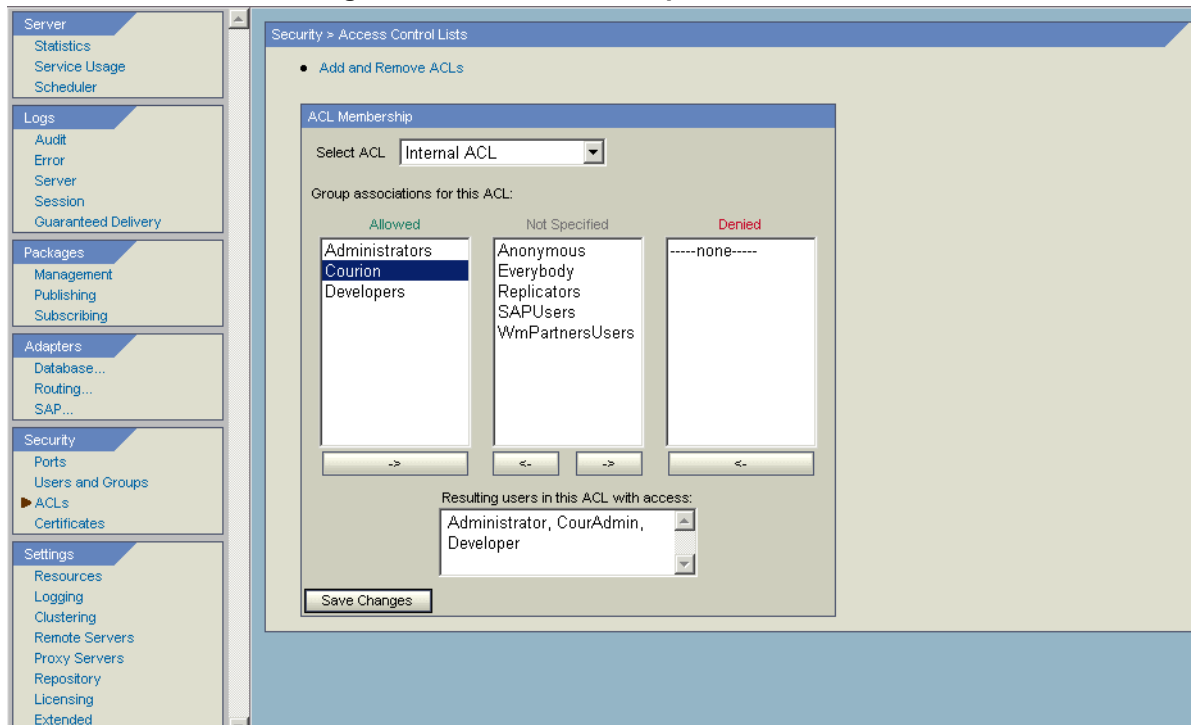
- a. Navigate to **SECURITY > ACCESS CONTROL LISTS**. Select **SAPUsers ACL** from the drop down ([Figure 300](#)). Select **COURION** from the Not Specified list, and click the <- button.

Figure 300: Associate Group to SAPUsers ACL



- b. Similarly for Internal ACL, navigate to **SECURITY > ACCESS CONTROL LISTS**. Select **INTERNAL ACL** from the drop down ([Figure 301](#)). Select **COURION** from the Not Specified list, and click the <- button.

Figure 301: Associate Group to Internal ACL



- c. Click on **SAVE CHANGES**.

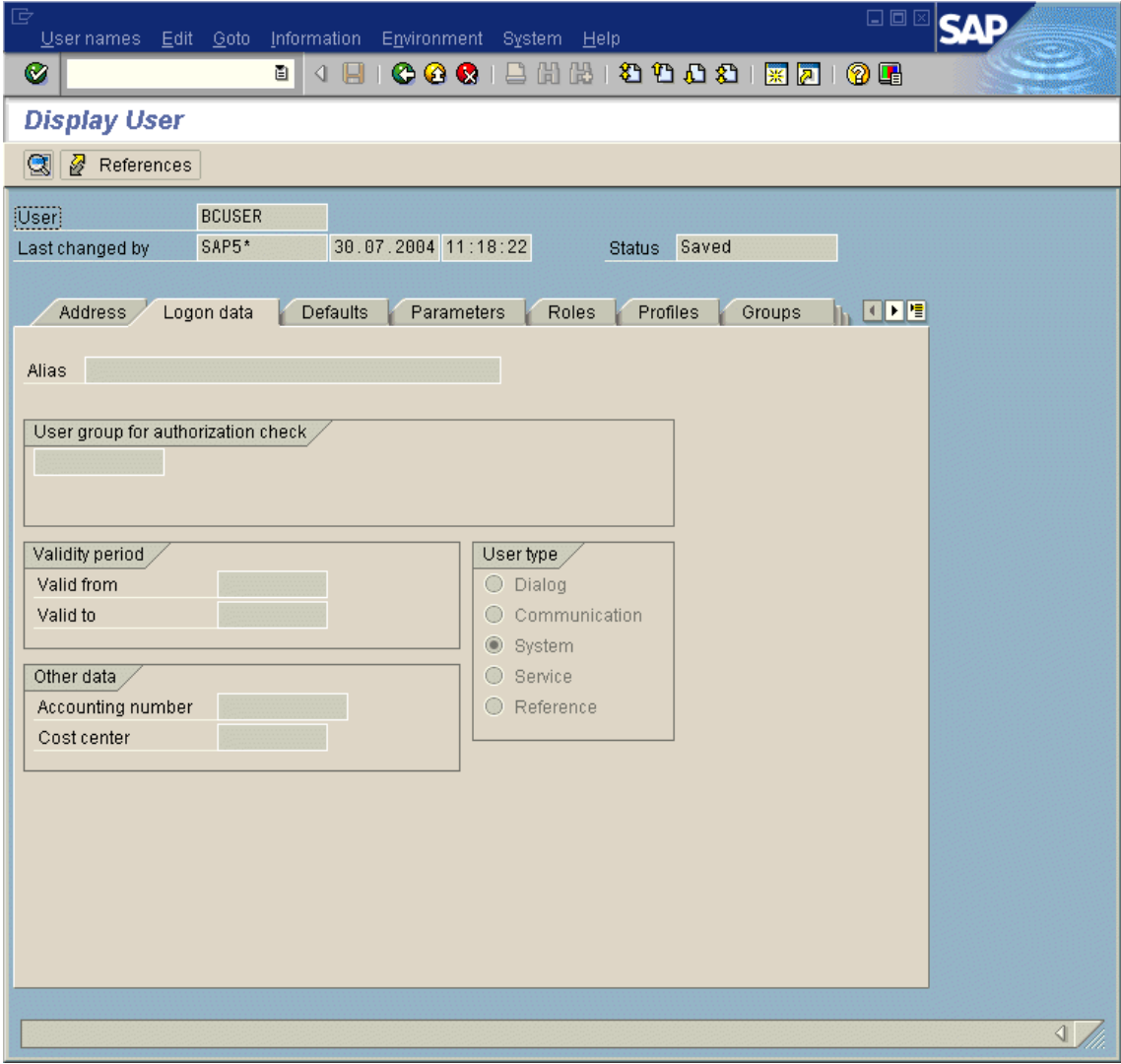
On the SAP system:

- Create a user on the SAP system, and assign the user to the SYSTEM user type to ensure logon concurrency.
- Assign the SAP_ALL and S_USER_ALL profiles to the user.
- Enter the credentials on the Business Connector in the SAP Server definition.

The following information and screens are examples only. For more details, please refer to SAP documentation.

[Figure 302](#) shows a user, “BCUSER,” assigned to the SYSTEM user type.

Figure 302: User Assigned to System User Type



The screenshot shows the SAP 'Display User' transaction for user 'BCUSER'. The interface includes a menu bar (User names, Edit, Goto, Information, Environment, System, Help) and a toolbar. The main area displays user details: 'User: BCUSER', 'Last changed by: SAP5*', '30.07.2004 11:18:22', and 'Status: Saved'. Below this are tabs for Address, Logon data, Defaults, Parameters, Roles, Profiles, and Groups. The 'Address' tab is active, showing fields for Alias, User group for authorization check, Validity period (Valid from, Valid to), and Other data (Accounting number, Cost center). A 'User type' section on the right lists options: Dialog, Communication, System (selected), Service, and Reference.

User	
User	BCUSER
Last changed by	SAP5*
	30.07.2004 11:18:22
Status	Saved

Address Logon data Defaults Parameters Roles Profiles Groups

Alias

User group for authorization check

Validity period

Valid from

Valid to

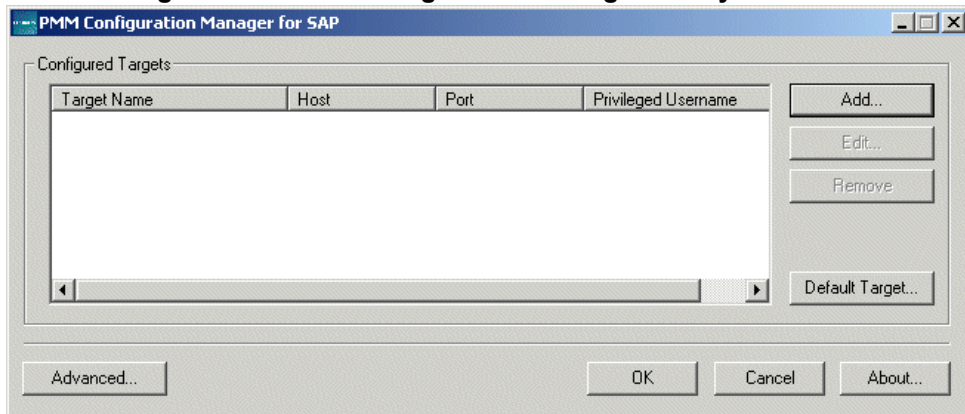
Other data

Accounting number

Cost center

User type

- ☐ Dialog
- ☐ Communication
- ☒ System
- ☐ Service
- ☐ Reference

Figure 304: PMM Configuration Manager for mySAP.com

2. From this dialog box, you can:

- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Edit a target created with an earlier version of the PMM Configuration Manager with the **DEFAULT TARGET** button.
- Obtain the product version number. Click the **ABOUT** button.
- Enable advanced properties. Click the **ADVANCED** button. See [“Advanced Properties” on page 588](#) for details.

When you select the **ADD** or **EDIT** option from the PMM, the Add/Edit Target Configuration dialog box appears.

Figure 305: Add / Edit Target Configuration for mySAP.com

3. Enter the following configuration parameters:

TARGET INFORMATION

- **SAP SYSTEM** — Provide the SAP R/3 server name. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

bXML TEMPLATE FILES

- Template files that are compatible with SAP R/3 version 4.6c are provided with the Core Access Assurance Suite. Optional support is provided to specify template files for non-SAP R/3 version 4.6c. See [“Specifying Template Files for non-SAP R/3 version 4.6c” on page 588](#).

UNLOCK USER BEFORE A PASSWORD RESET

- **BAP_USER_UNLOCK** — By default, the PMM does not unlock user accounts before password resets. The PMM provides this option to enable unlocking of user accounts prior to password resets.
- **Note:** SAP provides three lock types:
 - too many failed logon attempts
 - local administrative lock, and
 - global administrative lock.

Note: The unlock functionality in SAP does not differentiate between the lock types when unlocking a user. If the unlock command completes successfully, the R/3 system returns a message "User SOMEUSER unlocked, if this is permitted in this system." For more information, refer to SAP documentation.

BUSINESS CONNECTOR CONNECTION INFORMATION

- **HOST** — Provide the Business Connector name (either the server name or the IP address)
 - **PORT** — Provide the port for the Business Connector
 - **PRIVILEGED USERNAME** — Provide the user name for a user with password reset privileges.
 - **PASSWORD** — Provide the password for the privileged user
4. Click the **OK** button to save the changes and exit the configuration program.

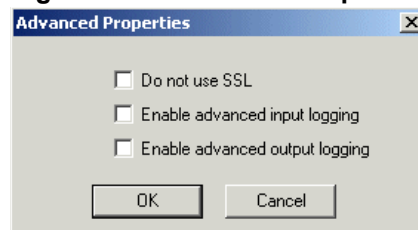
You have configured a target for the mySAP.com PMM.

Advanced Properties

The **ADVANCED PROPERTIES** offers options that you can use for debugging or when changes are made to the Business Connector.

When you click the **ADVANCED** option, the Advanced Properties dialog box appears as in [Figure 306](#).

Figure 306: Advanced Properties



The check box options are not enabled by default.

- **DO NOT USE SSL** — Allows HTTP (non-SSL) connections between the PMM for mySAP.com and the Business Connector. To configure HTTPS (SSL) connections between the PMM for mySAP.com and the Business Connector, see [“Using Multiple R/3 Servers with a Single Business Connector” on page 578](#).
- **ENABLE ADVANCED INPUT LOGGING** — Writes log files to the CourionService directory of the form YYYY_MM_DD-HH_MM_SS-<BAPI>-<USER>.log that contain details of the requests submitted to the Business Connector over an HTTP/HTTPS connection.

Note: Using this option creates a log file that includes secure information such as USERNAME and clear text PASSWORD.

- **ENABLE ADVANCED OUTPUT LOGGING** — Writes log files to the CourionService directory of the form YYYY_MM_DD-HH_MM_SS-<BAPI>-Response-<USER>.log with the complete text returned from a BAPI call.

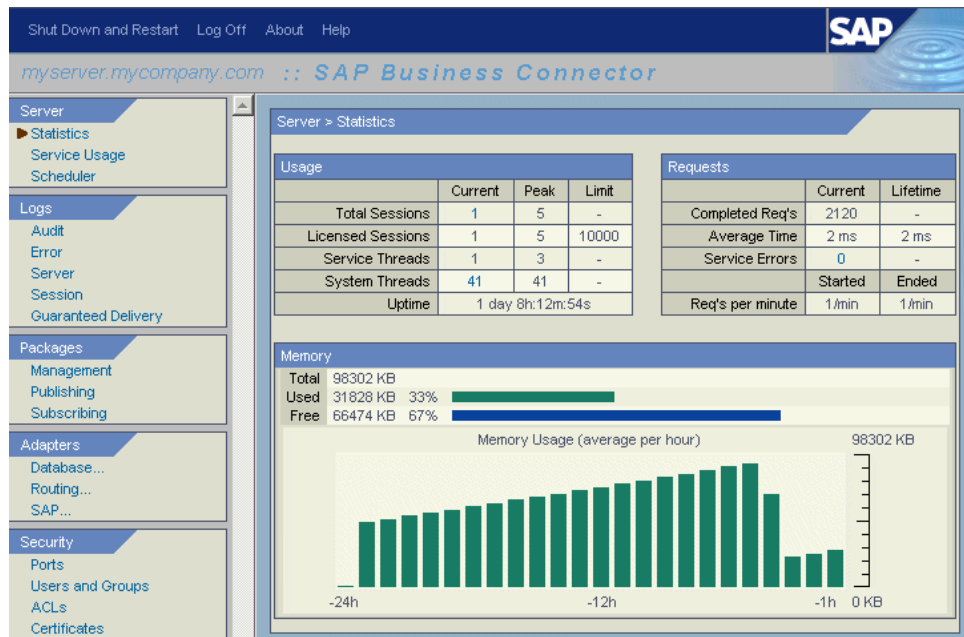
Note: The log files do not contain secure information. However, each reset attempt generates more than ten extra log files in the CourionService directory.

Specifying Template Files for non-SAP R/3 version 4.6c

To generate the template files, please refer to SAP documentation. The following information and screens are examples only.

1. Open the Business Connector interface. See [Figure 307](#).

Figure 307: SAP Business Connector Interface



2. Select Adapters>SAP. This opens a new browser window. Select Lookup. See [Figure 308](#).

Figure 308: SAP Adapters

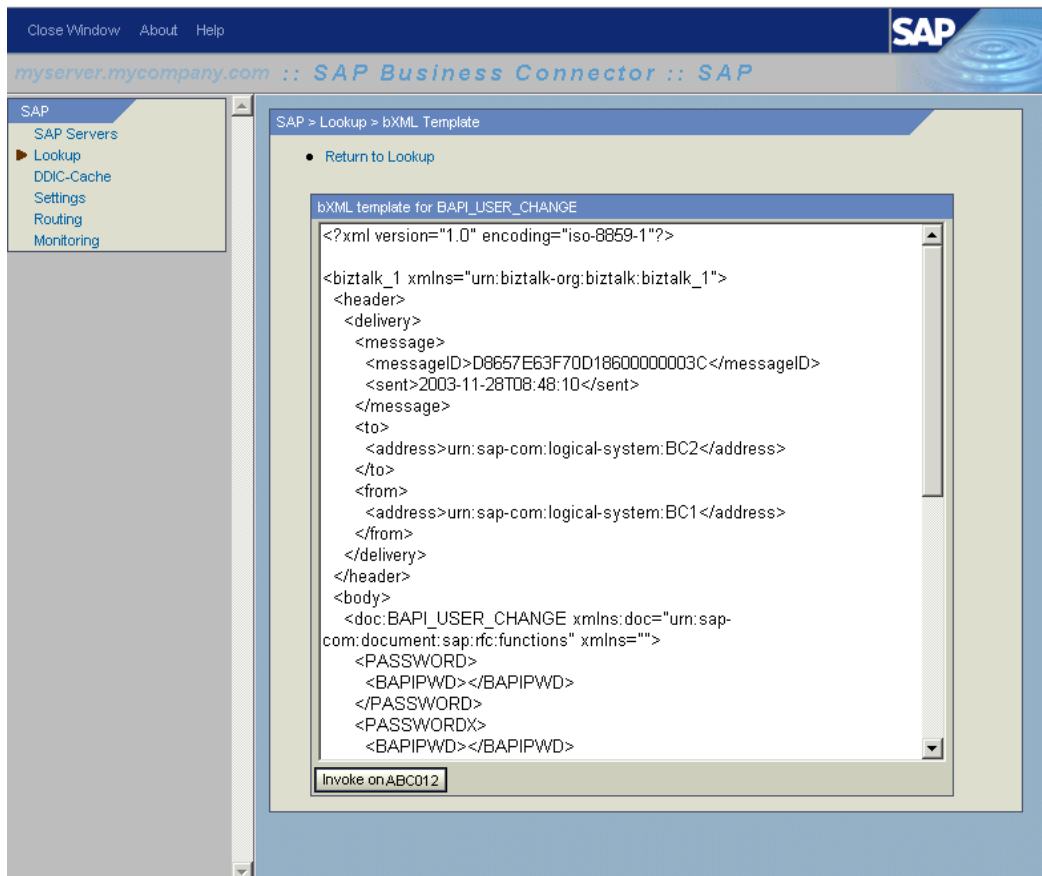
The screenshot shows the 'SAP > Lookup' window. The left sidebar has a tree view with categories: SAP (SAP Servers, Lookup, DDIC-Cache, Settings, Routing, Monitoring). The main content area contains several sections for looking up SAP data:

- RFC Lookup:** Server Name dropdown menu (ABC012).
- Function By Name:** Function Name text field (BAPI_USER_CHANGE), with buttons for Lookup, RFC-XML, and bXML.
- BAPI By Name:** Business Object and BAPI text fields, with buttons for Lookup and bXML.
- Function Search:** Function Name and Group Name text fields, with a Search button.
- Table By Name:** Table Name text field, with a Lookup button.

3. Select the R/3 system for which you want to obtain the template file from the drop down in the RFC Lookup.
4. Type the Function Name in the Function by Name field. C
5. Click the bXML button.

A template file for BAPI_USER_CHANGE is generated. See [Figure 309](#).

Figure 309: bXML Template



6. Copy the contents of the Lookup to a text file and save it in the CourionService directory.
7. Similarly, create template files for SUSR_USER_CHANGE_PASSWORD_RFC, BAPI_USER_EXISTENCE_CHECK, AND BAPI_USER_UNLOCK.
8. In the PMM for mySAP.com, browse to the CourionService directory where you saved the new text files.

User Must Change Password at Next Logon

The **USER MUST CHANGE PASSWORD AT NEXT LOGON** feature gives administrators the ability to force end users to change their passwords the next time they log in after performing a password reset with PasswordCourier. Take advantage of this feature when editing SAP targets. Click the advanced properties button and set the **USER MUST CHANGE PASSWORD AT NEXT LOGON** flag appropriately.

You can use the Password Target Groups and add the new SAP targets to the appropriate groups as explained in *Configuring Workflows with the Core Access Assurance Suite Administration Manager*.

Note: You must add the SUSR_USER_CHANGE_PASSWORD_RFC routing rule on the SAP server (see [Figure 295](#)) when users are not forced to change passwords. It should be configured similarly to the BAPI_USER_CHANGE routing rule. Please see the SAP administrator for details on how to configure this routing rule.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Notes and Warnings

- There is a known problem in some SAP R/3 implementations where a programmatic password reset that violates the R/3 strength rules succeeds, but the user is not able to log in using that new password. There is a known fix for this on the SAP system - refer to SAP Note number 0369761 or contact your SAP customer support representative.
- The Core Access Assurance Suite tries to unlock SAP user accounts regardless of their lock types when a mySAP.com target is configured to unlock accounts before resetting a user's password. If the user account for the password reset is locked and the password reset fails, the user's account unlocks, but the password reset fails when the **UNLOCK USER BEFORE A PASSWORD RESET** is enabled in the PMM target configuration.

Chapter 60: Sun Directory Server — Connector

The Connector for Sun Directory Server is capable of connecting to any LDAP-compliant directory server including the Sun Directory Server and the IBM® Tivoli® Directory Server.

This chapter explains how to configure the Connector for Sun Directory Server:

- [*“Configuring the Connector for Sun Directory Server” on page 594*](#)
- [*“Support for SHA Hashing” on page 600*](#)

Configuring the Connector for Sun Directory Server

The Connector for Sun Directory Server supports the following operations on any LDAP-compliant target including the Sun Directory Server and the IBM Tivoli Directory Server:

- Authentication and query against a LDAP-compliant target
- Create and delete an entry in a LDAP-compliant target
- Add, Change, Create, Enable, Disable, Delete, Verify, and View actions in a LDAP-compliant target.

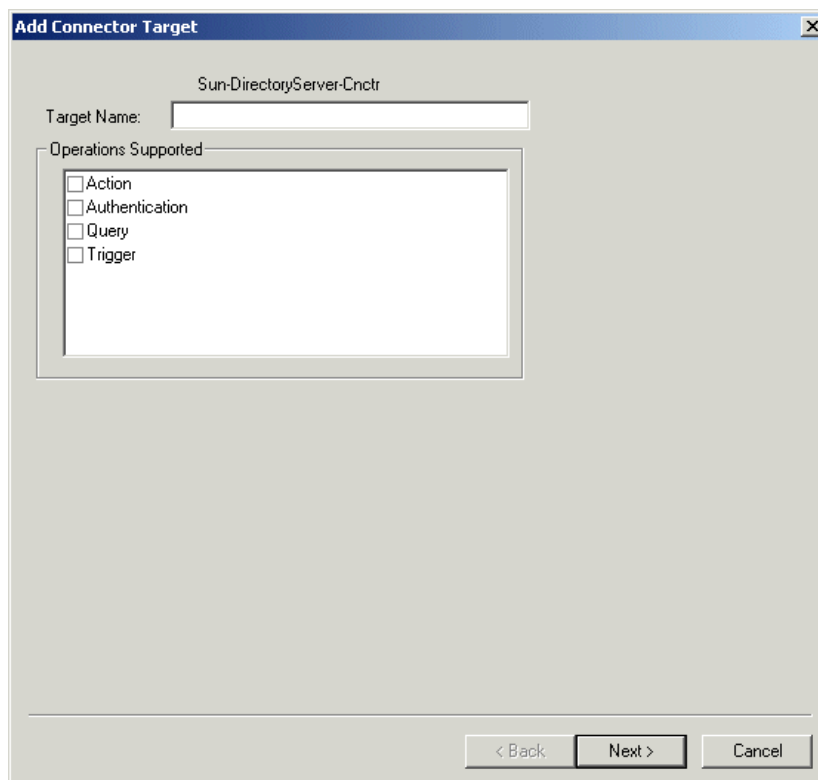
Note: If you have configured a target for this connector for a Core Password or Core Provisioning version previously, you can retain the existing Netscape/iPlanet configuration. If you have not configured the target for Netscape/iPlanet, then use the Sun-DirectoryServer-Cnctr. The functionality of the two connectors is the same.

Follow these steps to add a Sun Directory Server:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Select **SUN-DIRECTORY-SERVER-CNCTR**
3. Click the right mouse button and choose **ADD TARGET....**

The Add Connector Target dialog box appears

Figure 310: Add Sun Directory Server Target



4. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.

5. Select one or more operations.

- Select **ACTION** to enable the Add, Change, Create, Delete, Disable, Enable, Verify, and View actions on a target data source.
- Select **AUTHENTICATION** to use the target data source for authenticating end user access to the provisioning application.
- Select **QUERY** to enable the provisioning application to use queries to find data in the target data source.
- Select **TRIGGER** to allow access to two groups of triggers. These triggers (MVAAAddValue - objectClass and MVARemoveValue - objectClass) add or remove a value from a multi-valued attribute in an object. There are three parameters for each trigger (CN, Attribute and Value). CN is the object(s) to modify. Commas are used to separate entries, so they must be escaped in each individual entry with "^2C". Attribute is the attribute to change. Value is the value to set or remove. Values must match exactly. Triggers are configured on the Trigger Subform in the Administration Manager. See the manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* for details.

6. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 311: Connector Configuration Manager for Sun Directory Server

Connector Configuration Manager for Sun Directory Server

Target Configuration

Directory server:

Directory server port: ☐ Use secure connection

Certificate database:

*Privileged username:

Password:

Search Container Configuration

*Topmost container for performing searches:

* Entries must contain a fully distinguished name

< Back Cancel

7. Enter the following information.

- DIRECTORY SERVER** — Enter the name (or IP address) of the LDAP server on which the provisioning actions are performed.

- b. **DIRECTORY SERVER PORT** — Enter the TCP/IP port number used by the LDAP server to communicate with the connector. The default is 389 for a nonsecure connection or 636 for an SSL connection.

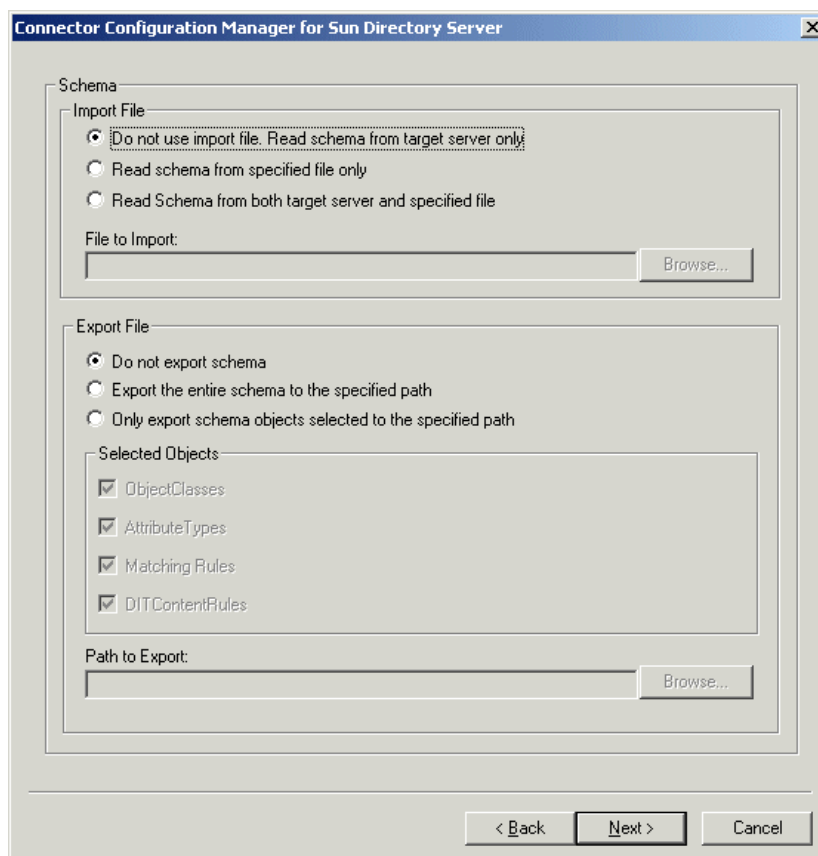
If the SSL option is not enabled on the Sun Directory Server, connection to the server must use a nonsecure port with port number 389.

- c. **USE SECURE CONNECTION** — Check this if SSL are used to secure the traffic.
- d. **CERTIFICATE DATABASE** — If the connection to the Sun Directory Server uses SSL, specify the filename of a p7b file, such as `cert7.db`, that contains certificates used by the LDAP server. The Connector Configuration Manager uses this certificate file to determine if it can trust the server's SSL certificate.
- Note:** This connector now uses the Microsoft WinLDAP API which leverages the Windows Certificate store. Certificates in this folder are not actually used.
- e. **PRIVILEGED USERNAME** — Enter the name that identifies the user who has sufficient rights to add, delete, modify and search the sub-tree of the directory.
- f. **PASSWORD** — Enter the privileged user's password.
- g. **TOPMOST CONTAINER FOR PERFORMING SEARCHES** — Enter the base Distinguished Name (search base) of the container from which queries, such as those made by a custom macro, begin. You can specify multiple search base trees by using a semicolon to separate the Distinguished Names. Use the format "`o=name`", for example, `o=corp.yourDir.com`.

8. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 312: Connector Configuration Manager for Sun Directory Server (2)



9. Enter the following information:

Note: For most configurations, the default settings of **DO NOT USE IMPORT FILE** and **DO NOT EXPORT SCHEMA** are the appropriate settings.

Import File — Selections to control how external schema information is provided to the connector.

- a. **DO NOT USE IMPORT FILE. READ SCHEMA FROM TARGET SERVER ONLY**
- b. **READ SCHEMA FROM SPECIFIED FILE ONLY**
- c. **READ SCHEMA FROM BOTH TARGET SERVER AND SPECIFIED XML FILE**
- d. **FILE TO IMPORT** — The location of the XML file to be imported that contains the additional schema information. See [“Import File Example” on page 598](#) for an example of this file.

Export File — Selections to control how to export existing schema information for the connector.

- a. **DO NOT EXPORT SCHEMA**
- b. **EXPORT THE ENTIRE SCHEMA TO THE SPECIFIED PATH**
- c. **ONLY EXPORT SCHEMA OBJECTS SELECTED TO SPECIFIED PATH**
- d. **PATH TO EXPORT** — The folder directory entry to export the schema information to file.

Note: This feature is not implemented yet.

10. Click **NEXT**.

The Connector Configuration Manager displays the following dialog box:

Figure 313: Connector Configuration Manager for Sun Directory Server (3)

The screenshot shows a dialog box titled "Connector Configuration Manager for Sun Directory Server". Inside, there is a section titled "Create Object Configuration". Below this title, there is a text field labeled "Container for directory entry creation:". Below the text field is a button labeled "Retrieve Objects". Below the button are three dropdown menus: "Object class for account actions:", "Password field for account object:", and "Profile UID field for account object:". Below the dropdown menus is a checkbox labeled "Enforce case-insensitive comparison". At the bottom of the dialog box, there is a note: "* Entries must contain a fully distinguished name". At the very bottom of the dialog box, there are three buttons: "< Back", "Finish", and "Cancel".

11. Enter the following information:

- a. **CONTAINER FOR DIRECTORY ENTRY CREATION** — Enter the Distinguished Name of the container which the provisioning application uses for all actions, including creating and deleting entries and authentication.

Only one container can be entered here.

- b. **RETRIEVE OBJECTS** — Click this button to retrieve the list of objects which can be used for account actions, object class, and account passwords. This list lets you specify the password field to ensure that the provisioning application does not copy it from the Model Account.

The differences between a Profile and an Account are determined by the workflow. Generally a user only has one profile and may have many accounts.

- c. **OBJECT CLASS FOR ACCOUNT ACTIONS** — Select the name of the object class that defines the attributes for the resource entries to be managed by the provisioning application. Typically, the object class is "inetOrgPerson".
- d. **PASSWORD FIELD FOR ACCOUNT OBJECT** — Select the attribute to be used as the account password. For example, userPassword.
- e. **PROFILE UID FIELD FOR ACCOUNT OBJECT** — Select the attribute to be used as the profile UID. For example, uid (user identifier) or cn (common name). The current setting is active only when the Sun Directory Server is used for the IdentityMap.

Note: If you want to store the IdentityMap on the Sun Directory Server (in the LDAP directory), you must extend the LDAP schema to store the IdentityMap. See the manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* for information about how to do this.

- f. **ENFORCE CASE-INSENSITIVE COMPARISON** — If you leave this box unchecked, the LDAP server applies its own matching rules when searching. Otherwise the connector retrieves all related entries (and values) and perform case-insensitive comparison.

12. Click **FINISH**.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Import File Example

The import file is used to provide additional DITContentRules to the schema information to associate object classes with auxiliary objects. To create a DITContentRule the object class OID or Name must be provided along with the auxiliary object name(s) that contain that auxiliary attributes of an object.

The following xml syntax is used to provide this information:

```
<?xml version="1.0" encoding="UTF-8"?>
<ditcontentrules>
  <ditcontentrule>
    <oid></oid>
    <name></name>
```

```
<auxobjects>
  <auxobject></auxobject>
  <auxobject></auxobject>
  <auxobject></auxobject>
</auxobjects>
</ditcontentrule>
</ditcontentrules>
```

To discover the correct auxiliary objects that contains the needed auxiliary attributes, you can use any LDAP browser to export the schema to research the information.

Authentication Configuration

The Sun Directory Server connector supports two methods of authenticating a user:

- Structured queries used with communities
- Native authentication mechanism (LDP binding)

For the Sun Directory Server, the Administration Manager has two additional fields in its authentication configuration form. They are BindUsername and BindPassword. If you select these fields, the provisioning application uses the native query method of authentication.

Note: You can use these attributes for LDAP binding only, not for any other purpose.

Support for SHA Hashing

The Connector for Sun Directory Server supports SHA hashing for passwords in the Add and Create actions and for authentication. Follow these steps to configure SHA hashing for a password after you have configured the connector:

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Configuration Editor
with the “Run as Administrator” privilege.
2. Navigate to the following location:
WMI>CourCnctrFrameworkMgr>CourTarget
3. Locate the connector target in the list.
4. View the AttrNameArray and find the item with the name “PasswordHash”.
5. Note the item number.
6. View the AttrValueArray, find the item number noted above and change its value to SHA (uppercase). This enables password hashing for the Add and Create actions, and for authentication.
7. Stop the CourionService.
8. Restart the Connector Framework Manager.
9. Start the CourionService.

Note: If the connector target is modified from within the Connector Configuration Manager at any point, this manual setting is overridden. If this occurs, perform these steps again to enable SHA hashing.

Chapter 61: Sun Kerberos — PMM

This chapter explains how to configure the PMM for Sun Kerberos:

- [*“Configuring the PMM for Sun Kerberos” on page 602*](#)

Configuring the PMM for Sun Kerberos

The Password Management Module (PMM) for Sun Kerberos lets Core Access Assurance Suite applications reset passwords automatically on systems using the Sun Kerberos protocol.

The correct access key is necessary to run this PMM. For more information on access keys, please contact Core Security.

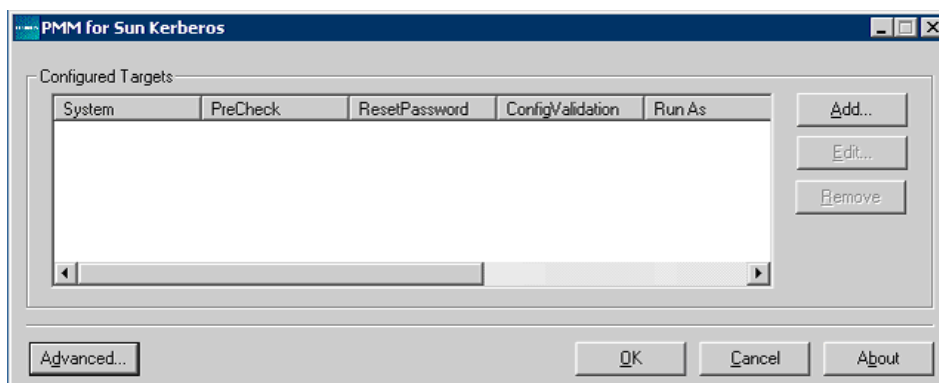
Prerequisites

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

1. From the Start menu, select:
Programs >Core Access Assurance Suite>Password Management Modules>Sun Kerberos
The PMM Configuration Manager for Sun Kerberos appears.

Figure 314: PMM Configuration Manager for Sun Kerberos



2. From this dialog box, you can:
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Edit a target created with an earlier version of the PMM Configuration Manager with the **DEFAULT TARGET** button.

- Obtain the product version number. Click the **ABOUT** button.
- Enable advanced properties. Click the **ADVANCED** button. See [“Advanced Properties” on page 605](#) for details.

When you select the **ADD** or **EDIT** option from the PMM, the Add/Edit Target Configuration dialog box appears.

Figure 315: Add / Edit Target Configuration for Sun Kerberos

- Enter the following target configuration information:
 - TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
 - For all three **COMMAND LINE** fields, enter the following text, as shown in [Figure 315](#):
cscript.exe /nologo /b PMMSunKerberos5.vbs
- Leave the **RUN COMMANDS AS USER** checkbox unchecked.
- Fill in the Configuration Parameters as shown in the table below. Enter the parameter name in the **PARAMETER** text box, then enter the appropriate value in the **VALUE** text box. If the **SECURE ATTRIBUTE** checkbox is selected, you must enter the value in both the **VALUE** and **VERIFY** text boxes. Click **ADD** to move the entry to the list on the right side.

Table 34: Configuration parameters for Sun Kerberos PMM

Parameter Name	Value	Secure Attribute?	Required?
HostServer	Host server name or IP that has the Key Distribution Center (KDC) service.	No	Yes
HostPort	Port number to connect on host server. Used to override default connection type port number. Default to protocol default type.	No	No
ConnectionPrompt	Command prompt to detect to determine command return. Default: #	No	No
ConnectionTimeout	The amount of time (in seconds) before password reset timeout.	No	No
Protocol	Protocol to make to server. Default: sshauto detect Options: raw, telnet, ssh1, ssh2, sshauto	No	No
Encryption	Encryption type to communicate with server. Default: aes Options: any - any suitable encryption des - DES encryption 3des - triple DES encryption aes - AES encryption blowfish - BLOWFISH encryption aes128 - AES128 encryption aes192 - AES192 encryption cast128 - CAST128 encryption	No	No
Authentication	Authentication method to use with server. Default: password Options: password, publickey	No	No
LoginUser	Login name to authenticate with server.	No	No
LoginPassword	Login password used for password authentication	Yes	Option Specific
PrivateKey	Private key used for public key authentication. URL to location of key for user.	No	Option Specific
PrivateKeyType	Type of private key encoding. Default: rsa Options: rsa, dsa	No	No
Passphrase	Passphrase used to access private key	Yes	Option Specific
PWChgUsrName	User with password change rights on key distribution center server. Enter PWChange user name if different from login user.	No	No

Table 34: Configuration parameters for Sun Kerberos PMM

Parameter Name	Value	Secure Attribute?	Required?
PWChgUsrPasswd	User password for user with password change rights on key distribution center server. Enter PWChange user password if different than login password.	Yes	Option Specific

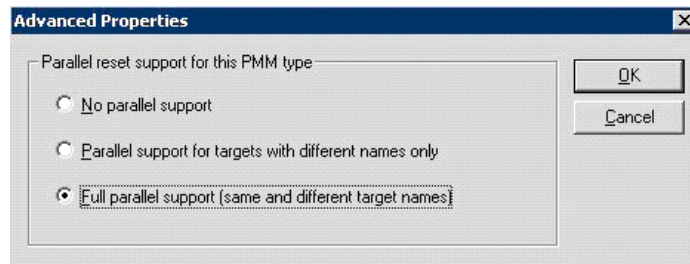
Parameters marked Option Specific are required settings, depending on what Authentication is set to. For Password authentication the Login password is required for the Login User. For Public Key authentication the PrivateKey, Passphrase, and PWChgUserPassword options are required for authentication.

If Authentication is set to Public Key for the Login User then the PWChgUsrPasswd setting is required to authenticate against the Key Distribution Center (KDC). If Authentication is set to Password for the Login User and the password for the Key Distribution Center (KDC) is the same as the login password, then the PWChgUsrPasswd setting is not required.

6. Click **OK** to configure the PMM.

Advanced Properties

When you click the **ADVANCED** option, the Advanced Properties dialog box appears as in [Figure 316](#).

Figure 316: Advanced Properties

For the PMM for Sun Kerberos, the **FULL PARALLEL SUPPORT** option should be selected.

Creating a Workflow for the Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Chapter 62: Sun Solaris — PMM and Connector

This chapter explains how to configure the PMM and Connector for Sun Solaris. It also explains installing and configuring the Sun Solaris agent, required by the PMM.

Major topics are:

- [*“Configuring the PMM for Sun Solaris” on page 608*](#)
- [*“Writing Password Management Scripts” on page 611*](#)
- [*“Installing and Configuring the Sun Solaris PMM Agent” on page 612*](#)
- [*“Configuring the Connector for Sun Solaris” on page 616*](#)

Configuring the PMM for Sun Solaris

The Password Management Module (PMM) for Sun™ Solaris™ enables Core Access Assurance Suite users to reset passwords automatically on Solaris systems.

The correct access keys are necessary to run this PMM. For more information on access keys, please contact Core Security.

Prerequisites

A PMM agent for Sun Solaris must be installed on each Sun SPARC™ machine on which password resets are performed.

Note: The agent must be installed on the SPARC platform. The X86 platform is not supported.

The PMM agent depends on libstdc++.so.6. You can install this library by installing g++ 4.4.3 or higher or by installing libgcc 4.4.3 or higher.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

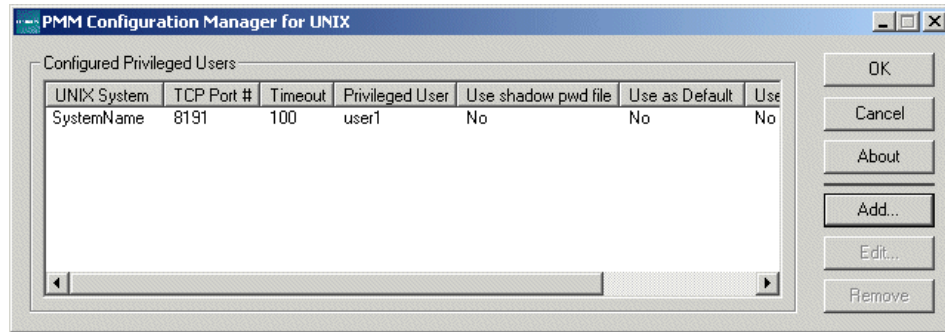
PMM Configuration

The Sun Solaris PMM requires the Sun Solaris PMM agent. If the Sun Solaris PMM agent is not installed, go to [“Installing and Configuring the Sun Solaris PMM Agent” on page 612](#) and install and configure it; then return here.

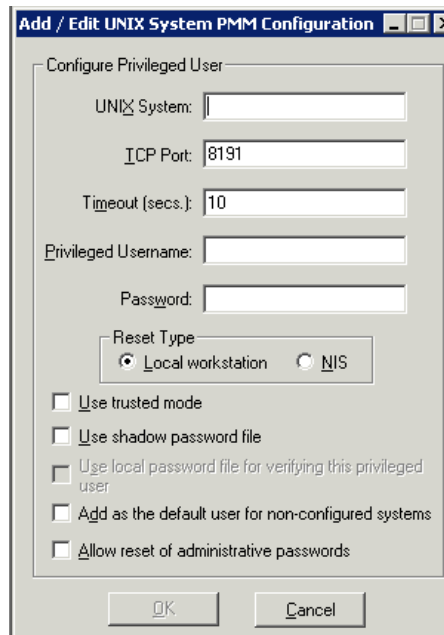
The PMM configuration allows an administrator to specify a user who is used to carry out the password reset process for each Sun Solaris system. The specified users must be valid users on the servers on which the resets are performed. By specifying several users during installation, the PMM can select the user and password pair that is appropriate for the server on which a reset is requested.

Also, you can specify one privileged user name/password pair for all servers not explicitly configured.

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Password Management Modules
2. Click **SUN SOLARIS** and, when prompted, **YES** to begin the configuration. The PMM Configuration Manager appears.

Figure 317: PMM Configuration Manager for Sun Solaris

3. From this dialog box, you can
 - Add a new target. Click the **ADD** button.
 - Edit an existing target. Highlight the target name and click the **EDIT** button.
 - View the targets already configured in the **CONFIGURED TARGETS** list.
 - Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
 - Obtain the product version number. Click the **ABOUT** button.
4. When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 318: Add / Edit UNIX System PMM Configuration for Sun Solaris

5. Enter the Sun Solaris server on which password resets are being performed. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.
6. Enter the TCP/IP port on which the Sun Solaris agent is listening. The default is 8191.
7. Enter the amount of time (in seconds) before password reset timeout in the **TIMEOUT (SECS)** field. The default value for this field is 10 seconds.

8. Enter the name of the privileged user.
Note: The privileged user configured requires no special privileges; the account is only used to activate the password reset executed by the agent software.
9. Enter and verify the password for the privileged user.
10. Determine the reset type to be performed and select “Local Workstation” or “NIS” as appropriate.
11. If **LOCAL WORKSTATION** is checked and a shadow password file is being used by the Sun Solaris system to authenticate users, check the **USE SHADOW PASSWORD FILE** check box.
12. If NIS is chosen and the privileged user exists in the local database and not in the NIS map, check the **USE LOCAL PASSWORD FILE FOR VERIFYING THIS PRIVILEGED USER** check box. Additionally, if the local database where the privileged user’s password file uses a shadow file, check the **USE SHADOW PASSWORD FILE** check box.
13. Determine if this user is to be the default user for all servers not specifically configured in the PMM Configuration Manager. If it is, check the **ADD AS THE DEFAULT USER FOR UNCONFIGURED SYSTEMS** check box.
14. If password resets of users with a UID or GID of zero is allowed, click in the **ALLOW RESET OF ADMINISTRATIVE PASSWORDS** check box.
15. If the password file is stored in a shadow file, check the **USE SHADOW PASSWORD FILE** check box.
16. Click the **OK** button to save the configuration.
17. If desired, continue to configure additional users for other servers.
18. Click the **OK** button in the PMM Configuration Manager for Sun Solaris to save the changes and exit the configuration program.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Access Assurance Suite Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Writing Password Management Scripts

The PMM for Sun Solaris has the ability to run a sequence of UNIX shell commands to perform a password reset. This allows the PMM for Sun Solaris to reset any password which has an administrative password reset available via the UNIX shell.

The Sun Solaris agent reads a specialized script language. The syntax of the language is as follows:

- S N send-string - Send 'send-string' to a pseudo terminal (pty) and pause for N number of seconds before continuing. The send string can contain any of the following substitution macros:
 %u - The user name to be reset
 %p - the plain text password
 %e - the encrypted password
- V N verify-string - Verify that 'verify-string' is found in the output from the pty after waiting N number of seconds for a response and continue when a response is received. The verify string can contain any of the substitution macros described in the send command. It is necessary to have a verify string at the end. If the final verify command isn't received, the end user receives a failure message.
- ; comment-string - A comment string. Comments must be alone on a line. Commands cannot have trailing comments.

Use a scripting language such as Perl or shell script to write a script that performs a password reset.

The following is an example of a script that uses a custom Perl script to reset a user's password:

```
; Send to launch custom reset script
s 2 perl password_reset_cmd %u %p
; Verify successful message
v 2 "Password reset was successful"
```

Note: Arguments to the “s” and “v” commands must be enclosed with quotation marks.

To tell the PMM for Sun Solaris agent to use the script for performing resets, go to the directory where the agent was installed and locate the pxy_def file. Open the file with a text editor and add the following line:

- SCRIPT_NAME:pwd.scr

where pwd.scr is the name of the created script file.

For the change to take effect, start and stop the agent.

Installing and Configuring the Sun Solaris PMM Agent

A PMM agent for Sun Solaris must be installed on each Sun SPARC™ machine (running Solaris 6.0 or higher) on which password resets are performed.

Note: The agent must be installed on the SPARC platform. The X86 platform is not supported.

The PMM agent depends on libstdc++.so.6. You can install this library by installing g++ 4.4.3 or higher or by installing libgcc 4.4.3 or higher.

Installing the Agent

The PMM agent runs as a daemon on the UNIX machine. Table 35 describes the agent installation components included with the PMM for Sun Solaris.

Table 35: PMM Agent Components for Sun Solaris

PMM for Sun Solaris agent files	pwdcour_unixpxy pxy_def install uninstall
PMM for Sun Solaris agent tar file	unixsol.tar

1. Copy the tar file for the Sun Solaris system from the UNIX folder located in the directory where the Core Access Assurance Suite is installed to a temporary directory on the Sun Solaris machine on which you want to install the agent.
2. Log on to the machine as a superuser and proceed to the directory where the tar file was placed.

Note: The installation fails if it is not performed by a user with superuser privileges.

3. Extract the installation files for the platform using the following command:

```
tar -xvf unixsol.tar
```

This creates and places all of the install files inside of a subdirectory named courion.

4. Change to that directory and then execute the installation shell script by typing `./install`.
5. Follow the prompts and answer the questions needed for installation. The following information is required:
 - The install directory for the agent (the default is `/usr/local/courion`)
 - The password file (the default is `/etc/passwd`)
 - The library path to libstdc++.so.6 (the default is `/usr/local/lib`)
 - Whether or not NIS is being used (if NIS is being used, the agent must be installed on the same machine as the NIS master.)

- If NIS is being used, the following information is required:

- The default path to yp database directory (/var/yp)-
- The path to make (/var/yp)
- The TCP/IP port available to the agent (default is 8191)

Agent installation is complete when these four steps are performed. If any changes need to be made, make them before finishing the last step (specifying the TCP/IP port).

After it is installed, launch the agent by rebooting or by executing the following command:

```
/etc/rc3.d/S99pwdcour_unixpxy start
```

Configuring the Agent

After the agent is installed on the Sun Solaris host, a configuration file is placed in the agent's installation directory (the default installation directory is /usr/local/courion). The configuration file is called pxy_def. This file has several parameters that control the agent's actions and configuration. A text editor, such as vi, can be used to change the pxy_def file. Table 36 provides a description of the parameters.

Table 36: PMM agent for Sun Solaris Configuration Parameters

Parameter Syntax	Description
INST_DIR: <i>install_dir</i>	This is the directory in which the agent is installed. By default, the agent is installed in /usr/local/courion.
LOG_FILE: <i>log_file</i>	This is the name of the file to which the agent logs all messages. If the directory is omitted, the log_file is automatically created in the directory specified by INST_DIR. If this parameter is omitted, the default value is pxy.log.
LOG_LEVEL: <i>n</i>	Log messages have a log level 'n' associated with them. The log level ranges from 0-2. Depending on the log level you specify in the pxy_def file, the PMM displays log messages for the log level specified and below. For example, if you specify log level 1, then the log file includes messages with log level 0 and 1. To see more log messages, increase the log level in the pxy_def file. By default, the log level specified is 0.
MAKE_DIR: <i>make_directory</i>	This is the directory in which the make command can be found. It is used to rebuild the NIS password map. If the directory is omitted, the default is /var/yp. Note: This argument is only relevant when the PMM is configured for native NIS reset support.
NIS_YMAKE_CMD: <i>make_cmd</i>	This the command line used to rebuild and/or push the NIS password map. If it is omitted, the default command is: cd%s;%s/make passwd NOPUSH=TRUE. The first "%s" is a substitution macro for the value specified by Y_DIR. The second "%s" is a substitution macro for the value specified by MAKE_DIR. Note: This argument is only relevant when the PMM is configured for native NIS reset support.

Table 36: PMM agent for Sun Solaris Configuration Parameters (Continued)

Parameter Syntax	Description
NIS_UPMAKE_RESP: <i>response</i>	This is the expected response from the command used to rebuild and/or push the NIS password map. If this value is omitted, the default response is “updated passwd.” Note: This argument is only relevant when configured for native NIS reset support.
NIS_PASSWORD_FILE	This parameter is used to specify the path to the NIS password file on the local machine. It is necessary to use this file when NIS password files that are not /etc/passwd are being used.
PASSWORD_FILE: <i>passwd_file</i>	This represents the fully qualified file name of the password file against which users are validated and native workstation and/or NIS resets are performed. If the file is omitted, the default is /etc/passwd.
PWD_ERR_MSG: <i>err_msg</i>	This is a custom error message displayed to the user when an error occurs during a password reset. If it is omitted, a technical error description is displayed.
SCRIPT_NAME: <i>script_file</i>	This is the name of the script file to run for resets. For more information on scripts, see “Writing Password Management Scripts” on page 611 . If this parameter is omitted, a native password reset (either workstation or NIS) is performed.
SHDW_FILE: <i>shadow_file</i>	This is the fully qualified file name of the shadow file against which users are validated and native workstation resets are performed. This value is consulted if the PMM Configuration Manager is configured with the “use shadow password file” check box checked. If it is omitted, the default is /etc/security/shadow.
SVR_NAME: <i>server</i>	This represents the host name of the server on which the agent is installed. There is no default value. This value must be valid.
SVR_PORT: <i>port_number</i>	This is the TCP/IP port number on which the agent listens for incoming requests. There is no default value. The port number specified here must be the same as the one used during PMM configuration. This value must be present.
VALIDATION_USER: <i>username</i>	This represents the user name of the user authorized to perform password resets via the PMM for Sun Solaris agent. This user name must match the privileged user configured for this server on the machine running on the Connector Framework Manager. If this parameter is omitted, the default value is root. Note: The privileged user configured requires no special privileges, the account is only used to activate the password reset executed by the agent software.
YP_DIR: <i>yp_dir</i>	This is the directory where the NIS password file exists. If it is omitted, the default value is /var/yp. Note: This argument is only relevant when the PMM is configured for native NIS password reset support.

Starting and Stopping the Agent

For any changes to take effect, stop and then start the agent using the startup script. To start the PMM agent, run the startup script with the argument **START**. Run the script with the **STOP** argument to stop the agent.

- To start: `/etc/rc3.d/S99pwdcour_unixpxy start`
- To stop: `/etc/rc3.d/S99pwdcour_unixpxy stop`

Displaying the Version Information

To output the version of the proxy, execute the following command from the UNIX prompt:
`/usr/local/courion/pwdcour_unixpxy -v`

This outputs the version information to the command window, e.g. 7.50.00.113

There is not an option in the `/etc/pwdcour_unixpxy` file to output the version information; you have to run it directly from the install directory (default for AIX is `/usr/local/courion`).

The default install directory is the same for each platform the proxy is installed on (`/usr/local/courion`).

Uninstalling the Agent for Upgrading

To upgrade the PMM agent for Sun Solaris, uninstall the previous agent and then install the new agent. The uninstall script deletes all files in the installation directory. Therefore, the present working directory must be a directory other than the installation directory.

To uninstall the PMM agent for Sun Solaris, execute the uninstall script by typing
`<installdir>/uninstall.`

Note: Before beginning the uninstall process, backup the `<installdir>/pxy_def` to another directory, where `<installdir>` is the installation directory, typically `/usr/local/courion`. Also backup the reset script file to another directory if scripted resets are being used.

1. Follow the prompts and answer the questions. It is necessary to know the install path.
2. After untarring the distribution files for the new PMM for Sun Solaris agent, install the new agent by following the steps outlined in [“Installing and Configuring the Sun Solaris PMM Agent” on page 612](#).
3. Merge custom entries from the backed up `pxy_def` file into the new `<installdir>/pxy_def` file.
4. Restore the backup reset script to the desired directory. Make sure the new `pxy_def` file refers to that script.

Configuring the Connector for Sun Solaris

The PMM for Sun Solaris supports the following operations on a target:

- Add, Change, Create, Delete, Disable, Enable, Verify, and View
- Authentication

Prerequisites

ActivePerl must be installed on each server in which the Connector Framework or Connector Framework Manager is installed. See [“Installing ActivePerl” on page 695](#) for information on installing ActivePerl. Reboot the server after you have installed ActivePerl.

Scripts that Support Provisioning on Sun Solaris Systems

Table 37 shows the scripts and connection methods you can use with Sun Solaris systems.

Table 37: Scripts that Support Provisioning on Sun Solaris Systems

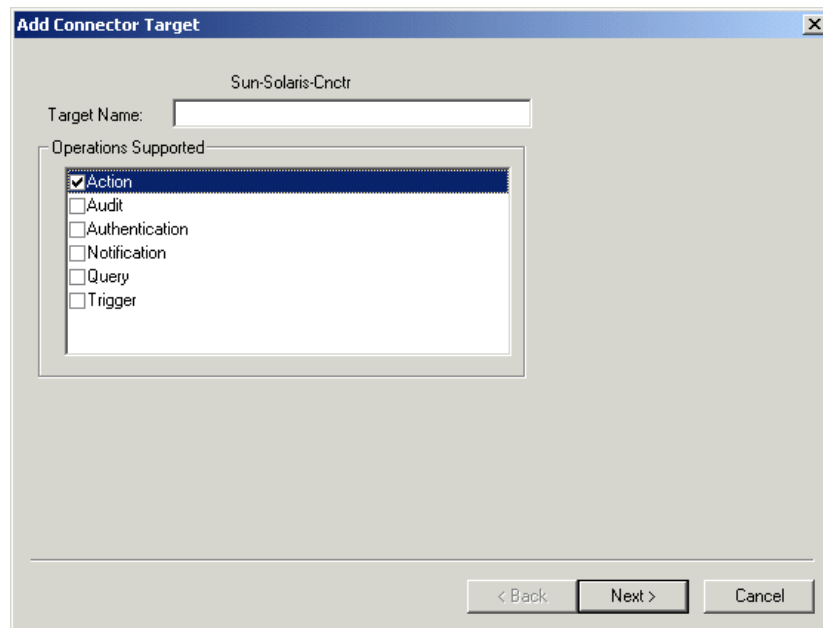
Script	Connection Method
<code>solssh.pl</code>	Standard, using SSH
<code>solssh_sudo.pl</code>	Standard, using SSH with the <code>sudo</code> command

Note: The `sudo` command can assign a specific user account with minimum privileges, other than root, on the Sun Solaris system to perform provisioning actions.

Note: You may need to modify these scripts for your customized UNIX environment.

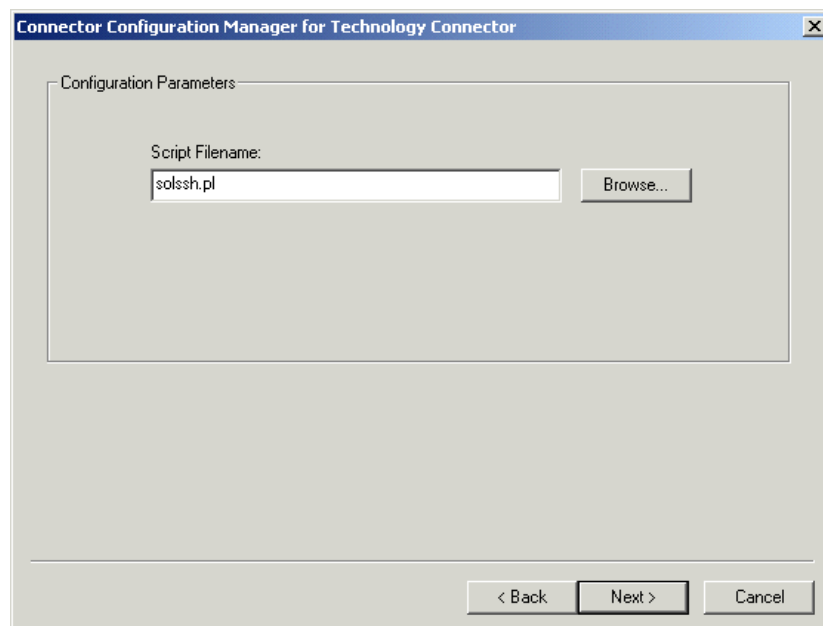
Connector Configuration

1. From the Start menu, select:
Programs>Core Access Assurance Suite>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **SUN-SOLARIS-CNCTR**, and click **OK**.
3. Select **SUN-SOLARIS-CNCTR**
4. Click the right mouse button and choose **ADD TARGET....**
The Add Connector Target dialog box appears.

Figure 319: Add Sun Solaris Target

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. Select **ACTION** to enable all operations on the target.
Select **AUTHENTICATION** to use the target data source for authenticating end user access to the Core Access Assurance Suite.
- NOTE:** Other operations that appear in this dialog box are not supported.
7. Click **NEXT**.

The Configuration Manager screen for Technology appears.

Figure 320: Connector Configuration Manager for Sun Solaris

8. The default `solssh.pl` script providing the functionality for performing connector operations is entered for the **SCRIPT FILENAME**. If you want to use a different script, browse to the location and select the name of that script. Click the **NEXT** button.

The second window of the Connector Configuration Manager for Sun Solaris technology appears.

Figure 321: Connector Configuration Manager for Sun Solaris (2)

9. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks (“*”) for security.

SSH Parameters:

- **ROOT PASSWORD** — (Applies to the `sol.pl` and `solssh.pl` scripts only.) This is the password value of the super user. Use this configuration parameter only if you do not want to connect to the server directly as "root" but as a normal user. In that case, the root password value is used to change a normal user to become the super user to execute commands sent from the provisioning application. To connect directly to the Sun™ Solaris™ server as "root", make sure the SSH server is configured to set the "PermitRootLogin" option to "yes."
- **SSH AUTHENTICATION METHOD** — Two authentication methods are supported for SSH: password authentication and public key authentication. Password authentication is the default value, or you can enter `password` to specify this value. Enter the value `publickey` to use public key authentication.
- **SSH CIPHER TYPE** — The cipher type used to encrypt the session. The three supported cipher types are: 3DES, AES and Blowfish. Enter the value `3des` for 3DES cipher type; `aes` for AES cipher type; and `blowfish` for Blowfish

cipher type. If you do not configure a value for the cipher type, the Connector for Sun Solaris negotiates with the SSH server to select the appropriate cipher to use for encrypting the session.

- **SSH PRIVATE KEY** — The full path of private key file of the SSH User. The path must be in one of these formats:

drive:\\yourdir\\your-private-key-file

or

drive/yourdir/your-private-key-file

This private key file is generated using the SSH key generator tool on the SSH server. Make sure the public key of the same type (RSA or DSA) of this user is in the `authorized_keys` file for it to work properly. This configuration parameter is only required if the authentication method is public key authentication.

- **SSH PRIVATE KEY TYPE** — Specify the type of the private key: RSA or DSA. The default key type is RSA or you can enter the value `rsa`. To specify that the private key is a DSA key, enter the value `dsa`.
- **SSH PRIVATE KEY'S PASSPHRASE** — The passphrase of the private key. If the private key provided is protected by a passphrase, then enter that passphrase. Otherwise, leave it blank.
- **SSH SERVER** — The Sun Solaris server that has SSH server installed.
- **SSH USER** — The account name used to connect to the Sun Solaris server.
- **SSH USER'S PASSWORD** — The password of the SSH User. This configuration is only required if the authentication method is a password authentication.

10. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Courion web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 63: Sybase Adaptive Server Enterprise — PMM and Connector

This chapter explains how to configure the PMM and Connector for Sybase® Adaptive Server® Enterprise:

- [*“Configuring the PMM for Sybase Adaptive Server Enterprise” on page 622*](#)
- [*“Configuring the Connector for Sybase Adaptive Server Enterprise” on page 628*](#)

Configuring the PMM for Sybase Adaptive Server Enterprise

The Password Management Module (PMM) for Sybase ASE enables Core Server applications to automatically reset passwords on the Sybase Adaptive Server. The PMM for Sybase ASE is installed with the Core Server Core Server.

The PMM for Sybase ASE requires an access key. For information about the access key, please contact Core Server.

Prerequisites

Microsoft Open Database Connectivity with ODBC Admin Services must be enabled.

The PMM target you define during PMM configuration must also be defined in the PMM Gateway connector. You must configure the target before defining it in the PMM Gateway Connector, although you can access the PMM configuration from within the PMM Gateway Connector configuration. Using the PMM Gateway connector is explained in [“Using the PMM Gateway Connector to Define PMM Targets” on page 61](#).

PMM Configuration

DSNs identify a data source so the Core Server can make connections to the database to issue password reset commands. Once the reset is complete, the software closes the connection to the database. This process occurs for every database reset.

The target DSN contains the information necessary to make an ODBC connection to a database server. During target configuration, information about database driver(s) is required, as well as specified user name(s) that have sufficient rights to execute database password reset commands. The Sybase ASE Driver Setup asks for information including, but not limited to:

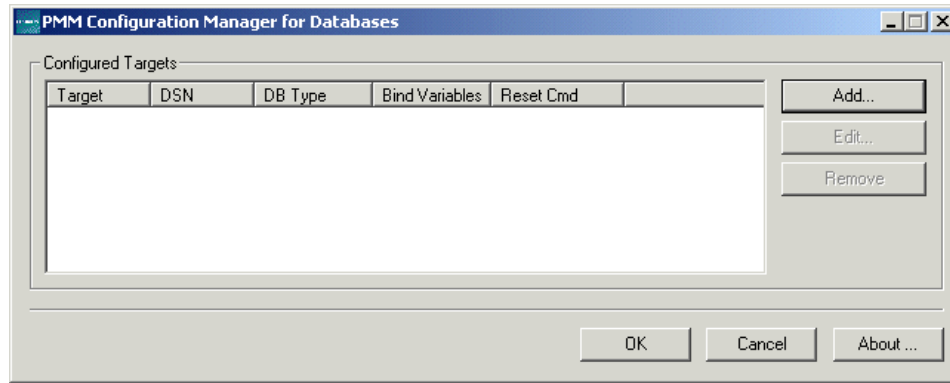
- DSN
- Description (of the DSN)
- Server
- Database name

Note: If the PMM is not configured using "Advance Mode," then the privileged user supplied in the target configuration must be able to execute the "sp_password" command, besides having the ability to open a connection to the database server to perform a password reset.

Note: Avoid using "ODBC" in the DSN because doing so can result in an error message.

To configure a DSN using the PMM for Sybase ASE:

1. From the Start menu, select:
Programs>Core Server Core Server>Password Management Modules>Sybase.
The Configure PMM for Databases dialog box displays.

Figure 322: PMM Configuration Manager for Sybase ASE

2. From this dialog box, you can

- Add a new target. Click the **ADD** button.
- Edit an existing target. Highlight the target name and click the **EDIT** button.
- View the targets already configured in the **CONFIGURED TARGETS** list.
- Remove a target. Highlight the target name and click the **REMOVE** button. Click **YES** when the interface prompts you to confirm that you want to remove the target.
- Obtain the product version number. Click the **ABOUT** button.

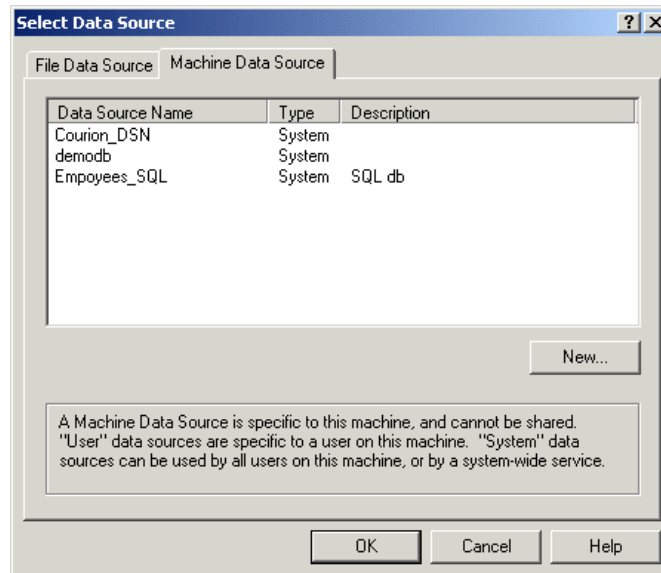
When you select the Add or Edit option, the Add/Edit Target Configuration dialog box appears.

Figure 323: Add/Edit Target for Sybase ASE

3. **TARGET NAME** — Enter the target name that uniquely identifies the configuration information. You need to use this same name when you configure the target in the PMM Gateway Connector configuration.

4. **RESET PASSWORD COMMAND** — The default command for a reset is:
`sp_password "%adminpwd", "%pwd", "%user"`
5. To set the Data Source, click the **SELECT DSN...** button.
 The Data Source Name screen displays (not shown here).
6. Choose the **MACHINE DATA SOURCE** tab.
 The Machine Data Source dialog box appears.

Figure 324: Machine Data Source



7. On the Machine Data Source tab, select a System Data Source from the available list or define a new data source.

To select an existing data source:

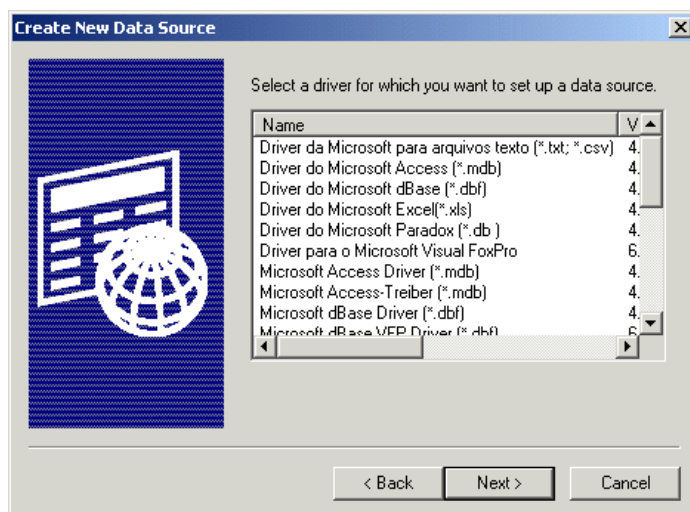
- a. Click on the appropriate DSN target in the **DATA SOURCE NAME** column and click the **OK** button.
- b. The Configure PMM for Databases dialog displays the target in the **DATA SOURCE NAME** field. Go to step 8.

To define a new data source:

- a. Click the **NEW** button.
 The Create New Data Source dialog appears.

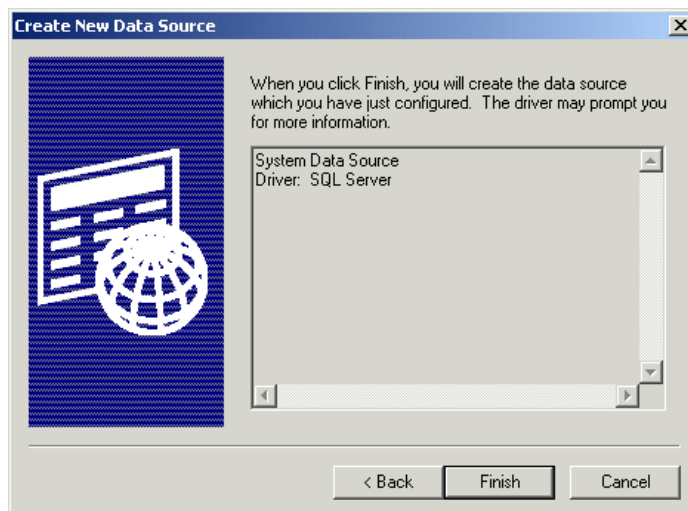
Figure 325: Create New Data Source

- b. Select the **SYSTEM DATA SOURCE** option and click the **NEXT** button.

Figure 326: Data Source Driver Selection

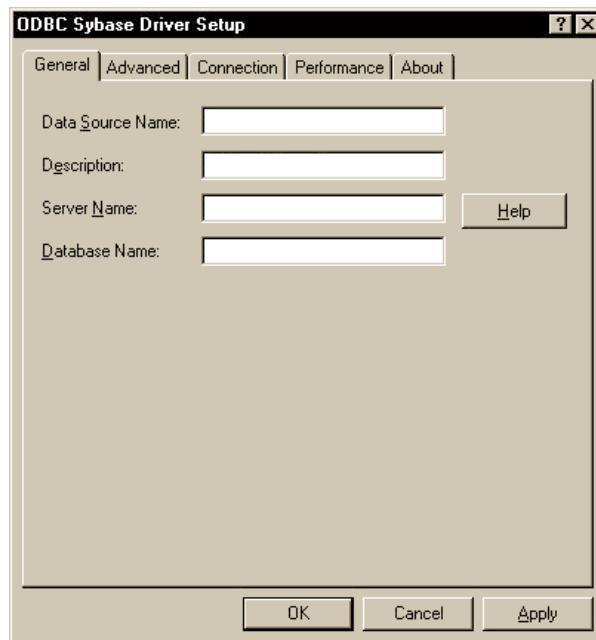
- c. Scroll through the resulting list of data source drivers and select the appropriate Sybase driver, then click the **NEXT** button.

The Create New Data Source Summary screen appears.

Figure 327: Create New Data Source Summary

- d. Click **FINISH**.

The ODBC Sybase Driver screen for Sybase appears.

Figure 328: ODBC Sybase Driver Setup

- e. Configure the data source as needed.

After you configure the DSN, the Configure Database Targets dialog displays the newly-created DSN in the **DATA SOURCE NAME** field.

8. Type the administrator username and password into the corresponding fields to authenticate the administrator for the DSN.
9. Click the **ADD** button to add the DSN to the defined targets list at the bottom of the dialog.

Repeat this procedure for each data source on which you want password reset commands executed.

Creating a Workflow for a Target

After configuring one or more targets for the PMM, use the Administration Manager on the provisioning platform or the customization manager on the classic platform to define target configurations for use in password reset workflows. The manual *Configuring Workflows with the Core Server Administration Manager* explains how to do this on the provisioning platform and the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* explains how to do this on the classic platform.

Sybase Password Limitations

Although Sybase SQL Anywhere passwords cannot start with a number, the passwords can contain numbers. Sybase Adaptive Server Enterprise Edition passwords must contain at least six characters. For more Sybase information, please see the Sybase documentation.

Configuring the Connector for Sybase Adaptive Server Enterprise

The Connector for Sybase ASE supports the following operations on a target: Add, Change, Create, Delete, Disable, Enable, Verify, and View.

Sybase ASE Data Source Configuration

You need to configure a data source using the “Sybase ASE OLE DB Configuration Manager” (an optional installation component of the Sybase client accessed via Start – All Programs – Sybase – OLE DB Provider – Configuration Manager). Create a separate data source for each database on the server that requires provisioning actions.

The Connector for Sybase ASE only assigns the user as a member of the “current” database as defined by the data source configuration. During a Create, Add or Change action, the dbname attribute only sets the “default database” for the user. For example, using the configuration shown in figure [Figure 329](#), a workflow using the change, create, or add actions would assign the new user to the “Employees” database on the “Acme” server. The default database (dbname) is configurable.

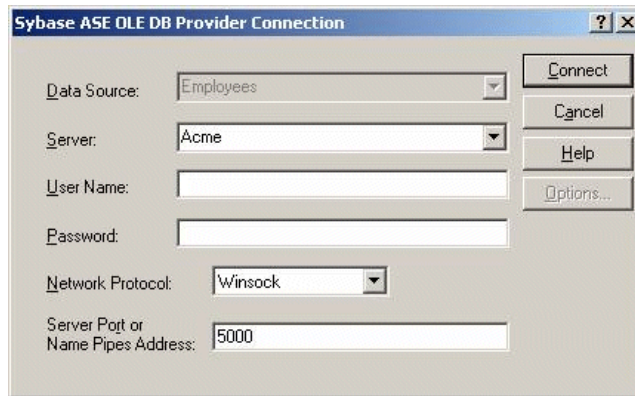
Figure 329: Sybase ASE Data Source Configuration

The screenshot shows the "Sybase ASE OLE DB Provider Setup" dialog box with the "General" tab selected. The fields are as follows:

- Data Source Name: Employees
- Description: (empty)
- Server Name: Acme
- HA Server Name: (empty)
- Database Name: Employees
- Network Protocol: Winsock (dropdown)
- Server Port or Name Pipes Address: 5000
- HA Server Port or Name Pipes Address: (empty)
- Sybase LDAP Schema:
 - ☐ Use Sybase LDAP Schema
 - Sybase LDAP URL: (empty)
 - Sybase Server Name: 389
 - ☐ Use LDAP HA Failover Server

Buttons at the bottom: Test Connect, OK, Cancel, Apply, Help.

Although not required, Core Security recommends that you test the connection to the Sybase Server. Click the **TEST CONNECT** button and the Sybase ASE OLE DB Provider Connection screen appears, as shown in [Figure 330](#).

Figure 330: Sybase ASE Test ConnectionThe image shows a Windows-style dialog box titled "Sybase ASE OLE DB Provider Connection". It contains several input fields: "Data Source:" with a dropdown menu showing "Employees"; "Server:" with a dropdown menu showing "Acme"; "User Name:" and "Password:" as empty text boxes; "Network Protocol:" with a dropdown menu showing "Winsock"; and "Server Port or Name Pipes Address:" with a text box containing "5000". On the right side, there are four buttons: "Connect", "Cancel", "Help", and "Options...".

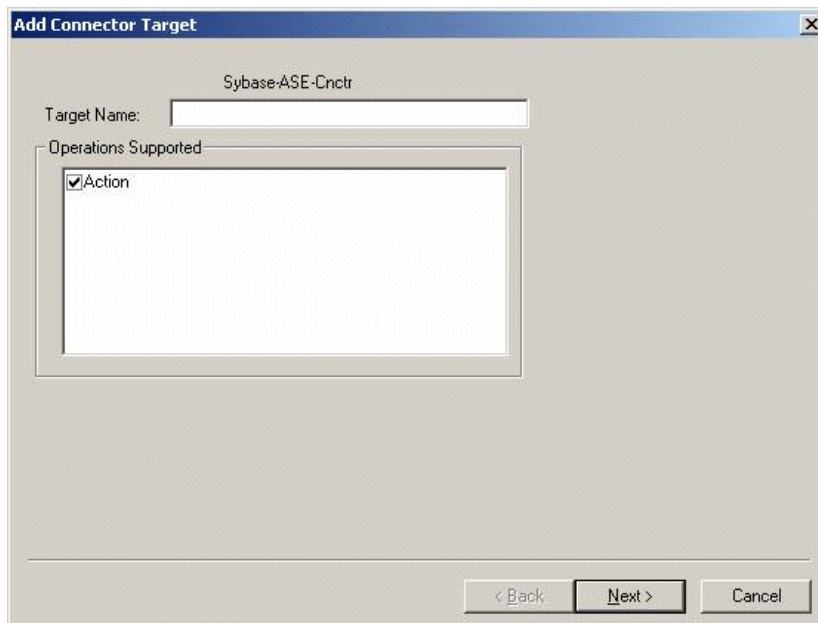
The **USER NAME** and **PASSWORD** values entered here should be the values entered for **PRIVUSERNAME** and **PRIVPASSWORD** during the connector configuration.

Connector Configuration

Follow these steps to add a Sybase ASE target:

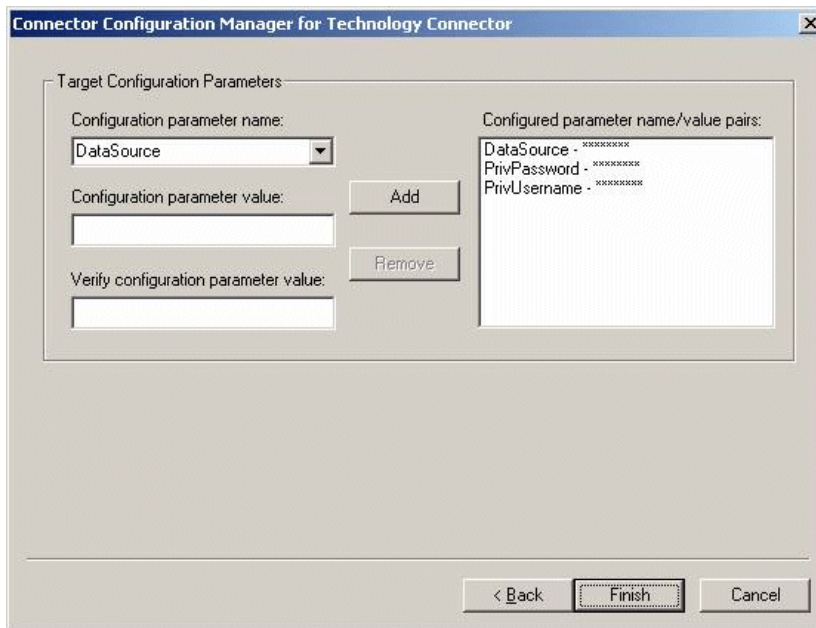
1. From the Start menu, select:
Programs>Core Server Core Server>Connector Configuration Manager
2. Choose **FILE > ADD CONNECTOR**, select **SYBASE-ASE-CNCTR**, and click **OK**.
3. Select **SYBASE-ASE-CNCTR**
4. Click the right mouse button and choose **ADD TARGET...**

The Add Connector Target dialog box appears.

Figure 331: Add Sybase ASE TargetThe image shows a Windows-style dialog box titled "Add Connector Target". At the top, it says "Sybase-ASE-Cnctr". Below that is a "Target Name:" label followed by an empty text box. Underneath is a section titled "Operations Supported" which contains a list box with a single item "Action" that has a checked checkbox next to it. At the bottom of the dialog, there are three buttons: "< Back", "Next >", and "Cancel".

5. Enter a name (alias) for the target in the **TARGET NAME** text box. This name identifies the target in the Administration Manager interface.
6. **ACTION** is selected by default, to enable all operations on the target. Click **NEXT**.
The Connector Configuration Manager for Technology Connector dialog box appears.

Figure 332: Connector Configuration Manager for Sybase ASE



7. The drop-down menu, **CONFIGURATION PARAMETER NAME**, is populated with the names of the available parameters. From the drop-down list, select each configuration parameter, supply a value and confirm the value, then add the pair to the list box on the right side of the window by clicking the **ADD** button.
 - **DataSource** — OLE DB Data Source Name.
 - **PrivPassword** — The privileged user's password.
 - **PrivUsername** — The privileged user's username.

Note: You can add only one parameter at a time, but you can select and remove multiple items at the same time. Adding a value for the same parameter a second time overwrites the previous value. Values are always displayed as asterisks ("*") for security.
8. Click the **FINISH** button.

Adding, modifying, or removing a connector after the Connector Framework Manager is configured requires stopping and restarting the Core Server and Core Server web services. When you perform any of these operations and exit the Connector Configuration Manager, a dialog box appears asking if you want to restart the services.

The target is now available for each action supported by this connector.

Chapter 64: Using the Cour390 Agent

This chapter explains installing, configuring, and using the Cour390 agent, an agent required by the many platforms designed to work with z/OS systems. These platforms include RACF, CA-Top Secret, and CA-ACF2.

This chapter includes the following sections:

- [*"About the Cour390 Agent" on page 632*](#)
- [*"Configuring the Cour390 Agent" on page 635*](#)
- [*"Configuring the Security Interface" on page 642*](#)
- [*"Configuring the RACF Security Interface" on page 642*](#)
- [*"Configuring the CA-ACF2 Security Interface" on page 649*](#)
- [*"Configuring the CA-Top Secret Security Interface" on page 653*](#)
- [*"Providing Information to the Core Server Administrator" on page 658*](#)
- [*"Defining Words that Cannot Be Used As Passwords" on page 659*](#)
- [*"Using the Cour390 Authorization Checking File" on page 660*](#)
- [*"Operating the Cour390 Agent" on page 662*](#)
- [*"Cour390 SMF Report" on page 667*](#)
- [*"Error and Status Messages" on page 672*](#)

About the Cour390 Agent

The Cour390 agent provides services to the Core Access Assurance Suite on z/OS systems that use RACF, CA-ACF2, or CA-Top Secret. These services include provisioning resources, resetting passwords, and performing other Core Access Assurance Suite related tasks.

The same agent is used in the PMM and Connector for RACF®, and the PMM and Connector for CA-ACF2®. Agent configuration requirements for Core Password, Core Provisioning, Core Compliance, or RoleCourier should be addressed if these products are being used.

This chapter uses the term “z/OS” for both z/OS and OS/390 systems.

Cour390 Agent Requirements

To use the Cour390 agent, you must have:

- z/OS or OS/390 — any version

You must also have one of the following security packages:

- CA-ACF2 — Release 6.0 or higher
- CA-Top Secret — Version 4.4 or higher
- RACF — any version

Installing or Upgrading the Cour390 Agent

This section explains installing and upgrading the Cour390 agent on a z/OS system. It assumes that the Core Access Assurance Suite is installed, as explained in *Installing the Core Access Assurance Suite*.

Upgrading means installing a newer version of the agent while an older one is installed. The procedure is identical to the initial installation.

To install or upgrade the agent, follow these steps:

1. Execute the update file,
`courion-install-directory/os390/os390agent.exe` where
`courion-install-directory` is the Core Security installation directory on the
 Core Server system). This extracts the following files:

LOADLIB.XMT — Cour390 agent load library

SAMPLIB.XMT — A library containing sample JCL parameter files and
 sample commands

2. If you choose, pre-allocate the sequential data sets, use the following attributes:

Organization: PS

Record format: FB

Record length: 80

Block size: 3120

Space unit: BLKS

Primary quantity: LOADLIB 350
 SAMPLIB 40

Secondary quantity: optional

Directory blocks: 0

3. Upload LOADLIB.XMT and SAMPLIB.XMT to your z/OS system. Upload the files as binary files, without any text conversions.
4. If you choose, pre-allocate space for the PDS files you create in the next step.
 - a. For LOADLIB PDS, use the following attributes:

Organization: PO

Record format: U

Record length: 0

Block size: 13030

Space unit: BLKS

Primary quantity: 140

Secondary quantity: optional

Directory blocks: 20

For SAMPLIB PDS, use the following attributes:

Organization: PO

Record format: FB

Record length: 80

Block size: 27920

Space unit: BLKS

Primary quantity: 10

Secondary quantity: optional

Directory blocks: 10

5. Use the TSO RECEIVE command to reformat each uploaded file into a partitioned data set (PDS).

Do not direct the output of the RECEIVE command to a PDS containing any SAMPLIB members you have modified or are using.

For an upgrade, if you have any customized SAMPLIB members, do not specify the name of the existing PDS in the RETRIEVE command. Using the same name overlays your custom SAMPLIB or members. The goal is to replace all Cour390 executables, while leaving any customized SAMPLIB members intact.

6. Make the changes necessary to cause the Cour390 started task to use the new executables. You can do either of the following:
 - Copy all modules from the new LOADLIB to the Cour390 LOADLIB, replacing any existing modules of the same name. For an upgrade, you must stop the Cour390 agent first ([“Commands to the Cour390 Agent”](#)).
 - or
 - Replace the data set name in the Cour390 STEPLIB DD with the name of the new LOADLIB; then APF-authorize the new LOADLIB using the command
`SETPROG APF, ADD, DSNAME=ds-name,VOLUME=volser | SMS`
7. For an initial installation, configure the agent as explained in the next section.

For an upgrade, stop and start the agent, using the stop command `P procname` (`P Cour390`) or start command `S procname` (`S Cour390`). For more detail, see [“Commands to the Cour390 Agent”](#).

Configuring the Cour390 Agent

Configuring the Cour390 agent includes the following general procedures:

- Modifying the Sample JCL To Run the Agent and
- Creating the GLOBAL Member

Modifying the Sample JCL To Run the Agent

Member COUR390 of SAMPLIB contains sample JCL for the agent. To modify it to run the agent, follow these steps.

1. Change value of `QUAL=` to the high level qualifier of your Cour390 Loadlib and Samplib.
2. Change the values of `OUTC=` and `DUMPC=` to match your site's values.
3. Ensure that the library defined in `STEPLIB` `APF-` authorized before starting.
4. Ensure that the necessary security system definitions are made before issuing the operator command `START`.
5. Ensure that this JCL is placed into a `PROCLIB` defined to JES before issuing the Installing operator command `START`.

Continue to the next section.

Creating the GLOBAL Member

The GLOBAL member enables you to set configuration options for Cour390. These parameters define Cour390 communications, operations, password rules, and logging information. Member GLOBAL of SAMPLIB contains example GLOBAL parameters.

During initialization, the Cour390 agent reads the data set allocated to DDname GLOBAL to determine the options chosen. The major part of configuring the Cour390 agent is editing this file. Changes you must make in the GLOBAL member include specifying the following:

- TCP/IP Communications Parameters
- Encryption Information Parameter
- Cour390 Request Validation Resource

These parameters are explained in [“Essential Parameters in the GLOBAL Member” on page 636](#). Other parameters control agent options and password resets, as follows:

- [“Agent Control Parameters” on page 637](#) control agent options such as `ERRROUTE`, `ERRDESC`, `INFORROUTE`, and `INFODESC`
- [“Cour390 Password Reset Parameters” on page 638](#) specify options for password resets and accompanying resumes.

Table 38 explains the essential parameters in the GLOBAL member.

Table 38: Essential Parameters in the GLOBAL Member

TCP/IP Communications Parameters
TCPIPJOBNAME = <i>up-to-8-chars</i> Specifies the TCP/IP job name of the IBM or Cisco IOS TCP job. The job name can contain up to 8 characters. If you do not configure TCPIPJOBNAME, the agent cannot use TCP communications. The following conditions must be satisfied: • Cour390 must run on the same physical CPU as TCP/IP • TCP/IP must be at one of the following release levels: - IBM TCPIP V3R1 or higher - or - InterLink TCPaccess 4.1 and higher (4.1 needs CUM9706 or above) - or - Cisco IOS for S/390 Release 1 and above (only the base is required)
TCPIPPORT={5000-<i>to</i>-65535} Specifies the IP Port on which Cour390 listens for incoming connection requests from remote Cour390 nodes. The valid range is from 5000 to 65535 and the default is 47474.
Encryption Information Parameter
3DES_SEED=xxx (called "Security Phrase" in Core Server configuration dialog.) This parameter defines the installation-specific value that Cour390 uses to generate a key for use in its 3DES encryption/decryption algorithm. This value can contain any character values, including spaces, and must be at least 8 characters, and no more than 32 characters (including embedded spaces). This value must match the value specified for the Security Phrase when creating an Core Access Assurance Suite connector or PMM target for a platform such as RACF, CA-CAF2, or CA-Top Secret. There is no default for this parameter.
Cour390 Request Validation Resource
COURIER_RESOURCE=xxx COURIER_RESOURCE= specifies the Facility Class Resource Profile name. The sample GLOBAL member uses the default value \$COURIER. The name specified here is the resource name you define during security-system configuration (such as that of RACF).

Table 39, following, lists the agent control parameters.

Table 39: Agent Control Parameters

ERRDESC= (nn) (1,2,3,...n) Specifies the default descriptor codes to use for Cour390 error messages. Specify as many as you need. The default value is 11, which indicates Critical Eventual Action Required and causes the message to remain on the operator console until action is taken. Core Security recommends a less severe designation. The sample Global file specifies a value of 4, designating Cour390 error messages as System Status messages.
ERRROUTE= (n) (1,2,3,...n) Specifies the default console route code to use for Cour390 error messages. Specify as many route codes as you need. The default value is 1, which demands action by an operator at a master console. Core Security recommends a less severe designation. The sample Global file specifies a value of 15, an installation-defined value typically associated with low-severity messages.
INFODESC= (nn) (1,2,3,...n) Specifies the default descriptor code for information messages from Cour390. Specify as many descriptor codes as you need. The default value is 4, which designates Cour390 informational messages as System Status messages. Note that the sample Global file specifies the default.
INFOROUTE= (nn) (1,2,3,...n) Specifies the default console route code for information messages from Cour390. Specify as many route codes as you need. The default value is 11, which designates Cour390 informational messages as Programmer Information. The sample Global file specifies a value of 15, an installation-defined value typically associated with low-severity messages.
ESS_SMF#= {NO 128-to-255} Defines the SMF record number that Cour390 uses when writing a history record to SMF. A value of NO indicates that no history records are written to SMF. The default is NO. Please refer to “Cour390 SMF Report” on page 667 for more information on the layout of the Cour390 SMF Log Record.
ESSDEBUG=NO LOG WTO} Specifies the type of debugging information to generate when running Cour390. The default is NO. NO - No messages are issued. It is recommended that you issue messages only if you are debugging a problem. LOG - Messages are issued to the JES log. We recommend using LOG during installation and whenever you are gathering documentation for Core Security support. WTO - Messages are issued to the system log and the JES log.

Table 40 describes all the password reset parameters. You can examine and use these now, or you can skip to the next section, [“Configuring the Security Interface” on page 642](#), and return to the table after Cour390 is up and running.

Table 40: Cour390 Password Reset Parameters

ESS_EXPIRE_PASSWORD={YES NO} This parameter determines whether the Core Access Assurance Suite expires a user's password (that is, force a user to change the password at next logon), when the password change was requested by an administrator. This parameter applies only to workflows that specify the option 'User must change password at next Logon'. YES - The password expires and the user is forced to change it at the next logon. NO - The password does not expire and the user is not be forced to change it at the next logon.
ESS_ACCEPT_REVOKE_RESUME= {YES NO} This parameter defines whether Cour390 accepts Resume requests that are part of a password reset workflows. It affects only the Cour390 password reset requests that specify the option to Resume Revoked users. YES - Cour390 accepts RESUME requests from password reset workflows. NO - Cour390 rejects RESUME requests from password reset workflows.
RRSF_PASSWORD_SUPPORT={YES ALL} For RACF only. This parameter enables support of the RACF Remote Sharing Facility (RRSF). When you specify YES or ALL, the agent resets the password in a manner that allows RRSF to propagate the new password to accounts linked to the target user ID. When you specify ALL, a RACF RESUME request always issues the Resume command, even if the user account is not Revoked. This assures that no accounts linked to the user account are revoked when the reset occurs, and may be useful for installations that do not propagate application updates on all systems.
PWRESET_METHOD= {CLEAR COMMAND} For RACF only. CLEAR - Cour390 uses RACF Callable Services to perform a temporary reset using a random password value, then performs a reset with the new password in clear text. COMMAND - Cour390 uses RACF Callable Services to reset passwords. CLEAR or COMMAND - Cour390 uses RACF Callable Services to resume RACF users, when the Agent and PMM are configured to resume revoked RACF users. For more information, see “Coexisting with RACF Exits and Other Password Maintenance Products” on page 648
ESSRESETLASTUSEDDEDATE= (also ESSRESETLASTUSEDDEDATEONRESUME) = {YES NO } For RACF only. Note: ESSRESETLASTUSEDDEDATE replaces ESSRESETLASTUSEDDEDATEONRESUME. Core Security supports both versions of this parameter at this time. YES — Cour390 resets the Last Used Date before resetting the user's password. This means password resets succeed regardless of the period of inactivity. NO (default) — Cour390 does not reset the Last Used Date. This means a password reset fails if a user account inactive past the RACF INACTIVE period.

Table 40: Cour390 Password Reset Parameters (Continued)

ESSADMINREPLACEBADPASSWORD= {YES NO } For RACF only. YES — Allows an Core Access Assurance Suite administrative user to replace a password that violates RACF password rules or that matches the user's existing password. NO (default) — Prevents the action above.
ACF2_ENABLE= { ALL CANCEL SUSPEND EXPIRE } For CA-ACF2 only This parameter allows the Cour390 Administrator to control which CA-ACF2 values are reset when Cour390 enables CA-ACF2 user accounts as part of a password reset request. Values are: ALL — Cour390 resets the CANCEL and SUSPEND flags, and sets the Expire Date to zero, when enabling a CA-ACF2 user account. This is the default. CAN (cancel) — Cour390 resets only the CANCEL flag when enabling a CA-ACF2 user account SUS (suspend) — Cour390 resets only the SUSPEND flag when enabling a CA-ACF2 user account EXP (expire) — Cour390 only sets the Account Expiration date to zero when enabling a CA-ACF2 user account You can one or more of the values listed above if you enclose the list in parentheses with values separated by a comma or space; for example, (CAN,SUS,EXP).
PWC_TOPS_RESUME_TARGETS= <i>targetname</i> [...] For CA-Top Secret only The parameter PWC_TOPS_RESUME_TARGETS designates one or more Top Secret targets to which the Cour390 agent should direct Unsuspend (Resume) Commands. The value specified for the operand must follow the syntax of the Top Secret REMOVE command TARGET parameter. The Cour390 agent does not verify the validity of the value specified.
ALLOW_SPECCHAR_PWS={YES NO } For CA-ACF2 and CA-Top Secret only. YES - Accepts passwords containing non-alphanumeric characters. NO (default) - Restricts password content to letters, numbers and the characters '\$', '#' and '@'.

Table 40: Cour390 Password Reset Parameters (Continued)

ESSSTRONGPASSWORDRULES governs the rules enforced on password changes. The Strong Password Rules feature lets you enforce strict password length and content rules on the z/OS system. While this feature is enabled, additional password validation is done based on a table consisting of reserved (not allowed) passwords and configurable GLOBAL parameters when a user changes his/her password at logon time. This parameter specifies whether the password length and content rules should or should not be applied to password changes. These rules are not enforced when an administrator changes a user account's password. NO — Cour390 does not enforce password length and content rules for password changes. YES — Cour390 enforces password length and content rules for password changes. For the following parameters to be enforced, ESSSTRONGPASSWORDRULES must be YES, and the PMM must enable Strong Password rules. NO renders the following parameters meaningless: • ESS_PASSWORD_SYNTAXRULES= • ESSMINIMUMPASSWORDLENGTH= • ESSREQUIRELETTERSANDNUMBERS= • ESSREQUIRESPECIALCHARACTERS= • ESSUNIQUECHARACTERSREQUIRED= • ESSMINIMUMLETTERSREQUIRED= • ESSRESERVEDWORDLIST=
ESS_PASSWORD_SYNTAX_RULES= { LOCAL RACF BOTH} This parameter defines the type of syntax rule checking that Cour390 that perform: LOCAL — Cour390 uses its own internal strong password rules to validate the password. RACF — Cour390 uses the RACF Password Syntax rules as defined by the SETROPTS PASSWORD command to validate the password. RACF only. BOTH — Cour390 uses both Cour390 and RACF rules to determine if a password is valid. RACF only. If you specify RACF or BOTH for a system which is not running RACF, a message is displayed, and the parameter defaults to LOCAL. (ESSSTRONGPASSWORDRULES must be YES.)
ESSALLOWLONGPASSWORDS = {YES NO} This parameter specifies whether the agent should accept passwords longer than 8 characters (and truncate at 8 characters) or reject all passwords longer than 8 characters. The default is YES, to allow long passwords and to truncate. For example, value YES (default) allows AB2CD4 or AB2CD4EF6G (new password=AB2CD4EF); value NO disallows AB2CD4EF6G
ESSMINIMUMPASSWORDLENGTH= <i>n</i> Specifies the minimum length of a password. The minimum value accepted is 1 and the maximum is 8 on z/OS. The default is 6. (ESSSTRONGPASSWORDRULES must be YES.) For example, default value 6 allows AB2XY4 and disallows AB2XY.

Table 40: Cour390 Password Reset Parameters (Continued)

ESSREQUIRELETTERSANDNUMBERS= { YES NO } Can require a password to contain both letters (alpha) and numbers (numeric). This prevents a user from choosing common words as passwords that can be broken easily. The default is NO. We recommend the value YES. (ESSSTRONGPASSWORDRULES must be YES.) For example, value YES allows AB2XY4, disallows ABCDEF, 123456
EESSREQUIRESPECIALCHARACTER= {YES NO} Can force users to include a special character in passwords. Can force users to include in passwords one or more of the characters '\$', '#' and '@'. The default is NO. (ESSSTRONGPASSWORDRULES must be YES.) For example, value YES allows AB2\$XY4 and disallows AB2XY4
ESSUNIQUECHARACTERSREQUIRED#= {nn ESSMINIMUMPASSWORDLENGTH-2} Specifies the number of unique characters required in a password. The minimum number is 1 and the maximum is the same as the maximum length of the password (8 on z/OS). (ESSSTRONGPASSWORDRULES must be YES.) The default values follow these rules: If ESSMINIMUMPASSWORDLENGTH <= 4 then ESSUNIQUECHARACTERSREQUIRED#=ESSMINIMUMPASSWORDLENGTH If ESSMINIMUMPASSWORDLENGTH#= 5 then ESSUNIQUECHARACTERSREQUIRED = 4 If ESSMINIMUMPASSWORDLENGTH# >= 6 then ESSUNIQUECHARACTERSREQUIRED# = ESSMINIMUMPASSWORDLENGTH – 2
ESSMINIMUMLETTERSREQUIRED = {nn 2} Specifies the minimum number of letters required. The minimum value is 1 and the maximum is 8 on z/OS. The default is the "minimum password length plus 1" divided by 2. (ESSSTRONGPASSWORDRULES must be YES.) For example, value 4 allows AB2XY4 and disallows AB2468
ESSRESERVEDWORDLIST ={LOCAL USER BOTH} Defines the type of reserved word checking that Cour390 performs when validating a password during its Strong Password Rule checking. Valid values are: LOCAL — Cour390 should use its Reserved Word list. USER — Cour390 should use the user reserved word list. BOTH —Cour390 should use both the Cour390 and user reserved word lists. If you do not wish to use any reserved words for password validation, set the parameter ESSRESERVEDWORDLIST to USER and leave the word list blank. (ESSSTRONGPASSWORDRULES must be YES.)

Configuring the Security Interface

A security interface allows the agent to provide services to Core Access Assurance Suite applications. The configuring process differs for each of the three security systems, but the common goals are to:

- Define the ID for the Cour390 agent Started Task.
- Define the ID for the Core Security Administrative User. All Core Access Assurance Suite applications that request z/OS services must provide the ID and password of this user.
- Define the Core Security Resource Profile.
- Permit the Core Security Administrative User Read access to the Core Security Resource.

For CA-Top Secret, you must also define a Top Secret Facility for the Cour390 agent, and decide whether to run it in warn mode or permit wide access to the Facility.

Proceed to configure your security interface, which is one of the following:

- [“Configuring the RACF Security Interface” on page 642](#)
- [“Configuring the CA-ACF2 Security Interface” on page 649](#)
- [“Configuring the CA-Top Secret Security Interface” on page 653](#)

Configuring the RACF Security Interface

This section explains how to define the UserIDs and Resource Profiles necessary to operate the Cour390 agent in a RACF environment. Before doing this, you (or someone) must have configured the agent itself, as explained in [“Configuring the Cour390 Agent” on page 635](#).

You must activate the RACF subsystem, which is required to support the R_admin callable service used by the Cour390 agent, prior to configuring the RACF security interface.

Member RACFJOB contains JCL to execute the commands. [Figure 333](#) is a sample RACF Member file with commands for performing these steps.

The steps below show the commands and syntax for RACF under TSO. They also specify the RACF ISPF-Program Development Facility (PDF) option you can use to perform the identical function. The examples use UPPERCASE to show words that you should type exactly as shown, and italics to show entries that represent values you choose.

Follow these steps:

1. Define a RACF User ID for the Cour390 agent. The User ID should be defined as Protected (NOPASSWORD NOOIDCARD) to prevent unauthorized use. The User ID must include an OMVS segment to permit the Started Task to use TCP/IP. For example,

```
ADDUSER stcuid DFLTGRP(stcgrp)
NAME('Cour390 agent')
SPECIAL
NOPASSWORD NOOIDCARD
```

```
OMVS (UID(uid
HOME (/home) )
```

where:

stcuid is the z/OS User ID you want to assign to the Cour390 agent.

stcgrp is the group to which you want the started task assigned.

Cour390 agent is the text name you choose for the Core Server.

/home is a valid USS File system folder name.

uid is the USS User ID you want to assign to the Cour390 agent.

Or use RACF PDF option 4.1.

Note: If you are using Core Provisioning or Core Compliance on RACF, the ID must have the RACF attribute SPECIAL. If you are using PasswordCourier, and you specify PWRESET_METHOD={COMMAND or CLEAR}, the ID must either have SPECIAL, or be granted at least UPDATE access to the FACILITY class profile IRR.PASSWORD.RESET.

2. Define Data set Profiles for the data sets containing the Core Security programs and parameter files.

```
ADDSD 'courhlq.*'          OWNER(stcuid) UACC(NONE) GENERIC
ADDSD 'courhlq.LOADLIB'    OWNER(stcuid) UACC(NONE)
ADDSD 'courhlq.SAMPLIB'    OWNER(stcuid) UACC(NONE)
```

where:

*courhlq.** is the high-level qualifier of the data sets containing Core Security programs and parameter files.

courhlq.LOADLIB is the name of the load library containing Core Security programs.

courhlq.SAMPLIB is the name of the load library containing Core Security parameters.

stcuid is a user ID of your choice to own the Core Security data set profiles.

(Or use RACF PDF option 1.1.)

3. Permit access to Core Security resources to both the Cour390 agent User ID and the RACF Group that includes the people in your site who are responsible for maintaining Core Security products on z/OS.

```
PERMIT 'courhlq.LOADLIB' ID(*) ACCESS(EXECUTE)
PERMIT 'courhlq.LOADLIB' ID(stcuid sysgrp) ACCESS(ALTER)
PERMIT 'courhlq.SAMPLIB' ID(stcuid sysgrp) ACCESS(ALTER)
PERMIT 'courhlq.*'      ID(stcuid sysgrp) ACCESS(ALTER)
```

where:

courhlq is the high-level qualifier shown in step [2](#) above.

stcuid is the User ID of the Cour390 agent, as defined in step [1](#) above.

sysgrp is the RACF group that includes the people at your site responsible for maintaining Core Security products on z/OS.

(Or use RACF PDF option 1.4.)

4. Add a Resource to the STARTED Resource Class that describes the Cour390 agent. For example,

```
RDEFINE STARTED member.job STDATA(USER(stcuid) GROUP(stcgrp) )
```

where:

STARTED is the name of the (RACF-defined) Resource Class.

member is the member name in the procedure data set.

job is the name specified on the PROC statement of the member in the

procedure data set; this is the name under which the server job runs, and is typically the same as the member name.

stcuid is the User ID of the Cour390 agent, as defined in step [1](#).

stcgrp is the name of the group identified (or defined) in step [1](#).

(Or use RACF PDF option 2.1)

5. Define the Courion Agent Resource to the FACILITY class. The name of the Core Security Agent Resource is specified in the GLOBAL parameter COURION_RESOURCE (Table 38, [“Essential Parameters in the GLOBAL Member” on page 636](#)). The default is to name this resource \$COURIER. For example,

```
RDEFINE UACC(NONE) FACILITY courres
```

where:

FACILITY is the name of the (RACF-defined) Resource Class.

courres is the name chosen to describe the Courion Agent Resource, and specified in GLOBAL parameter COURIER_RESOURCE.

(Or use RACF PDF option 2.1)

6. Define the Cour390 Administrative User ID to RACF. This is the ID specified as the \$COURIER Account during configuration of the Core Access Assurance Suite NT client. This User ID is used to validate that a request originates from an authorized Core Security client. The ID needs no specific authorities, except access to the Core Security Agent Resource (see step [5](#)), and can be assigned to any Group. For example,

```
ADDUSER admin DFLTGRP(admingrp) NAME('Authorized-Admin-Id')
PASSWORD(adminpw) NOOIDCARD
```

admin is the administrator User ID that you provide to the Core Access Assurance Suite Client during client configuration.

admingrp is the administrator group.

Authorized-admin-id is the text name you choose for the Cour390 Administrative User ID.

adminpw is the administrator password.

(Or use RACF PDF option 4.1.)

7. Assure that the password of the Cour390 Administrative User ID does not expire. For example:

```
PASSWORD NOINTERVAL USER(admin)
```

where:

admin is the User ID defined in step [6](#), above.

(Or use RACF PDF option 4.2.)

8. Permit the PWC Initiating User ID to access the Core Security resource defined above. For example:

```
PERMIT courres ACCESS(READ) CLASS(FACILITY) ID(admin)
```

where:

courres is the name chosen for the Courion Agent Resource in step [5](#) above.

admin is the administrator user ID defined in step [6](#).

(Or use RACF PDF option 2.4)

9. Refresh the RACF database to activate the changes just made.

```
SETROPTS REFRESH RACLIST(STARTED,FACILITY)
```

(Or use RACF PDF option 5.6)

For further information on adding Cour390 to the STARTED Resource Class, please refer to the IBM *RACF Security Administrator's Guide* and *RACF Command Language Reference* manuals.

Agent configuration for RACF is complete (but you might want to read [*“Coexisting with RACF Exits and Other Password Maintenance Products” on page 648*](#)).

Continue to [*“Providing Information to the Core Server Administrator” on page 658*](#).

Sample RACF Member

[Figure 333](#) shows a sample RACF Member. It summarizes the steps explained above.

Figure 333: Sample RACF Member

```

/*****
/*      Courion Corporation z/OS Agent Server      **
/*      Copyright Courion Corporation              **
/*      ****                                       **
/* Member:      RACF                               **
/* Function:     Courion z/OS Core Access Assurance Suite      **
/*               server RACF definitions                    **
/*               ****                                       **
/* Make the following modifications prior to execution:      **
/*               ****                                       **
/* Change '$$stcjobnm$$' to the jobname of the Agent started task. **
/* Change '$$stcuid$$' to the UserID you want to assign to the **
/*               Agent started task.                      **
/* Change '$$stcgrp$$' to whichever group you want the Agent **
/*               started task assigned.                   **
/* Change '$$sussuid$$' to a Unix System Services uid to be assigned **
/*               to the Agent started task.      Superuser is not required. **
/* Change '$$home$$' to a valid USS File system directory name **
/* Change '$$admin$$' to the userid assigned the Courion **
/*               administrative user.                     **
/* Change '$$adminpw$$' to the password to be assigned to the **
/*               administrative user's id.                 **
/* Change '$$admingrp$$' to the RACF group you want the $$admin$$ **
/*               connected to as default group.           **
/* Change '$$courhlq$$' to the high-level-qualifier of the Agent **
/*               LOADLIB and SAMPLIB datasets.           **
/* Change '$$courres$$' to the value you assign to the Agent **
/*               resource, as specified in the Agent GLOBAL parameter **
/*               COURIER_RESOURCE. The default value is $COURIER. **
/* Change '$$sysgrp$$' to the RACF group you want to have ALTER **
/*               access to the dataset profiles.          **
/*               ****                                       **
/* Next, save these changes and use member RACFJOB to execute the **
/*               commands.                                **
/*****
/*
/* Add the userid for the Agent started task. The SPECIAL attribute
/* is REQUIRED for AccountCourier. For PasswordCourier, this can be
/* removed unless the GLOBAL parameter PWRESET_METHOD is specified. As
/* an alternative, $$stcuid$$ can be permitted at least UPDATE access
/* to FACILITY class profile IRR.PASSWORD.RESET when GLOBAL parameter
/* PWRESET_METHOD is specified. This syntax is provided in
/* comments at the end of this member.
/*
ADDUSER $$stcuid$$ DFLTGRP($$stcgrp$$)      -
      NAME('Courion Server')                -
      SPECIAL                                -
      NOPASSWORD NOOIDCARD                   -
      OMVS(UID($$sussuid$$) HOME(/$$home$$))
/*

```

Figure 248: Sample RACF GLOBAL Member (Continued)

```

/* Enter any site specific group connect commands here for the
/* server userid.
/*
ADDUSER $$admin$$ DFLTGRP($$admingrp$$)      -
      NAME('Authorized Admin Id')           -
      PASSWORD($$adminpw$$) NOOIDCARD
PASSWORD NOINTERVAL USER($$admin$$)
/*
/* Enter any site specific group connect commands here for the
/* administrative userid.
/*
/*
/* Tailor the following dataset profiles to meet your
/* site's specifications. Core Security strongly recommends
/* restricting access to both the LOAD and SAMPLIB datasets.
/*
ADDSD '$$courhlq$$.*'   OWNER($$stcuid$$) UACC(NONE) GENERIC
ADDSD '$$courhlq$$LOADLIB' OWNER($$stcuid$$) UACC(NONE)
ADDSD '$$courhlq$$SAMPLIB' OWNER($$stcuid$$) UACC(NONE)
PERMIT '$$courhlq$$LOADLIB' ID(*) ACCESS(EXECUTE)
PERMIT '$$courhlq$$LOADLIB' ID($$stcuid$$ $$sysgrp$$) ACCESS(ALTER)
PERMIT '$$courhlq$$SAMPLIB' ID($$stcuid$$ $$sysgrp$$) ACCESS(ALTER)
PERMIT '$$courhlq$$.*'   ID($$stcuid$$ $$sysgrp$$) ACCESS(ALTER)
/*
/* Use the line below if you want all users to have read access
/* PERMIT '$$courhlq$$.*' ID(*) ACCESS(READ)
/*
/* Define the Courion started task to the STARTED class. Remove
/* this statement if your site uses ICHRIN03 for defining
/* started tasks.
/*
RDEF STARTED $$stcjobnm$$.$$stcjobnm$$ STDATA(USER($$stcuid$$) -
      GROUP($$stcgrp$$) TRUSTED(NO) PRIVILEGED(NO))
/*
/* Define the $COURIER profile to the FACILITY class and
/* give the admin user defined above READ access. This is required
/* for all Courion Core Access Assurance Suite products that access
/* the z/OS server.
/*
RDEF FACILITY $$courres$$ UACC(NONE)
PERMIT $$courres$$ ACCESS(READ) CLASS(FACILITY) ID($$admin$$)
/*
/* Un-comment the next statement if you are NOT using AccountCourier
/*
/* AND
/* You are using PasswordCourier
/*
/* AND
/* You are using Global PWRESET_METHOD (=CLEAR or =COMMAND)
/*
/* AND
/* You did not assign SPECIAL to $$stcuid$$ above.
/*PERMIT IRR.PASSWORD.RESET CL(FACILITY) ACCESS(UPD) ID($$stcuid$$)
/*
/* Refresh in-memory classes to affect the changes made.
/*
SETROPTS REFRESH RACLIST(FACILITY STARTED) GENERIC(DATASET)

```

Coexisting with RACF Exits and Other Password Maintenance Products

This section explains how certain Cour390 options interact with features that propagate RACF passwords.

PWRESET_METHOD {CLEAR | COMMAND} Parameter

By default, Cour390 updates passwords by specifying an encrypted password value to RACF, using a standard SAF interface. A RACF exit or other facility that intercepts the password change and attempts to propagate it might not recognize that the value is encrypted, and is unable to propagate the password correctly. Use the PWRESET_METHOD parameter to avoid this problem by performing password changes with clear-text values.

Use PWRESET_METHOD=CLEAR when your installation uses a RACF exit (such as ICHPWX01, the New Password Exit) and you want the final user password change to be completed through the RACROUTE REQUEST=VERIFY interface. This option causes the Cour390 agent to update the user's password with a temporary value using RACF Callable Services, then uses RACROUTE REQUEST=VERIFY to set the password (using clear text) to the value specified by the user.

Use PWRESET_METHOD=COMMAND to cause the agent to reset the password using the ALU command, specified through the RACF Callable Services.

Using either PWRESET_METHOD option may require you to configure the agent User ID with additional privileges. See the note under step 1 in [“Configuring the RACF Security Interface” on page 642](#) for more information.

If you have finished configuring the RACF security interface, continue to [“Providing Information to the Core Server Administrator” on page 658](#).

.

.

Configuring the CA-ACF2 Security Interface

This section explains how to define the UserIDs and Resource Profiles necessary to operate the Cour390 agent in a CA-ACF2 environment. Before doing this, you (or someone) must have configured the agent itself, as explained in [“Configuring the Cour390 Agent” on page 635](#).

For the agent to work properly with your CA-ACF2 system, you need to define two new logon IDs (LIDs) to your system and two new data set and resource rules for the agent system.

Member ACF2 of the SAMPLIB data set contains example CA-ACF2 commands for performing these steps. Member ACF2JOB contains JCL to execute these commands. [Figure 334](#) shows a sample ACF2 member.

Follow these steps:

1. Create the LID to be used by the Cour390 agent started task as follows:

```
SET LID
INSERT courlid NAME(Cour390-agent) GROUP(stcgrp) STC
```

where:

Cour390-agent is the text name you choose for the Cour390 agent.

courlid is the Cour390 agent LID. The default is COUR390.

stcgrp is the group to which you want the Cour390 agent assigned

2. Create the Cour390 administrative LID.

```
SET LID
INSERT admin GROUP(admingrp) PASSWORD(adminpw) -
NAME(Authorized-Admin-Id)
```

where:

admin is the LID assigned the Core Security administrative user.

admingrp is the group to which you want the administrative user assigned.

Authorized-admin-id is the text name you choose for the Cour390 Administrative User ID.

adminpw is the password to be assigned to the administrative user's LID.

3. Create the OMVS profile for the agent LogonID:

```
SET PROFILE(USER) DIVISION(OMVS)
INSERT courlid UID(uid) HOME(/home)
```

courlid is the Cour390 agent LID.

uid is the Unix System Services uid to be assigned to the Cour390 started task. Superuser is not required.

home is a valid USS File system directory name.

4. Create rules for access to Cour390 data sets. Tailor the following access rules to meet your site's specifications. Core Security strongly recommends restricting access to both the LOADLIB and SAMPLIB data sets.

```
SET RULE
COMPILE
$KEY (courhlg) MODE(ABORT)
SAMPLIB UID (courlid) READ(A) WRITE(A) EXECUTE(A)
SAMPLIB UID (-) READ(P) WRITE(P) EXECUTE(P)
```

```
SAMPLIB UID(courlid)    READ(A) WRITE(A) EXECUTE(A)
SAMPLIB UID (-)        READ(P) WRITE(P) EXECUTE(P)
```

where:

*courhlg.** is the high-level qualifier of the data sets containing Core Security programs and parameter files.

courlid is the Cour390 agent userID defined in step 1 above.

5. Define the \$COURIER profile to the FACILITY class and allow access to the Cour390 administrative LogonID created in step [2](#), above. All Core Access Assurance Suite applications that request z/OS services must provide the LogonID and password of a user with access to this facility. To do this, use the following sequence of ACF2 commands.

```
SET RES(FAC)
COMPILE
$KEY($COURIER) TYPE(FAC)
UID(admin) ALLOW
STORE
```

6. Once the ACF2JOB runs, rebuild the ACF2 folder of resident resource rules by executing, from the ACF command or the operator console, the following commands:

```
F ACF2,REBUILD(FAC)
F ACF2,REBUILD(USR),CLASS(P)
F ACF2,OMVS
```

[Figure 334](#) shows a sample CA-ACF2 member file.

Agent configuration for CA-ACF2 is complete. Continue to [“Providing Information to the Core Server Administrator” on page 658](#).

*Sample CA-ACF2 Member***Figure 334: Sample CA-ACF2 Member**

```

*****
**          Courion Corporation z/OS Agent Server          **
**          Copyright, 2001, 2006 Courion Corporation      **
**_____**
**
** Member:      ACF2                                     **
** Function:    Courion z/OS Core Access Assurance Suite  **
**              server CA-ACF2 definitions.                **
**                                                    **
** Make the following modifications prior to execution:    **
**                                                    **
** Change '$$courlid$$' to the LID you want to assign to the **
** Agent started task. The remaining commands presume    **
** that the USERID for this LID is the same as the LID.   **
** Change '$$stcgrp$$' to the group to which you want the Agent **
** started task assigned.                                  **
** Change '$$uid$$' to a Unix System Services uid to be assigned **
** to the Agent started task. Superuser is not required.  **
** Change '$$home$$' to a valid USS File system directory name. **
** Change '$$admin$$' to the userid assigned the Courion   **
** administrative user.                                    **
** Change '$$cour$$' to the high-level-qualifier of the Agent **
** LOADLIB and SAMPLIB datasets.                          **
** Change '$$courres$$' to the value you assign to the Agent **
** resource, as specified in the Agent GLOBAL parameter   **
** COURIER_RESOURCE. The default value is $COURIER.       **
** Change '$$adminpw$$' to the password to be assigned to the **
** administrative user's id.                               **
** Change '$$admingrp$$' to the group that you want the $$admin$$ **
** user assigned.                                          **
**                                                    **
*****
SET LID
INSERT $$courlid$$ NAME(Cour390 agent) GROUP($$stcgrp$$) STC

INSERT $$admin$$ GROUP($$admingrp$$) PASSWORD($$adminpw$$) -
    NAME(Authorized Admin Id)

SET PROFILE(USER) DIVISION(OMVS)
INSERT $$courlid$$ UID($$uid$$) HOME(/$$home$$)
**
** Tailor the following access rules to meet your
** site's specifications. Core Security strongly recommends
** restricting access to both the LOADLIB and SAMPLIB datasets.
**
SET RULE
COMPILE
$KEY($$courhlq$$) MODE(ABORT)
    SAMPLIB UID($$courlid$$) READ(A) WRITE(A) EXECUTE(A)
* Add more statements as necessary for anyone requiring access
    SAMPLIB UID(-)          READ(P) WRITE(P) EXECUTE(P)
    LOADLIB UID($$courlid$$) READ(A) WRITE(A) EXECUTE(A)

```

Figure 249: Sample CA-ACF2 Member (Continued)

```
*  Add more statements as necessary for anyone requiring access
LOADLIB UID(-)          READ(P) WRITE(P) EXECUTE(P)
STORE
**
**  Define the COURIER_RESOURCE profile to the FACILITY class and
**  allow the admin user defined above access.  This is required
**  for all Courion Core Access Assurance Suite products that access
**  the z/OS server.
**
SET RES(FAC)
COMPILE
$KEY($$coursres$$) TYPE(FAC)
      UID($$admin$$) ALLOW

STORE
**
**  After completing this step, rebuild the ACF2 Directory of
**  resident resource rules by executing the following command,
**  from the ACF command or the operator console:
**      F ACF2,REBUILD(FAC)
**
```

Configuring the CA-Top Secret Security Interface

This section explains how to define the UserIDs and Resource Profiles necessary to operate the Cour390 agent in a CA-Top Secret environment. Before doing this, you (or someone) must have configured the agent itself, as explained in [“Configuring the Cour390 Agent” on page 635](#).

Member TSS of the SAMPLIB data set contains example CA-Top Secret commands for performing these steps. Member TSSJOB contains JCL to execute the commands. [Figure 335](#) shows a sample CA-Top Secret member.

The configuration of the agent for interface to CA-Top Secret requires the Agent Started Task to be defined as multiuser address space CA-Top Secret FACILITY. Unless you define the Facility in DORM or WARN Mode, FAC(COUR390) must be added to the ACIDs of all users who use Core Access Assurance Suite to reset their passwords, as well as to the ACID of the Courion Administrative user.

The agent also requires an AccessorID (ACID), which requires CA-TOP SECRET Administrative Authority to accomplish CA-Top Secret administrative functions.

The agent ACID must be established as a security administrator to have administrative authority in the CA-Top Secret environment. The authorities required differ depending on the functionality being used.

To perform Password-resets and Resume ACIDs, the agent requires the following administrative authorities:

- ACID(MAINTAIN) — to change passwords
- ACID(CREATE) — to add and delete ACIDs
- MISC1(SUSPEND) — to suspend ACIDs
- MISC8(REMASUSP) — to resume ACIDs
- MISC2(TARGET) — to allow the Agent to direct resume commands to the targets specified in Global PWC_TOPS_RESUME_TARGETS

To perform Account Provisioning actions, the agent must have authorities equal to any ACID it acts upon. In this environment, Core Security recommends that you assign the agent all Top Secret administrative authorities (as shown in the example below).

The agent uses a Resource in the IBMFAC resource class to validate incoming requests. All requests must include the ACID/password of an ACID that has read access to the IBMFAC resource specified in Global parameter COURIER_RESOURCE. You must create both the IBMFAC resource and the Cour390 Administrative User for that purpose. The sample Global member uses the resource name \$COURIER.

Follow these steps:

1. Add the Agent Facility to the CA-Top Secret Facilities Matrix Table.

To add the Agent Facility to CA-Top Secret, you must associate the agent to a CA-Top Secret facilities matrix table entry. To accomplish this, select one of the available CA-Top Secret Default user entries and redefine it as the Facility for the Cour390 agent. Refer to the "FACILITIES" control option in your CA-Top Secret Control Options Guide for discussions of user entries and definitions of selected facility attributes.

```
TSS MODIFY (FAC (userfac=PGM=ESS, ID=ZC, NAME=cour390) )
```

```
TSS MODIFY (FAC (cour390=AUTHINIT, MODE=WARN, ACTIVE) )
```

Where: *userfac* is current name of the user facility to be assigned to the agent.
cour390 is the name you want to use to define the agent facility.

Consider the following CA-Top Secret options carefully when you are defining the facility for the Cour390 agent:

`NAME=cour390` This is the default name for the agent started task (STC). This entry is user-defined.

`PGM=ESS` These are the first three characters of the load module used to initialize the agent within the CA-Top Secret environment.

`AUTHINIT` The agent runs as an (APF) authorized program.

`MODE=WARN` To avoid the need to assign all users to the facility.

`ACTIVE` Needed only if Facility userfac was previously inactivated.

2. Define a Group for the agent ACID. This step is optional. You may instead choose to assign the agent ACID to an existing Group.

```
TSS CREATE(group) NAME('group-for-cour390') TYPE(GROUP) -
      DEPT(dept)
```

Where *group* is the ACID of the Group you want to create.

group-for-cour390 is the text name you choose for the Group ACID.

dept is the ACID of the Department to which you want the Group assigned.

3. Define an ACID for the Agent Started Task.

```
TSS CREATE(stcid) NAME('cour390-agent-ACID') TYPE(SCA) -
      PASSWORD(NOPW) FAC(STC,cour390)
```

Where *stcid* is the ACID you want to create for the agent.

cour390-agent-ACID is the text name you choose for the ACID.

cour390 is the name of the Facility you defined in step [1](#).

4. Define the agent as a started task.

```
TSS ADD(STC) PROCNAME(stcname) ACID(stcid)
```

Where *stcname* is the name of Agent Started Task procedure

stcid is the agent ACID you created in step [3](#).

5. Add OMVS information to the agent ACID

```
TSS ADD(stcid) HOME(home) UID(uid) -
      GROUP(group-for-cour390) DFLTGRP(group) FAC(cour390)
```

Where *stcid* is the agent ACID you created in step [3](#).

uid is the OMVS UID you choose for the agent ACID.

group-for-cour390 is the group name you chose or created in step [2](#).

cour390 is the name of the Facility you defined in step [1](#).

6. Grant the agent ACID the necessary Top Secret administrative authorities

For Password reset and Resume only:

```
TSS ADMIN(stcid) ACID(CREATE,MAINTAIN) MISC1(SUSPEND) -
      MISC2(TARGET) MISC8(REMASUSP) DATA(BASIC)
```

For Account Provisioning actions (with or without Password Reset and Resume)

```
TSS ADMIN(stcid) ACID(ALL) FACILITY(ALL) DATA(ALL) MISC1(ALL) -
      MISC2(ALL) MISC3(ALL) MISC4(ALL) MISC8(ALL) MISC9(ALL)
```

Where *stcid* is the agent ACID you created in step [3](#). You may tailor the authorities above to suit your installations needs, as discussed above.

7. Define a Core Security resource in the IBMFAC resource class.

```
TSS ADD (facowner) IBMFAC (courier)
```

Where *facowner* is the name of the ACID that is to own the resource.
courier is the name of the Courion resource being defined. This name must be specified in Global parameter COURIER_RESOURCE. By default, the agent uses the resource name \$COURIER.

8. Define an ACID for the Courion Administrative User. The ACID and password defined in this step are needed during the configuration of Core Access Assurance Suite applications that use the Cour390 agent.

```
TSS CREATE(admin) NAME('courion-administrative-ACID') -  
    TYPE(USER) PASSWORD(adminpw) DEPT(dept) FAC(cour390)
```

Where *adminid* is the ACID you want to create.
courion-administrative-ACID is the text name you choose for the ACID.
adminpw is the password for the ACID
dept is the department to which the ACID should be assigned.
cour390 is the name of the facility you defined in Step 1.

9. Authorize the Cour390 administrative user to use the Core Security resource.

```
TSS PERMIT(adminid) IBMFAC($courier) ACCESS(READ)
```

Where *adminid* is the ACID of the Cour390 Administrative User.
\$courier is the name of the Core Security resource.

10. Protect Cour390 LOADLIB and SAMPLIB, using your installation standards. Core Security recommends restricting access to the agent STC ACID and your system maintenance personnel.

[Figure 335](#) shows a sample CA-Top Secret member.

Agent configuration for CA-Top Secret is complete. Continue to [“Providing Information to the Core Server Administrator” on page 658](#).

*Sample CA-Top Secret Member***Figure 335: Sample CA-Top Secret Member**

```

/*****
/*      Courion Corporation z/OS Agent Server      **
/*      Copyright, 2001, 2006 Courion Corporation  **
/*      ****
/*
/* Member:      TSS
/* Function:    Courion z/OS Core Access Assurance Suite  **
/*              server CA-Top Secret definitions
/*
/* Make the following modifications prior to execution:
/*
/* Change '$$userfac$$' to the dummy USERxx facility to rename to
/* 'COUR390', FAC(COUR390) must be added all user's ACIDs
/* that are allowed to use PasswordCourier for resetting
/* their passwords.
/* Change '$$stcid$$' to the ACID you want to assign to the
/* Agent started task.
/* Change '$$uid$$' to a Unix System Services uid to be assigned
/* to the Agent started task. Superuser is not required.
/* Change '$$home$$' to a valid USS File system directory name
/* Change '$$gid$$' to a Unix System Services group id to be
/* assigned the group created below (optional).
/* Change '$$group$$' to the ACID you want to assign to the
/* group being created below (optional).
/* Change '$$admin$$' to the userid assigned the Courion
/* administrative user.
/* Change '$$adminpw$$' to the password to be assigned to the
/* administrative user's id.
/* Change '$$dept$$' to the department to which $$admin$$ belongs.
/* Change '$$facowner$$' to the ACID which is to own the $COURIER
/* IBM facility class.
/*
/*****
/*
/*      +-----+
/*      | I M P O R T A N T   N O T I C E |
/*      +-----+
/*
/* This job must be submitted under the MSCA as it defines
/* $$stcid$$ as an SCA type ACID. Only the MSCA can create these.
/*
/*****
/*
TSS MODIFY (FAC ($$userfac$$=PGM=ESS, ID=ZC, NAME=COUR390))
TSS MODIFY (FAC (COUR390=AUTHINIT, MODE=WARN, ACTIVE))

TSS CREATE ($$group$$) NAME ('Courion z/OS Agent Default group') TYPE (GROUP) -
DEPT ($$dept$$)

TSS CREATE ($$stcid$$) NAME ('Courion z/OS Agent ACID') TYPE (SCA) -
PASSWORD (NOPW) FAC (STC, COUR390)

TSS ADD (STC) PROCNAME ($$stcid$$) ACID ($$stcid$$)

TSS ADD ($$stcid$$) HOME ($$home$$) UID ($$uid$$) - GROUP ($$group$$)
DFLTGRP ($$group$$) FAC (COUR390)

```


Figure 336: Sample CA-Top Secret Member (Continued)

```

/*****
/* These are the authorities required by PasswordCourier.  If you      **
/* are installing AccountCourier, delete this command and use the      **
/* command below.                                                    **
/*****
TSS ADMIN($$stcid$$) ACID(CREATE,MAINTAIN) MISC1(SUSPEND) -
      MISC2(TARGET) MISC8(REMASUSP) DATA(BASIC)

/*****
/* These are the authorities required by AccountCourier and          **
/* ComplianceCourier.  If you are installing PasswordCourier only,    **
/* you should delete this command.                                     **
/*                                                                      **
/* Because Top Secret requires an ACID to have all the authorities of **
/* any ACID it creates, Core Security recommends assigning the Agent ACID
**
/* ALL Top Secret administrative authorities.  If you know the subset **
/* of authorities in use by your target community, you may alter this**
/* command to assign only those authorities.                          **
/*                                                                      **
/*****
TSS ADMIN($$stcid$$) ACID(ALL) FACILITY(ALL) DATA(ALL) MISC1(ALL) -
      MISC2(ALL) MISC3(ALL) MISC4(ALL)  MISC8(ALL) MISC9(ALL)

TSS ADD($$group$$) GID($$gid$$)

TSS CREATE($$admin$$) NAME('Courion Administrative ACID') TYPE(USER) -
      PASSWORD($$adminpw$$) DEPT($$dept$$) FAC(COUR390)

TSS ADD($$facowner$$) IBMFAC($COURIER)

TSS PERMIT($$admin$$) IBMFAC($COURIER) ACCESS(READ)
/*
/* Add any dataset profiles you require for the server here.
/* Core Security strongly recommends that the LOADLIB dataset be protected
/* as it is APF authorized.  We also recommend READ protection of the
/* SAMPLIB dataset, as it may contain sensitive data.

```

Providing Information to the Core Server Administrator

Now that you have configured the Cour390 agent and its security interface, you need to communicate with the person configuring the dependent Core Access Assurance Suite connector or PMM. That person needs to know the following values:

- IP address or DNS name of the z/OS system
- Port number specified in Global parameter TCPIPPORT, see Table 38, [*“Essential Parameters in the GLOBAL Member” on page 636*](#)
- Name and password of the Core Server Administrator ID
- Value specified in the parameter 3DES_SEED, see Table 38, [*“Essential Parameters in the GLOBAL Member” on page 636*](#).

Next, you might want to read about [*“Defining Words that Cannot Be Used As Passwords” on page 659*](#) or [*“Using the Cour390 Authorization Checking File” on page 660*](#).

Note that the agent must be started before you can configure any dependent Core Access Assurance Suite connector or PMM. To start it, see [*“Operating the Cour390 Agent” on page 662*](#).

Defining Words that Cannot Be Used As Passwords

Cour390 enables you to define a list of words that cannot be used as passwords. Based on the setting of the GLOBAL ESSRESERVEDWORDLIST parameter, Cour390 checks the Cour390 Reserved Word List, the User Defined Reserved Word List, or both lists.

The reserved password table is also checked to reject anagrams (reserved words spelled backwards) and fuzzy reserved words (if a password is a prefix of a reserved word).

Cour390 checks the Reserved Word Lists only if the GLOBAL ESSSTRONGPASSWORD rules parameter is set to YES. If a password is the same as a reserved word, or is a prefix of the reserved word, the password change request is rejected.

Defining the Reserved Word List

To define the reserved word list, you must add the user defined reserved words to the file allocated to DDname ESSWORDL in the Cour390 JCL. An example is contained in member ESSWORD of file Cour390 SAMPLIB. The syntax for the reserved word list is:

- an * in column 1 indicates a comment
- words can be from 1 to 8 characters
- multiple words can be specified in a single record
- words are delimited by a comma or by one or more spaces
- words can be defined in columns 1 to 71
- If a word ends in column 71, there must be a space in column 72
- words cannot be continued from one record to another
- words should be defined in uppercase. Although Cour390 converts words to uppercase, any word containing a special character such as an umlaut should be coded in uppercase.

Checking and Refreshing the Reserved Word List

For the Reserved Word List to be checked, the GLOBAL parameter ESSRESERVEDWORDLIST must be set to USER or BOTH. The ESSWORDL DD statement must point to the list of reserved words that you created.

User defined words can be updated while Cour390 is running. To activate a new copy of the reserved word list, use the command F *cour390*, ESSRESERVEDREFRESH.

Using the Cour390 Authorization Checking File

The authorization checking file defines users whose passwords cannot be reset. Use the ESSAUTH member to list the Userids whose passwords cannot be reset: specific Userids, generic Userids, or a combination.

You can specify Generic User IDs in the password checking file. To do this, enter a partial user ID followed by an asterisk. The application interprets any ID that begins with the string preceding the asterisk to be a match. For example, "ABC*" is a match for any ID beginning "ABC," such as "ABCDE" or "ABCXY."

Creating the Authorization Checking File

To create the Cour390 Authorization Checking File, follow these steps:

1. Create the Cour390 Authorization checking file. Use it to identify users whose password cannot be reset. You can use any valid filename.
2. Enter a line for each user whose password changes you want to prevent. Each line must begin in column 1. Use the format

```
DENYPWCHANGE,USERID=userID
```

If you have a User ID defined (or defined generically) using this parameter, Cour390 does not honor a password change request from that User ID. The default is to honor all requests.

All lines must begin with DENYPWCHANGE. The parameters that follow can be in any order. An asterisk in line 1 indicates a comment.

You can specify many parameter lines. To continue a line, place a comma and at least one space after the last parameter on the line. For example,

```
DENYPWCHANGE,USERID=TSTUSR
```

```
DENYPWCHANGE,USERID=AUDIT*
```

These lines cause Cour390 to honor all password change requests except TSTUSR and all User IDs starting with AUDIT.

```
DENYPWCHANGE,USERID=*
```

If you use the asterisk this way, Cour390 denies all password change requests.

3. Modify the following DD statement in the Cour390 startup JCL pointing to the parameter file created in step 1.

```
//ESSAUTH DD DSN=cour390.samplib(ESSAUTH),DISP=SHR
```

where:

cour390.samplib(ESSAUTH) names the parameter file. When the Cour390 started task is started, Cour390 validates the parameter definitions and display messages about errors. After validating, Cour390 displays the following message:

```
ZCOS1811I ESSAUTH Processing complete - Good Records
xxxxxxx Error records yyyyyyy
```

If an error occurs, a message is displayed with the record number and text of the errant record.

Refreshing the Authorization Checking File

To refresh the Cour390 ESSAUTH file without bringing Cour390 down and up:

1. Change the Cour390 member defined by the ESSAUTH DD statement.
2. Type the following operator command at the console:

```
F Cour390,ESSAUTHREFRESH
```

This results in a message similar to the following:

```
ZCOE1811I  ESSAUTH Processing complete - Good records: xxxx  
Error records: yyyy
```

Operating the Cour390 Agent

This section explains detail how to operate the Cour390 agent from the z/OS operator's console. It describes:

- Commands to the Cour390 Agent
- FTP Communications Tracing
- Troubleshooting

Commands to the Cour390 Agent

There are ten commands, some of which start/stop the TCP interface and TCP packet tracing, shown in Table 41. They all use a procedure name, which must be member of a JES PROCLIB that contains the Cour390 startup JCL (for example, `xxxx.PROCLIB(Cour390)`). In examples, the table shows the procedure name (*procname*) as COUR390.

Table 41: Commands to the Cour390 Agent

Command Function	Command Syntax	Example
Displays agent status	D A, <i>procname</i>	D A, COUR390
Starts agent	S <i>procname</i>	S COUR390
Stops agent. Prevents the agent from accepting requests and stops it after current transmissions end.	P <i>procname</i> F <i>procname</i> , STOP	S COUR390
Displays agent version in the form shown for message ZCOS2571I on page 688 .	F <i>procname</i> , VER	F COUR390, VER
Activate changes to the Global parameter file	F <i>procname</i> , GLOBALREFRESH	F COUR390, GLOBALREFRESH
Starts agent TCP packet tracing	F <i>procname</i> , TCPTRON	F COUR390, TCPTRON
Stops agent TCP packet tracing	F <i>procname</i> , TCPTRON	F COUR390, TCPTROF
Starts agent TCP interface. Use this command only if the agent TCP interface did not start properly or was ended via the TERMTCP command.	F <i>procname</i> , STARTTCP	F COUR390, STARTTCP
Stops the agent TCP interface. Use this command only if the TCP subsystem has come down while Cour390 was running. This command terminates all TCP responder tasks.	F <i>procname</i> , TERMTCP	F COUR390, TERMTCP
Refreshes the agent Authorization checking file after updating.	F <i>procname</i> , ESSAUTHREFRESH	F COUR390, ESSAUTHREFRESH

To see if Cour390 is up and running, issue the following display command:

```
D A, COUR390 (where Cour390 is the agent process name)
```

FTP Communications Tracing

To solve a communication problem, Technical Support might ask you to take a trace of the activity in error. You can turn the TCP tracing facility on and off using the commands shown in [Table 41, “Commands to the Cour390 Agent,” on page 662](#). The following DD statement must be included in the start up JCL to enable the tracing facility.

```
//TCPTRAC DD SYSOUT=&OUTC
```

Steps to taking a trace are:

1. Start the TCP trace.

```
F Cour390, TCPTRON
```
2. Perform the activity you need to trace.
3. Turn off the TCP trace

```
F Cour390, TCPTROFF
```

TCP trace data is sent to DD statement TCPTRAC defined in the Cour390 JCL.

Troubleshooting

Use this section to troubleshoot errors that occur with Cour390. When you are trying to diagnose errors, specify Global parameter ESSDEBUG=LOG to record information in the agent log.

Table 42: Troubleshooting Cour390 Errors

Activity	Problem	Solution
Issuing the RECEIVE command	You receive the following message: You receive the following message: Incorrect Record / Block Length	Make the record length fixed block 80.
	You receive the following message: <pre>RECEIVE INDS(hlq.recv.loadlib) Restore not possible. Input data is not complete. The first record is: Received file appears not to be an Interactive Data Transmission Facility file.X'00FF0000' Data set X.RECEIVE.INVALID.FILE from USERID on N1 Enter copy parameters or 'DELETE' or 'END' +</pre> You transmitted the file with ASCII / EBCDIC conversion.	Transmit the file as a binary file, with no conversion.
Agent startup (Starting the started task)	Cour390 issues the message <pre>"ZCOS0013E Server: Cour390 not APF Authorized - started task terminating"</pre> and terminates. Problem is that Cour390 is not running in an APF authorized LOADLIB.	You must authorize the LOADLIB and ensure that there are no non-APF libraries specified in the STEPLIB DD of the agent JCL. This is explained in "Installing or Upgrading the Cour390 Agent" on page 633.
Agent startup	TCP transmission errors. Cour390 cannot communicate with TCP server. Possible messages ZCOV1710E and ZCOV1713E during Cour390 startup. Possible causes: TheCour390 Started Task started before TCP was fully initialized. Incorrect jobname specified in Global parm TCPIPJOBNAME. Incorrect or in-use port specified in Global parm TCPIPPORT	Allow the TCP/IP task to fully initialize before starting Cour390. Specify the correct job name. Specify a valid, unused port.

Table 42: Troubleshooting Cour390 Errors (Continued)

Activity	Problem	Solution
Any	Validation failure during PMM or connector configuration Possible causes: Incorrect userid/password for the Core Server Administrative user during PMM or Connector configuration The Core Security Administrative user does not have access to the Core Security Resource. The Core Security Administrative userid has expired or is revoked.	Examine the agent log for message ZCOE1843E or ZCOE2143E, which contains a detailed description of the problem. (Global parameter ESSDEBUG=LOG must be specified.) Find and use the correct userid and password. Have the security administrator assign the ID Read access to the Courion Resource Profile created during Cour390 configuration. Have the security administrator restore the userid.
Any	Validation failure during PMM or connector configuration, with garbage in the Userid field of messages ZCOE1849I or ZCOE2149I. The value specified in Global parameter 3DES_SEED does not match the value specified for the Security Phrase field during PMM/Connector configuration. Message ZCOE1849I sometimes contains a garbage Userid because of failures not related to the Security Phrase. In these cases, Courion password-related applications have issued two consecutive requests for the requests for the same service (typically, within milliseconds). The first request failed, and the second was issued using different encryption.	The value specified in Global parameter 3DES_SEED does not match the value specified for the Security Phrase field during PMM/Connector configuration. When examining the value in the GLOBAL parameter, verify that there are no sequence numbers in columns 73-80.

If the above hints do not help and you still require technical assistance contact support@CoreSecurity.com.

Members Distributed with the Cour390 Agent

The following members can be found in the SAMPLIB PDS distributed with the Cour390 agent.

Table 43: Z/OS Members Used with the Cour390 Agent

Member Name	Description
ACF2	CA-ACF2. The ACF2 member contains the ACF2 commands that define the users and resources needed by the Cour390 agent. Follow the instructions in this member to modify it and submit member ACF2JOB to execute the commands. See section “Configuring the CA-ACF2 Security Interface” on page 649 for instructions in using this member. You can modify and use member ACF2JOB to execute the customized commands you create.
APFAUTH	The APFAUTH member contains the operator command necessary to APF authorize the Cour390 Load Library. During agent installation, you add the APF command to the appropriate PROGxx member in use at your installation.
CONFIG	The CONFIG member is retained for compatibility with previous releases. The Cour390 JCL must include a CONFIG DD statement. We recommend using the CONFIG DD, and the CONFIG member of SAMPLIB, as coded in the example JCL shipped with Cour390.
ESSAUTH	The ESSAUTH member contains entries describing UserID that cannot be reset by the Core Access Assurance Suite. Use the DENY PWCHANGE operation to list specific or generic UserIDs for which password resets should be denied. Details appear in “Using the Cour390 Authorization Checking File” on page 660
GLOBAL	The GLOBAL member contains examples of the options you need to specify for the Cour390 agent. Before attempting to start the Cour390 agent, you should customize a copy of this member as described in section “Creating the GLOBAL Member” on page 635.
RACF	RACF. The RACF member contains the RACF commands that define the users and resources needed by the Cour390 agent. See “Configuring the RACF Security Interface” on page 642 for instructions in using this member. You can modify and use member RACFJOB to execute the customized commands you create.
TSS	CA-Top Secret. The TSS member contains the CA-Top Secret commands that define the users and resources needed by the Cour390 agent. See “Configuring the CA-Top Secret Security Interface” on page 653 for instructions in using this member. You can modify and use member TSSJOB to execute the customized commands you create.

Cour390 SMF Report

This section describes:

- Generating a Cour390 Transaction Detail Report.
- Format of log records Cour390 writes to SMF.
- Cour390 return codes.

Cour390 SMF Report Program (ESSMFRPT)

If you define an SMF Record Number to Cour390, it writes an SMF record whenever a Core Password or Core Provisioning request completes. You define the SMF record number to be used by Cour390 with the GLOBAL parameter ESS_SMF#. The same record number is used by both PasswordCourier and AccountCourier.

If you do not want Cour390 to write SMF records, either omit the parameter ESS_SMF# from GLOBAL, or code ESS_SMF#=NO.

Program ESSMFRPT uses Cour390 SMF records to produce a Cour390 Transaction Detail Report. SAMPLIB member ESSMFRPT contains the following sample JCL, used to execute this program.

```
//REPORT    EXEC PGM=ESSMFRPT
//STEPLIB   DD  DISP=SHR,DSN=COUR390.LOAD
//INPUT     DD  DISP=SHR,DSN=$$SMF$$           <===== SMF data
//GLOBAL    DD  DISP=SHR,DSN=COUR390.SAMPLIB(GLOBAL)
//ESSREQ    DD  SYSOUT=*                       <===== Transaction detail
//SYSPRINT  DD  SYSOUT=*
//SYSUDUMP  DD  SYSOUT=*
```

The GLOBAL DD statement is required for ESSMFRPT to determine the SMF record number used by Cour390. The data set referenced must contain the parameter ESS_SMF#=n, where n is the SMF record number used by Cour390. This can be the GLOBAL member used by Cour390, or another data set containing a copy of the ESS_SMF# parameter used by Cour390.

The INPUT DD statement is required, and points to a dataset containing Cour390 SMF records. ESSMFRPT bypasses any non-Cour390 SMF records in the input dataset.

The ESSREQ DD statement defines the target for the Cour390 Transaction Detail Report. In this example, ESSREQ is written to a SYSOUT dataset. It can be directed to any sequential dataset, and uses the DCB attributes:

```
RECFM=FBA
LRECL=133
BLKSIZE=1330
```

The SYSPRINT DD is required and contains status and diagnostic messages. In this example, SYSPRINT is written to a SYSOUT dataset. It can be directed to any sequential dataset, and uses the DCB attributes:

```
RECFM=FB
LRECL=120
BLKSIZE=1200
```

Format of Cour390 Log Records

Cour390 log records are written to SMF when a request completes – either successfully or unsuccessfully. The log record is written only if the GLOBAL parameter ESS_SMF# specifies a valid SMF record number. By specifying ESS_SMF#=NO, Cour390 does not write a log record to SMF.

The Cour390 Log record is written using the same format as the RACF SMF80 record. The following fields in the header section of the SMF80 record reflect information unique to PasswordCourier:

SMF80USR	The User ID associated with the request
SMF80EVT	The Cour390 request type
SMF80EVQ	The Cour390 return code
SMF80REL	The offset to the first Cour390 relocate section
SMF80VRM	The Cour390 Version
SMF80JBN	The name of the Cour390 started task

Cour390 uses the relocate section to fully define all of the fields that are used. The format of the relocate section is as follows:

: byte 0	The data type
: byte 1	The length of the data (not including byte0 or byte1)
: byte 2-n	The data

The following relocate sections are used. They do not correspond with the relocate sections used by RACF in the SMF80 record.

Table 44: Cour390 Relocate Sections

Data Type	Description
1	The User ID acted upon by the request
2	Not currently implemented
3	Not currently implemented
4	Not currently implemented
5	The Cour390 request type Bit 0: 1: indicates an asynchronous response 0: indicates a request Bits 1-7. x'01' Validate Userid/Password x'02' Change Password request x'03' Delete user x'05' Resume User x'06' Reset Violation x'07" Add User
6	Not currently implemented
7	The Cour390 return code (documented in the following table)
8	The Cour390 text message associated with the request

Table 44: Cour390 Relocate Sections (Continued)

9	The Cour390 RESUME date (nulls if request not RESUME) This date is an 8-byte binary value in the following format: Bytes 0,1 yyyy year including century (in binary) Bytes 2,3 mmmm month (x'0001 through x'000c') Bytes 4,5 dw dw Day of the week (x'0001' through x'0007') Bytes 6,7 dddd Day of the month (x'0001 through x'001f')
10	The name of the remote node associated with the request
11	Not currently implemented
12	Not currently implemented
13	The User Name of the new user (Add User requests only)
14	The Model Userid used to create the new user (Add User requests only)
15	The Revoke Date (Add User requests only)
16	The Resume Date or "Immediate" (Add User and Resume requests only)

Cour390 Return Codes

Table 45: Cour390 Return Codes

Return Code (Hex)	Description
00	Transaction successful
01	Transaction pending
02	Request rejected/system shutdown pending
0b	User ID not defined to security system.
10	Password not valid
14	Password not valid
14	Password expired
18	New password invalid
20	Account Suspended
22	Account Revoked
30	Password Truncated
31	Null Password
32	Password has spaces
33	Password Has Bad Characters (Validation/Change)
34	Request denied by configuration
35	Request not honored
36	Password too short
37	Password contains reserved word
38	Password has no upper case letters
39	Password has no lower case letters
3a	Password has no numbers
3b	Password has no special characters
3c	Password has too few letters
3d	Password has too few unique characters

Table 45: Cour390 Return Codes (Continued)

3e	Password matches the User ID
40	Delete request: Account revoked, not deleted
41	Not authorized for requested command
50	Product not authorized

Error and Status Messages

The Cour390 agent might display (or write to the log file) any of the following messages when it starts or while it runs.

ZCOS0000I Another Server with the name: xxxx is active

Explanation: Another Core Security Agent with the same name is already active. The Agent issuing the message automatically shuts down.

ZCOS0001E Variable error text

Explanation: Cour390 received an error from the Security System (RACF, ACF2 or Top Secret) while processing a request. The variable text describes the nature of the error. Contact Courion Support, providing the full text of this message.

ZCOS0012I OSIMSGS LOG File Freed

Explanation: This is an informational message issued in response to the RELEASE,LOG Cour390 Operator command.

ZCOS0022I CPU Information: Version Code=xxxx Id Number=yyyy Model Number=zzzz

Explanation: WTO to issue CPU information from the Core Security Agent.

ZCOS0023E ***LOG DATASET FULL - MESSAGE NOT LOGGED*******

Explanation: The log data set is full and does not record any more messages.

ZCOS0024I Message xxxx not found

Explanation: If you receive this message, contact Core Security customer support. Supply the message number that you received as indicated by the "xxxx".

ZCOS0026I Cour390 Agent Suite xxxx initialized

Explanation: The Cour390 Agent started task is starting.

ZCOS0031I Core Security Advanced TCP services xxxx

Explanation: This message states whether the TCP services are loaded or not, and the reason.

ZCOS0032I [Cour390SNA | Cour390TCP |PasswordCourier] request by xxxx Denied - Application NOT authorized by GLOBAL key

Explanation: This application must be authorized by applying the correct licensing key for the product in the Global member.

ZCOS0038I Core Security Agent xxxx Shutting Down

Explanation: The Core Security Agent started task is in the process of termination. This is a normal message.

ZCOS0039I RDJFCB failed - Audit DSN not found

Explanation: The Audit data set must be defined before bringing up the Core Security Agent started task. Use the DEFAUDIT member in the Samplib data set as an example of how to define the Audit data set.

ZCOS0056E ESSERVER: SYNTAX ERROR IN PARM FIELD: xxxx

Explanation: During startup of the Cour390 task an error was detected in the PARM field specified on the EXEC statement. Correct the error and restart Cour390.

ZCOS0057E ESSERVER: INVALID PARAMETER IN PARM: xxxx

Explanation: An invalid parameter was detected. Correct the PARM field on the EXEC statement and restart Cour390.

ZCOS0058E ESSERVER: TOO MANY PARM PARAMETERS

Explanation: Too many parameters were passed to Cour390, correct the PARM field on the EXEC statement and restart Cour390.

ZCOS0059E ESSERVER: INVALID DATA IN PARAMETER: xxxx

Explanation: An invalid operand was passed to a parameter. Correct the PARM field on the EXEC statement and restart Cour390.

ZCOS0060E ESSERVER: Errors in PARM field - Started task terminating

Explanation: An error detected parsing the parameters. See previous message for a detailed description of that error.

ZCOS0099I SERVER: XXXXXXXX SUCCESSFULLY TERMINATED

Explanation: The Core Security Agent specified in the message shut down successfully.

ZCOS0234I Message data set closed

Explanation: This is a normal message that appears during shut down of the started task.

ZCOS0235I Audit data set closed

Explanation: This is a normal message that appears during shut down of the started task.

ZCOS0789E LOAD FAILED FOR MODULE xxxx

Explanation: This message is displayed when the started task is brought up. If you receive this message contact Core Security customer support.

ZCOS0804E Logging error detected - taking SNAP dump - logging is terminated

Explanation: An Internal error has occurred. Save the dump that produced and contact Core Security customer support for assistance.

ZCOS0820I Performing LOGSNAP to DD SNAPLOG

Explanation: A snap dump is being taken and is sent to the data set that is defined in the SNAPLOG DD statement in the started task PROC.

ZCOS0821I LOGSNAP Dump Complete

Explanation: A snap dump was taken and is now complete.

ZCOS0822E Error opening SNAPLOG DD stmt - LOGSNAP terminated

Explanation: A snap dump could not be taken because the SNAPLOG DD statement in the started task procedure is either missing or incorrect.

ZCOS0823I LOGSNAP Log address range: xxxx Vector address range: yyyy Log STOKEN=zzzz

Explanation: This is an informational message used for debugging purposes.

ZCOS0996I Stop command being processed

Explanation: This is a normal message that appears during shut down of the started task.

ZCOS0997I Core Security Server Suite dataspace initialization complete

Explanation: This is a normal message that appears during start up of the started task.

ZCOS0998I Core Security Server Suite Cross Memory Services environment setup successfully completed

Explanation: This is a normal message that appears during start up the started task.

ZCOS0999I Core Security Server Suite deleting dataspaces

Explanation: This is a normal message that appears during shut down of the started task.

ZCOS1001E Error opening DD statement GLOBAL - using default global values

Explanation: There was an error encountered while opening the DD statement for the global parameters. Under this condition the default global values are used.

ZCOS1002E xxxx GLOBAL parameter invalid

Explanation: The Global parameter specified is invalid. Check your global definitions and correct the error.

ZCOS1012E SMF parameter invalid - must be NO, or numeric value between 192 and 255

Explanation: Check your global definitions and correct the error.

ZCOS1016E ERRDESC parameter invalid - refer to installation manual for correct format

Explanation: Check your global definitions and correct the error.

ZCOS1017E ERRROUTE parameter invalid - refer to in installation manual for correct format

Explanation: Check your global definitions and correct the error.

ZCOS1019E INFOROUTE parameter invalid - refer to installation manual for correct format

Explanation: Check your global definitions and correct the error.

ZCOS1020E Maximum length exceeded for parameter xxxx

Explanation: The parameter specified is invalid. Check your global definitions and correct the error.

ZCOS1039E ESSCLASS must be TERMINAL/DATASET/FACILITY

Explanation: Check your global definitions and correct the error.

ZCOS1040E ESSVOLSER must be 6 bytes or less

Explanation: Check your global definitions and correct the error.

ZCOS1052E Global configuration dataset is empty - no parameters found

Explanation: Check your global definitions and correct the error.

ZCOS1053E ESSDEBUG must be WTO/LOG/NO - error

Explanation: Check your global definitions and correct the error.

ZCOS1055E ESSTIMEOUT MUST BE NUMBER SUFFIXED BY S, M, H, OR D - SEE Core Security MANUAL FOR DETAILS

Explanation: Check your global definitions and correct the error.

ZCOS1056E ESSLOCKUSER must be YES/NO - error

Explanation: Check your global definitions and correct the error.

ZCOS1057E IO_BUFNO must be a value between 1 and 255

Explanation: Check your global definitions and correct the error.

ZCOS1059E TCPIPJOBNAME must be from 1 to 8 characters

Explanation: Check your global definitions and correct the error.

ZCOS1060E TCPIPSPORT must be 2500 or a value from 5000 to 65535

Explanation: Check your global definitions and correct the error.

ZCOS1061E ESSHARMONIZATION must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1062E ESSALLOWLONGPASSWORDS must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1063E ESSMINIMUMPASSWORDLENGTH must be a value from 4 to 8

Explanation: Check your global definitions and correct the error.

ZCOS1064E ESSREQUIREUPPERANDLOWERCASE must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1065E ESSREQUIRELETTERSANDNUMBERS must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1066E ESSREQUIRESPECIALCHARACTER must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1067E ESSUNIQUECHARACTERSREQUIRED# must be a value from 4 to 8

Explanation: Check your global definitions and correct the error.

ZCOS1068E ESSMINIMUMLETTERSREQUIRED must be a value from 2 to 8

Explanation: Check your global definitions and correct the error.

ZCOS1069E RESETINTERVAL must be a numeric value from 1 to 60

Explanation: Check your global definitions and correct the error.

ZCOS1073E ESSSTRONGPASSWORDRULES must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1074E MAX_AUDIT_RECORDS must be numeric and greater than 99 - using default of 25000

Explanation: Check your global definitions and correct the error.

ZCOS1075E TRAP_IPADDR PARAMETER IS INVALID

Explanation: Check your global definitions and correct the error.

ZCOS1086E ESS_ACCEPT_REVOKE_RESUME MUST BE YES, ALL, MVS OR NO

Explanation: Check your global definitions and correct the error.

ZCOS1087E [ESS_SMF# | ESS_SMF#] MUST BE IN THE RANGE OF 128 to 255

Explanation: Check your global definitions and correct the error.

ZCOS1088E Invalid GLOBAL parameter on record NNN: Record follows

Explanation: The parameter on the indicated record is not valid. Message ZCOS1089E displays the record.

ZCOS1089E GLOBAL DATA: xxxxxxxxxxxxxxxxxxxxxxxxx

Explanation: This is the invalid record in the global definitions. Check your global definitions and correct the error.

ZCOS1090E ESS_EXPIRE_PASSWORD must be YES or NO

Explanation: Check your global definitions and correct the error.

ZCOS1091E ESS_REQUIRE_NODE_DEFINITION MUST BE YES OR NO

Explanation: Check your global definitions and correct the error.

ZCOS1096E ESS_PASSWORD_SYNTAX_RULES must be LOCAL, RACF, or BOTH

Explanation: The ESS_PASSWORD_SYNTAX_RULES parameter in the global definitions must be LOCAL, RACF, or BOTH. Check your global definitions and correct the error, then recycle the started task.

ZCOS1097W Local security is not RACF - defaulting ESS_PASSWORD_SYNTAX_RULES to LOCAL

Explanation: This is only a warning message and no action is required. However, since it was detected that RACF is not running on the system, the ESS_PASSWORD_SYNTAX_RULES parameter in the global definitions should be changed to LOCAL or removed and defaulted. Check your global definitions and correct the error, then recycle the started task.

ZCOS1101E Error opening DD statement CONFIG - unable to read node configuration file

Explanation: Check your CONFIG DD statement in your startup JCL. Correct the error and re-start the task.

ZCOS1102E CONFIG DD statement not defined with RECFM=FB and LRECL=80 - error

Explanation: Check your CONFIG DD statement in your startup JCL. Correct the error and re-start the task.

ZCOS1103E CONFIG file error - member name exceeds 8 bytes - reading next record

Explanation: Check your global definitions and correct the error.

ZCOS1104E Error reading CONFIG member xxxx - proceeding to the next member

Explanation: Check your global definitions and correct the error. Initialization continues, but the member xxxx stated in the message is not available for use.

ZCOS1342E ALLOW_SPECCHAR_PWS must be YES or NO. Option ignored.

Explanation: Global parameter ALLOW_SPECCHAR_PWS was entered with an invalid value. The Agent continues processing, and rejects passwords containing non-alphanumeric characters. To eliminate the error message, check your global definitions and correct the error, then recycle the started task.

ZCOS1343E ALLOW_SPECCHAR_PWS is not valid on RACF systems. Option ignored.

Explanation: Global parameter ALLOW_SPECCHAR_PWS=YES was specified on a RACF system. RACF does not support special characters in passwords. The Agent continues processing, and rejects passwords containing non-alphanumeric characters. To eliminate the error message, check your global definitions and correct the error, then recycle the started task.

ZCOT1621E Invalid Core Security request type xxxx received

Explanation: Transfer type is usually Send or Receive.

ZCOT1623E ATTACH for Module: FUSASNAR Failed - xxxx

Explanation: Could not attach module. Call Core Security customer support.

ZCOT1631E *Text-of-RACROUTE-failure-message*

Explanation: A RACROUTE request has failed. See the appropriate security packages documentation for the reason for the failure.

ZCOV1710E TCPERR xxxx on yyyy req ip=zzzz : nnnn

Explanation: A TCP/IP error has occurred. TCP return code is xxxx. yyyy is the type of TCP/IP request. zzzz is the IP address. nnnn is the meaning of the return code if known.

ZCOV1711E TCP Address Zero - possibly TCP connection not started

Explanation: Bad configuration or TCP/IP is not started. One possible cause is that the parameter specified for the TCP/IP jobname is incorrect in the global parameters.

ZCOV1712I TCP INITAPI successful for TCP STC xxxx - ASID yyyy

Explanation: This is an informational message that can also be used for debugging purposes.

ZCOV1713E TCP INITAPI FAILED FOR TCP STC xxxx - ASID yyyy - TCP processing terminated

Explanation: A TCP/IP request – INITAPI – has failed for TCP/IP job xxxx in ASID yyyy. Check that TCP/IP is still active. If the problem persists enable the Core Security Agent TCP/IP tracing (F servername,TCPTRON) and contact Core Security customer support.

ZCOT1714E IP nnn.nnn.nnn.nnn - received invalid data xxxx on yyyy request

Explanation: An error occurred with IP address nnn.nnn.nnn.nnn, data returned was xxxx on request yyyy. If the problem persists enable the Core Security Agent TCP/IP tracing (F servername,TCPTRON) and contact Core Security customer support.

ZCOT1715E IP nnn.nnn.nnn.nnn - received data length xxxx longer than Max Req. yyyy ConcatLen zzzz

Explanation: An internal error has occurred for IP address nnn.nnn.nnn.nnn. A record of length xxxx was received which exceeded yyyy or zzzz. If the problem persists enable the Core Security Agent TCP/IP tracing (F servername,TCPTRON) and contact Core Security customer support.

ZCOT1716E Invalid LU6.2 GDS received for IP nnn.nnn.nnn.nnn - GDS=xxxx

Explanation: An internal error has occurred for IP Address nnn.nnn.nnn.nnn, an invalid GDS xxxx was received. If the problem persists enable the Core Security Agent TCP/IP tracing (F servername,TCPTRON) and contact Core Security customer support.

ZCOT1717I TCP Responder Terminated for TCP Job xxxx in ASID yyyy

Explanation: This is a normal termination message.

ZCOT1718E FMH7 received in response to xxxx command - SENSE=yyyy Message follows

Explanation: An error has occurred refer to the following messages for a detailed description of the error.

ZCOT1719I TCP ASID xxxx now Listening on Port yyyy to TCP job zzzz

Explanation: This is a normal message that is displayed when the started task is setup to use TCP/IP. It states the started task name, the port it is listening on and the name of the TCP/IP job running on the system.

ZCOT1720E error opening TCPTRAC DD - TCP tracing Disabled

Explanation: The Core Security Agent encountered an error trying to open the file specified in the TCPTRAC DD statement specified in the startup PROC. Check the contents of the DD statement to verify that they were specified correctly.

ZCOT1721I TCP ASID xxxx NOT Listening on Port yyyy to TCP job zzzz

Explanation: This message is displayed when the started task is not setup to use TCP/IP. It states the started task name, the port and the name of the TCP/IP job running on the system.

ZCOT1722I IP request received from IP Addr: xxxx

Explanation: A request was received for a transfer using the IP address xxxx.

ZCOT1727E Zero length LU62 GDS received for IP nnn.nnn.nnn.nnn - GDS=xxxx

Explanation: GDS xxxx was received for IP address nnn.nnn.nnn.nnn with a zero length. This is an internal error. Recreate the problem with the Core Security Agent TCP/IP Tracing activated (F servername, TCPTRON) and contact Core Security customer support.

ZCOT1728E Error Data GDS (12F4) received for IP nnn.nnn.nnn.nnn - Errordata=xxxx

Explanation: An error data GDS was received from IP address nnn.nnn.nnn.nnn. The error data returned was xxxx. Recreate the problem with Core Security Agent TCP/IP Tracing activated (F servername, TCPTRON) and contact Core Security customer support

ZCOT1729E Invalid TCP GDS received for IP nnn.nnn.nnn.nnn

Explanation: An invalid GDS was received from IP address nnn.nnn.nnn.nnn. Recreate the problem with the Core Security Agent TCP/IP Tracing activated (F servername, TCPTRON) and contact Core Security customer support.

ZCOT1730E Invalid IP Dotted Decimal address: nnn.nnn.nnn.nnn

Explanation: The IP address giving in the IPADDR parameter was not of the proper format: nnn.nnn.nnn.nnn or is not defined to your system.

ZCOT1731I TCP Responder Program Terminating

Explanation: This is a normal message that is displayed when the started task is brought down.

ZCOT1732E Invalid Knet Header received for IP nnn.nnn.nnn.nnn - header=xxxx

Explanation: An invalid header xxxx received from IP address nnn.nnn.nnn.nnn. Recreate the problem with the Core Security Agent TCP/IP Tracing activated (F servername, TCPTRON) and contact Core Security customer support.

ZCOS1733I TCP RESPONDER WAITING FOR SUBTASKS TO END BEFORE QUIESCE

Explanation: This is a normal message that is displayed when there is a request to shut down the Core Security Agent while there are transactions using TCP/IP that are still active. When the transactions are completed then the Core Security Agent shuts down.

ZCOE1803I xxxx for Userid yyyy rejected: GLOBAL set to reject all xxxx requests

Explanation: Request xxxx was rejected due to GLOBAL option settings.

ZCOE1805E ESSAUTHF Open failed on DD ESSAUTH - Bypassing ESSAUTH File processing

Explanation: The Core Security Agent encountered an error trying to open the file specified in the ESSAUTH DD statement specified in the startup PROC. The Core Access Assurance Suite uses the security rules on the system and does not check the ESSAUTH member for security rules. If you wish to use the ESSAUTH member for security, then check the contents of the DD statement to verify that they were specified correctly.

ZCOE1806E ESSAUTH Invalid Request Type - Must be INCLUDE/EXCLUDE/DENYPWCHANGE: Record xxxx

Explanation: Each line of the ESSAUTH member must begin with INCLUDE, EXCLUDE or DENYPWCHANGE. Anything else is invalid.

ZCOE1807E ESSAUTH USERID/ALIAS parameters must be both Generic or both NOT Generic: Record xxxx

Explanation: An error was encountered processing the ESSAUTH DD statement. Either, the USERID is generic and the ALIAS is specific, or, the USERID is specific and the ALIAS is generic. The USERID and ALIAS must both be generic i.e.: USERID=PR*,ALIAS=NT* Or, The USERID and ALIAS must be both specific i.e.: USERID=IBMUSER,ALIAS=NTUSER

ZCOE1808E ESSAUTH Required parameter xxxx missing on yyyy request: Record zzzz

Explanation: Include, Exclude and Denypwchange are the values that are required first in the ESSAUTH member. The Include statement must also include the USERID, NODE and DOMAIN parameters.

ZCOE1809E ESSAUTH Invalid Parameter xxxx: Incorrect length or incorrect parameter: Record xxxx

Explanation: The parameter xxxx is invalid. It is either incorrect or too long.

ZCOE1810E ESSAUTH Node: xxxx not found in Node table: Record xxxx

Explanation: Value given for the NODE parameter in the ESSAUTH member is not correct. Check the Node and CONFIG members in the Samplib to make sure that it is defined properly.

ZCOE1811I ESSAUTH Processing complete - Good records: xxxx Error records: yyyy

Explanation: When the Core Access Assurance Suite started task is brought up, it checks the ESSAUTH DD statement and then the ESSAUTH member. Each line of this member is checked for validity and reported in this message at startup.

ZCOE1812E ESSAUTH End of File received - expecting continuation record

Explanation: The Include, Exclude and Denypwchange can be continued on multiple lines. Most likely one of the lines ends in a comma, therefore the Core Access Assurance Suite is expecting the record to be continued on the next line.

ZCOE1813E ESSAUTH Found INCLUDE/EXCLUDE/DENYPWCHANGE - expecting continuation data: xxxx

Explanation: The Include, Exclude and Denypwchange can be continued on multiple lines. Most likely one of the lines ends in a comma, therefore the Core Access Assurance Suite is expecting the record to be continued on the next line.

ZCOE1830E PasswordCourier: Event received - PasswordCourier audit processing not turned on

Explanation: The Core Access Assurance Suite received an event record, but the audit processing was not turned on. The audit processing can be turned on by using an operator command (F server_name,SECAUDIT,YES) or by using a Global parameter (ESS_AUDIT_SMF=YES)

ZCOE1832I PasswordCourier Enterprise coldstart complete: xxxx requests purged from SPASS dataspace

Explanation: This is an informational message. This message is displayed when the Core Access Assurance Suite is brought up using the coldstart parameter when there were requests left on the queue.

ZCOE1833I PasswordCourier: Clearing task error flag for node xxxx - task put back on dispatch chain

Explanation: When an Core Access Assurance Suite transaction received a network error, it is marked as an error. When the interval specified by the GLOBAL RESETINTERVAL expires, the error flags for all transactions are reset, and the transactions can be executed again.

ZCOE1834I Alert msg from xxxx: yyyy

Explanation: The Core Access Assurance Suite displays this message when a network component has detected an alert, and wants to issue a notification message to the z/OS console. xxxx defines the name of the computer, while yyyy is the text message that was sent._

ZCOE1836I PasswordCourier: Responder Transaction tttttttttttt Terminated with node xxxx

Explanation: This is a normal informational message that is displayed when a request completes – either successfully or unsuccessfully. tttttttttttt is the 16 byte Transaction ID.

ZCOE1837I PasswordCourier: Responder Transid tttttttttttt started for Userid xxxx from NODE xxxx

Explanation: This is an informational message, where tttttttttttt is the 16 byte Transaction ID.

ZCOE1838E PasswordCourier: Network error received on Responder request from Node: xxxx

Explanation: There was an error with the node that is displayed in the message.

ZCOE1839E PasswordCourier: Return code xxxx received from ESSTLV: yyyy

Explanation: **Cour390 encountered an internal error while processing a PasswordCourier or AccountCourier request. Contact Courion Customer Support, supplying the full text of this message.**

ZCOE1840E PasswordCourier: Invalid request type: xxxx received - activity terminated

Explanation: Cour390 received an invalid request from a remote user. Request type xxxx is not known to Cour390. Contact Courion Customer Support, supplying the full text of this message.

ZCOE1842I PasswordCourier: xxxx request completed successfully for Userid: yyyy Node: zzzz

Explanation: This is an this is a normal message displayed when the request was successful.

ZCOE1843E xxxx << message from ESSRACR >>

Explanation: Cour390 encountered an internal error while processing a PasswordCourier request. Contact Core Security Customer Support, supplying the full text of this message.

ZCOE1844E PasswordCourier: New password failed Validation code=xxxx: yyyy

Explanation: The new password that was entered does not comply with the password rules that have been defined.

ZCOE1845E PasswordCourier: New password failed Strong Password Content Rules code=xxxx: yyyy

Explanation: The new password that was entered does not comply with the password content rules that have been defined.

ZCOE1846E PasswordCourier: Request xxxx for Userid yyyy failed: DENIED by ESSAUTH config file

Explanation: This request was denied because of the rules that have been defined in the ESSAUTH member. Please check the rules for that userid in the ESSAUTH member and re-submit the request.

ZCOE1847E PasswordCourier: Response xxxx for Userid yyyy failed code=zzzz: nnnn

Explanation: Informational message stating the type of request (xxxx), the user (yyyy), the return code (zzzz) and the reason for the return code (nnnn).

ZCOE1849I PasswordCourier: xxxx Userid=yyyy Code=zzzz: nnnn

Explanation: This is an informational message that states whether or not the transaction was successful.

ZCOE1850I PasswordCourier: SMF record written for event code: xxxx

Explanation: This is an informational message that an SMF record was written.

ZCOE1851I PasswordCourier: Initiator activity started with node xxxx

Explanation: This is an informational message.

ZCOE1852I PasswordCourier: Initiator activity Terminated with node xxxx

Explanation: This is an informational message.

ZCOE1853E PasswordCourier: Initiator received Deallocate without response for node: xxxx

Explanation: Informational message that the request has finished (whether good or bad) and is now being purged from the Core Access Assurance Suite data space.

ZCOE1855I PasswordCourier: Initiator xxxx request for user: yyyy Return Code=zzzz: nnnn

Explanation: Informational message stating the type of request (xxxx), the user (yyyy), the return code (zzzz) and the reason for the return code (nnnn).

ZCOE1856E PasswordCourier: Initiator xxxx for Userid yyyy failed code=zzzz: nnnn

Explanation: Informational message stating the type of request (xxxx), the user (yyyy), the return code (zzzz) and the reason for the return code (nnnn).

ZCOE1858E PasswordCourier: Password content rules failed code=xxxx: yyyy

Explanation: This message indicates the code for the failure and the reason for the failure.

ZCOE1859I PasswordCourier: Transaction *transid* Added to ESSDSP - ALET=xxxx Addr=yyyy

Explanation: This is an informational message.

ZCOE1860I PasswordCourier: Transaction *transid* Refreshed in ESSDSP - ALET=xxxx Old Addr=yyyy New Addr=zzzz

Explanation: This is an informational message.

ZCOE1861E PasswordCourier: OSISX00B ALET invalid - contact Core Security customer support

Explanation: This is an internal error and should not be issued. If you receive this error, contact Core Security customer support.

ZCOE1862E PasswordCourier: OSISX00B no free slots on ESSDSP

Explanation: This means that there is no more space in the Core Access Assurance Suite work queue. Purge old requests from the queue or let activities complete. You may wish to rebuild the work queue to make it larger.

ZCOE1863I PasswordCourier: Transaction *transid* Purged from ESSDSP - ALET=xxxx Addr=yyyy

Explanation: This is an informational message.

ZCOE1864I PasswordCourier: ESSAUTH INCLUDE USER=*userid*

Explanation: This is an informational message that states that the user is defined in the ESSAUTH member that is used for strong password content rules.

ZCOE1865I PasswordCourier: ESSAUTH EXCLUDE ALL USER=*userid*

Explanation: This is an informational message that states that the user is excluded in the ESSAUTH member that is used for strong password content rules and is not affected by any changes made by the Core Access Assurance Suite.

ZCOE1866I PasswordCourier: ESSAUTH USER=*userid* NOT FOUND

Explanation: This is an informational message that states that the user is not defined in the ESSAUTH member that is used for strong password content rules.

ZCOE1867I PasswordCourier: ESSAUTH INCLUDE User=xxxx Node=yyyy Domain=zzzz

Explanation: This is an informational message about user information in the ESSAUTH member.

ZCOE1868I PasswordCourier: ESSAUTH EXCLUDE User=xxxx Node=yyyy Domain=zzzz

Explanation: This is an informational message about user information in the ESSAUTH member.

ZCOE1869I PasswordCourier: ESSAUTH EXCLUDE ALL User=xxxx

Explanation: This is an informational message about user information in the ESSAUTH member.

ZCOE1870I PasswordCourier: Successful ESSRACR request xxxx for user yyyy

Explanation: This is an informational message that states that the Core Access Assurance Suite has authenticated the userid and password for this user.

ZCOE1871I PasswordCourier: ESSRACR xxxx request for user yyyy failed code=zzzz: nnnn

Explanation: This is an informational message that states that the Core Access Assurance Suite could not authenticate the userid and password for this user.

ZCOE1872E ESSAUTH too many parameters entered for one ESSAUTH request: xxxx

Explanation: There are too many parameter for the Include, Exclude of Denypwchange record of the ESSAUTH.

ZCOE1873E ESSAUTH Duplicate request parameter entered: Record xxxx

Explanation: There is a duplicate record in the ESSAUTH member.

ZCOV1880E RACF CVT NOT FOUND - ENDING

Explanation: In an attempt to stop the RACF password change exit, the RACF Communications Vector Table (CVT) was not found.

ZCOE1896I ESSSNAP Dump Complete

Explanation: A snap dump was taken and is now complete.

ZCOE1897I Performing ESSSNAP to DD SNAP

Explanation: A snap dump is being taken and is sent to the data set that is defined in the SNAP DD statement in the started task PROC.

ZCOE1898E Error opening SNAP DD stmt - ESSSNAP terminated

Explanation: A snap dump could not be taken because the SNAP DD statement in the started task PROC is either missing or incorrect.

ZCOE1899I xxxx

Explanation: Debug message for Core Security's internal use.

ZCOE1930I PasswordCourier: Transaction transid for user userid failed: User not authorized by ESSAUTH table

Explanation: The global parameter ESSVALIDATEINCOMING is set to YES to determine whether incoming requests (requests initiated in another the Core Access Assurance Suite node and sent

to this Core Access Assurance Suite node) are validated against the Core Access Assurance Suite ESSAUTH table. This user could not be validated.

ZCOE1931I Incoming Validate failed User=userid code=RC: message

Explanation: The global parameter ESSVALIDATEINCOMING is set to YES to determine whether incoming requests (requests initiated in another the Core Access Assurance Suite node and sent to this Core Access Assurance Suite node) are validated against the Core Access Assurance Suite ESSAUTH table. This user could not be validated.

ZCOE1932I PasswordCourier: Transaction transid for user userid failed: User excluded by ESSAUTH node node_name

Explanation: The global parameter ESSVALIDATEINCOMING is set to YES to determine whether incoming requests (requests initiated in another the Core Access Assurance Suite node and sent to this Core Access Assurance Suite node) are validated against the Core Access Assurance Suite ESSAUTH table. This user is specifically EXCLUDED in the ESSAUTH table.

ZCOE1933I ESSWORDL Processing complete - Number of Reserved Words: XX Discarded: XX Truncated: XX

Explanation: This is an informational message. After reading the user defined reserved word list this message gives the number of words added to the list, the number discarded because they are duplicates or go into column 72, and the number truncated because they are more the eight characters.

ZCOE1934E ESSWORDL FINDVECT Request Failed

Explanation: This is an internal error and should not be issued. If you receive this error, contact Core Security customer support.

ZCOE1935E ESSWORDL Open failed on DD ESSWORDL - Bypassing ESSWORDL File processing

Explanation: The Core Access Assurance Suite was unable to open the file specified in the start up JCL with the ESSWORDL DD statement. Check the accompanying messages on the console and correct the problem.

ZCOE1936W ESSWORDL Duplicate reserved word found is be discarded: word

Explanation: This word has already been processed, so it is discarded. Remove the duplicate word from the list.

ZCOE1937E DD ESSWORDL required but not found - command execution terminated

Explanation: The ESSWORDL DD statement is missing from the start up JCL for this STC. Add the DD statement and recycle the STC.

ZCOE1938E ESSWORDL Column 72 not blank - Discarding word: @1

Explanation: Column 72 must be left blank in the user defined reserved word list. If a word does not fit on the line with a space in column 72, simply add the word to the next line. Any word going into column 72 is discarded.

ZCOE1939E ESSWORDL Reserved Word more than 8 characters is truncated: @1

Explanation: Reserved words in the user defined reserved word list must be a maximum of eight characters. Any words longer than eight characters are truncated at eight.

ZCOE1940I PasswordCourier Initiator Success: ChangePW=XX ValidatePW=XX Resume=XX Revoke=XX Delete=XX Unknown=XX

Explanation: This is an informational message about the number of successful initiator requests.

ZCOE1941I PasswordCourier Initiator Failed: ChangePW=XX ValidatePW=XX Resume=XX Revoke=XX Delete=XX Unknown=XX

Explanation: This is an informational message about the number of failed initiator requests.

ZCOE1942I PasswordCourier Responder Success: ChangePW=XX ValidatePW=XX Resume=XX Revoke=XX Delete=XX Unknown=XX

Explanation: This is an informational message about the number of successful responder requests.

ZCOE1943I PasswordCourier Responder Failed: ChangePW=XX ValidatePW=XX Resume=XX Revoke=XX Delete=XX Unknown=XX

Explanation: This is an informational message about the number of failed responder requests.

ZCOE1944I PasswordCourier Request Totals: ChangePW=XX ValidatePW=XX Resume=XX Revoke=XX Delete=XX Unknown=XX

Explanation: This is an informational message about the total number of each request type.

ZCOE1945I PasswordCourier Total Requests=XX Success=XX Failed=XX TimePurge=XX OperPurge=XX AsyncReq=XX AsyncRsp=XX

Explanation: This is an informational message about the number of total requests.

ZCOE1946E ESSHRMON Abend xxx Recovered - PSW = xxxxxxxx xxxxxxxx Abend within installation ICHPWX01 Exit

Explanation: This message is displayed when the Core Access Assurance Suite has branched to a RACF Password exit (ICHPWX01) during strong password rules checking, and the exit ICHPWX01 abends. Use this and other accompanying messages to debug theabend.

ZCOE1947E ESSHRMON ENTPT=xxxxxxx ICHPWX01=xxxxxxx

Explanation: This message is displayed when the Core Access Assurance Suite has branched to a RACF Password exit (ICHPWX01) during strong password rules checking, and the exit ICHPWX01 abends. Use this and other accompanying messages to debug theabend.

ZCOE1948E ESSHRMON ABENDED REGS rr-rr: xxxxxxxx xxxxxxxx xxxxxxxx xxxxxxxx

Explanation: This message is displayed when the Core Access Assurance Suite has branched to a RACF Password exit (ICHPWX01) during strong password rules checking, and the exit ICHPWX01 abends. Use this and other accompanying messages to debug theabend.

ZCOE1949I GLOBAL parameter ESSCALL_PASSWORD_SECURITY_EXIT changed to NO due to Abend

Explanation: This is an informational message displayed when the Core Access Assurance Suite has branched to a RACF Password exit (ICHPWX01) during strong password rules checking, and the exit ICHPWX01 abends. The ESSCALL_PASSWORD_SECURITY_EXIT global parameter changed to NO for the life of the Core Access Assurance Suite STC due to the abend. When the problem is corrected, recycle the Core Access Assurance Suite STC.

ZCOE1950E ESSHRMON ABEND xxx RECOVERED - NO SDWA PROVIDED: Abend within installation ICHPWX01 exit

Explanation: This message is displayed when the Core Access Assurance Suite has branched to a RACF Password exit (ICHPWX01) during strong password rules checking, and the exit ICHPWX01 abends. Use accompanying messages to debug the abend.

ZCOE1951E ESSAUTH RESOURCE/GROUP Parameters both entered on Reocrd NN: not allowed

Explanation: In the Core Access Assurance Suite ESSAUTH file, an entry defined with both the RESOURCE and GROUP parameters. These two parameters are mutually exclusive. NN identifies the record number that is in error. You must determine which parameter should be used. Either the GROUP or RESOURCE parameter should be removed from the ESSAUTH entry.

ZCOS2210E ERROR NOT RUNNING AS A STARTED TASK. PLEASE RERUN JOB AS A STARTED TASK

Explanation: The Cour390 started task can not be run as a batch job, it must be run as a started task. Correct the error and bring up Cour390 as a started task.

ZCOS2215E ERROR DELETING CIB ENTRY

Explanation: The Core Security Agent was attempting to process an operator MODIFY console command and received an error trying to free the CIB. If the Core Security Agent does not respond to Operator commands, contact Core Security customer support. Otherwise, this message can be treated as an informational message.

ZCOS2250E ERROR SETTING CIB

Explanation: The Core Security Agent was attempting to process an operator MODIFY console command and received an error trying to free the CIB. If the Core Security Agent does not respond to Operator commands, contact Core Security customer support. Otherwise, this message can be treated as an informational message.

ZCOE2298I xxxx

Explanation: Debug message for Core Security's internal use.

ZCOE2299I xxxx

Explanation: Debug message for Core Security's internal use.

ZCOE2805E Error xxxx1 xxxx2 storage, PGM: ESSARACF, FN: xxxx3

An error occurred while COUR390 attempted to obtain or release virtual storage. Contact Core Security Support, supplying the full text of the message.

xxxx1 is a numeric value, representing the Return Code from the z/OS storage services

xxxx2 is either "Obtaining" or "Releasing"

xxxx3 describes the specific storage area Cour390 was processing. This value varies and should simply be reported to Support. It means nothing to the user.

ZCOE2806E RACF Error xxxx1/xxxx2, PGM: ESSARACF, FN: xxxx3, Data: xxxx4

An error occurred while COUR390 requested a RACF service. Contact Core Security Support, supplying the full text of this message and any messages ZCOE2807I or ZCOE2808I that directly follow this message.

Message 2806 is always followed by one or more occurrences of Messages 2807 and 2808, containing further details of the problem being described.

xxxx1 and xxxx2 are numeric values, representing Return Codes from RACF

xxxx3 and xxxx4 describes the specific function and data that Cour390 was processing. This values vary and should simply be reported to Support. They mean nothing to the user.

ZCOE2807I RACF Parm area: xxxx1

Message 2807 follows message 2806 and contains debugging information for use by Core Security Support personnel.

ZCOE2808I RACF Message: xxxx1

Message 2808 follows message 2806 and contains the RACF messages describing the error. This should be supplied to Core Security Support personnel.

ZCOE2809E Internal Error, PGM: ESSARACF, FN: xxxx1, Data: xxxx2

An error occurred in COUR390 processing. Contact Core Security Support, supplying the full text of the message.

xxxx1 describes a function internal to COUR390 processing

xxxx2 describes the specific processing in which the error occurred. This value varies and should simply be reported to Support. It means nothing to the user.

**ZCOS2571I Core Security Enterprise Server: ssssssss Version:v.vv Build: uu.bbb
Created: mm/dd/yy hh:mm Maint: xxxxxxxx.**

Explanation:

ssssssss is the name of the Cour390 Agent specified by the user during installation.

v.vv is the Cour390 product version number, e.g., 7.20

uu is the Cour390 product update number, or 0 for a base release.

bbb is the Cour390 product build number.

mm/dd/yy hh:mm are the date and time of the Cour390 product build

xxxxxxx is the ID of any maintenance applied to Cour390. This value is non-blank only when the customer provided with interim maintenance (typically in the form of a ZAP).

Message 2571 is issued in response to the modify command VER, which is intended to be used at the direction of Core Security support personnel.

ZCOS2574I DATASPACE: xxxx HAS AN STOKEN OF yyyy

Explanation: The user entered the command: F server_name,STK command. The output of this command is the STOKEN of the Queue Data In Virtual(DIV) dataspace STOKEN.

ZCOS2575I Modify command received

Explanation: This is a normal message that is displayed after any valid modify command is entered.

ZCOS2576I Command not supported: xxxx

Explanation: This is an informational message that is displayed after a modify command was entered that is not supported.

ZCOS2579I Modify STOP command received, shutting down server: xxxx

Explanation: This is a normal message that is issued when the STOP modify command is used to shut down server xxxx.

ZCOS2580I PROCESSING SNAP

Explanation: The Core Security Agent is processing the snap dump that was taken.

ZCOS2582I Modify RESET command received

Explanation: This is an informational message.

ZCOS2583I Modify QUIESCE command received: xxxx

Explanation: This is a normal message that is issued when the QUIESCE modify command is used to shut down server xxxx.

ZCOS3207I DEBUG MODE IS NOW [ACTIVE | INACTIVE]

Explanation: The above message indicates that the debug facility has either been turned on or turned off.

ZCOB4104E Load failed for module OSIRECOV or OSIETCO1

Explanation: The Core Security Agent was attempting to load its error recovery modules, but failed. See the accompanying CSV messages displayed by z/OS for more information on the cause of the failure. Two possible causes for this error could be that not enough REGION was supplied on the EXEC card or there is an invalid STEPLIB.

ZCOB4124W PARM STRING PARAMETER

Explanation: This message indicates that a Cour390 parameter specified in the PARM statement of the EXEC JCL card is overriding a parameter specified in the SYSIN file.

ZCON4251E Failure loading ESTAE routing

Explanation: An error occurred attempting to load the recovery routine. Increase the region size. If the problem persists contact Core Security customer support.

ZCOS6000I xxxx DATASPACE CREATED

Explanation: This is an informational message that indicates that a dataspace successfully created. xxxx is the name of the dataspace that created.

ZCOS6100E ERROR CREATING DATASPACE: xxxx

Explanation: An error occurred creating dataspace xxxx. Accompanying messages should show the return codes received while trying to create the dataspace.

ZCOS7161I Core Server Anchor Block at xxxxxxxx reused

Explanation: The Core Server has reused the storage previously allocated for its main control block, at address xxxxxxxx. This is an informational message. The location of the Core Server Anchor is only of importance to the user when Courion Support personnel request information related to diagnosing problems with Cour390.

ZCOS7162I Core Server Anchor Block allocated at xxxxxxxx

Explanation: The Core Server has created its main control block in common storage, at address xxxxxxxx. This is an informational message. The location of the Core Server Anchor is only of importance to the user when Courion Support personnel request information related to diagnosing problems with Cour390.

ZCOM7224E << IBM Error message>>

Explanation: A Dynamic Allocation failure has occurred. The associated Allocation error message is displayed. Refer to the appropriate IBM Messages manual for a detailed description of the failure. Correct the error and re-submit the transfer.

ZCOM7225E DYNALLOC Failed R15=xxxx RC=yyyy Info Reason Code=zzzz Error RC=nnnn

Explanation: A Dynamic Allocation failure has occurred. Register 15 is xxxx. The return code is yyyy the information reason code is zzzz the error code is nnnn. The associated error message (if any) is issued with ZCOM7224E. Correct the problem and re-submit the transfer.

ZCOM7226E DYNALLOC failed due to invalid xxxx "yyyy"

Explanation: An invalid parameter was passed to dynamic allocation where xxxx is the name of the parameter and yyyy is that parameter. Correct the error and re-submit the transfer.

ZCOS7500I xxxx USES A SYSTEM LINKAGE INDEX OF xxxx FOR ENHANCED CROSS MEMORY SERVICES

Explanation: This is an informational message.

ZCOS7650I CREATING TABLE ENTRY FOR XMS SERVICES

Explanation: This is an informational message.

ZCOS7700I CONNECTION TO XMS ENTRY TABLE SUCCESSFUL XMS SERVICES ARE NOW ENABLED

Explanation: This is an informational message.

ZCOS8161E Courion Anchor Slot occupied by non-Courion data. Anchor value is xxxxxxxx

Explanation: During initialization, the Cour390 Agent determined that the value in the Core Security Anchor Slot of the IBM Customer Anchor Table was occupied by a value that was not

placed there by a Core Security product. Cour390 cannot initialize without using this Anchor Slot. This message is followed by messages ZCOS8162E and ZCOS8163R. For the Cour390 Agent to initialize, a Console Operator must reply YES to message ZCOS8163R.

IBM has assigned the fullword slot at offset X 'F4' of the Customer Anchor Table to Core Security. This field should contain only Courion data. Value xxxxxxxx in the message is the value found in the anchor. The customer should make every effort to determine what this value represents and why it is present in the Courion Anchor Slot. Contact Core Security Support for assistance with this endeavor.

Note: Allowing Cour390 to overwrite this value without identifying the process that is using it erroneously can have unpredictable results.

ZCOS8162E Core Access Assurance Suite Server cannot initialize without using this IBM-assigned Anchor Slot

Explanation: This message follows message ZCOS8161E and is intended to clarify the situation for the Console Operator.

ZCOS8163R Reply YES to overwrite or CAN to cancel Core Server

Explanation: This message follows messages ZCOS8161E and ZCOS8162E. The Cour390 agent remains inactive until a console operator has issued a valid reply. As indicated by the message text, valid replies are YES, which causes Cour390 to overwrite the Anchor value and continue initialization, or CAN to preserve the current contents of the Anchor and cancel the agent.

Note: Allowing Cour390 to overwrite this value without identifying the process that is using it erroneously can have unpredictable results.

ZCOS8164I Core Server Anchor has overwritten the non-Courion Anchor

Explanation: This message follows message ZCOS8162E and a reply of YES by the console operator. This message is informational, and means that the Cour390 Agent is continuing with initialization.

ZCOS8165I Core Server is cancelled. Contact your local Systems Programmer and Courion Support

Explanation: This message follows message ZCOS8162E and a reply of CAN by the console operator. This message is informational, and means that the Cour390 Agent terminates.

ZCOS8166E Reply must be YES or CAN. Core Server awaiting proper reply before continuing initialization

Explanation: This message follows message ZCOS8162E and an invalid reply by the console operator (i.e., anything other than YES or CAN). This message is followed by a recurrence of message ZCOS8163R, until Cour390 receives a valid reply.

ZCOS8167E Customer Anchor Table error. Core Server terminating

Explanation: This message follows repeated occurrences of messages ZCOS8161E, ZCOS8162E and ZCOS8163R and only appears when there are multiple processes attempting to update the Cour390 Anchor. This indicates that the non-Core Security code using this Core Security Anchor is updating the value concurrently with Cour390. In this situation, the customer must determine what this value represents and why it is present in the Core Security Anchor Slot before attempting to restart the Cour390 Agent. Contact Core Security Support for assistance with this endeavor.

ZCON9000D Now at Program: xxxx

Explanation: This is a diagnostic message.

ZCOS9001I STOP command being processed.

Explanation: This is a normal informational message that is displayed when STOP command is issued to bring the started task down.

ZCOS9100I ALET NUMBER CREATED: xxxx DSPTOKEN yyyy

Explanation: This is an informational message which shows the STOKEN that was returned when a dataspace was created.

ZCOS9210E ERROR SETTING UP XMS ENVIRONMENT

Explanation: An error occurred trying to setup the cross memory environment. Previous errors should give more information about the exact cause of the error.

ZCOS9220E ERROR ISSUING LXREX MACRO

Explanation: An error occurred executing the LXREX macro to create the cross memory environment. Contact Core Security customer support for assistance.

ZCOS9230E ERROR ISSUING AXSET MACRO

Explanation: An error occurred executing the AXSET macro to create the cross memory environment. Contact Core Security customer support for assistance.

ZCOS9240E ERROR ISSUING [ETCRE | ETCON] MACRO

Explanation: An error occurred executing the ETCRE/ETCON macros to create the cross memory environment. Contact Core Security customer support for assistance.

ZCOS9245E ERROR LOADING OSISX00x PROGRAM

Explanation: An error occurred loading one of the Core Security cross memory programs (OSISX000 through OSISX00F). An z/OS CSV error should also be displayed. The CSV message should indicate the cause of the load failure.

ZCOS9300E ERROR LOADING MODULE [OSISANK0 | OSISDDC0 | OSISSNP0]

Explanation: There was a problem loading the module specified. Please contact Core Security customer support if you receive this error.

ZCOS9314E ERROR LOADING MODULE xxxx

Explanation: There was a problem loading the module specified. Please contact Core Security customer support if you receive this error.

ZCON9777D xxxx

Explanation: This is diagnostic message.

ZCON9998I Detail MSG: xxxx

Explanation: This is a diagnostic message. It displays information from the agent internal control blocks.

Appendix A: Installing ActivePerl

Follow these steps to install ActivePerl:

1. Follow this link to download the ActivePerl installation:
<http://www.activestate.com/store/languages/register.plex?id=ActivePerl>
2. After downloading ActivePerl installation, run the install to install ActivePerl on the system.
3. If prompted to do so, please reboot the system after installing ActivePerl.

Installing Required Perl Modules

To use many Courion connectors, you must download and install the following Perl modules:

XML-DOM

You can download and then manually install these modules. Download them from

<http://ppm.activestate.com/PPMPackages/5.6/MSWin32-x86-multi-thread/>
or
www.cpan.org

Another way to install the modules is with the programmer's package management tool included in the ActivePerl package. This tool requires internet connectivity from the system where the packages are to be installed. To use the package management tool to install the XML-DOM module, type the following command from a command prompt on the machine where ActivePerl was installed:

```
ppm install XML-DOM
```


INDEX

Numbers

3DES_SEED parameter 636

A

Active Directory
 connector 266
 PMM 258
 Active Script connector 282
 ActiveX Data Objects (ADO)
 downloads with AD 263
 downloads with Lotus Notes 152
 downloads with Windows 380
 ActiveX Data Objects (ADO) connector 288
 ADAM connector 272
 adapters, SAP 589
 agent
 Cour390, see Cour390 agent
 HP-UX PMM
 configuring 109
 installing 108, 121
 starting and stopping 111
 uninstalling 111
 IBM AIX PMM
 configuring 137
 installing 136
 starting and stopping 139
 uninstalling 139
 IBM i5/OS (OS/400) connector
 configuring 237
 installing 233
 starting 238
 stopping 239
 IBM i5/OS (OS/400) PMM
 commands and keywords 214
 configuring 220
 installing 217
 start command 224
 starting and stopping 226
 uninstalling 226
 Linux
 configuring 493
 installing 492
 starting and stopping 495
 uninstalling 495
 Netscape Directory Server and iPlanet Directory Server 392
 OpenVMS
 configuring 429
 installing 427
 logging 432
 starting 430
 stopping 430
 uninstalling 431
 RSA SecurID, for UNIX
 configuring 541
 installing 540
 starting and stopping 543

 uninstalling 543
 RSA SecurID, for Windows
 configuring 544
 installing 544
 starting and stopping 546
 uninstalling 546
 Sun Solaris PMM
 configuring 613
 installing 612
 starting and stopping 615
 uninstalling 615

AIX

connector 140
 PMM 132
 PMM agent
 configuring 137
 installing 136
 starting and stopping 139
 uninstalling 139
 API, PeopleSoft 472
 authority delivered with IBM i5/OS (OS/400) connector agent 235

B

BlackBerry connector 502, 510
 Business Connector Interface, SAP 589
 Business Connector routing rules, SAP 575
 bXML template files, SAP 587

C

CA-ACF2
 connector 185
 PMM 180
 security interface in Cour390 agent 649
 CA-Top Secret
 connector 195
 PMM 190
 security interface in Cour390 agent 653
 Citrix Presentation Server connector 68, 520
 Citrix SDK, installing 71
 Citrix SSO connector 64
 Citrix XenApp connector 68, 520
 configuration
 data source name 622
 TCP/IP installation parameters 202
 Conform to Native Password feature
 i5/OS (OS/400) 221
 connector
 Active Directory 266
 Active Script 282
 ActiveX Data Objects (ADO) 288
 ADAM 272
 adding 57
 BlackBerry 502, 510
 CA-ACF2 185
 CA-Top Secret 195
 Citrix Presentation Server 68, 520
 Citrix SSO 64
 Citrix XenApp 68, 520
 Epic 96
 Exchange 2000 300, 334, 340, 348, 354
 Exchange 2007 and 2010 306
 Exchange 5.5 296
 HP OpenView ServiceCenter 100
 HP-UX 112

- HTML Email 126
- HTML Email (enhanced) 128
- IBM AIX 140
- IBM i5/OS (OS/400) 230
- IBM Lotus 171
- IBM z/OS systems with CA-ACF2 185
- IBM z/OS systems with RACF 205
- Imprivata OneSign 244
- JavaScript 86
- Kronos Workforce Central 255
- Linux 416, 497
- Microsoft Active Directory Attribute Trigger connector 276
- Microsoft Identity Integration Server (MIIS) 312
- Microsoft Office365 Exchange Online 339
- Microsoft Office365 Lync Online 347
- Microsoft Office365 SharePoint Online 353
- Netscape SMTP 396
- Novell GroupWise 403
- Novell NDS eDirectory 411
- Novell SUSE 416
- ODBC 318
- OpenVMS 425
- Oracle 8i, 9i 441
- Oracle E-Business 456
- Oracle Internet Directory 464
- PeopleSoft PeopleTools 8.48 483
- Peregrine ServiceCenter 100
- PMM Gateway 61
- RACF 205
- Red Hat 497
- Remedy Action Request System 43
- RIM BlackBerry 502, 510
- Role Connector 78
- SAP 556
- SAP Logon 567
- SQL server 367
- SQL Usage 82
- Sun Directory Server 594
- Sun Solaris 616
- Sybase Adaptive Server 628
- VBScript 370
- VBscript 90
- Web Services 92
- Windows NT 383
- connector framework target assignment 54
- Core 81
- Cour390 agent
 - about 632
 - configuration to support PasswordCourier and AccountCourier 642
 - control parameters 637
 - distributed members 666
 - error and status messages 672
 - GLOBAL member parameters 636
 - installation 633
 - Log Record 668
 - operation 662
 - password reset parameters 638
 - RACF interface 642
 - return codes 670
 - security interface 642
 - security interface to CA-ACF2 649
 - security interface to CA-Top Secret 653
 - server configuration 635
 - SMF report 667
 - SMF Report Program (ESSMFRPT) 667
 - TCP/IP communications parameters 636

- troubleshooting 664
- CourLocal ActiveX control 263

D

- data source
 - create 437, 625
 - machine 624
 - machine (SQL) 362
 - Microsoft Access with ODBC 322
 - Microsoft SQL with ODBC connector 325
 - name (DSN)
 - about, Oracle 436
 - about, Sybase 624
 - configuration with SQL Server PMM 360
 - ODBC for Oracle E-Business PMM 448
 - ODBC with Oracle 329
 - Oracle 436
- distributed installation 54
- domain
 - local, password resets, Active Directory 263
 - local, password resets, Windows 380
 - master, single or multiple model 381
 - single model 381
- DSN, see data source name

E

- enhanced logging, PMM for Lotus Notes 153
- Epic connector 96
- eTrust SiteMinder PMM 48
- Exchange 2000 connector 300, 334, 340, 348, 354
- Exchange 2007 and 2010 connector 306
- Exchange 5.5 connector 296
- External API, PeopleSoft 472

F

- forced password change on next logon for PeopleSoft targets 474

G

- GLOBAL member parameters, Cour390 agent 636

H

- history, admin password, Windows 375
- HP OpenView ServiceCenter connector 100
- HP-UX
 - connector 112
 - PMM 104, 118
 - PMM agent
 - configuring 109
 - installing 108, 121
 - starting and stopping 111
 - uninstalling 111
- HTML Email connector 126
- HTML Email connector (enhanced) 128

I

- IBM AIX
 - connector 140
 - PMM 132
 - PMM agent

- configuring 137
 - installing 136
 - starting and stopping 139
 - uninstalling 139
- IBM i5/OS (OS/400)
 - connector 230
 - agent
 - configuring 237
 - installing 233
 - starting 238
 - stopping 239
- PMM 210
 - agent
 - commands and keywords 214
 - configuring 220
 - installing 217
 - start command 224
 - starting and stopping 226
 - uninstalling 226
 - required forced password change 212
- IBM Lotus connector 171
- IBM z/OS
 - installation, Cour 390 agent 633
- IBM z/OS systems with CA-ACF2
 - connector 185
 - PMM 180
- IBM z/OS systems with RACF
 - connector 205
 - PMM 200
- ID Vault feature
 - configuring 165
 - prerequisites 150
- Imprivata OneSign connector 244
- installation
 - Cour390 agent 633
- iPlanet Directory Server
 - PMM 388

J

JavaScript custom macros connector 86

K

Kronos Workforce Central
 connector 255
 PMM 252

L

Linux

- agent
 - configuring 493
 - installing 492
 - starting and stopping 495
 - uninstalling 495
- connector 416, 497
- PMM 488

Lotus connector 171
 Lotus Domino PMM 146
 Lotus Notes PMM 150

M

machine data source (SQL) 362
 machine data source (Sybase) 624

macros

- about 695

macros, JavaScript connector 86
 macros, VBScript 90
 master domain model 381
 Microsoft Access data source with ODBC connector
 data source 322
 Microsoft Active Directory
 connector 266
 PMM 258
 Microsoft Active Directory Attribute Trigger 276
 Microsoft Active Script connector 282
 Microsoft ActiveX Data Objects (ADO) connector 288
 Microsoft ADAM connector 272
 Microsoft Exchange 2000 connector 300, 334, 340,
 348, 354
 Microsoft Exchange 2007 and 2010 connector 306
 Microsoft Exchange 5.5 connector 296
 Microsoft Identity Integration Server (MIIS)
 connector 312
 Microsoft ODBC
 data source for Oracle E-Business 453
 Oracle 8i, 9i, driver setup 438
 Microsoft ODBC connector 318
 Microsoft Office365 Exchange Online connector 339
 Microsoft Office365 Lync Online connector 347
 Microsoft Office365 PMM 333
 Microsoft Office365 SharePoint Online
 connector 353
 Microsoft SQL data source with ODBC
 connector 325
 Microsoft SQL server
 connector 367
 PMM 360
 Microsoft VBScript connector 370
 Microsoft Windows 2000 PMM 374
 Microsoft Windows NT
 connector 383
 PMM 374
 multiple master domain model 381
 multiple server configuration
 Lotus Notes PMM 158
 mySAP.com PMM 574

N

Netegrity SiteMinder PMM 48
 Netscape Directory Server
 agent 392
 Netscape Directory Server PMM 388
 Netscape SMTP connector 396
 Novell GroupWise
 connector 403
 PMM 400
 Novell NDS eDirectory
 connector 411
 PMM 408
 Novell SUSE connector 416

O

ODBC
 See Microsoft ODBC
 ODBC connector 318
 OpenVMS
 agent
 configuring 429

- installing 427
- logging 432
- starting 430
- stopping 430
- uninstalling 431
- connector 425
- PMM 422
- Oracle
 - data source with ODBC connector 329
- Oracle 8i, 9i
 - connector 441
 - driver setup for ODBC 438
 - PMM 434
 - data source 436
- Oracle E-Business
 - connector 456
 - PMM 446
- Oracle E-Business PMM
 - Microsoft ODBC 453
 - ODBC as data source 448
- Oracle Internet Directory connector 464
- OS/390, see IBM z/OS systems
- OS/400, see IBM i5/OS (OS/400)

P

- password
 - admin resets for Windows NT and 2000 374
 - change, IBM i5/OS (OS/400) 212
 - Conform to Native Password feature, i5/OS (OS/400) 221
 - forcing a change on next logon, PeopleSoft 474
 - history of admin password for Windows 375
 - limitations, Sybase 627
 - management script with AIX 135
 - management script with HP-UX 107
 - management script with Linux 491
 - management script with Sun Solaris 611
 - reset of local domain, Active Directory 263
 - reset of local domain, Windows 380
 - reset parameters for Cour390 638
 - reset, excluded accounts in Oracle E-Business 455
 - strong rules, Cour390 agent 640
- PeopleSoft
 - PMM 472
 - applications to configure before PMM 473
- PeopleSoft PeopleTools 8.48
 - connector 483
- Peregrine ServiceCenter connector 100
- PMM
 - Active Directory 258
 - CA-ACF2 180
 - CA-Top Secret 190
 - eTrust SiteMinder 48
 - security options 49
 - HP-UX 104, 118
 - IBM AIX 132
 - IBM i5/OS (OS/400) 210
 - IBM z/OS systems with CA-ACF2 180
 - IBM z/OS systems with RACF 200
 - Kronos Workforce Central 252
 - Linux 488
 - Lotus Domino 146
 - Lotus Notes 150
 - Microsoft Office365 333
 - mySAP.com 574
 - Netegrity SiteMinder 48

- security options 49
- Netscape Directory Server and iPlanet Directory Server 388
- Novell GroupWise 400
- Novell NDS eDirectory 408
- OpenVMS 422
- Oracle 8i, 9i 434
- Oracle E-Business 446
- PeopleSoft 472
 - applications to configure before PMM 473
- RACF 200
- Red Hat 488
- Remedy Action Request System 40
- RSA Access Manager 514
- RSA SecurID 532
- SAP 548
- SAP Logon 563
- SQL server 360
- Sun Kerberos 602
- Sun Solaris 608
- Sybase Adaptive Server 622
- Windows 2000 374
- Windows NT 374
- PMM Gateway connector 61

R

- RACF
 - connector 205
 - PMM 200
 - security interface to Cour390 642
- Red Hat
 - connector 497
 - PMM 488
- Remedy Action Request System
 - connector 43
 - PMM 40
- RIM BlackBerry connector 502, 510
- Role Connector 78
- routing rules, Business Connector, SAP 575
- RSA Access Manager
 - PMM 514
- RSA SecurID
 - agent for UNIX
 - configuring 541
 - installing 540
 - uninstalling 543
 - agent for Unix
 - starting and stopping 543
 - agent for Windows
 - configuring 544
 - installing 544
 - starting and stopping 546
 - uninstalling 546
 - PMM 532

S

- SAP
 - adapters 589
 - Business Connector Interface 589
 - Business Connector routing rules 575
 - configuring for mySAP.com PMM 574
 - connector 556
 - PMM 548
 - SAP Logon
 - connector 567

- PMM 563
- SAP, see also mySAP.com
- script
 - AIX password management 135
 - HP-UX password management 107
 - Linux password management 491
- Secure Socket Layer, see SSL
- security options
 - Active Directory PMM 258
 - PMM for eTrust SiteMinder 49
 - PMM for Netegrity SiteMinder 49
- server, multiple, Lotus Notes PMM 158
- server, multiple, See also multiple server
- single domain model 381
- single server configuration
 - Lotus Notes PMM 158
- SMTP
 - Netscape connector 396
- Solaris
 - see Sun Solaris
- SQL server
 - connector 367
 - data source with ODBC connector 325
 - PMM 360
- SQL Usage
 - connector 81
- SQL usage connector 82
- SSL (Secure Socket Layer)
 - certificate with Lotus Notes 151
 - certificate with MS Exchange 2000 303
 - certificate with mySAP PMM 579
 - with MS Active Directory 268
 - with Netscape Directory Server 390
 - with Sun Directory Server 466, 596
- strong password rules, Cour390 agent 640
- Sun Directory Server connector 594
- Sun Kerberos PMM 602
- Sun Solaris
 - connector 616
 - PMM 608
 - PMM agent
 - configuring 613
 - installing 612
 - starting and stopping 615
 - uninstalling 615
- Sybase Adaptive Server
 - connector 628
 - PMM 622
 - password limitations 627

T

- target
 - creating workflow for, See also the specific connector or PMM
- targets
 - assigning to a connector framework 54
- TCP/IP
 - communications parameters, Cour390 agent 636
 - installation parameters, configuration 202
- template files, SAP 587
- temporary directory information, Lotus Notes PMM 154
- tokens, disabled (RSA SecurID) 541

V

- VBScript connector 370
- VBScript macros connector 90

W

- Web Services connector 92
- Windows 2000
 - PMM 374
- Windows NT
 - connector 383
 - PMM 374
- workflow, creating for a target, See the connector or PMM

Z

- z/OS
 - Cour390 return codes 670
 - error and status messages 672
 - Operator Console Basics 662
 - RACF Security Interface
 - systems, see IBM z/OS systems
 - Troubleshooting 664
- z/OS Mainframe
 - with CA/ACF2 PMM 180
 - with CA-Top Secret PMM 190
 - with RACF 200
- z/OS, see also Cour390 agent

