



Using the Identity Mapping Solution

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.

Contents

Chapter 1 - Introduction to the Identity Mapping Solution	7
Chapter 2 - Installing and Accessing the Identity Mapping Solution	9
Installing Identity Mapping and Post-Installation Setup	10
Creating Connection Strings for Data Mapping	10
Using the Identity Mapping Interface	12
Chapter 3 - Setting Up Data Collection Rules	15
Post-Installation Setup for Data Collection	16
Creating Data Collection Entities	16
Adding Tomcat Server Entries in the Web.config File	16
Creating Staging Tables for the Collector for Epic	17
Confirming Configuration of Data Source Systems	17
Installing Data Collectors	17
Creating a Data Collection Rule	19
Specifying a Target System as the Collection Source	20
Specifying Fields for the Generic Collector for CSV	21
Specifying Fields for the Collector for Microsoft Active Directory	22
Specifying Fields for the Generic Collector for Microsoft SQL Server	23
Specifying Fields for the Collector for Oracle Sun Directory LDAP	24
Specifying Fields for a Standard Collector	25
Selecting Attributes	25
Select Attributes for a Generic CSV File	26
Attribute Selection for Collection of Entitlements	27
Filtering Data	28
Copying Cleansed Data to Production Tables	31
Manually Copying Cleansed Data to Production Tables	31
Cleansed Profile Data	32
Cleansed Entitlement Data	32
Applying a Pre- or Post-Processor	33
Examples of Pre-Processors	33
Examples of Post-Processors	33
Pre-Requisites for Selecting a Processor to run with a Collection Rule	33
Configuring the Tomcat Server to Avoid Logging of Sensitive Data	34
Specifying a Pre-Processor	34
Extending the Rule with a Post-Processor	35
Removing a Pre-Processor or Post-Processor	36
Scheduling the Data Collection Rule	36
Securing Data Collection	38
Configuration required for Collector for Microsoft Active Directory and Collector for Oracle Sun Directory	
LDAP	38
Creating a Keystore	38
Enabling Windows Authentication for Data Collection	39
Configuring the CustomerConnStrings.config File	39
Running the Tomcat Service under a Windows User Account	40
Changing the Identity in Application Pools	40
Copy NTLMAuth.dll to [JavaHOME]\Bin Folder	41
Moving the Collector Files to Tomcat Lib Folder	41
Enabling Windows Authentication for SQL and EPIC Collectors for Connecting to the Source Database	
Server	42
Notes	42
Running a Data Collection Rule	43
Running Multiple Data Collection Rules	43

Viewing Data Collection Results	44
Sort Options	44
Filtering Options	45
Filtering a Column using Two Criteria	45
Filtering upon Multiple Columns	45
Recognizing when Filters are Applied	46
Editing a Data Collection Rule	47
Disabling a Data Collection Rule	48
Deleting a Data Collection Rule	49
Uninstalling a Data Collector	49
Chapter 4 - Setting Up Data Feeds	51
Adding Data Feeds	53
Viewing Data Feed Details	55
Chapter 5 - Creating Identity Mapping Rules	57
Managing Identity Mapping Rules	58
Creating an Identity Mapping Rule	59
Chapter 6 - Executing Rules to Map Accounts	63
Executing Rules Periodically	64
Creating a Job	64
Data Feed Consistency Check	65
Scheduling a Job	65
Executing Rules Immediately	67
Viewing Rule History	68
Right-Click Column Menu Options	69
Chapter 7 - Creating Entitlement Mapping Rules	71
Mapping Collected Entitlements	72
Creating an Entitlement Mapping Rule	72
Running an Entitlement Mapping Rule	74
Viewing the Results of Entitlement Mapping	75
Chapter 8 - Mapping Accounts Manually	77
Adding an Inclusion Map	78
Enabling an Inclusion Map	80
Disabling an Inclusion Map	81
Removing Inclusion Maps	82
Chapter 9 - Deleting Mapped Accounts	83
Chapter 10 - Viewing Reports	85
Viewing the Overview Window	86
Viewing Account Information	88
Configuring the Grid	89
Right-Click Column Menu Options	90
Viewing Profile Information	91
Viewing Mapped Information	92
Viewing Customized Information	93
Appendix A - Troubleshooting	95
Log Files Available for Debugging Identity Mapping	95
Optional Flags to Control Deletion of IdentityMap Records	95
Timeout Configuration	96
Reduced Performance when Previewing or Collecting Large Amounts of Data	96
Problems with Proxy User Account used for Data Collection	97
Section 1: Create Database User	97
Section 2: Map User	97
Section 3: Create Credentials and Proxy	98
Log Files for Debugging ETL Errors with Data Collection Rules	98
Problem: "ETL Job Failed" error	98
Problem: "Tomcat Server is not accessible" Error	99

Solution 1	99
Solution 2	99
Solution 3	100
Solution 4	100
Solution 5	101
Problem: Tomcat service is not Starting	101
Solution 1	101
Solution 2	101
Problem: "Job Failed" Error	102
Index	103

Chapter 1: Introduction to the Identity Mapping Solution

The Identity Mapping Solution is a component of the Access Assurance Suite that resides within the Access Assurance Portal. It provides a user-friendly interface for an administrator to establish an enterprise-wide Data Mapping process including the following:

- Identifying sources of account, profile, and entitlement data including HR systems or Active Directory
- Configuring data collection rules or data feeds that collect and filter account, profile, and entitlement data
- Creating identity mapping rules to match user accounts with the user profile information, either automatically or manually.
- Executing mapping rules on data feeds periodically using the scheduler, or immediately.
- Reviewing the information to take timely action to resolve any discrepancies.
- Providing auditing and reporting on the Identity Mapping process.

This manual describes how to use the Identity Mapping user interface (available through the Access Assurance Portal) to configure data collection rules or data feeds, define and test mapping rules, and publish results for use by other applications. The manual includes the following chapters:

- [*“Installing and Accessing the Identity Mapping Solution” on page 9*](#) introduces the Identity Mapping User Interface and describes how to use the menu options to set up the workflow.
- [*“Setting Up Data Collection Rules” on page 15*](#) describes how to use the Data Collection Rule wizard to set up data collection rules.
- [*“Setting Up Data Feeds” on page 51*](#) describes how to add and manage data feeds.
- [*“Creating Identity Mapping Rules” on page 57*](#) describes how to create and configure rules.
- [*“Executing Rules to Map Accounts” on page 63*](#) describes how to schedule rules to execute at a specific time or run immediately.
- [*“Mapping Accounts Manually” on page 77*](#) describes how to manually map accounts to profiles.
- [*“Deleting Mapped Accounts” on page 83*](#) describes how to delete mapped accounts.
- [*“Viewing Reports” on page 85*](#) describes the information you can view using the reporting feature.

Chapter 2: Installing and Accessing the Identity Mapping Solution

This chapter describes Identity Mapping post-installation setup. It also describes how to use the interface to configure the Identity Mapping workflow. This chapter includes the following sections:

- [*“Installing Identity Mapping and Post-Installation Setup” on page 10*](#)
- [*“Using the Identity Mapping Interface” on page 12*](#)

Installing Identity Mapping and Post-Installation Setup

The Identity Mapping Solution is installed with the Core Access Assurance Suite as described in the manual *Installing the Access Assurance Suite*.

Creating Connection Strings for Data Mapping

After you have installed the Access Assurance Suite, navigate to the CourionService folder, and do the following:

1. Edit the connection string in the
[CoreSecurityInstallPath]\CourionService\config\
IdentityMapping.WCFHost.ConnectionStrings.config file to point it to the Courion
database:

```
<add name="dbConnectionString" connectionString="Data Source=
$$YOURSERVERHERE$$;Initial Catalog= $$YOURDBHERE$$;Trusted_Connection=True;
providerName="System.Data.SqlClient" />
```

Replace \$\$YOURSERVERHERE\$\$ with the name of the database server.

Replace \$\$YOURDBHERE\$\$ with the name of the database.

Note: By default, Courion software is installed in the following path: C:\Program Files (x86)\Courion Corporation. In this manual, the path to the installed files is referred to as [CoreSecurityInstallPath].

2. Edit the connection string in the
[CoreSecurityInstallPath]\CourionService\config\
Scheduler.WCFHost.ConnectionStrings.config file to point it to the Courion
database:

```
<add name="dbConnectionString" connectionString="Data Source=
$$YOURSERVERHERE$$;Initial Catalog= $$YOURDBHERE$$;Trusted_Connection=True;
providerName="System.Data.SqlClient" />
```

Replace \$\$YOURSERVERHERE\$\$ with the name of the database server.

Replace \$\$YOURDBHERE\$\$ with the name of the database.

3. Modify the properties of the Courion Identity Mapping service to set Startup type to automatic.

The Courion Identity Mapping service is a WCF (Windows Communication Foundation) service that provides an API (application programming interface) for operations including the set up of rules, data feeds, rule execution, and reporting.

4. Start the Courion Identity Mapping service.
5. Modify the properties of the Courion Scheduler service to set Startup type to automatic.

The Courion Scheduler service is a WCF service used to schedule rule executions.

6. Start the Courion Scheduler service.

Note: If you modify a connection string, you need to restart the respective service. For example, if you modify the connection string for the Courion Scheduler service, then you need to restart this service.

Note: The account used to log in to the Access Assurance Portal to access Identity Mapping needs to be a member of the IDM Admins dynamic community. For more information about communities, refer to the manual *Configuring the AccountCourier Access Request Manager™ Solution*.

Using the Identity Mapping Interface

The interface for Identity Mapping is available through the Access Assurance Portal. To access the interface you need to be a member of the IDM Admins dynamic community. By default, this means you need to be a member of the IDM Admins Active Directory group.

To access the Portal on the server where it is installed, navigate to:

`http://localhost/CoreARMS/AspxCommon/PortalHome.aspx`

To access the Portal from another system, navigate to:

`http://[machine-name or IP address]/CoreARMS/AspxCommon/PortalHome.aspx`

The Access Assurance Portal Login page appears, as shown in [Figure 1](#).

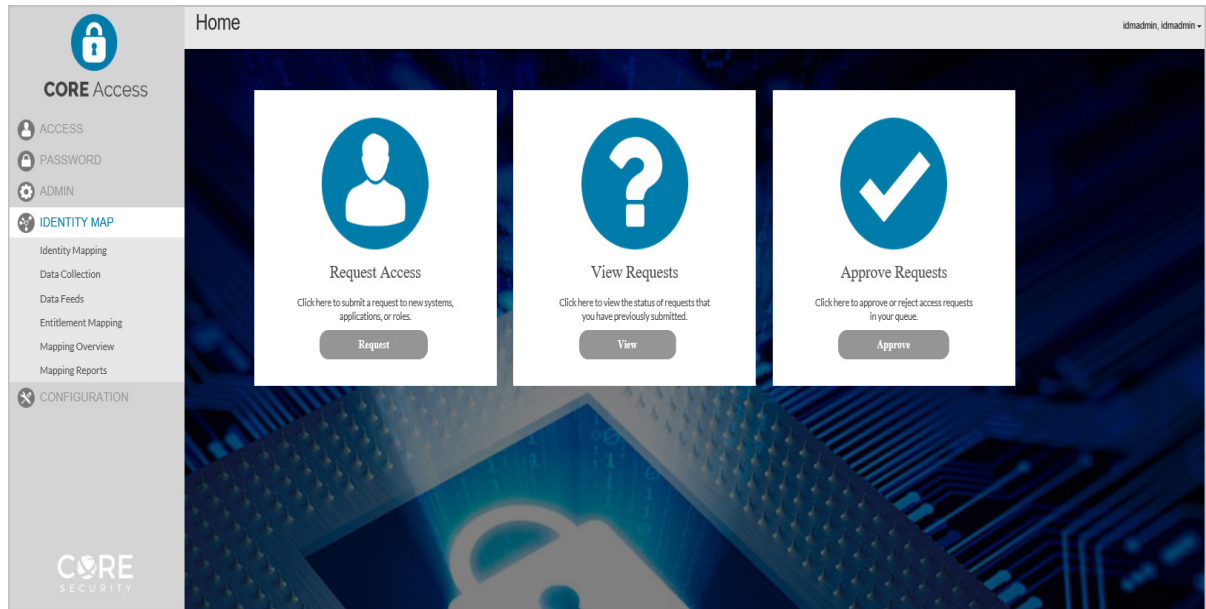
Figure 1: Access Assurance Portal Login



Note: If the Integrated Windows Authentication feature is configured, you are automatically authenticated in to the Access Assurance Portal. For more information, refer to the manual *Installing the Access Assurance Suite*.

Upon authentication, you can access the Data Collection options by clicking the Mega Menu which is shown in [Figure 2](#).

Figure 2: Data Collection Options



The main menu contains the following data collection and mapping administration options:

- **DATA COLLECTION:** Create and schedule data collection rules that collect and filter data from source systems. For more information, refer to [“Creating a Data Collection Rule” on page 19](#).
- **DATA FEEDS:** Use data feed tables to set up the data feed for Identity Mapping. For more information about data feeds, refer to [“Setting Up Data Feeds” on page 51](#).
- **IDENTITY MAPPING:** Specify rules against data feeds to map accounts to profiles.
 - To create rules, refer to [“Creating Identity Mapping Rules” on page 57](#).
 - To execute rules, refer to [“Executing Rules to Map Accounts” on page 63](#).
 - To view rule history, refer to [“Viewing Rule History” on page 68](#).
 - To manually map accounts, refer to [“Mapping Accounts Manually” on page 77](#).
 - To delete mapped accounts, refer to [“Deleting Mapped Accounts” on page 83](#).
- **ENTITLEMENT MAPPING:** Specify rules against data feeds to map assigned entitlements to profiles. For more information, refer to [“Mapping Collected Entitlements” on page 72](#).
- **MAPPING OVERVIEW:** View charts to view account information by target, type or date. The window also displays the last rule that was run, and related information. For more information, refer to [“Viewing the Overview Window” on page 86](#).
- **MAPPING REPORTS:** View the mapped information. For more information about reporting, refer to [“Viewing Account Information” on page 88](#).

Note: Several input fields within the Identity Mapping Solution support the type-ahead feature. This feature enables you to enter text into a field while the Identity Mapping Solution provides the closest match to auto-complete it.

Chapter 3: Setting Up Data Collection Rules

This chapter describes how to configure data collection rules using the Identity Mapping user interface. Data collection rules enable you to collect and filter data that will be used by the Identity Mapping process. The functionality is described in the following sections:

- [*"Post-Installation Setup for Data Collection"*](#)
- [*"Creating a Data Collection Rule"*](#)
- [*"Securing Data Collection"*](#)
- [*"Viewing Data Collection Results"*](#)
- [*"Deleting a Data Collection Rule"*](#)

Post-Installation Setup for Data Collection

Creating Data Collection Entities

The data collection rules functionality requires the following configuration for database communication:

1. In a text editor, open the [CoreSecurityInstallPath]\CourionARMS\CustomerConnStrings.config file for editing.
2. If the CustomerConnStrings.config file is encrypted, the commands to decrypt the file are as follows:

```
cd C:\Windows\Microsoft.Net\Framework\v4.0.30319
```

```
aspnet_regiis.exe -pdf connectionStrings "C:\ProgramFiles (x86)\  
Courion Corporation\CourionARMS\CustomerConnStrings.config"
```

3. Uncomment the DataCollectionEntities connection string and then make the following changes:
 Replace \$\$YOURSERVERHERE\$\$ with the name of the database server.
Note: You can specify a port number if you want to use a non-default port.
 Replace \$\$YOURUSERIDHERE\$\$ with the username for the database user.
 Replace \$\$YOURDBPASSWORDHERE\$\$ with the password for the database user.
4. Save your changes and exit.
5. To prevent passwords from being passed in clear text, you can encrypt the CustomerConnStrings.config file. In a command window, encrypt the connection strings using the following commands:

```
cd C:\Windows\Microsoft.Net\Framework\v4.0.30319
```

```
aspnet_regiis.exe -pef connectionStrings "C:\ProgramFiles (x86)\  
Courion Corporation\CourionARMS\CustomerConnStrings.config"
```

Adding Tomcat Server Entries in the Web.config File

The Tomcat Server is required for data collection rules functionality. Before users access the Access Assurance Portal Page to create data collection rules, you should do the following:

1. Open the [CoreSecurityInstallPath]\CourionARMS\Web.config file for editing.
2. Add the following entry in which you replace \$\$SERVERNAMEWITHDOMAIN\$\$ with the name of the Tomcat server:

```
<add key="TomcatBaseUri" value="http://$$SERVERNAMEWITHDOMAIN$$:8080/>
```

Note: The server name must be in the form of the IP address or the fully-qualified domain name of the Web server (Tomcat server); do not use "localhost".
3. Add the following entry which points to the Tomcat home directory, where version is the version number that has been installed:


```
<add key="TomcatInstallDir" value="C:\Tomcat\apache-tomcat-version"/>
```

4. Save your changes and exit the file.

Creating Staging Tables for the Collector for Epic

If you plan to collect data using the Collector for Epic, you should run the scripts to create staging tables for the Epic data.

1. While logged in to the database as an administrative user, run the following script to create the EpicAccount table:

```
[CoreSecurityInstallPath]\CourionARMS\ContentRepository\Epic\EpicAccount.table
```

2. While logged in to the database as an administrative user, run the following script to create the EpicProfile table:

```
[CoreSecurityInstallPath]\CourionARMS\ContentRepository\Epic\EpicProfile.table
```

3. While logged in to the database as an administrative user, run the following script to create the EpicEntitlement table:

```
[courion-installationfolder]\CourionARMS\ContentRepository\Epic\EpicEntitlement.table
```

Confirming Configuration of Data Source Systems

For data collection to work, you (or another administrator) configure the Access Assurance Portal to communicate with the systems which contain the data you want to collect. The configuration process is described in the *Configuring Password Management Modules (PMMs), Connectors, and Agents* manual.

After you have identified the sources of profile, account, and entitlement data, you should make sure that the Portal can communicate with the systems where the databases, files, or directory-based repositories exist.

Data collection rules are designed to run on the Courion server system from which you have configured the source systems. If your Courion environment is a distributed setup and you have configured targets to communicate with a remote Configuration Framework Manager or a remote Connector Framework, you cannot run data collection upon those targets. Instead, you should run Connector Configuration Manager on the Courion server system and configure the targets again.

Installing Data Collectors

Before you create a data collection rule, you should install the data collectors that you plan to use. From the Mega Menu in the Access Assurance Portal, select **MANAGE CONTENT**.

To install a collector, do the following:

1. Click one or more check boxes next to the name of the collector(s) you want to install. (Collectors are one type of content; you can also use this dialog box to install report type content.)
2. Click **INSTALL**. A confirmation dialog box appears.
3. Click **OK**. The installation should take a few minutes. The content state will change to Queued and then change to Installed as shown in [Figure 4](#).

Figure 4: Manage Content window with all Collectors Installed

Manage Content						
<div> <input type="button" value="Install"/> <input type="button" value="Uninstall"/> </div>						
<input type="checkbox"/>	Name	Type	Description	Release Date	Install / Uninstall Date	State
<input type="checkbox"/>	Active Certification Review Cycle	Report	Active certification review cycles	Mon Sep 01 2014		New
<input type="checkbox"/>	Request Summary	Report	Access request raised by application and department	Mon Sep 01 2014		New
<input type="checkbox"/>	User Life Cycle	Report	Request raised in user's life cycle	Mon Sep 01 2014		New
<input type="checkbox"/>	Active Directory	Collector	Collector to collect data from any Active Directory	Thu Mar 26 2015	Tue Apr 07 2015	Installed
<input type="checkbox"/>	Epic	Collector	Collector to collect data from any Epic	Thu Mar 26 2015	Tue Apr 07 2015	Installed
<input type="checkbox"/>	Generic CSV	Collector	Collector to collect data from any Generic CSV	Thu Mar 26 2015	Tue Apr 07 2015	Installed
<input type="checkbox"/>	Generic SQL	Collector	Collector to collect data from any Generic SQL	Thu Mar 26 2015	Tue Apr 07 2015	Installed
<input type="checkbox"/>	Sun Directory LDAP	Collector	Collector to collect data from any Sun Directory LDAP	Thu Mar 26 2015	Tue Apr 07 2015	Installed

4. Restart the Apache Tomcat service so that Tomcat can deploy the new collector(s). This step is necessary.

Creating a Data Collection Rule

The following is an overview of the steps to create a new data collection rule using the Data Collection wizard:

1. Specify the type of data to collect and the system from which to collect data.
2. Select the attributes you want to collect and map them to attributes for the destination table.
3. Filter the data.
4. Optionally, extend the collection rule by adding a pre-processor or a post-processor to manipulate the data.
5. Schedule the data collection rule to run.

Before you begin, you need the following information:

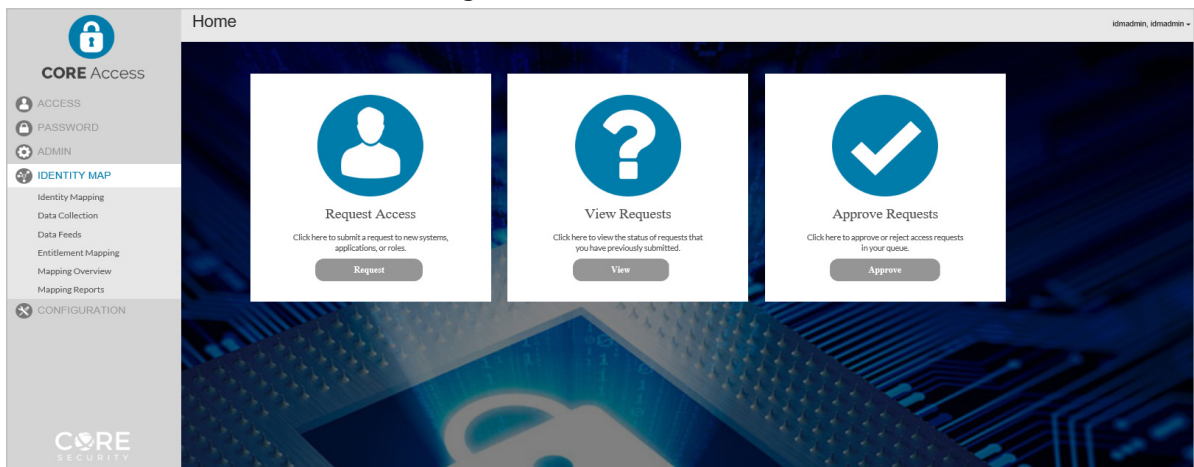
- For collection using a generic CSV file: the path to the file, a privileged username and password to access the CSV file, the field delimiter, and the line feed record delimiter.
- For collection using a generic SQL database: the path to the SQL database, a privileged username and password to connect to the SQL database, and the database table name with the schema name.
- For collection using the Collector for Epic: the path to the SQL database, a privileged username and password to connect to the SQL database, and the database table name with the schema name.

You may also want to confirm the following about your Courion environment:

- In the Windows Services, make sure that the SQL Server Agent service and Apache Tomcat service are running.
- Open the [CoreSecurityInstallPath]\CourionARMS\Web.config file in a text editor and make sure that the Tomcat Server entries (hostname, port number and directory) are correct for your environment.

From the Mega Menu in the Access Assurance Portal, select **DATA COLLECTION** as shown in [Figure 5](#).

Figure 5: Data Collection



The Data Collection Rules window appears as in [Figure 6](#).

Figure 6: Data Collection Rules

Data Collection Rules									
<input type="checkbox"/> Auto Refresh									
<input type="button" value="Add New Rule"/> <input type="button" value="Delete Rules"/>									
<input type="checkbox"/>	Rule Name	Collector	Target	Type	Status	Last Run Result	Run Rule	Edit Rule	
<input type="checkbox"/>	AD_Ent	Active Directory	Active Directory	Accounts, Assigned Entitlements	Idle	Accounts: 16298 Assigned Entitlements: Total - 851; New to catalog - 851	<input type="button" value="Run"/>	<input type="button" value="Edit"/>	
<input type="checkbox"/>	CSV_Collection	Generic CSV	Condition Evaluator	Accounts, Assigned Entitlements	Idle		<input type="button" value="Run"/>	<input type="button" value="Edit"/>	
<input type="checkbox"/>	SQL_Collection	Generic SQL	InitProfile	Accounts, Assigned Entitlements				<input type="button" value="Edit"/>	
<input type="checkbox"/>	AD Collection	Active Directory	Active Directory	Accounts, Assigned Entitlements	Scheduled	Accounts: 16259 Assigned Entitlements: Total - 851; New to catalog - 0	<input type="button" value="Run"/>	<input type="button" value="Edit"/>	
<div> <input type="button" value="Previous"/> <input checked="" type="button" value="1"/> <input type="button" value="Next"/> <input type="button" value="Last"/> </div> <div> 5 items per page </div> <div> 1 - 4 of 4 items </div>									

Specifying a Target System as the Collection Source

Access Assurance Suite collects structured information from databases or directory-based repositories such as Active Directory.

- To create a new data collection rule, click **ADD NEW RULE**. The Data Collection Rule wizard opens with the **SELECT SOURCE** page as shown in [Figure 7](#).

Figure 7: Select Source

Select Source

Select Attributes

Filter Data

Select Processor

Schedule Rule

Exit Wizard

Select Source

Data Collection Options

☒ Accounts
 ☐ with Assigned Entitlements
 ☐ Entitlement Catalog
 ☐ Profiles

Rule Name *

Rule Description

Source System *

Collector *

Select target

Select collector

Back
Next


- Configure the following fields in the **SELECT SOURCE** page:

COLLECTION TYPE: Specify the type(s) of data you are collecting. The options are **ACCOUNTS**, **ACCOUNTS WITH ENTITLEMENT**, **ENTITLEMENT CATALOG**, OR **PROFILES**.

RULE NAME: Enter a name to uniquely identify the data collection rule.

RULE DESCRIPTION: Specify a description for the data collection rule.

SOURCE SYSTEM: Select the source of the data from the drop-down list. The list displays all of the connectors that have been configured using the Connector Configuration Manager. For more information, refer to the *Configuring Password Management Modules (PMMs), Connectors, and Agents* manual. (If you add a

connector while using this wizard, click the Refresh button  to ensure that the drop-down list includes all configured connectors.)

Note: If the source will be a consolidated file that originates from multiple target systems, select **MULTIPLE TARGETS**. When the Select Attributes page appears, be sure to map the column which contains the target name to the TargetID column.

COLLECTOR: The Collector drop-down list displays collectors that have been installed and are supported by the source system you selected. Collectors are designed to work with specific source systems or applications and include knowledge of what components should be mapped to user profiles, user accounts and entitlements of the Access Assurance Suite. There are several types of collectors:

- A generic collector can be used for any application that can be managed through the specific technology of the collector. It can be configured to map data from the source into the user profiles, user accounts and entitlements. Examples of generic collectors are the Generic Collector for CSV and Generic Collector for Microsoft SQL Server.
- Standard collectors apply to third-party sources including Microsoft Active Directory and Epic

Depending on the collector that you choose, additional fields may be required as described in the following sections.

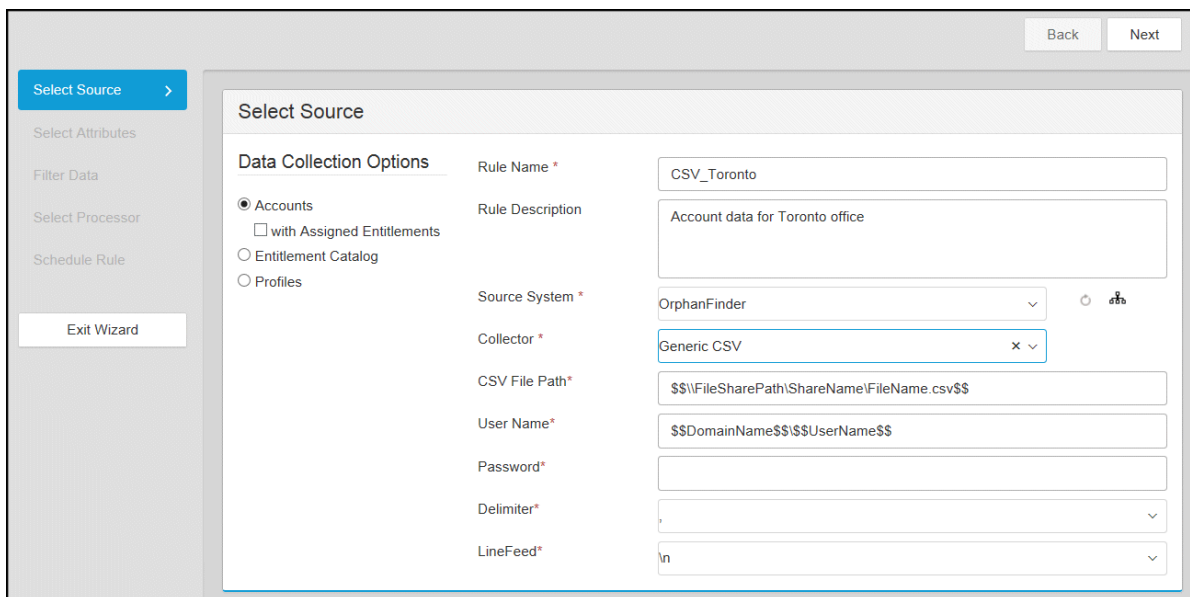
3. Click **NEXT**. The Select Attribute page appears.

Note: By clicking **NEXT**, the data collection rule is saved. If you later choose **EXIT** to leave another wizard page without saving, the data collection rule still exists with the items specified on the Select Source page.

Specifying Fields for the Generic Collector for CSV

For example, the Generic Collector for CSV requires the following additional fields shown in [Figure 8](#):

Figure 8: Additional Fields for Generic Collector for CSV



The screenshot shows the 'Select Source' wizard page. On the left is a sidebar with navigation links: 'Select Source' (active), 'Select Attributes', 'Filter Data', 'Select Processor', 'Schedule Rule', and 'Exit Wizard'. The main area is titled 'Select Source' and contains the following fields:

- Data Collection Options:**
 - ☒ Accounts
 - ☐ with Assigned Entitlements
 - ☐ Entitlement Catalog
 - ☐ Profiles
- Rule Name ***: CSV_Toronto
- Rule Description**: Account data for Toronto office
- Source System ***: OrphanFinder
- Collector ***: Generic CSV
- CSV File Path ***: \$\$\FileSharePath\ShareName\FileName.csv\$\$
- User Name ***: \$\$DomainName\$\$\\$\$UserName\$\$
- Password ***: (empty field)
- Delimiter ***: ,
- LineFeed ***: \n

At the top right of the main area are 'Back' and 'Next' buttons.

CSV FILE PATH: Specify the path to the comma-separated values (CSV) file. The field provides the expected format which is a Universal Naming Convention path.

USER NAME: Specify a privileged username to be used to connect to the CSV file. This privileged user must have Read & Execute and Read permissions on the CSV file and the Read permission on the folder containing the CSV file.

PASSWORD: Specify the password to be used to connect to the CSV file.

DELIMITER: Specify the character, which separates fields in each record. The maximum length of the delimiter is five characters. Note that the character '\$' cannot be used as a delimiter.

LINEFEED: Specify the character, which separates each record in the file.

Specifying Fields for the Collector for Microsoft Active Directory

The Collector for Microsoft Active Directory requires the following additional field as shown in [Figure 9](#):

Figure 9: Additional Fields for Collecting Profile Data using the Collector for Microsoft Active Directory

The screenshot shows a 'Select Source' dialog box with a sidebar on the left containing 'Select Source', 'Select Attributes', 'Filter Data', 'Select Processor', 'Schedule Rule', and 'Exit Wizard'. The main area is titled 'Select Source' and contains the following fields:

- Data Collection Options:**
 - ☒ Accounts
 - ☐ with Assigned Entitlements
 - ☐ Entitlement Catalog
 - ☐ Profiles
- Rule Name ***: Profiles from Seattle
- Rule Description**: Profiles from Seattle office
- Source System ***: Active Directory (dropdown)
- Collector ***: Active Directory (dropdown)
- Base Distinguished Name**: dc=yourorg,dc=example,dc=com (text input with a clear button)
- Protocol***: LDAPS(SSL) with specific certificate (dropdown)
- Keystore Path**: (empty text input)
- Keystore Password**: (empty text input)

At the bottom right are 'Back' and 'Next' buttons.

BASE DISTINGUISHED NAME: Specify the connection string using the suggested format to connect to the AD database.

PROTOCOL: In this drop-down list, you can select from three options: **LDAPS(SSL) WITH SPECIFIC CERTIFICATE**, or **LDAPS(SSL) WITH ALL CERTIFICATES**, and **LDAP**. The communication between the collector and the data source system varies depending on the option you select:

- When the **LDAPS(SSL) WITH SPECIFIC CERTIFICATE** option is selected, the collector uses certificates added in the keystore to validate the server certificate sent by the data source system, and then initiates the communication using LDAP over SSL. For this option, you must enter values for the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields. This option is displayed by default.

- When **LDAPS(SSL) WITH ALL CERTIFICATES** option is selected, the collector accepts any certificate sent by the data source system and initiates the communication using LDAP over SSL. For this option, the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields are not required.
- When the **LDAP** option is selected, the communication between the collector and the data source system happens using the insecure LDAP protocol. For this option, the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields are not required.

KEYSTORE PATH: Enter the full path and file name of the CourionKeystore.jks that contains the trusted certificates. For example, C:\MyCertsFolder\CourionKeystore.jks. For more information on creating a Keystore, refer to the section, [“Creating a Keystore” on page 38](#).

KEYSTORE PASSWORD: Enter the Password that you created while creating the keystore.

Specifying Fields for the Generic Collector for Microsoft SQL Server

For example, the Generic Collector for Microsoft SQL Server requires the following additional fields shown in [Figure 10](#):

Figure 10: Additional Fields for the Generic Collector for Microsoft SQL Server

The screenshot shows the 'Select Source' configuration window. On the left is a sidebar with navigation links: 'Select Source' (highlighted), 'Select Attributes', 'Filter Data', 'Select Processor', 'Schedule Rule', and 'Exit Wizard'. The main area is titled 'Select Source' and contains the following fields:

- Data Collection Options:** A section with radio buttons for 'Accounts' (selected), 'with Assigned Entitlements', 'Entitlement Catalog', and 'Profiles'.
- Rule Name:** A text field containing 'Accounts from Phoenix'.
- Rule Description:** A large empty text area.
- Source System:** A dropdown menu showing 'Active Directory'.
- Collector:** A dropdown menu showing 'Generic SQL'.
- Connection String:** A text field with the placeholder 'Data Source = \$\$ServerName\$\$; Initial Catalog = \$\$DatabaseName\$\$; Port ='.
- User Name:** An empty text field.
- Password:** An empty text field.
- Table Name:** An empty text field.
- Additional Parameters:** An empty text field.

At the bottom right of the window are 'Back' and 'Next' buttons.

CONNECTION STRING: Specify the database server and database that is the source of data. You can also change the Port number if you want to use a non-default port.

USER NAME: Specify a privileged username to be used to connect to the SQL database.

PASSWORD: Specify the password to be used to connect to the SQL database.

TABLE NAME: Specify the database table with schema name (for example, Schema.Name.TableName) from which to collect the data.

ADDITIONAL PARAMETERS: Specify any additional parameters supported by standard SQL. To specify an SQL Server instance name, the format is: Instance=*instance_name*.

Specifying Fields for the Collector for Oracle Sun Directory LDAP

The Collector for Oracle Sun Directory LDAP requires the following additional fields as shown in [Figure 11](#):

Figure 11: Fields for using the Collector for Oracle Sun Directory LDAP

PROTOCOL: In this drop-down list, you can select from three options: **LDAPS(SSL) WITH SPECIFIC CERTIFICATE**, or **LDAPS(SSL) WITH ALL CERTIFICATES**, and **LDAP**. The communication between the collector and the data source system varies depending on the option you select:

- When the **LDAPS(SSL) WITH SPECIFIC CERTIFICATE** option is selected, the collector uses certificates added in the keystore to validate the server certificate sent by the data source system, and then initiates the communication using LDAP over SSL. For this option, you must enter values for the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields. This option is displayed by default.
- When **LDAPS(SSL) WITH ALL CERTIFICATES** option is selected, the collector accepts any certificate sent by the data source system and initiates the communication using LDAP over SSL. For this option, the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields are not required.
- When the **LDAP** option is selected, the communication between the collector and the data source system happens using the insecure LDAP protocol. For this option, the **KEYSTORE PATH** and **KEYSTORE PASSWORD** fields are not required.

KEYSTORE PATH: Enter the full path and file name of the CourionKeystore.jks that contains the trusted certificates. For example, C:\MyCertsFolder\CourionKeystore.jks. For more information on creating a Keystore, refer to the section, [“Creating a Keystore” on page 38](#).

KEYSTORE PASSWORD: Enter the Password that you created while creating the keystore.

PORT: Specify the port number to connect to the data source system. Generally, port 389 is used for LDAP and port 636 for LDAP over SSL. Contact the system administrator of your data source system to confirm the port numbers.

Specifying Fields for a Standard Collector

The Collector for Epic is an example of a standard collector. It requires the additional fields as shown in [Figure 12](#):

Figure 12: Additional Fields for the Collector for Epic

The screenshot shows a 'Select Source' wizard interface. On the left is a sidebar with navigation links: 'Select Source' (highlighted with a blue arrow), 'Select Attributes', 'Filter Data', 'Select Processor', 'Schedule Rule', and 'Exit Wizard'. The main area is titled 'Select Source' and contains the following fields:

- Data Collection Options:** A group box containing three radio buttons: 'Accounts' (selected), 'with Assigned Entitlements' (unchecked), 'Entitlement Catalog' (unchecked), and 'Profiles' (unchecked).
- Rule Name ***: A text input field containing 'Accounts from Epic'.
- Rule Description**: A large text area.
- Source System ***: A dropdown menu showing 'Active Directory'.
- Collector ***: A dropdown menu showing 'Generic SQL'.
- Connection String***: A text input field containing 'Data Source = \$\$ServerName\$\$; Initial Catalog = \$\$DatabaseName\$\$; Port = '.
- User Name***: A text input field containing 'sa'.
- Password***: A password input field with masked characters (dots).
- Table Name***: A text input field containing 'etl.EpicAcct'.
- Additional Parameters**: A large text area.

At the bottom right of the wizard are 'Back' and 'Next' buttons.

CONNECTION STRING: Specify the connection string using the suggested format to connect to the SQL database. You can also change the Port number if you want to use a non-default port.

USER NAME: Specify a privileged username to be used to connect to the SQL database.

PASSWORD: Specify the password to be used to connect to the SQL database.

TABLE NAME: Specify the database table with schema name (for example, Schema.Name.TableName) from which to collect the data.

ADDITIONAL PARAMETERS: Specify any additional parameters supported by standard SQL. To specify an SQL Server instance name, the format is: Instance=*instance_name*.

Selecting Attributes

If you have specified a collector other than the Collector for Microsoft Active directory, the wizard makes the connection to the target system and provides sample data so that you can map columns to a staging table. The Select Attributes page populates with column headings from the source table. The wizard intelligently suggests possible mappings to columns in the destination table. In many cases, the mappings of source columns to destination columns will be correct for your environment. You may not need to modify anything on the Select Attributes page.

When using the Collector for Microsoft Active Directory to collect accounts only or accounts with assigned entitlements, the Data Collection Wizard intelligently maps the objectSid and AccountUID attributes. Because the mapping of objectSID to AccountUID is central to the creation of the Identity Map, the ability to modify the mapping between these columns is disabled.

The following table summarizes the names of tables which are populated depending upon the data collection type.

Table 1: Destination Tables by Collection Type

Collection Type	Destination Table(s)
Accounts	Account_Staging
Accounts with Assigned Entitlements	Account_Staging Entitlement_Staging
Entitlement Catalog	Entitlement_Staging
Profiles	Profile_Staging

Select Attributes for a Generic CSV File

The following figures show the mapping of attributes in a CSV file which has header information.

Figure 13: Select Attributes for CSV File

Select Attributes

Source Attribute	Destination Field	Source Attribute	Destination Field
Username	UserName	ProfileID	EmployeeID
TargetID	Department	--Skip--	--Skip--
--Skip--	--Skip--	--Skip--	--Skip--
--Skip--	--Skip--	--Skip--	--Skip--
--Skip--	--Skip--	--Skip--	--Skip--

Sample Source Data

Sample Size: 50 ☒ First row is header ☒ Hide blank columns

Username	ProfileID	TargetID
	ptest00005	iSeries1
PF00005		iSeries3
PF00006	ptest00005	iSeries4
PF00007	ptest00005	iSeries5

1 - 5 of 10 items

If the first row of data in the source contains header information, click the **FIRST ROW IS HEADER** check box as shown in [Figure 13](#).

To map a source attribute to a different destination attribute, use the **DESTINATION FIELD** drop-down list to select a different attribute.

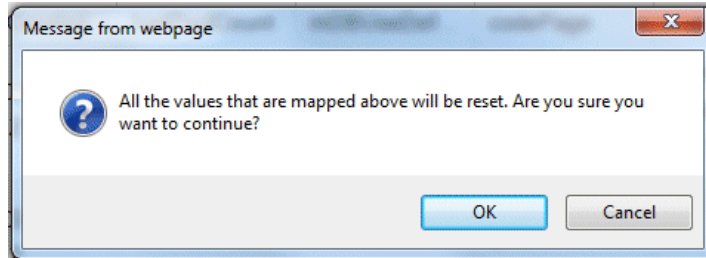
To map a different source attribute, use the **SOURCE ATTRIBUTE** drop-down list to select a different attribute.

To avoid collection of certain attributes, go to the **SOURCE ATTRIBUTE** drop-down list for that attribute and select **--Skip--**.

If an attribute you want to map is not visible, the easiest way to find it is to click the **+ADD MORE** button, and click the **DESTINATION FIELD** drop-down list, and scroll down to find the attribute name.

When you have finished making any mapping changes, click **PREVIEW**. A confirmation dialog box appears.

Figure 14: Select Attributes: Applying Column Headings



Click **OK**. The Select Attributes page refreshes. The sample data reflects the changes you made. This data is temporarily stored in the custom_mapping_review table.

Attribute Selection for Collection of Entitlements

The following figure shows an example of collecting entitlement data. The Select Attributes page populates with column headings from the source table. The wizard intelligently suggests possible mappings to columns in the destination table.

Figure 15: Mapped Attributes

Source Attribute	Destination Field	Use as Entitlement Attribute	Multi Value	Separator	Enclosure	Escape
objectSid	AccountUID	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
accountExpires	ExpiredOn	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
IsExpired	IsExpired	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
employeeID	EmployeeID	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
sAMAccountName	UserName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
displayName	FullName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
givenName	FirstName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
middleName	MiddleName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--
sn	LastName	<input type="checkbox"/>	<input checked="" type="checkbox"/>		--Skip--	--Skip--

In many cases, the mappings of source columns to destination columns will be correct for your environment. You may not need to modify anything. In other cases, you may map the same Source column to more than one Target column. Sometimes you may want to map a Source column to a custom attribute because that attribute can better accommodate the data.

To map account attributes and establish which attribute is needed for entitlements, do the following:

1. Scan through the **SAMPLE SOURCE DATA** grid to locate the column which contains entitlement data. If needed, scroll to the right.
2. Knowing the name of the column, find the corresponding Source Attribute. In that row, click the **USE AS ENTITLEMENT ATTRIBUTE** check box to indicate the name of the column which contains entitlement data. If you are using an Active Directory database, the memberOf attribute may contain entitlements.
3. If the column contains multiple entitlements in each row, click the **MULTI VALUE** check box. Then specify the character which consistently separates each entitlement. The **SEPARATOR** drop-down list suggests delimiting characters but you can also enter other characters.
4. If each entitlement is enclosed by a set of parentheses, specify that by using the **ENCLOSURE** drop-down list. If some entitlements contain the enclosure character and are preceded by an escape character, select the escape character from the **ESCAPE** drop-down list.

Filtering Data

The sample data may contain hundreds or thousands of records which may or may not be relevant to identity management. Therefore, you can use the Filter Data page to configure the data collection rule to exclude the data that is not relevant.

5. Click **NEXT**. The Filter Data page appears.
6. In the Filter Data page, click **PREVIEW**. The page refreshes to display a sampling of the collected data as shown in [Figure 16](#).

By default, blank columns are not shown. To display blank columns, uncheck **HIDE BLANK COLUMNS**.

By default, the page shows a sample of 100 records. Use the **SAMPLE SIZE** control to increase or decrease the amount of records. (If you selected the Collector for Oracle Sun Directory LDAP, the maximum sample size is 1000 records.)

If you want to view more than five records on a page, use the **ITEMS PER PAGE** control to increase the amount of records displayed on a page.

Figure 16: Filter Data Page

Rule Name: profile from 83update2 Back Next

Select Source ✓
Select Attributes ✓
Filter Data >
Select Processor ✓
Schedule Rule ✓
Exit Wizard

Filter Data

Available Filters

Filter Name		
First Name is blank		
Last Name is blank		
Job Title is blank		
Profile is blank		
Job Code is blank		
Active Directory profile is disabled (51		

[+ New Filter...](#)

Selected Filters (Data will be excluded)

Filter Name

[✕ Clear All](#)

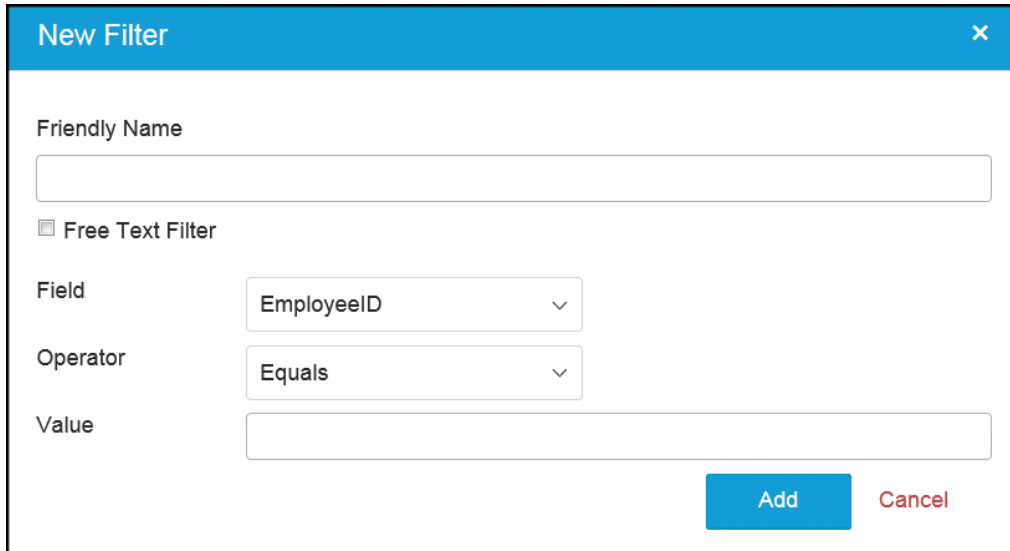
Sample Size: 100 Preview ☒ Hide blank columns

ProfileUID	FirstName	LastName	EmployeeNo	JobTitle	Email	Status
1345	1345	1346	1345	03/24/2010	1345@f.com	66048
13Dec1	Thirteen	December One		King	Thirteen.DecemberOne	66048
3465	3465				rVixen@hiphop.dom	66048
5442	sa	dgh	3456	03/24/2010		66048
8787	hiji	787v	787	03/24/2010		66048

1 2 3 4 5 6 7 8 9 10 ... 5 Items per page 1 - 5 of 100 items

- In the Filter Data page, you can exclude data by adding filters to the **SELECTED FILTERS** list. For example, to exclude data records which have a blank First Name column, select **FIRST NAME IS BLANK** and click the **>**.
- To preview the impact of applying the selected filters, click **PREVIEW**. The page refreshes with filtered results.
- If the **AVAILABLE FILTERS** list does not contain the field you wish to filter upon, you can add a new data filter. Click **NEW FILTER**. A popup appears as shown in [Figure 17](#).


Figure 17: New Filter



- **FRIENDLY NAME:** Specify a name for the filter that you and your peers understand and that distinguishes the filter from other user-defined filters.
- **FIELD:** Using the drop-down list, select the field for this filter.
- **OPERATOR:** Using the drop-down list, select the operator for this filter.
- **VALUE:** Specify the value that completes the filter logic to match only the data you want to exclude.

Note: When two filters operate on the same field (column), data will be excluded if it has a column that matches either of the filters. If filter A or filter B is true for a record, that data will be excluded.

Note: When two filters operate on different fields (columns), data will be excluded if both columns of the same record match both filters. If filter A and filter B are true for the same record, that record will be excluded.

- Click **ADD** to add the filter (or **CANCEL** to exit without saving changes). The new user-defined filter you created appears near the bottom of the **AVAILABLE FILTERS** list with a user-defined symbol  preceding it.
- To use your new user-defined filter, scroll down the **AVAILABLE FILTERS** list, select the filter, and click **>**.
- Click **PREVIEW**. When the data refreshes, confirm that the data to be excluded was not collected.
- Click **NEXT**. The Select Processor page appears.

To create and specify a user-defined filter using the SQL WHERE clause, do the following:

- Specify a name for your user-defined filter and click the **FREE TEXT FILTER** check box.
- In the text box, enter the filter syntax.
- Click **CHECK SYNTAX**.
- If the syntax passes, click **ADD**. A confirmation message appears.
- Click **OK**. The New Filter dialog disappears. The name of your user-defined filter appears in the **AVAILABLE FILTERS** list and the **SELECTED FILTERS** list.

6. Click **PREVIEW**. When the data refreshes, confirm that the data to be excluded was not collected.
7. Click **NEXT**. The Select Processor page appears.

Copying Cleansed Data to Production Tables

If your data source was created specifically for data collection (such as a CSV file) and you know that the data being collected will map accurately to the production tables, check the **COPY DATA TO PRODUCTION** check box on the Select Processor page of the wizard.

Figure 18: Copy Data to Production Check Box

Select Processor

Copy Data to Production* ☒

Pre Processor

Processor : ▼ Clear Processor

Continue On Failure : ☐

When the rule runs, the collected data is automatically copied from the destination table to the appropriate production table(s).

Collection Type	Destination Table(s)	Production Table(s)
Accounts	Account_Staging	not applicable
Accounts with Assigned Entitlements	Account_Staging Entitlement_Staging	Entitlement Entitlement_Configuration Entitlement_Mapping_Target
Entitlement Catalog	Entitlement_Staging	Entitlement Entitlement_Configuration Entitlement_Mapping_Target
Profiles	Profile_Staging	Profile

Manually Copying Cleansed Data to Production Tables

However, in many cases, profile and entitlement data must be cleansed, improved or used as a trigger to initiate external workflows before they are loaded into the respective production tables and before the identity mapping rules are applied. Before running a rule, you should make sure that the **COPY DATA TO PRODUCTION** check box on the Select Processor page of the wizard is un-checked. (This does not apply to account data.)

You may need to edit and run a data collection rule several times before the data that you collect is what you expect.

Cleansed Profile Data

You may also need to alter the data in the Profile_Staging table manually. If you have cleansed data in the Profile_Staging table that is ready to be copied to the Profile table, you can run the SetProfile stored procedure (in the Courion database) as follows:

1. Find the rule ID from [etl].[CollectionRule] table by passing CollectionRuleName in the where clause of the following SELECT statement where \$\$MyCollectionRuleName\$\$ is the name of the profile collection rule:

```
SELECT [CollectionRule_ID],[CollectionRuleName] FROM
[etl].[CollectionRule] WHERE [CollectionRuleName]
='$$MyCollectionRuleName$$'
```

2. Execute the [dbo].[SetProfile] stored procedure with the data collection rule_id as the parameter which restricts the data associated with the collection rule. For example, if the SELECT statement returned the rule_ID as 1, the EXEC directive would be as follows:

```
EXEC [dbo].[SetProfile]

@Rule_Id = 1
```

Cleansed Entitlement Data

If you have added or modified data in the Entitlement_Staging table and the data is ready to be copied to the production tables which contain entitlements, you can run the usp_EntitlementCollection stored procedure (in the Courion database) as follows:

1. Find the rule ID from [etl].[CollectionRule] table by passing CollectionRuleName in the where clause of the following SELECT statement where \$\$MyCollectionRuleName\$\$ is the name of the entitlement collection rule:

```
SELECT [CollectionRule_ID],[CollectionRuleName] FROM
[etl].[CollectionRule] WHERE [CollectionRuleName]
='$$MyCollectionRuleName$$'
```

2. Execute the [dbo].[usp_EntitlementCollection] stored procedure with the data collection rule_id as the parameter which restricts the data associated with the collection rule. For example, if the SELECT statement returned the rule_ID as 1, the EXEC directive would be as follows:

```
DECLARE @RESULT nvarchar(500)

EXEC [dbo].[usp_EntitlementCollection]

@Rule_Id = N'1',
```


@RESULT = @RESULT OUTPUT

Applying a Pre- or Post-Processor

In addition to filtering the data that is collected, you can configure a data collection rule to do one or both of the following:

- Run a pre-processor against a data source before collection
- Run a post-processor against collected data after collection.

Note: A data collection rule can support one pre-processor, or one post-processor, or one pre-processor and one post-processor. More than one of either is not supported.

Note: If you selected the **COPY DATA TO PRODUCTION** check box and you specify a post-processor, the post-processor runs before the collected data is copied from the destination table to the appropriate production table(s).

Examples of Pre-Processors

You could write a batch file that creates a comma-separated values (CSV) file from Active Directory. By calling the batch file as a pre-processor, the resulting CSV file becomes the source for collected data.

You could write a Java Script file that accepts a CSV file as input and produces a different CSV file that has “cleaned” data for use as the source for data collection.

You could write a stored procedure to clean a database table and produce a different “cleaned” table for use as the source for data collection.

Examples of Post-Processors

You could write a stored procedure to clean data in the Profile_staging table (in preparation for the job which copies the data to the Profile table).

You could write a batch file that sends e-mail to you (or a mailing list) upon completion of the data collection rule.

Pre-Requisites for Selecting a Processor to run with a Collection Rule

Before using a processor with data collection rule, the following are assumed:

- You have written an executable batch file, PowerShell script, VB script, Javascript file, or stored procedure that you want to run upon the data.
- If you are using a stored procedure, it must be intended for a table in the Courier database and reside with the Courier database.
- If you are using a PowerShell script, it must be saved on the local server.
- You have done some testing of the script or stored procedure.

Configuring the Tomcat Server to Avoid Logging of Sensitive Data

You can configure the Tomcat Server to avoid logging of any sensitive information in the tomcat7-stdout.xxxx.log files, while running the pre- or post-processors.

Take the following steps to configure the Tomcat Server:

1. Navigate to the tomcat bin folder. For example, "C:\TomCat\apache-tomcat-7.0.42\bin".
2. Run the tomcat7w.exe file to open the Apache Tomcat 7 Properties popup.
3. Click on the **Logging** tab.
4. From the **REDIRECT STDOUT** text box, remove the entry 'auto'.
5. Click **APPLY** and then click **OK**.
6. Stop the Tomcat Server using services.msc and remove all the tomcat7-stdout.xxxx.log files.
7. Re-start the Tomcat Server.

Note: This configuration can be removed if required, to create the tomcat7-stdout.xxxx.log files for debugging purpose.

Specifying a Pre-Processor

To operate upon source data before the data collection rules run, specify the file to run as a pre-processor.

1. In the Data Collection wizard navigation frame, click **SELECT PROCESSOR**.

Figure 19: Select Processor

The screenshot shows the 'Select Processor' wizard. On the left, a navigation pane lists steps: 'Select Source' (checked), 'Select Attributes' (checked), 'Filter Data' (checked), 'Select Processor' (active), and 'Schedule Rule' (checked). Below these is an 'Exit Wizard' button. The main content area is titled 'Select Processor'. It includes a 'Copy Data to Production*' checkbox which is checked. Below this is the 'Pre Processor' section, containing a 'Processor' dropdown menu currently showing 'Select processor', a 'Clear Processor' button, and an unchecked 'Continue On Failure' checkbox. At the bottom is a 'Parameters' section with 'Add' and 'Delete' buttons and a table with columns 'Name', 'Value', and 'Edit'. The table is empty, and a message at the bottom right states 'No items to display'.

2. From the **PROCESSOR** drop-down list, select the type of processor file. Depending upon your selection, the wizard refreshes to show related fields.
3. If you want the collection rule to continue upon an error or failure of the processor, click the **CONTINUE ON FAILURE** check box.

4. In the **FILE PATH** field, enter the path to the processor file. Hover over the field for the suggested format to use.
5. Note: If you are using a stored procedure that uses a schema other than dbo, you must specify that schema with the stored procedure name such as etl.sp_validity.
6. If the file or script accepts or requires parameters, click **+ADD** to add a parameter. The Add/Edit Parameter popup appears. The order in which you add parameters is the same order in which the value of parameter **VALUE** is passed to the processor file.
7. In the **NAME** field, you must enter a name for the parameter.
8. In the **VALUE** field, you may enter a value that is passed to the processor.
9. Click **SAVE**.
10. Repeat Steps 6 through 9 as needed for each parameter.
11. If you want to add a post-processor, go to that section. If you are finished adding a pre-processor, click **NEXT**. The Schedule Rule page appears.

Extending the Rule with a Post-Processor

To run the processor upon the data that has been collected, specify a post-processor as follows:

1. In the Data Collection wizard navigation frame, click **SELECT PROCESSOR**. Scroll down to the **POST PROCESSOR** section.

Figure 20: Post Processor section

Post Processor

Processor : i

Continue On ☒ Failure :

Parameters

	Name	Value	Edit
+ Add	- Delete		

No items to display

2. From the **PROCESSOR** drop-down list, select the type of processor file. Depending upon your selection, the wizard refreshes to show related fields.
3. If you want the collection rule to continue upon an error or failure of the processor, click the **CONTINUE ON FAILURE** check box.
4. In the **FILE PATH** field, enter the path to the processor file. Hover over the field for the suggested format to use.
5. Note: If you are using a stored procedure that uses a schema other than dbo, you must specify that schema with the stored procedure name such as etl.sp_validity.
6. If the file or script accepts or requires parameters, click **+ADD** to add a parameter. The Add/Edit Parameter popup appears.

7. In the **NAME** field, you must enter a name for the parameter.
8. In the **VALUE** field, you may enter a value that is passed to the processor.
9. Click **SAVE**.
10. Repeat Steps 6 through 9 as needed for each parameter.
11. If you are finished adding a post-processor, click **NEXT**. The Schedule Rule page appears.

Removing a Pre-Processor or Post-Processor

To remove the association between a data collection rule and a pre-processor (or a post-processor), do the following:

1. In the Data Collection wizard navigation frame, click **SELECT PROCESSOR**.
2. In the **PRE-PROCESSOR** (or **POST-PROCESSOR**) section, click **CLEAR PROCESSOR**.
3. Click **NEXT** to apply the change.

Scheduling the Data Collection Rule

After you have confirmed that the data collection rule is likely to work as you expect, you can schedule the rule to run. You can also run the data collection rule immediately by exiting the wizard and following the steps described in [“Running a Data Collection Rule”](#).

Figure 21: Schedule Rule Page

The screenshot shows the 'Schedule Rule' page of a data collection wizard. On the left is a sidebar with a list of steps: 'Select Source', 'Select Attributes', 'Filter Data', 'Select Processor', and 'Schedule Rule' (which is highlighted with a blue arrow). Below these steps is an 'Exit Wizard' button. The main content area is titled 'Schedule Rule' and contains the following settings:

- Rule Name:** rule1
- Is Enabled:** A checked checkbox.
- Start Date:** A date field showing 5/5/2014 with a calendar icon.
- Start Time:** A time field showing 9:08 AM with a clock icon.
- Recurrence Pattern:** Four radio button options: 'None' (selected), 'Daily', 'No End Date', and 'End by' (with a date field).

At the top right of the main area are 'Back' and 'Finish' buttons. At the bottom right are also 'Back' and 'Finish' buttons.

1. By default, the rule is enabled. If you determine that a rule is no longer needed, you can disable it by de-selecting the **IS ENABLED** check box.
2. **START DATE** field: Specify the date when the data collection rule will run.
3. **START TIME** field: Specify a time for the data collection rule to run. If the collection may require a significant portion of database resources, schedule the rule to begin when demand for resources is low.
4. If you want to run the rule every day beginning on the start date, select **DAILY** as the recurrence pattern.

5. **END BY** field: If you specified daily recurrence, you can specify an end date as the last date the rule will run.
6. Click **FINISH**. The wizard closes and the Data Collection Rules window appears.

Note: For additional scheduling options, use Microsoft SQL Server Management Studio to manage each data collection rule as a separate job.

Securing Data Collection

This section explains the steps required for securing communication between the collector and data source system from where the data is collected. It also describes the additional steps required for Collector for Microsoft Active Directory and Collector for Oracle Sun Directory LDAP.

You must either enable Windows Authentication or Force Protocol Encryption in order to securely connect to Microsoft SQL Server from the collectors. To enable Windows authentication, refer to the section, [“Enabling Windows Authentication for Data Collection” on page 39](#). Refer to the *Implementation Guide* for information on enabling the Force Protocol Encryption.

Courion strongly recommends that you use Force Protocol Encryption to ensure that not only the login credentials but the data communication is also encrypted using the server certificate installed on the SQL Server.

Configuration required for Collector for Microsoft Active Directory and Collector for Oracle Sun Directory LDAP

This section describes the configuration required for the Collector for Microsoft Active Directory and Collector for Oracle Sun Directory LDAP to secure data collection. The secure communication is established using Lightweight Directory Access Protocol (LDAP) over the Secure Sockets Layer (SSL) protocol.

After installing the Collector for Microsoft Active Directory and Collector for Oracle Sun Directory LDAP, create a Keystore. The Keystore is a repository of certificates that the collectors use to communicate securely with the data source systems.

Creating a Keystore

To create a Keystore, follow these steps:

1. Log in to the Courion server as a local administrator where the Apache Tomcat service is installed.
2. Create a Keystore using the Java Keytool. The Java Keytool (keytool.exe) resides in the Java Home\bin folder. To create a Keystore, follow these steps:
 - a. Export a public key certificate (.DER), which is used to configure data source system with SSL protocol. Contact the system administrator of your data source system to get the public key certificate.
 - b. Launch the command prompt with "Run as Administrator," and run the following command:


```
<Java HOME\bin>keytool -import -trustcacerts -file
<Exported public key certificate path and filename> -
keystore <local file path>\CourionKeystore.jks
```
 - c. Upon running the command, a prompt appears for creating a password. Note down the file name, CourionKeystore.jks, and the password you created. Use these values later to configure the additional fields for the collectors in a data collection rule.

Enabling Windows Authentication for Data Collection

This section describes the steps required to enable Windows authentication for data collection.

If SQL authentication is used to connect to Microsoft SQL Server from an application, the data (including the user password) is transmitted in TDS packets, which is considered to be less secure. By enabling Windows authentication, you are ensuring that the communication is secured using the NTLM protocol.

Configuring the CustomerConnStrings.config File

1. Log in as a local administrator on the Courion server.
2. Navigate to the [CoreSecurityInstallPath]\Courion Corporation\CourionARMS folder and open the CustomerConnStrings.config file in a text editor.
3. Create a Windows user account that is an Active Directory domain user and a local administrator on the Courion server. The newly created Windows user account must meet the following requirements:
 - "It must be a member to the same domain as the Courion server.
 - It must have the same privileges on the Courion database as an SQL user account mentioned in the DataCollectionEntities connection string.
4. Change the **DataCollectionEntities** connection string to use Windows authentication instead of SQL authentication.

The following is an example of Windows authentication:

```
<add name="DataCollectionEntities"
connectionString="metadata=res://*/
DataCollectionModel.csdl|res://*/
DataCollectionModel.ssdl|res://*/
DataCollectionModel.msl;provider=System.Data.SqlClient;
provider connection string=&quot;
Data Source=$$YOURSERVERHERE$$;
Initial Catalog=$$YOURDBHERE$$;
Integrated Security=true;multipleactiveresultsets=True;
App=EntityFramework&quot;;"
providerName="System.Data.EntityClient" />
```

5. Change the **dbConnectionString** connection string to use Windows authentication instead of SQL authentication.

The following is an example of Windows authentication:

```
<add name="dbConnectionString" connectionString=
"Data Source=$$YOURSERVERHERE$$;
Initial Catalog=$$YOURDBHERE$$;Integrated Security=true"
providerName="System.Data.SqlClient" />
```

Note: Replace \$\$YOURSERVERHERE\$\$ with the name of the database server. Replace \$\$YOURDBHERE\$\$ with the name of the Courion database.

The above configuration uses integrated authentication to connect to the Courion database for data collection.

Running the Tomcat Service under a Windows User Account

To ensure that the collectors use integrated authentication to communicate with the destination Courion database, configure Tomcat service under the Windows user account that is specified for the DataCollectionEntities connection string. This is the same Windows user account that was created in the section, [“Configuring the CustomerConnStrings.config File” on page 39](#).

1. Open the Windows Services Console.
2. In the **DETAILS** pane, right-click the **APACHE TOMCAT SERVICE**, and then click **PROPERTIES**.
3. Click on the **LOG ON** tab and select the **THIS ACCOUNT** option.
4. Click on the **BROWSE** button to select the same Windows account user, which is specified for the DataCollectionEntities connection string. Click **OK** to finish.
5. In the **PASSWORD** and **CONFIRM PASSWORD** fields, specify the password for the configured Windows user account, and then click **OK**.
6. A warning is displayed asking to restart the Tomcat service. Restart the service.

Changing the Identity in Application Pools

To ensure that data collection uses integrated authentication to communicate with the destination Courion database, configure CoreARMS Application Pool with the same Windows user account that is specified for the DataCollectionEntities connection string.

1. Open IIS Manager.
2. In the **CONNECTIONS** pane, expand the server node and click **APPLICATION POOLS**.
3. On the Application Pools page, select the **COREARMS** application pool and then click **ADVANCED SETTINGS** from the **ACTIONS** pane.
4. For the **IDENTITY** property, click the ellipsis (...) button to open the **APPLICATION POOL IDENTITY** dialog box.
5. To use a custom identity, select the **CUSTOM ACCOUNT** radio button and click **SET...** to open the **SET CREDENTIALS** dialog box. Provide the value for the **USER NAME** field with the same Windows user account (DomainName\username) mentioned in the DataCollectionEntities connection string. Enter the password for the Windows user account in the **PASSWORD** text box and retype it in the **CONFIRM PASSWORD** text box. Then click **OK**.
6. Click **OK** to close the **APPLICATION POOL IDENTITY** dialog box.
7. Recycle the Application Pool or restart IIS.

Copy NTLMAuth.dll to [JavaHOME]\Bin Folder

Download the NTLMAuth.dll file from the following link (64bit or 32bit as per your system) and copy it to the [JavaHome]\bin folder.

<http://sourceforge.net/projects/jtds/files/jtds/1.3.1/jtds-1.3.1-dist.zip/download>

Moving the Collector Files to Tomcat Lib Folder

To move the collector files to the Tomcat Lib folder, perform the following steps:

1. Stop the Apache Tomcat service.
2. Move all the files from [Tomcat-installation-folder]\webapps\genericsql_0.1\WEB-INF\lib folder to [Tomcat-installation-folder]\lib folder, **except genericsql_0_1.jar, processor_0_1.jar, systemRoutines.jar, userRoutines.jar** files.
3. Move all the files from [Tomcat-installation-folder]\webapps\activedirectory_0.1\WEB-INF\lib folder to [Tomcat-installation-folder]\lib folder, **except activedirectory_0_1.jar, activedirectory_collector_0_1.jar, processor_0_1.jar, systemRoutines.jar, userRoutines.jar** files.
4. Move all the files from [Tomcat-installation-folder]\webapps\epic_0.1\WEB-INF\lib folder to [Tomcat-installation-folder]\lib folder, **except epic_0_1.jar, processor_0_1.jar, systemRoutines.jar, userRoutines.jar** files.
5. Move all the files from [Tomcat-installation-folder]\webapps\genericcsv_0.1\WEB-INF\lib folder to [Tomcat-installation-folder]\lib folder, **except genericcsv_0_1.jar, processor_0_1.jar, systemRoutines.jar, userRoutines.jar** files.
6. Move all the files from [Tomcat-installation-folder]\webapps\sundirectoryldap_0.1\WEB-INF\lib folder to [Tomcat-installation-folder]\lib folder, **except sundirectoryldap_0_1.jar, processor_0_1.jar, systemRoutines.jar, userRoutines.jar** files.

Note: Always overwrite files while moving them from one folder to another.

7. Start the Apache Tomcat service.

Notes:

- If you uninstall a collector from the Manage Content page on the Courion Portal and then reinstall it, the installation process copies all the collector files under tomcat<version>\webapps folder. You must follow the steps again to make Windows authentication work.
- If you upgrade the Courion Access Assurance Suite with a higher version in the future, you must install the collectors again and move and overwrite the new files to the [Tomcat-installation-folder]\lib folder.

Enabling Windows Authentication for SQL and EPIC Collectors for Connecting to the Source Database Server

SQL and EPIC collectors require the SQL connection credentials on the Select Source page of the Data Collection wizard. If you select SQL authentication, the SQL user password is transmitted in TDS packets, which is considered less secure. Alternatively, choosing Windows authentication ensures that the communication is secured using NTLM protocol.

To use Windows Authentication for SQL and EPIC collectors to connect to a data source system (Microsoft SQL Server), enter the Windows username and password in the **USER NAME** and **PASSWORD** fields respectively. Also, specify the domain name such as "domain=<domain name>" in the **ADDITIONAL PARAMETER** field on the Select Source page as shown in [Figure 22](#).

Figure 22: Select Source Page

Select Source

Data Collection Options

- ☒ Accounts
 - ☐ with Assigned Entitlements
- ☐ Entitlement Catalog
- ☐ Profiles

Rule Name * ent_SQL

Rule Description

Source System * InitProfile

Collector * Generic SQL

Connection String* Data Source = \$\$ServerName\$\$; Initial Catalog = \$\$DatabaseName\$\$; Port = 1433;

User Name* MyWindowsUserName

Password*

Table Name* dbo.MySourceTableName

Additional Parameters domain=MyDomain.com|

Notes

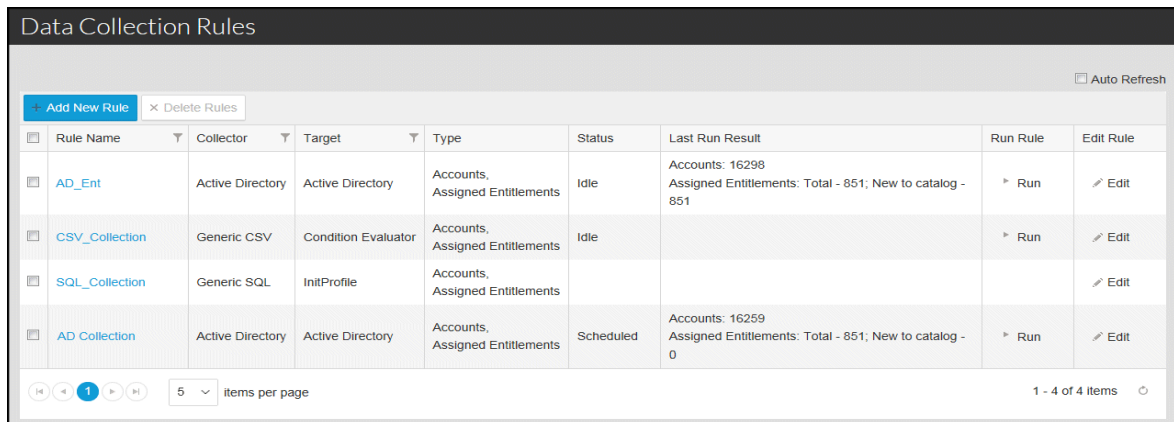
- If you update the Keystore Path or the Keystore Password in the Select Source page of the Data Collection wizard, you must restart the Apache Tomcat service for the changes to take effect.
- The Accounts and Assigned Entitlement option for Collector for Sun Directory LDAP collects only accounts, but the assigned entitlements are not collected. The Entitlement Mapping for the Sun Directory LDAP target is affected when the assigned entitlements are not collected.

Running a Data Collection Rule

Although the Data Collection Rule wizard allows you to schedule when each rule should run, you can also run a data collection rule immediately to collect and to save the data to the Identity Mapping database.

1. From the Mega Menu in the Access Assurance Portal, select **DATA COLLECTION**. The Data Collection Rules window appears.

Figure 23: Data Collection Rules window



The screenshot shows the 'Data Collection Rules' window. It features a table with columns: Rule Name, Collector, Target, Type, Status, Last Run Result, Run Rule, and Edit Rule. There are four rules listed: AD_Ent, CSV_Collection, SQL_Collection, and AD Collection. The AD Collection rule is highlighted in blue and has a status of 'Scheduled'. At the bottom, there are navigation buttons and a page indicator showing '1 - 4 of 4 items'.

Rule Name	Collector	Target	Type	Status	Last Run Result	Run Rule	Edit Rule
AD_Ent	Active Directory	Active Directory	Accounts, Assigned Entitlements	Idle	Accounts: 16298 Assigned Entitlements: Total - 851; New to catalog - 851	Run	Edit
CSV_Collection	Generic CSV	Condition Evaluator	Accounts, Assigned Entitlements	Idle		Run	Edit
SQL_Collection	Generic SQL	InitProfile	Accounts, Assigned Entitlements				Edit
AD Collection	Active Directory	Active Directory	Accounts, Assigned Entitlements	Scheduled	Accounts: 16259 Assigned Entitlements: Total - 851; New to catalog - 0	Run	Edit

2. Find the data collection rule that you want to run. (If you have created more than five data collection rules, you may have to use the page forward button to go to another page of data collection rules.) Also check the **STATUS** column to make sure that the rule is not currently running.
3. Click the **RUN** button that is in the same row as the rule. The Status will change to Running. (To ensure that the Status column is updated, make sure that the **AUTO-REFRESH** check box is checked.)

To view the results, wait for the status of the rule to be Idle and then follow the guidelines in [“Viewing Data Collection Results”](#).

Note: If you are using Access Insight and you plan to use the ETL jobs to copy data from the Courion database to the CMasterData database, make sure that the dates included in the data are in a format accepted by the datetime data type of the Microsoft SQL Server; otherwise the data from the dbo.Account_Staging table will not be transferred to the CMasterData database. For example, if you have collected account records containing the ExpiredOn date, you must make sure that all dates conform.

Running Multiple Data Collection Rules

At a given time, only two data collection rules can be running simultaneously. If a third data collection rule is run manually or is scheduled to start while two other rules are running, the third data collection rule will remain in Queued status. When one of the other rules finishes running, the status of the third data collection rule immediately changes from Queued to Running.

Viewing Data Collection Results

After you have successfully created and run a data collection rule, the rule name is a hyperlink to the data that was collected during the last successful run.

To view the data, click the rule name as shown in the Data Collection Rules window in [Figure 24](#).

Figure 24: Data Collection Rules

<input type="checkbox"/>	Rule Name	Collector	Target	Type	Status	Last Run Result	Run Rule	Edit Rule
<input type="checkbox"/>	AD_Ent	Active Directory	Active Directory	Accounts, Assigned Entitlements	Idle	Accounts: 16298 Assigned Entitlements: Total - 851; New to catalog - 851	▶ Run	✎ Edit
<input type="checkbox"/>	CSV_Collection	Generic CSV	Condition Evaluator	Accounts, Assigned Entitlements	Idle		▶ Run	✎ Edit
<input type="checkbox"/>	SQL_Collection	Generic SQL	InitProfile	Accounts, Assigned Entitlements				✎ Edit
<input type="checkbox"/>	AD_Collection	Active Directory	Active Directory	Accounts, Assigned Entitlements	Scheduled	Accounts: 16259 Assigned Entitlements: Total - 851; New to catalog - 0	▶ Run	✎ Edit

1 - 4 of 4 items

The Data Feed window appears as shown in [Figure 25](#).

Figure 25: Data Feed Window

EmployeeID	Username	Title	FullName	FirstName	MiddleName	LastName	Initials
Employee0	UserName0			FirstName0		LastName0	Initials0
Employee1	UserName1			FirstName1		LastName1	Initials1
Employee2	UserName2			FirstName2		LastName2	Initials2
Employee3	UserName3			FirstName3		LastName3	Initials3
Employee4	UserName4			FirstName4		LastName4	Initials4
Employee5	UserName5			FirstName5		LastName5	Initials5
Employee6	UserName6			FirstName6		LastName6	Initials6
Employee7	UserName7			FirstName7		LastName7	Initials7
Employee8	UserName8			FirstName8		LastName8	Initials8
Employee9	UserName9			FirstName9		LastName9	Initials9

1 - 10 of 10 items

If you determine that you need to modify an attribute mapping or modify a filter, click **BACK**. The Data Collection window appears showing all data collection rules. Click **EDIT** for the rule you want to modify.

Sort Options

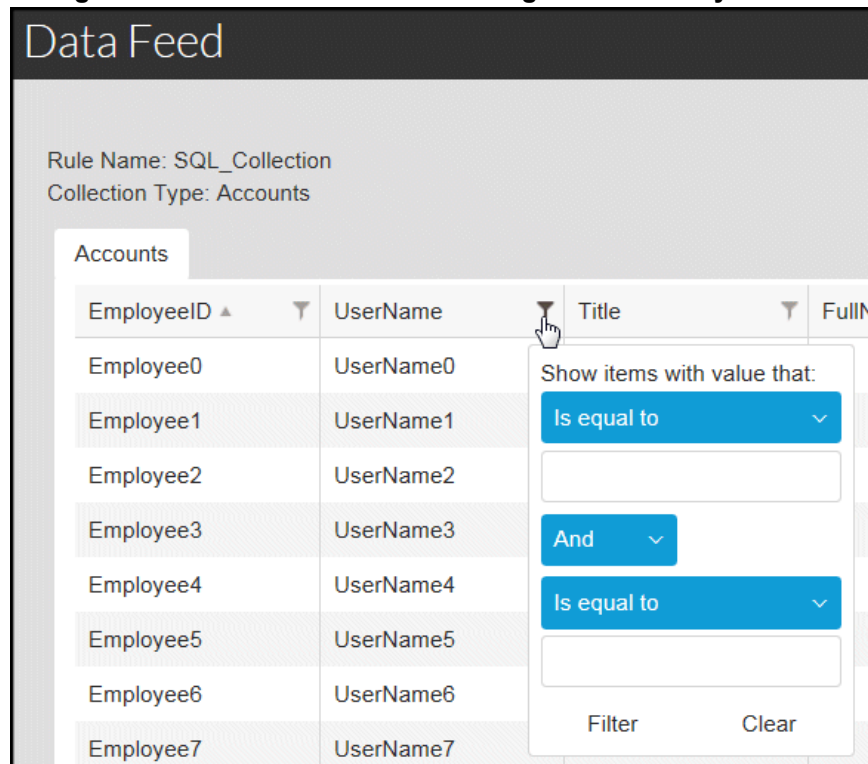
Click on any column heading to re-sort the entire table with that column sorted in ascending order, alphabetically or numerically.

If a column is already sorted in ascending order (as shown with an up arrow), click on that column heading to sort the entire table with that column sorted in descending order.

Filtering Options

A filter icon appears in each column header. To create a query with which to filter data by that column, click the filter icon to display a column query filter as shown in [Figure 26](#).

Figure 26: Data Feed Window showing Column Query Filter



Filtering a Column using Two Criteria

For any single column, you can filter the data using one or two criteria. When you specify two criteria, the logical operator can be 'AND' or 'OR'.

Filtering upon Multiple Columns

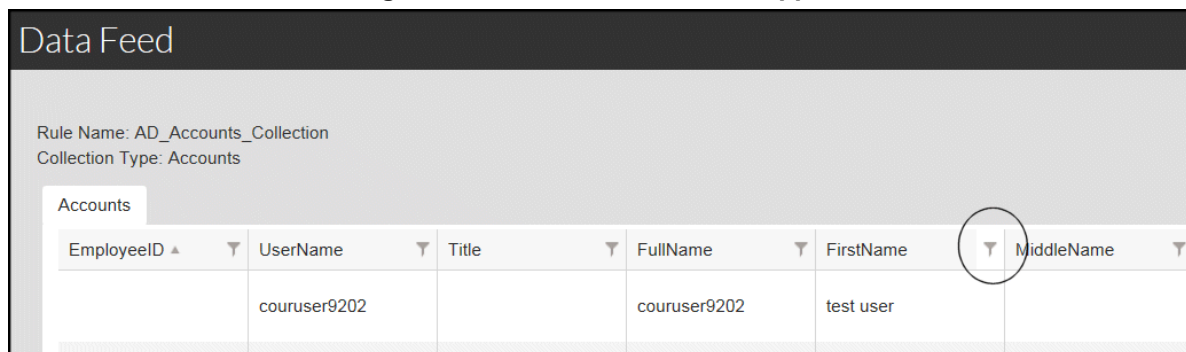
You can filter upon multiple columns. However, each filter is cumulative and therefore includes more and more records. For example, you might specify a filter for the UserName column, the State column, and the Department column. This could be represented as follows:

Show data if (data matches UserName filter criteria) AND (data matches State filter criteria) AND (data matches Department filter criteria).

Recognizing when Filters are Applied

When a filter is applied to the data, the filter icon has a slightly different background color as shown in [Figure 27](#).

Figure 27: Data Feed with Filter Applied




The screenshot shows a 'Data Feed' window with a dark header. Below the header, it displays 'Rule Name: AD_Accounts_Collection' and 'Collection Type: Accounts'. A tab labeled 'Accounts' is selected. Below the tab is a table with the following columns: EmployeeID, Username, Title, FullName, FirstName, and MiddleName. Each column has a small downward-pointing triangle icon to its right, indicating a filter. The filter icon for the 'MiddleName' column is circled. The table contains one row of data: EmployeeID is empty, Username is 'couruser9202', Title is empty, FullName is 'couruser9202', FirstName is 'test user', and MiddleName is empty.

EmployeeID	Username	Title	FullName	FirstName	MiddleName
	couruser9202		couruser9202	test user	

Editing a Data Collection Rule

After you have created a data collection rule, you may need to modify some aspects of it. For example, you may want to schedule it to run on a daily interval or you may want to filter out data based upon additional criteria.

1. From the Mega Menu in the Access Assurance Portal, select **DATA COLLECTION**. The Data Collection Rules window appears.
2. In the row which contains the rule you want to modify, click **EDIT**. The Select Source page appears.
3. To ensure that the wizard retrieves the latest changes to the configured source systems, click the Refresh button  .

Note: You can 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:

- d. In Internet Information Services Manager, right-click the DefaultAppPool service.
 - e. In the context menu, select Restart.
4. Using left frame navigation, you can go to the page where the rule needs to be modified.
 - To edit the date or time that the rule runs, click Schedule Rule.
 - To add or change a data filter, click Filter Data.
 - To edit how attributes are mapped, click Select Attributes.
 - To add or remove a pre- or post-processor, click Select Processor.

Note: If the data source requires a password, you will need to enter a password before navigating away from the Select Source page.

5. Edit the rule as needed.
6. Click **EXIT WIZARD**.
7. If you are ready to apply your changes, click **SAVE AND EXIT**. If you realize that you do not want to apply your changes, click **EXIT**.

Disabling a Data Collection Rule

If you have a data collection rule that may be needed on an infrequent basis, you can disable the rule instead of deleting it.

1. From the Mega Menu in the Access Assurance Portal, select **DATA COLLECTION**. The Data Collection Rules window appears.
2. In the row which contains the rule you want to disable, click **EDIT**. The Select Source page appears.
3. Using left frame navigation, go to the Schedule Rule page.

Figure 28: Schedule Rule Page

Rule Name: rule1

Back Finish

Select Source ✓

Select Attributes ✓

Filter Data ✓

Select Processor ✓

Schedule Rule >

Exit Wizard

Schedule Rule

Is Enabled : ☒

Start Date : 5/5/2014

Start Time : 9:08 AM

Recurrence Pattern

☒ None ☐ Daily ☐ No End Date ☐ End by

Back Finish

4. Click the **IS ENABLED** check box so that it is unchecked.
5. Click **FINISH** to apply this change. The data collection rule will be available for later use.

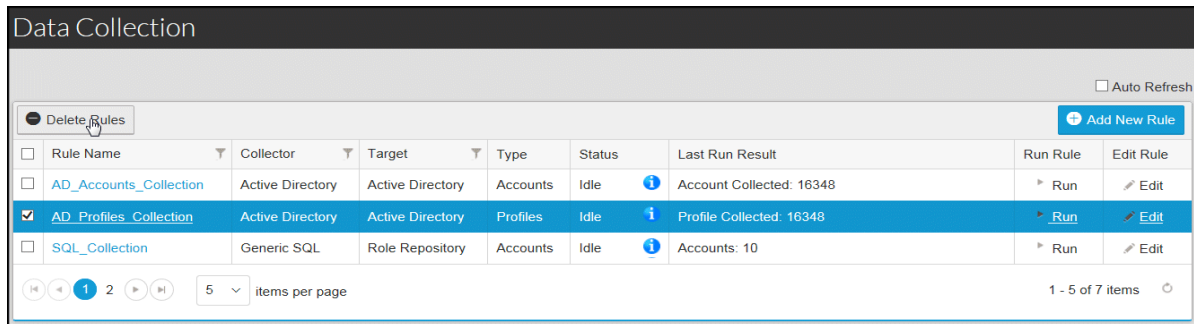
Deleting a Data Collection Rule

If a data collection rule no longer applies to your environment and you no longer need the data associated with the rule, you may want to delete it. When you delete a data collection rule, the data in the staging tables collected by that rule is also deleted.

To delete a data collection rule, do the following:

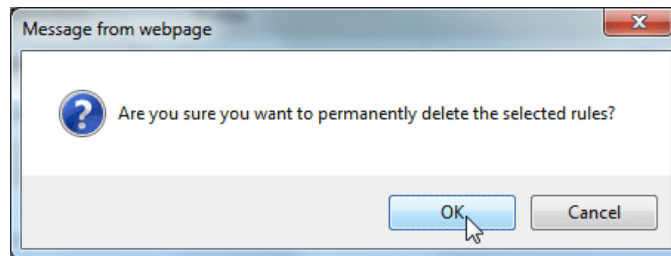
1. Click the check box to the left of the name of the rule you want to delete.
2. Click **DELETE RULES** as shown in [Figure 29](#).

Figure 29: Delete Rules Button



A dialog box appears to confirm whether or not to delete the selected rule(s) as shown in [Figure 30](#).

Figure 30: Confirmation of Deleting Data Collection Rule



3. Click **OK** to delete the rule.

Uninstalling a Data Collector

If you no longer plan to use a data collector, you can uninstall it as long as there are no data collection rules associated with it. To uninstall (or remove) a collector, do the following:

1. Restart the Apache Tomcat service to clear the cache of .jar files that would prevent collector removal.
2. In the Manage Content window, click one or more check boxes next to the name of the collector(s) you want to uninstall.
3. Click **UNINSTALL**. A confirmation dialog box appears.

4. Click **OK**. If there are no data collection rules associated with the collector, another dialog box confirms the name(s) of the collector(s) which will be removed. The removal should take a few minutes. The content state will change to Queued and then change to Uninstalled.

If one or more data collection rules is associated with a collector that you have marked for removal, a dialog box similar to [Figure 31](#) appears.

Figure 31: Collector in Use by Data Collection Rule



Before you can delete a data collector that is associated with one or more data collection rules, you must delete those data collection rules.

Chapter 4: Setting Up Data Feeds

This chapter describes how to configure data feeds using the Identity Mapping user interface.

A data feed is the structured user account information that has been collected from a system or application, and saved in data feed tables in the database created using the Courion.sql file. It contains user account names and attributes that are collected from target systems. The Identity Mapping process uses information from the data feed to map accounts to profiles.

Before you start configuring data feeds, set up data feed tables that may contain data from one or more target systems. Populate the data feed tables for data feeds by using Courion Collectors or by manually importing data. Contact Courion to learn more about the Collectors that are available.

Note: Any data feed tables you create need to reside on the same database server. The data feed table should contain username information to define the user identifier field in the data feed configuration.

Note: The Active Directory credentials (such as abc.dom\jsmith) used by the Courion Identity Mapping Service need to have access to the database and data feed tables.

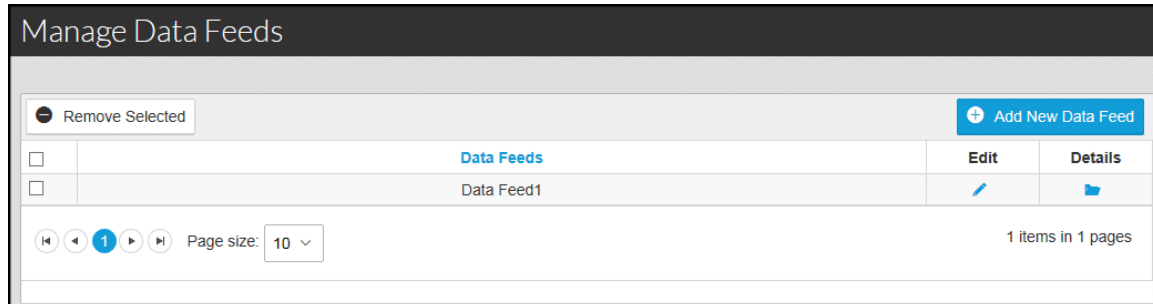
This chapter includes the following sections:

- [*“Adding Data Feeds” on page 53*](#)
- [*“Viewing Data Feed Details” on page 55*](#)

Once you have identified the data feed tables, you can start configuring the data feeds:

While logged into the Access Assurance Portal as a member of the IDM Admins dynamic community, you can click the Main Menu and select **DATA FEEDS**. The **MANAGE DATA FEEDS** window appears as in [Figure 31](#).

Figure 31: Manage Data Feed



From the **MANAGE DATA FEEDS** window, you can:

- Select **ADD NEW DATA FEED** to set up data feeds through the **ADD DATA FEEDS** window.
- Check the Select All check box in the header row to select all the data feeds, or check an individual check box to select a specific data feed.
- Select **REMOVE SELECTED** after you have checked the Select All or individual check boxes to remove data feeds.
- Click the Edit icon to edit an existing data feed.
- Click the Details icon to view the user account data stored in the data feed.

Adding Data Feeds

To add data feeds, select **ADD NEW DATA FEED**. The **ADD DATA FEEDS** window appears. The **DATA SOURCE** panel is shown in [Figure 32](#).

Figure 32: Add New Data Feed

The screenshot shows a window titled "Add/Edit Data Feed". Inside, there's a section titled "Data Source" with a blue information icon. Below this, there are four fields, each marked with an asterisk to indicate they are required:

- * Data Feed Name:** A text input field.
- * Database:** A drop-down menu currently showing "- Select a database -v".
- * Database Table:** A drop-down menu.
- * User Identifier:** A drop-down menu.

1. Configure the following fields in the **DATA SOURCE** panel:

DATA FEED NAME: Enter a name to uniquely identify the data feed.

DATABASE: Select the database you want from the drop-down list. The list displays all the databases available on the server.

DATABASE TABLE: Select the data feed table from the drop-down list. The list displays all the tables associated with the database you selected.

USER IDENTIFIER: Select the field that contains the unique user account identifier for the target systems in this data feed.

The screenshot shows a panel titled "Disabled Account Criteria" with a blue information icon. Below the title, it says "Account Disabled: (Conditions that determine when account is disabled)". There is a text prompt "Enter your custom query here:" followed by a large text input area. At the bottom left of the panel is a blue button labeled "Check Syntax".

2. If necessary, scroll to the **DISABLED ACCOUNT CRITERIA** panel. Enter the SQL WHERE clause which identifies whether an account is disabled, and click **CHECK SYNTAX**.

The **CHECK SYNTAX** feature checks for errors in the SQL WHERE clause you entered, including the SQL syntax, the alias, or the field name.

Note: Prefix all data feed columns with S., such as S.FirstName = "John". The S in the syntax is an alias to the configured data feed table.

When the Identity Mapping process executes, it uses the SQL WHERE clause you entered to identify disabled accounts. For example, S.Enabled=0 identifies

records in the selected data feed table which have an Enabled column with a value of 0 as disabled when mapping accounts.

Note: For information about how to write SQL statements, refer to Microsoft SQL Server documentation.

Data Feed Configuration

Set Grid Behavior

Set Number of Rows Per Page

10

☒ Enable Hiding
☒ Enable Sorting
☒ Enable Filtering

☒ Enable Resizing

Set Column Behavior

Refresh Columns

Column	Label	Order	Width	Visible	Movable	Detail View
No records to display.						

Save

Cancel

- If necessary, scroll to the **DATA FEED CONFIGURATION** panel. You can configure the behavior of the grid and fields displayed on the **DATA FEED DETAILS** window (which is described in [“Viewing Data Feed Details” on page 55.](#))

Enable the following options under **SET GRID BEHAVIOR**:

- **SET NUMBER OF ROWS PER PAGE:** Specify the number of records to display.
- **ENABLE HIDING:** Check to enable the hiding of columns.
- **ENABLE RESIZING:** Check to enable the resizing of columns.
- **ENABLE SORTING:** Check to enable sorting of data in each column. You can sort the information by clicking the individual column. The sorting order may be alphabetical or numerical, ascending or descending, based on the data type of the field.
- **ENABLE FILTERING:** Check to enable the filtering of information by column. If enabled, a filter text box appears in each column.

Enable the following options under **SET COLUMN BEHAVIOR**:

- **COLUMN:** Displays fields from the data feed table.
 - **LABEL:** Enter a label for the field. This label appears on the **DATA FEED DETAILS** window.
 - **ORDER:** Select the order in which you want to display the columns.
 - **WIDTH:** Specify the column width in em units. For measurement, 1 em = 16 pixels.
 - **VISIBLE:** Check to show the field; uncheck to hide it.
 - **MOVABLE:** Check to enable moving of columns.
 - **DETAIL VIEW:** Check to display fields in a collapsible **DETAILS** window. An icon appears in the first column that enables you to enlarge or collapse the window and view or hide the fields, respectively.
- Click **SAVE** when done or **CANCEL** to exit without saving changes.

Viewing Data Feed Details


The **DATA FEED DETAILS** window displays details for the data feed you select. Click the Details icon  to view the window as in [Figure 33](#).

Figure 33: Data Feed Details

Data Feed Details: Data Feed1

Data Feeds

[Back to Data Feeds](#)

Configure Grid

AccountStagingId	EmployeeID	UserName	Title	FullName	FirstName	MiddleName	LastName	Initials	JobTitle	Department
114361	ITC42_2000	ITC42_2000		ITC42_2000	ITC42_2000					
114362	40000	asdf123		asdf123	ddidd		asdf123		03/24/2010	
114363	sameer123	sameer123		sameer			dhek			
114364		tyou1		tyou1	QALead		ADTest			
114365		slee		Stan Lee						
114368		spuser		Super Portal User	Super		User			
114369		krblgt								
114370		nbSALES119		nb - SALES119	SALES119		SALES119			

A filter text box appears in each column and you can enter the text to filter on or select it from the drop-down list, when **ENABLE FILTERING** is checked through **CONFIGURE GRID**. Click **CONFIGURE GRID** to customize the grid display and the options available, such as enabling filtering or sorting of information. For additional details, refer to the **DATA FEED CONFIGURATION** panel described in [“Adding Data Feeds” on page 53](#).

Right-clicking on any column heading shows a menu with the options you enabled through **CONFIGURE GRID**. One or more of the following options appear in the right-click menu:

- **SORT ASCENDING** - Sorts information in ascending order, alphabetically or numerically, when **ENABLE SORTING** is checked.
- **SORT DESCENDING** - Sorts information in descending order, alphabetically or numerically, when **ENABLE SORTING** is checked.
- **CLEAR SORTING** - Clears any sorting that was applied to a column.
- **BEST FIT** - Adjusts the column width to display the most information.
- **COLUMNS** - Displays a list of the columns when **ENABLE HIDING** is checked. Check to show a column or uncheck to hide it.

Chapter 5: Creating Identity Mapping Rules

This chapter describes how to create and configure identity mapping rules to map user accounts to user profiles. The parameters defined in the rules inform the Identity Mapping process about:

- The data feed to which the identity mapping rule applies.
- The criteria to apply on the data feed for Identity Mapping.

Note: Any identity mapping rule you create applies to a single data feed. However, one data feed may have several mapping rules applied to it.

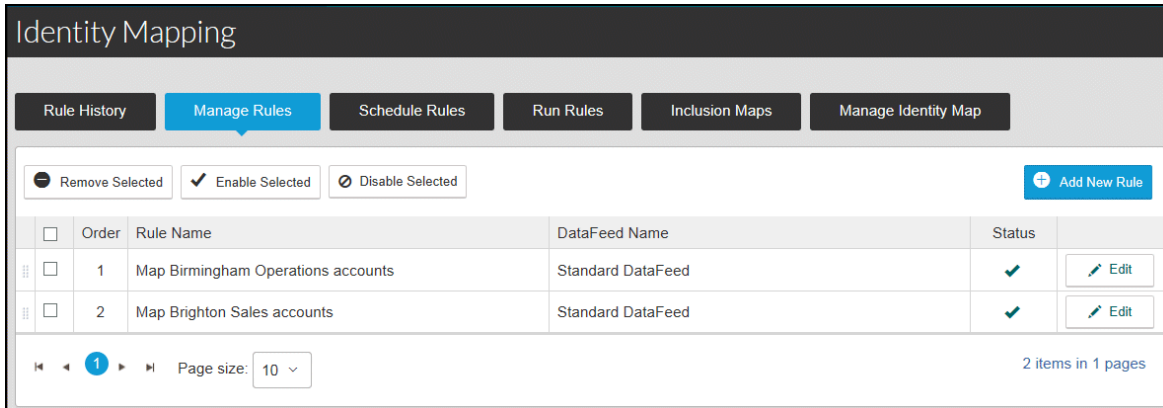
For information about data feeds, refer to the chapter [*“Setting Up Data Feeds” on page 51*](#).

Managing Identity Mapping Rules


To view the identity mapping rules that have been created, you can do the following:

1. Log into the Access Assurance Portal as the data mapping administrator.
2. Click the Main Menu and select **IDENTITY MAPPING**. The **MANAGE RULES** window appears. [Figure 34](#) shows an example in which two identity mapping rules are enabled.

Figure 34: Manage Rules



From the **MANAGE RULES** window, you can:

- Click the Edit icon  to edit an existing mapping rule.
- Select **REMOVE SELECTED** after you have checked the Select All or individual check boxes to remove mapping rules.
- Select **ENABLE SELECTED** to enable mapping rules after you have checked the Select All or individual check boxes.

The Status icon changes to  for enabled mapping rules.

- Select **DISABLE SELECTED** to disable mapping rules after you have checked the Select All or individual check boxes.

The Status icon changes to  for disabled mapping rules.

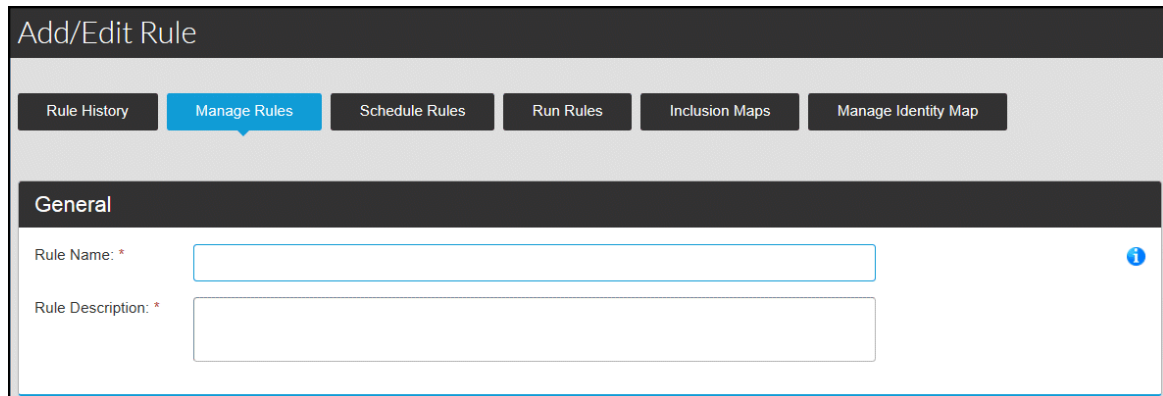
Note: You can click the **STATUS** icon to toggle the enabled/disabled status for an individual rule.

- Right-clicking on any column heading shows a menu with the following options:
 - **BEST FIT** - Adjusts the column width to display the most information.
 - **COLUMNS** - Displays a list of the columns when **ENABLE HIDING** is checked. Check to show a column or uncheck to hide it.

Creating an Identity Mapping Rule

1. To create an identity mapping rule, from the **MANAGE RULES** window, select **ADD NEW RULE**. The **ADD/EDIT RULE** window contains a section in which you name a new mapping rule, another section for configuring how the rule applies to a target, and another section to specify advanced settings.

Figure 35: Add New Rule



The screenshot shows the 'Add/Edit Rule' window. At the top, there's a dark header bar with the title 'Add/Edit Rule'. Below the header, there's a navigation bar with several tabs: 'Rule History', 'Manage Rules' (which is highlighted in blue), 'Schedule Rules', 'Run Rules', 'Inclusion Maps', and 'Manage Identity Map'. Below the navigation bar, there's a section titled 'General' with a dark header. Under the 'General' section, there are two input fields: 'Rule Name: *' and 'Rule Description: *'. The 'Rule Name' field is a single-line text box, and the 'Rule Description' field is a multi-line text box. To the right of the 'Rule Name' field, there is a small blue information icon (i).

2. In the **GENERAL** section, configure the following fields:
RULE NAME: Enter a name to uniquely identify the mapping rule.
RULE DESCRIPTION: Describe the function of the mapping rule. For example, "The rule maps accounts with Active Directory targets."
3. In the **CONFIGURE RULE** section, configure the data feed and mapping criteria, as shown in [Figure 36](#).

Figure 36: Configure Rule

- **USE STANDARD DATAFEED:** If you have configured data collection rules, select this check box.
- **DATA FEED:** If you are using your own ETL process to supply Identity Map data, select a data feed from the drop-down list. This drop-down list is populated with the data feeds you added on the **ADD DATA FEEDS WINDOW**. For additional information, refer to [“Adding Data Feeds” on page 53](#).

RULE APPLICATION: Select one of the following options to specify how the mapping rule applies to the data feed:

- **SPECIFY THE TARGET ID APPLIED TO ACCOUNTS DISCOVERED:** Select this if you want to specify a target ID for mapped accounts. This option ignores any target ID information in the data feed. (This option does not apply to Standard data feeds.)

TARGET ID: Specify the target ID, such as abc.dom.

A target ID uniquely identifies a target system. The target ID is stored in the IdentityMap table when accounts are mapped to user profiles. Other Access Assurance Suite™ applications, such as the AccountCourier® user provisioning solution, the ComplianceCourier™ policy verification solution, and the PasswordCourier® password provisioning solution use this same target ID in their configurations.

- **RULE APPLIES TO A SPECIFIC TARGET IN THE DATA FEED:** Select this if you want to restrict the rule to a specific target ID from the data feed table.

TARGET ID COLUMN: Select the column from the data feed that contains target IDs.

TARGET ID: Specify the target ID, such as AD.dom. If the target ID you specify is not available in the data feed column, the rule does not map any accounts from the data feed.

- **RULE APPLIES TO ALL TARGETS IN THE DATA FEED:** Select this if you want to specify the column in the data feed that contains the target IDs.

TARGET ID COLUMN: Select the column from the data feed that contains target IDs.

MATCH: Select one of the following options to specify how to match accounts to profiles:

- **MATCH TO CRITERIA IN THE PROFILE TABLE:** Matches accounts to profiles in the Profile table based on the condition you specify in the **PROFILE TO ACCOUNT QUERY** text box.

For example, if you specify `S.accountname = P.EmployeeNo`, the account from the data feed is matched to the employee number in the Profile table. The `P` in the syntax is an alias to the Profile table. The `S` in the syntax is an alias to the configured data feed table.

- **MATCH USERNAME TO ANOTHER TARGET:** Select this option to match an account by using an existing mapping from another target. Specify the target ID in the **TARGET ID** text box, such as `AD2.dom`.

This option is useful when you have several targets of a similar type, such as Active Directory, and you want to match the account to an existing mapping of another Active Directory target.

For example, if there is an account (`jsmithC` with `AD1.dom` as the target ID) that needs to be matched, then the Identity Mapping process uses an existing mapping, such as (`jsmith`, `AD2.dom`) in the IdentityMap table to map (`jsmith`, `AD1.dom`) to a profile.

If the accounts are successfully mapped to profiles, the information is written to the IdentityMap table that includes the triplet of account ID, target ID, and profile ID.

An account ID uniquely identifies a user account. A profile ID uniquely identifies a user profile.

Note: If an account is provisioned by the AccountCourier® user provisioning solution for a user, this information is written to the IdentityMap table. Similarly, if an account is deleted by the AccountCourier® user provisioning solution, the entry for that account is removed from the IdentityMap table.

Proceed to the **ADVANCED OPTIONS** section to specify a substitute for the Profile table, and restrictions to apply to the Profile and data feed tables, as shown in [Figure 37](#).

Figure 37: Advanced Options

Advanced Options

Profile Table Stand-in:
 -- Select a Profile table --

Restrictions:
 Profile Table

Data Feed Table

☒ Enabled
☐ Map Multiple Accounts
☐ Remap previously mapped accounts

Check Syntax **Check Syntax**

Save **Cancel**

4. In the **ADVANCED** section, configure the following fields:

- **PROFILE TABLE STAND-IN:** Select a substitute for the Profile table from the drop-down list.
- **ENABLED:** By default, the rule is enabled. You can check the check box to disable the mapping rule.
- **MAP MULTIPLE ACCOUNTS:** Check this to enable the mapping rule to match multiple accounts to a single user profile. If unchecked, the Identity Mapping process selects the first account that matches the rule and leaves the other accounts to be mapped by other rules, or to be marked as an orphan.

For example, you have the fields shown in Table 2 for the data feed table:

Table 2: Information from Data Feed Table

AccountName	EmployeeNo	Source	Enabled
PG35467	123	abc.dom	True
PG35467_test	123	abc.dom	True
PG35467	123	xyz.dom	False

If the rule to match is P.ProfileUID= S.EmployeeNo, then both accounts PG35467 and PG35467_test would be mapped to the same user profile.

- **REMAP PREVIOUSLY MAPPED ACCOUNTS:** Check this option to remap accounts that were mapped earlier. If a rule with different mapping criteria remaps the accounts, it can change the existing mappings in the IdentityMap table.

If unchecked, a mapping rule will not attempt to map accounts that are already mapped in the IdentityMap table.

Under **RESTRICTIONS**:

- **PROFILE TABLE:** Accepts a WHERE clause to filter the Profile table. For example, if you want to run this rule on profiles whose hire date is on or after 1/1/2011, enter P.HireDate >= '1/1/2011'.

The P in the syntax is an alias to the Profile table.

- **DATA FEED TABLE:** Accepts a WHERE clause to filter the data feed. For example, if you want to run this rule on data feed accounts whose first name begins with an A, enter S.FirstName like 'A%'.

The S in the syntax is an alias to the configured data feed table.

Note: For information about how to write SQL statements, refer to Microsoft SQL Server documentation.

5. Click **SAVE** when done.

Chapter 6: Executing Rules to Map Accounts

This chapter describes how to schedule identity mapping rules to run at a specific time or to run immediately. It includes the following sections:

- [*“Executing Rules Periodically” on page 64*](#)
- [*“Executing Rules Immediately” on page 67*](#)
- [*“Viewing Rule History” on page 68*](#)

Executing Rules Periodically

You can schedule identity mapping rules to run periodically using the Scheduler. To schedule rules to run at a specific time, you need to:

1. Create a job and select one or more rules.
2. Schedule the job to run at a specific time. At the scheduled time, the job starts to execute the rules it contains.

Creating a Job

To schedule one or more rules to run periodically, you create jobs. A job enables you to group rules and execute them together.

While logged into the Access Assurance Portal as a member of the IDM Admins dynamic community, you can click the Main Menu and select **IDENTITY MAPPING**. Select the **SCHEDULE RULES** tab to use the Scheduler. Select **ADD NEW JOB** to create a job. A new window appears as in [Figure 39](#).

Figure 39: Create New Job

JOB NAME: Enter a name to identify the job.

RULES SELECTED TO RUN: Select one or more rules from the **RULES AVAILABLE** pane using the arrows. The selected rules appear to the right. Alternatively, you can drag and drop the rules.

Note: If a rule is disabled, it does not appear in the **RULES AVAILABLE** pane.

Click **SAVE** when done. Once you have created the job, the **SCHEDULE JOB** popup appears. You can schedule the job now or click cancel to add the job to the list. You can schedule the job later by clicking **SCHEDULE** from the **SCHEDULE RULES** window. For more information refer to [“Scheduling a Job” on page 65](#).

The job you created appears on the **SCHEDULE RULES** window, with the options **EDIT**, **DELETE**, and **SCHEDULE**, as shown in [Figure 40](#). For example, the Job for Rule A appears with information about its current state. If you do not schedule the job, the **RECURRENCE TYPE** value is set to **NOT SCHEDULED**. Additional information appears after you schedule the job for execution.

Figure 40: List of Jobs

Name	Recurrence	Last Execution	Last Completion	Next Execution	Status			
Map the Corp Accounts				Not Scheduled	Sleeping	Edit	Delete	Schedule

Click **EDIT** to make changes to the job and the rules you want to add or remove.

Click **DELETE** to remove the job from the list.

Click **SCHEDULE** to specify the date and time for the selected job to run.

Note: Ensure that the Scheduler Service is running at the scheduled time. Otherwise, the job cannot run successfully. If you stop the Courion Identity Mapping Service manually, then you need to restart both the Identity Mapping Service and the Courion Scheduler Service.

Data Feed Consistency Check

While running mapping rules prior to performing any deletions on the IdentityMap table, the Identity Mapping process uses the following formula to determine if there is a faulty data feed as a safety precaution:

$$\text{Actual percentage of total data feed table records that get deleted} = 100 * (\text{The number of distinct user names in the data feed table that DO NOT exist in IdentityMap - candidates for deletion} / (\text{total number of distinct user names in the data feed table that are mapped})).$$

If the percentage value is less than the threshold, then deletion of IdentityMap records is enabled. If the percentage value is greater than or equal to the threshold, then deletion of IdentityMap records is disabled.

The Mapping_GlobalConfigValues table provides optional flags to control the deletion of IdentityMap records. For more information about the flags, refer to the section [“Optional Flags to Control Deletion of IdentityMap Records” on page 95](#).

Scheduling a Job

To schedule a job, select **SCHEDULE** on the **SCHEDULE RULES** window. The **SCHEDULE JOB** popup appears as in [Figure 41](#).

Figure 41: Schedule Job

Schedule Job

Start

Start Time: 12:00 AM

Start Date: [Calendar Icon]

☒ No End Date
☐ End After [] Occurrences
☐ End By [Calendar Icon]

Recurrence Pattern

☒ None
☐ Daily
☐ Weekly
☐ Monthly

Save Cancel

Specify the start time, and start and end dates by configuring the following fields in the **START** panel:

- Select the **START TIME** and **START DATE**. The job starts executing on the specified date and time.
- Select **NO END DATE** to schedule the job to run for an indefinite period of time.
- Select **END AFTER OCCURRENCES** to end job execution after a specified number of runs. Specify the number in the text box provided. For example, if you enter 2, the job stops running after it has run twice.
- Select a date from the **END BY** drop-down list to end job execution on the selected date.

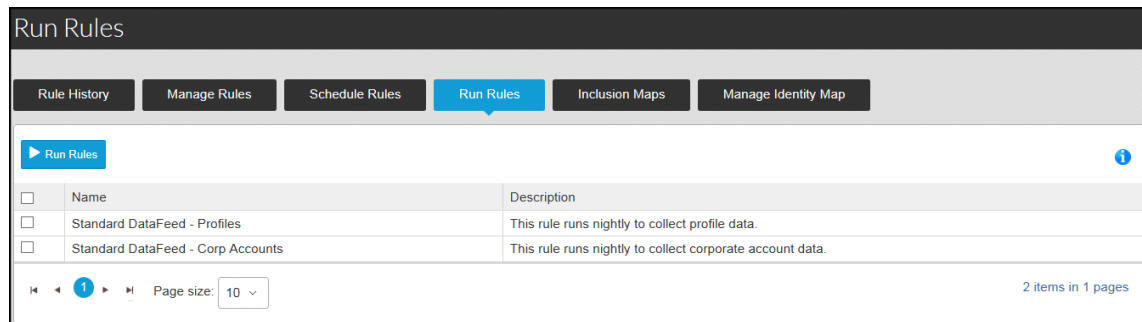
Select how frequently you want to run the job by configuring the following fields in the **RECURRENCE PATTERN** panel:

- Select **NONE** if you do not want to run the job recurringly.
- Select **DAILY** to run the job at the specified daily intervals.
- Select **WEEKLY** to run the job at the specified weekly intervals. You can also specify the days of the week.
- Select **MONTHLY** to run to job at the specified monthly intervals.

Executing Rules Immediately

While logged into the Access Assurance Portal as a member of the IDM Admins dynamic community, you can run rules immediately by clicking the Main Menu and selecting **IDENTITY MAPPING**. Select the **RUN RULES** tab to view the window displayed in [Figure 42](#).

Figure 42: Run Rules Immediately



Use the check box to select the individual rules, or check the Select All check box in the header row to select all the rules. Click **RUN RULES** to execute the selected rules.

A status message appears above the grid containing a hyperlink to the **RULE HISTORY** tab.

Note: Any disabled rules do not appear on this window.

Viewing Rule History

To determine if the rules were run successfully, click the Main Menu and select **IDENTITY MAPPING**. Select the **RULE HISTORY** tab to view the window displayed in [Figure 43](#).

Figure 43: Rule History

Rule History												
<div> Rule History Manage Rules Schedule Rules Run Rules Inclusion Maps Manage Identity Map </div>												
<div> Completed Successfully Error Occurred </div>												
Batch ID	Start	End	Message	Details	Accts Added	Accts Mapped	Orphans Found	Orphans Adopted	Conflicts Found	Accts Remove	Accts Duplicate	State
3	5/27/2014 5:38:02 AM	5/27/2014 5:38:03 AM	User Account Mapping Rule- 'Map2' execution completed successfully.	Details	10	10	0	0	0	0	0	Success
2	5/27/2014 5:35:48 AM	5/27/2014 5:35:49 AM	User Account Mapping Rule- 'Map2' execution completed successfully.	Details	10	0	10	0	0	0	0	Success
1	5/27/2014 5:30:56 AM	5/27/2014 5:30:58 AM	User Account Mapping Rule- 'Map1' execution completed successfully.	Details	10	0	10	0	0	0	0	Success

⏪
⏴
1
⏵
⏩
 Page size: 10
9 items in 1 pages

The window displays the history for rules that were scheduled to run periodically or immediately. Each row displays the start and end time of one or more rules executed in a batch.

A batch is created when a job or a set of rules are run as a single execution. A batch could include:

- A job scheduled to run with one or more rules.
- One or more rules selected manually to run at the same time.

A batch ID uniquely identifies a single batch.

The **RULE HISTORY** window also displays the rule status and the following additional columns:

- **ACCTS ADDED:** The number of new accounts that were added to the Mapping_Account table.
- **ACCTS MAPPED:** The number of accounts that were mapped.
- **ORPHANS FOUND:** The number of accounts that were not successfully mapped.
- **ORPHANS ADOPTED:** The number of orphaned accounts that were successfully mapped.
- **CONFLICTS FOUND:** The number of accounts which could not be mapped because the account matches more than one profile.
- **ACCTS REMOVED:** The number of accounts that were deleted from the IdentityMap table.
- **ACCTS DUPLICATE:** The number of accounts which could not be mapped because the match criteria suggests that these are duplicate accounts. It may be necessary to edit the mapping rule to match on additional criteria.

Note: The information is relevant to a specific batch and the rules that were run as part of it.

Right-Click Column Menu Options

Right-clicking on any column heading shows a menu with the following options:

- **Sort Ascending** - Sorts information in ascending order, alphabetically or numerically, when **Enable Sorting** is checked.
- **Sort Descending** - Sorts information in descending order, alphabetically or numerically, when **Enable Sorting** is checked.
- **Clear Sorting** - Clears any sorting that was applied to a column.
- **Best Fit** - Adjusts the column width to display the most information.
- **Columns** - Displays a list of the columns when **Enable Hiding** is checked. Check to show a column or uncheck to hide it.

Chapter 7: Creating Entitlement Mapping Rules

This chapter describes how to create rules that map collected entitlements to user profiles. It is intended for the data mapping administrator who has collected accounts with entitlements and who will use the collected entitlements to build the Access Catalog of the Access Request Manager, a component of the Access Assurance Suite.

Mapping Collected Entitlements

Prior to mapping entitlements to user profiles, the data mapping administrator should have completed the following actions:

1. Collected account data with assigned entitlements by using a data collection rule or by using a data feed.
2. Collected profile data by running a data collection rule or by using a data feed.
3. Populated the IdentityMap table by running an Identity Mapping rule. The Rule History tab of the Manage Rules window confirms whether the rules ran successfully.

After you have confirmed that these actions have been successful, you can create an entitlement mapping rule to map entitlements to user profiles.

Creating an Entitlement Mapping Rule

When creating an entitlement mapping rule, you use a wizard that is very similar to the wizard for creating a data collection rule. There are only three wizard panels:

- Select Source
- Filter Data
- Schedule Rule

To create a new entitlement mapping rule, do the following:

1. From the Main Menu in the Access Assurance Portal, select **ENTITLEMENT MAPPING**. The Entitlement Mapping window appears.
2. Click **ADD NEW RULE**. The Data Mapping Rule Wizard appears as shown in [Figure 43](#).

Figure 43: Select Source Data Mapping Rule Wizard

The screenshot shows the 'Data Mapping Rule Wizard' window. On the left is a sidebar with three steps: 'Select Source' (highlighted with a blue bar and a right arrow), 'Filter Data', and 'Schedule Rule'. Below these is an 'Exit Wizard' button. The main area is titled 'Select Source' and contains a 'Data Mapping Options' section with a radio button for 'Entitlements'. To the right of this are three input fields: 'Rule Name *' (a text box), 'Rule Description' (a larger text box), and 'Source System *' (a dropdown menu with 'Select target' as the current selection). 'Back' and 'Next' buttons are located at the top right and bottom right of the main area.

3. Configure the following fields in the **SELECT SOURCE** panel:
RULE NAME: Enter a name to uniquely identify the entitlement mapping rule.

RULE DESCRIPTION: Specify a description for the entitlement mapping rule.

SOURCE SYSTEM: Select the source from the drop-down list. The list displays all of the source systems for which data collection and identity mapping have been performed.

- Click **NEXT**. The Filter Data panel appears. The sample data may contain entitlement records which may or may not be relevant to access management. Therefore, you can configure the data mapping rule to exclude the data that is not relevant.

Note: By clicking **NEXT**, the entitlement mapping rule is saved. If you later choose **EXIT** to leave another wizard page without saving, the entitlement mapping rule still exists with the items specified on the Select Source page.

- You can exclude data by adding filters to the **SELECTED FILTERS** list. For example, to exclude data records which have a blank Employee ID column, select **ACCOUNT NAME IS BLANK** and click the **>**.
- Click **PREVIEW** to view a sample of the accounts with entitlements that remain.

Figure 44: Filter Data in Data Mapping Rules Wizard

Rule Name: Ent Map 1 Back Next

Filter Data

Available Filters

Filter Name
First Name is blank
Last Name is blank
Full Name is blank
Account Name is blank
Employee ID is blank
Title is blank

New Filter...

Selected Filters (Data will be excluded)

Filter Name
Account Name is blank

Clear All

Sample Size: 100 Preview Hide blank columns

EmployeeID	Username	FullName	FirstName	MiddleName	TargetID
Employee21	UserName21	FullName21	FirstName21	MiddleName21	Active Directory21

5 items per page 1 - 1 of 1 items

- If you want to add another filter, repeat the previous two steps until you have added the filters you want to use.
- Click **NEXT**. The Schedule Rule panel appears as shown in [Figure 45](#).

By default, the rule is enabled. If you later decide that the rule should be disabled, check the **IS ENABLED** check box to clear it.

Figure 45: Schedule Rule of Data Mapping Rule Wizard

Rule Name: Ent Map 1

Back Finish

Select Source ✓

Filter Data ✓

Schedule Rule >

Exit Wizard

Schedule Rule

Is Enabled : ☒

Start Date : 6/4/2014

Start Time : 2:52 PM

Recurrence Pattern

☒ None

☐ Daily

☒ No End Date

☐ End by

Back Finish

9. **START DATE** field: Specify the date when the entitlement mapping rule will run.
10. **START TIME** field: Specify a time for the entitlement mapping rule to run. If the mapping may require a significant portion of database resources, schedule the rule to begin when demand for resources is low.
11. If you want to run the rule every day beginning on the start date, select **DAILY** as the recurrence pattern.
12. **END BY** field: If you specified daily recurrence, you can specify an end date as the last date the rule will run.
13. Click **FINISH**. The wizard closes and the Entitlement Mapping window appears.

Note: For additional scheduling options, use Microsoft SQL Server Management Studio to manage each data collection rule as a separate job.

Running an Entitlement Mapping Rule

If you want to run an entitlement mapping rule immediately, you can do so as follows:

1. From the Main Menu in the Access Assurance Portal, select **ENTITLEMENT MAPPING**. The Entitlement Mapping window appears.
2. Find the rule that you want to run. In that row, click **RUN**.
3. When the rule finishes running, a summary of the results appears in the **LAST RUN RESULT** column.

Viewing the Results of Entitlement Mapping

To view the mapped entitlement data from the last time a rule successfully ran, you can do the following:

1. From the Main Menu in the Access Assurance Portal, select **ENTITLEMENT MAPPING**. The Entitlement Mapping window appears.
2. Find the rule for which you want to view the mapped entitlements. In that row, click the name of the rule.

The data shown in [Figure 46](#) is not realistic but it shows that the **MAPPING ENTITLEMENT** tab displays the data as it appears in the Account_Entitlement table.

Figure 46: Entitlement Mapping Results

Data Feed

Rule Name: ItestIE8
Mapping Type: Entitlements Back

Mapped Entitlement		Unassigned Entitlement		
ProfileUID ▲	BusinessName ▼	Name ▼	Value ▼	TargetId ▼
buser1	BusinessName1	Entitlement1	Value1	Target1
buser1	BusinessName2	Entitlement2	Value2	Target2
buser1	BusinessName3	Entitlement3	Value3	Target3
buser1	BusinessName4	Entitlement4	Value4	Target4
buser1	BusinessName5	Entitlement5	Value5	Target5
buser1	BusinessName6	Entitlement6	Value6	Target6
buser1	BusinessName7	Entitlement7	true	Target7
buser1	BusinessName8	Entitlement8	Value8	Target8
buser1	BusinessName9	Entitlement9	Value9	Target9
buser1	BusinessName10	Entitlement10	Value10	Target10

◀ 1 ▶ 10 items per page 1 - 10 of 10 items

For further confirmation that the entitlement mapping process has been successful, an administrator can log into the Access Catalog of the Access Request Manager, search for one or two known profiles, and make sure that all of the entitlements for those profiles have been correctly mapped.

Chapter 8: Mapping Accounts Manually

This chapter describes how to create inclusion maps using the **INCLUSION MAPS** window. Manually mapped accounts are called inclusion maps. The need to create inclusion maps arises if an account on a certain target cannot be mapped to a profile using the automated rules you have set up.

While logged into the Access Assurance Portal as a member of the IDM Admins dynamic community, you can click the Main Menu and select **IDENTITY MAPPING**, and navigate to the **INCLUSION MAPS** tab. The **INCLUSION MAPS** window appears as shown in [Figure 47](#).

Figure 47: Inclusion Maps

Profile ID	Account	Target Name	Description	Enabled	Edit

No records to display.

Page size: 10 0 items in 1 pages

Adding an Inclusion Map

To add a new inclusion map, from the **INCLUSION MAPS** tab, click **ADD NEW**. The **INCLUSION MAP** window appears as in [Figure 48](#).

Figure 48: Inclusion Map window

The screenshot shows a window titled "Inclusion Map" with a dark header bar containing an information icon. The main area contains the following fields:

- Profile UID: ***: A dropdown menu.
- Account: ***: A dropdown menu.
- Target Name: ***: A dropdown menu.
- Description:**: A large text area.
- Enable Inclusion Map:**: A checkbox that is currently checked.

At the bottom of the window are two buttons: **Save** (in a blue box) and **Cancel** (in a white box with a grey border).

Configure the following fields:

- **PROFILEUID:** Select a profile ID from the drop-down list. The list is populated from the Profile table.
Note: Since you are manually mapping the selected profile to an account, ensure that you have the correct profile ID selected.
- **ACCOUNT:** Select an account from the drop-down list or enter a new account.
- **TARGET NAME:** Select a target name from the drop-down list or enter a new target.
- **DESCRIPTION:** Enter a brief description for the new inclusion map.
- **ENABLE INCLUSION MAP:** Select the check box to enable an inclusion map; uncheck to disable an inclusion map.

Click **SAVE**.

The account you entered with the target name gets manually mapped to the selected profile ID. This information is written to the Mapping_ManualIDMap and IdentityMap tables.

The account and target details are written to the Mapping_Account table. If you have entered a new target name, this information is written to the Mapping_Target table.

If you schedule or manually run the rules, the Identity Mapping process maps user accounts to profiles based on those rules, and writes the successfully mapped accounts to the IdentityMap table. For accounts that have inclusion maps enabled, an inclusion map takes precedence over an automated rule. In other words, the Identity Mapping process updates an account that was automatically mapped in the IdentityMap table with the inclusion map. If there are any new inclusion maps that were added, those also get written to the IdentityMap table.

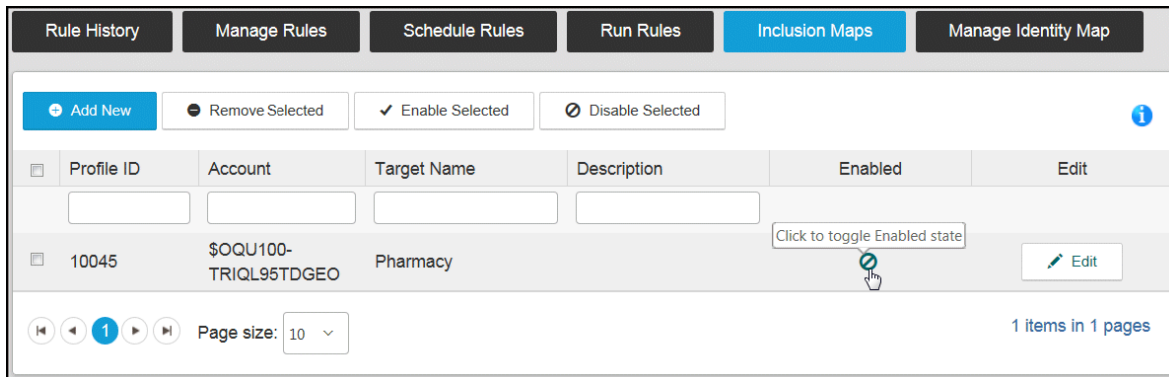
Note: The IdentityMap table contains a Batch ID field. When a mapping is created automatically by a rule, the Identity Mapping process generates a batch ID and populates the Batch ID field in the IdentityMap table. However, if an account is mapped manually, the Batch ID field in the IdentityMap table shows a NULL.

Enabling an Inclusion Map

When you create an inclusion map, it is automatically enabled (as long as you did not de-select the **ENABLE INCLUSION MAP** check box). However there may be instances in which an inclusion map was created but not enabled, or was disabled for some reason.

In [Figure 49](#), the inclusion map is disabled. Note the icon in the **ENABLED** column.

Figure 49: Inclusion Maps window showing a Disabled Inclusion Map

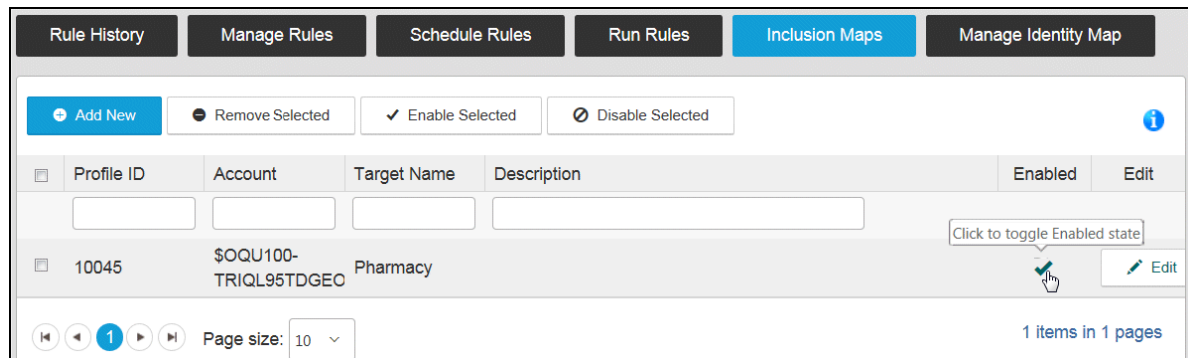


To enable an inclusion map, you can click the icon to change the status from disabled to enabled.

Disabling an Inclusion Map

To disable an inclusion map, you can click the icon to change the status from enabled to disabled. [Figure 50](#) shows an enabled inclusion map.

Figure 50: Inclusion Maps window showing an Enabled Inclusion Map



After you click the icon, it changes to show a disabled status as in [Figure 49 on page 80](#).

If you disable or delete an inclusion map, the account associated with the disabled/deleted inclusion map is removed from the IdentityMap table. The corresponding account entry in the Mapping_Account table is marked with the status "Deleted."

If you disable an inclusion map, the record for the disabled inclusion map in the IdentityMap table gets deleted.

Removing Inclusion Maps

To remove one or more inclusion maps, do the following:

1. Click the check box next to the inclusion map you want to remove. You can select more than one inclusion map. You can also click the check box in the header row which selects all inclusion maps.
2. Click **REMOVE SELECTED**. A dialog box appears for you to confirm the removal of the selected inclusion maps.
3. Click **OK** to confirm removal or **CANCEL** to not remove the selected item(s).

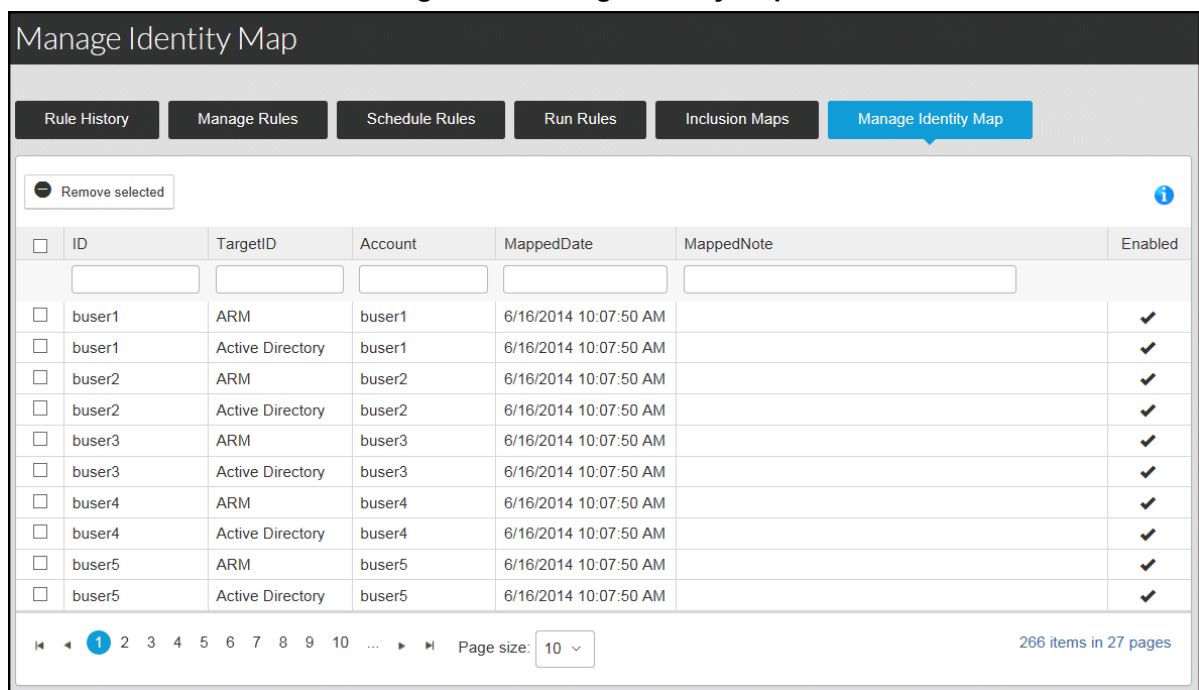
Note: When you remove an inclusion map, it is deleted from both the Mapping_ManualIDMap and IdentityMap tables.

Chapter 9: Deleting Mapped Accounts

This chapter describes how to delete mapped accounts from the IdentityMap table through the **MANAGE IDENTITY MAP** window.

While logged into the Access Assurance Portal as a member of the IDM Admins dynamic community, you can click the Mega Menu and select **IDENTITY MAPPING**. Click the **MANAGE IDENTITY MAP** tab. [Figure 52](#) shows an example of mapped accounts.

Figure 52: Manage Identity Maps



The screenshot shows the 'Manage Identity Map' window with a navigation bar containing tabs: Rule History, Manage Rules, Schedule Rules, Run Rules, Inclusion Maps, and Manage Identity Map (selected). Below the tabs is a 'Remove selected' button and an information icon. The main area contains a table with the following columns: ID, TargetID, Account, MappedDate, MappedNote, and Enabled. The table lists 10 rows of mapped accounts, each with a checkbox in the ID column. The bottom of the window shows a pagination bar with page numbers 1 through 10, a 'Page size: 10' dropdown, and a status '266 items in 27 pages'.

ID	TargetID	Account	MappedDate	MappedNote	Enabled
<input type="checkbox"/>					
<input type="checkbox"/> buser1	ARM	buser1	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser1	Active Directory	buser1	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser2	ARM	buser2	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser2	Active Directory	buser2	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser3	ARM	buser3	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser3	Active Directory	buser3	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser4	ARM	buser4	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser4	Active Directory	buser4	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser5	ARM	buser5	6/16/2014 10:07:50 AM		✓
<input type="checkbox"/> buser5	Active Directory	buser5	6/16/2014 10:07:50 AM		✓

To delete a single account, select an individual check box and click **REMOVE SELECTED**. To remove all the mapped accounts shown, select the **SELECT ALL** check box, and click **REMOVE SELECTED**.

Note: The mapped accounts you delete may reappear again in the IdentityMap table. For example, you delete an account dlarson mapped by Rule A. Later, if you run Rule A, or any other rule using a different mapping criterion against dlarson, the newly mapped dlarson reappears in the IdentityMap table.

Chapter 10: Viewing Reports

This chapter describes the reporting functionality to view information from tables, including Profile and IdentityMap. It includes the following sections:

- [*“Viewing the Overview Window” on page 86*](#)
- [*“Viewing Account Information” on page 88*](#)
- [*“Viewing Profile Information” on page 91*](#)
- [*“Viewing Mapped Information” on page 92*](#)
- [*“Viewing Customized Information” on page 93*](#)

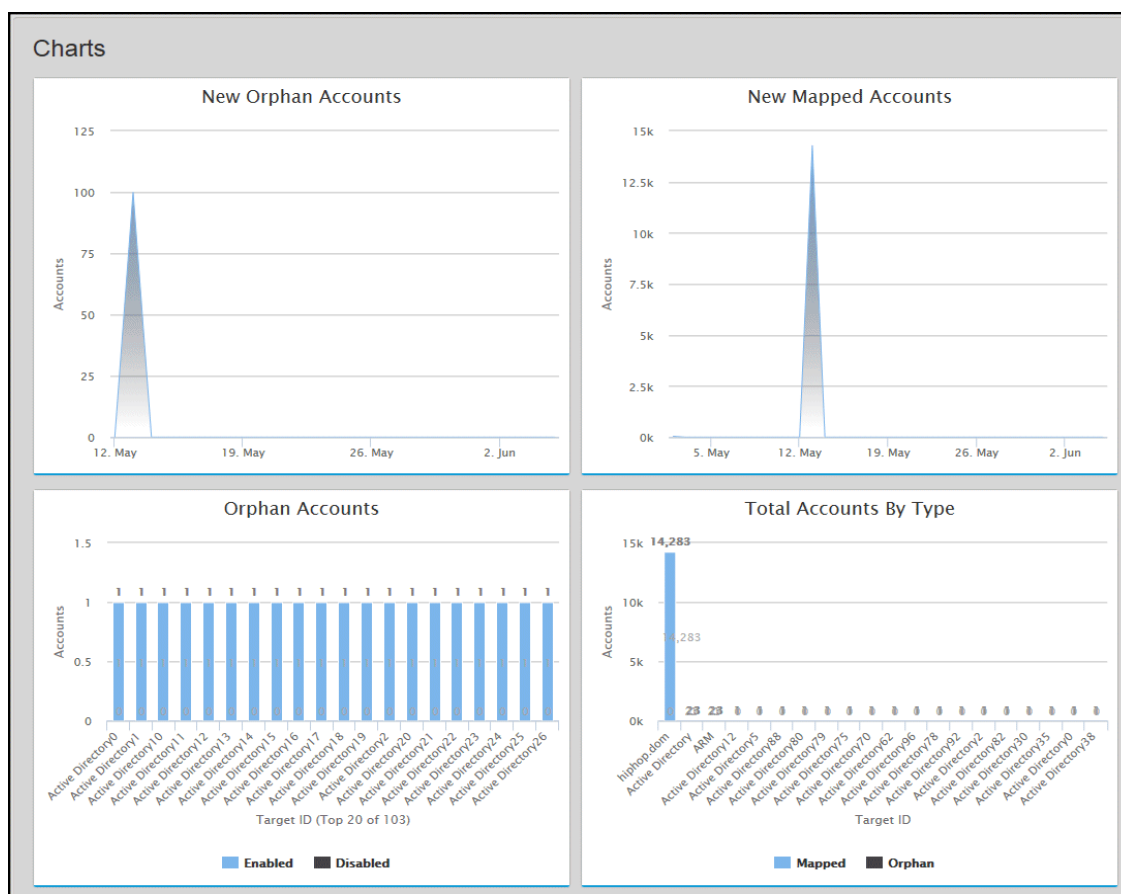
Viewing the Overview Window

The **OVERVIEW** window provides a snapshot of the accounts, the status of the Identity Mapping process, and links to edit identity mapping data feeds and mapping rules. From the Mega Menu, select **MAPPING OVERVIEW**. The **OVERVIEW** window is comprised of three sections:

- Charts
- Activity Summary
- Identity Mapping Configuration

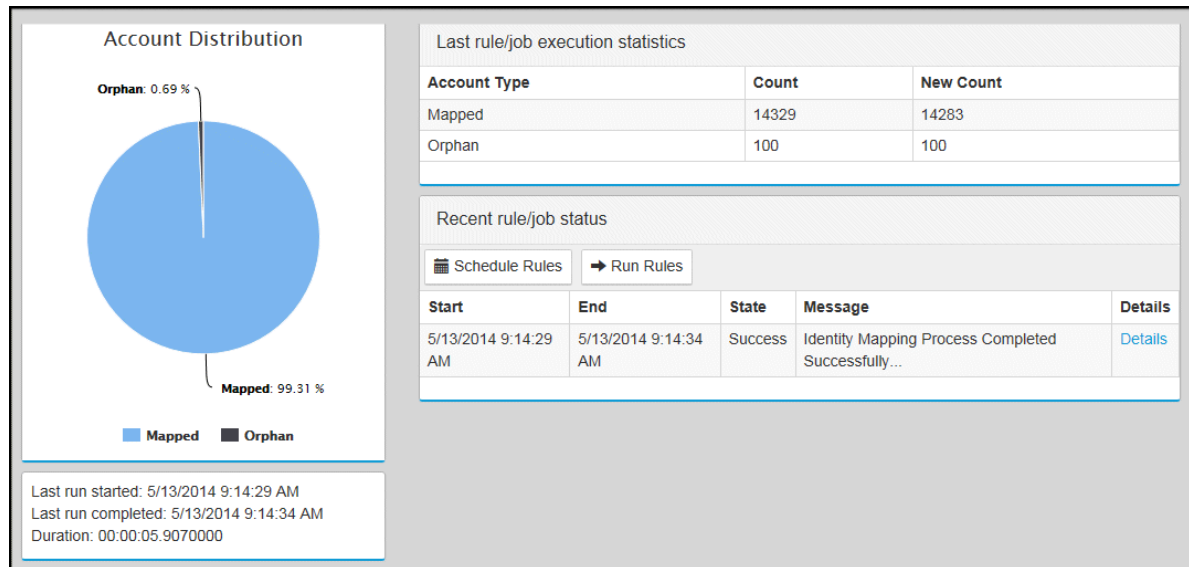
CHARTS - Displays information about accounts in various states, such as mapped or orphaned, as shown in [Figure 53](#). The account information is available by date or target for more granularity.

Figure 53: Charts



During the Identity Mapping process, accounts are categorized into account types depending on the mapping criteria defined in the mapping rule. All accounts are stored in the Mapping_Account table. Mapped accounts are stored in the IdentityMap table. For more information, refer to [“Viewing Account Information” on page 88](#).

ACTIVITY SUMMARY - Displays the latest status of the Identity Mapping process, as shown in [Figure 54](#). Click **SCHEDULE RULES** to view the rules that can be scheduled to run at a specific time. Click **RUN RULES** to view the list of rules to run. For more information, refer to [“Executing Rules to Map Accounts” on page 63](#).

Figure 54: Activity Summary

IDENTITY MAPPING CONFIGURATION - Provides a summary of the data feeds, rules, and inclusion maps, as shown in [Figure 55](#).

Figure 55: Identity Mapping Configuration

Identity Mapping Configuration		
Item	Enabled	Configure
DataFeeds	2	Configure
Rules	1	Configure
Inclusion Mappings	0	Configure

If you click **CONFIGURE** for any item, the respective configuration window appears. For example, if you click the Rules item, the **MANAGE RULES** window appears. This enables you to choose an identity mapping rule and edit it.

Viewing Account Information

From the Access Assurance Portal Mega Menu, select **MAPPING REPORTS**. Then select the **ACCOUNTS** tab. The Accounts Mapping Report appears as shown in [Figure 56](#). It displays information directly from the Mapping_Account table.

Figure 56: View Account Information

Accounts Profile Identity Map Custom			
Report: Accounts			
⚙️ Configure Grid			
TargetID	UserName	Enabled	AccountType
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>
hiphop.dom	!testing	True	Conflict
hiphop.dom	\$%	True	Conflict
hiphop.dom	\$\$User	True	Conflict
hiphop.dom	\$00V100-S2SNTCTL3OCD	True	Conflict
hiphop.dom	\$01V100-UQASP3JKCQBN	True	Conflict

Depending on the mapping criteria defined in a mapping rule, accounts are categorized into one of the following types:

- Mapped - An account that successfully maps to profile.
- Orphan - An account that was not mapped to any profile.
- Orphan Adopted - An orphan account that now maps successfully to a profile.
- Conflict - An account that could not be mapped because the account matches more than one profile.
- External - An account which cannot be categorized into any of the other types.
- Duplicate - An account which is one of several accounts which maps to a single profile.

Note: When you run an account mapping rule, any account that does not match the mapping criteria is identified as an orphan account.

The Accounts Mapping Report helps you to troubleshoot accounts that have not been successfully mapped.

Configuring the Grid

Click **CONFIGURE GRID** to configure and customize the view of the grid, as shown in [Figure 57](#).

Figure 57: Configure Grid

Access Assurance Portal

Set Grid Behavior

Set Number of Rows Per Page

☒ Enable Hiding
☒ Enable Sorting
☒ Enable Filtering
☒ Enable Resizing

Set Column Behavior

Column	Label	Order	Width	Visible	Movable	Detail View
TargetID	<input type="text" value="TargetID"/>	<input type="text" value="0"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
UserName	<input type="text" value="UserName"/>	<input type="text" value="1"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
Enabled	<input type="text" value="Enabled"/>	<input type="text" value="2"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AccountType	<input type="text" value="AccountType"/>	<input type="text" value="3"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>
AccountStatus	<input type="text" value="AccountStatus"/>	<input type="text" value="4"/>	<input type="text" value="10"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>	<input checked="" type="checkbox"/>

Using the **SET GRID BEHAVIOR** panel, configure the behavior of the grid and fields for the displayed table. You can configure the following options:

- **SET NUMBER OF ROWS PER PAGE:** Specify the number of records to display.
- **ENABLE HIDING:** Check to enable the hiding of columns.
- **ENABLE RESIZING:** Check to enable the resizing of columns.
- **ENABLE SORTING:** Check to enable sorting of data in each column. You can sort the information by clicking the individual column. The sorting order may be alphabetical or numerical, ascending or descending, based on the data type of the field.
- **ENABLE FILTERING:** Check to enable the filtering of information by column. If enabled, a filter text box appears in each column.

Configure the following options under **SET COLUMN BEHAVIOR**:

- **COLUMN**: Fields from the Mapping_Account table.
- **LABEL**: Enter a label for the field.
- **ORDER**: Select the order in which you want to display the columns.
- **WIDTH**: Specify the column width.
- **VISIBLE**: Check to show the field; uncheck to hide it.
- **MOVABLE**: Check to enable moving of columns.
- **DETAIL VIEW**: Check to display fields in a collapsible **DETAILS** window. An icon appears in the first column that enables you to enlarge or collapse the window and view or hide the fields, respectively.

Click **SAVE** when done.

Right-Click Column Menu Options

Right-clicking on any column heading shows a menu with the options you enabled through **CONFIGURE GRID**. One or more of the following options appear in the right-click menu:

- **SORT ASCENDING** - Sorts information in ascending order, alphabetically or numerically, when **ENABLE SORTING** is checked.
- **SORT DESCENDING** - Sorts information in descending order, alphabetically or numerically, when **ENABLE SORTING** is checked.
- **CLEAR SORTING** - Clears any sorting that was applied to a column.
- **COLUMNS** - Displays a list of the columns when **ENABLE HIDING** is checked. Check to show a column or uncheck to hide it.

Viewing Profile Information

From the Access Assurance Portal Mega Menu, select **MAPPING REPORTS**. Then select the **PROFILE** tab to view the information from the Profile table, as shown in [Figure 58](#).

Figure 58: View Profile Information

Accounts

Profile

Identity Map

Custom

Report: Profiles

⚙️Configure Grid

ProfileUID	ManagerID	RoleID	LocationID	FirstName	MiddleName	LastName
<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>
10002				Jeff		Winchell
10003				Beverly		Bierman
10004				Beverly		Bierman
10005				Sean		Nokes
10006				Nick		Chapman

To view the information in the stand-in profile tables, select the table from the **SELECT CUSTOM PROFILE TABLE** drop-down list.

A filter text box appears in each column and you can enter the text to filter on or select it from the drop-down list, when **ENABLE FILTERING** is checked through **CONFIGURE GRID**. Click **CONFIGURE GRID** to configure how the fields from the table are displayed. Refer to [“Configuring the Grid” on page 89](#) for additional information.

To view the right-click column menu options, refer to the section [“Right-Click Column Menu Options” on page 90](#).

Viewing Mapped Information

From the Access Assurance Portal Mega Menu, select **MAPPING REPORTS**. Then select the **IDENTITY MAP** tab to view the information from the IdentityMap table, as shown in [Figure 59](#).

Figure 59: View Mapped Information

Accounts

Profile

Identity Map

Custom

Report: Identity Maps

⚙️Configure Grid

TargetID	UserName	MappedDate	MappedNote	DisabledDate	DisabledNote	ID	ProfileUID
<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>	<div>▼</div>
hiphop.dom	\$3PU100-D1TT9LDMF3SQ	4/24/2014 2:56:30 PM	Inclusion Map			1084	10005
hiphop.dom	AUPG1	4/24/2014 2:27:58 PM	Add hiphop accounts to the ID Map			1058	10023
hiphop.dom	AUPG3	4/24/2014 2:27:58 PM	Add hiphop accounts to the ID Map			1059	10024
hiphop.dom	bbacct1	4/24/2014 2:27:58 PM	Add hiphop accounts to the ID Map			1038	10003

A filter text box appears in each column and you can enter the text to filter on or select it from the drop-down list, when **ENABLE FILTERING** is checked through **CONFIGURE GRID**. Click **CONFIGURE GRID** to configure how the fields from the table are displayed. Refer to [“Configuring the Grid” on page 89](#) for additional information.

To view the right-click column menu options, refer to the section [“Right-Click Column Menu Options” on page 90](#).

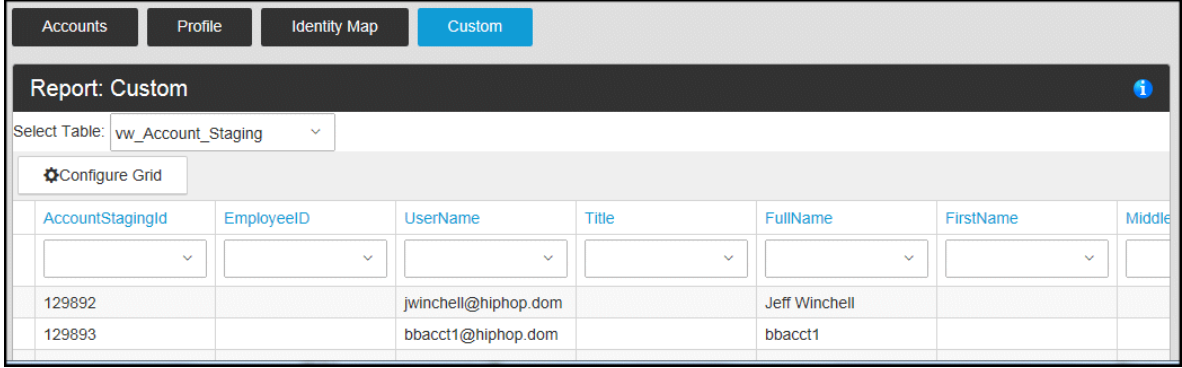
Note: If accounts are mapped with user profiles from a stand-in profile table, the mapped records may not show profile-related information, such as First Name.

Viewing Customized Information

From the Access Assurance Portal Mega Menu, select **MAPPING REPORTS**. Then select the **CUSTOM** tab. The window in [Figure 60](#) appears.

Select a table from the drop-down list and the information from the table appears in the window.

Figure 60: View Custom



AccountStagingId	EmployeeID	UserName	Title	FullName	FirstName	Middle
129892		jwinchell@hiphop.dom		Jeff Winchell		
129893		bbacct1@hiphop.dom		bbacct1		

When the table appears in the window, you can right-click on a column to view menu options to sort or group information. For additional information, see [“Right-Click Column Menu Options” on page 90](#).

You can use the **CONFIGURE GRID** option to configure how the fields from the table are displayed. Refer to [“Configuring the Grid” on page 89](#) for additional information.

Appendix A: Troubleshooting

This appendix describes steps you can take for debugging Identity Mapping, if needed.

Log Files Available for Debugging Identity Mapping

The Identity Mapping Solution provides the following log files in the [CoreSecurityInstallPath]\CourionService folder:

- **Portal Log for the web site:** Courion.DataMapping.Portal.Log.
- **Identity Mapping Service** (The WCF Service that provides data to the Web site): Courion.WCFHost.DataMapping.IdentityMapping.log.
- **Scheduler Service** (The WCF Service that executes scheduled jobs): Courion.SchedulerService.log.
- **Data Layer** (The library that performs all of the actions against the database): Courion.DataMapping.DataUtils.log.

Optional Flags to Control Deletion of IdentityMap Records

These are the optional flags in the Mapping_GlobalConfigValues table that you can use to control the deletions on the IdentityMap table:

- **BAD_FEED_OVERRIDE** - Set this flag to "1" to enable the deletion of IdentityMap records, although the data feed is faulty.

Note:

- If the flag is NOT present in the Mapping_GlobalConfigValues table, the deletion of IdentityMap records is NOT performed when the data feed is faulty.
- If the flag is present in the Mapping_GlobalConfigValues table, and has the value of "0", the deletion of IdentityMap records is NOT performed when the data feed is faulty, as determined by the formula in the section ["Data Feed Consistency Check" on page 65](#).
- If the flag is present in the Mapping_GlobalConfigValues table, and has the value of "1", the deletion of IdentityMap records is performed, regardless of the nature of the data feed, as determined by the formula in the section ["Data Feed Consistency Check" on page 65](#).

- **BAD_FEED_THRESHOLD** - Set this flag to configure the comparison percentage while checking for the faulty data feed. Enter an integer value between 0 and 100.

Note:

- If the flag is NOT present in the Mapping_GlobalConfigValues table, a default value of "5" is assumed.
- If the flag is present in the Mapping_GlobalConfigValues table, then the specified value is used for comparison.

Note: The accounts will be deleted from the IdentityMap table only. Conflict and Orphan accounts in the Mapping_Accounts table will not be deleted.

Timeout Configuration

The SQL_COMMAND_TIMEOUT configuration option enables you to modify the timeout value for the stored procedure to execute jobs successfully. You can add the configuration to the Mapping_GlobalConfigValues table:

- ConfigName = SQL_COMMAND_TIMEOUT
- ConfigValue = <time in seconds>

The default timeout value is 600 seconds.

Note: Provide a value of 0 seconds when the duration of time is unknown for the stored procedure to execute jobs successfully. If the stored procedure takes 5 or more hours, for example, then providing a value of 0 ensures that the stored procedure gets as much time as needed to successfully execute a job.

Reduced Performance when Previewing or Collecting Large Amounts of Data

When collecting large numbers of data records such as over 100,000 records, you may experience slower performance or failures while previewing attribute mappings or while running a rule.

To resolve this, you can try increasing the maximum memory pool for the Apache Tomcat service as follows:

1. On the AAS server, go to the bin directory where Tomcat is installed.
2. Right-click Tomcat7w.exe and select **RUN AS ADMINISTRATOR**.
3. Click the **JAVA** tab.
4. Based on the current maximum memory pool value, double the current amount. For example, if it is 512, change it to 1024.
5. Click **OK**.

Problems with Proxy User Account used for Data Collection

On the database server, the dbserver.sql file creates a proxy user account which is needed for creating data collection rules. This account has the necessary access for creating, reading, and running data collection rules as SQL jobs.

If you encountered an issue while using the dbserver.sql file to create the proxy user and credentials, refer to Section 3.

Section 1: Create Database User

This procedure assumes that you have executed the dbserver.sql file to create the proxy user and credentials on the database server. Go to Section 2 if you want to use a pre-existing user.

For detailed steps, refer to Microsoft SQL Server Management Studio documentation for the version you are using.

1. Log into Microsoft SQL Server Management Studio as the sa user (or another user with sysadmin privileges).
2. In the Object Explorer, go to Security and expand that folder.
3. Create a new login with the name: DataCollectionUser.
4. For authentication type, select SQL Server authentication.

Section 2: Map User

1. If needed, log into Microsoft SQL Server Management Studio as the sa user (or another user with sysadmin privileges).
2. In the Object Explorer, go to Security and expand that folder.
3. Select the properties of the DataCollectionUser or another pre-existing user.
4. Go to the User Mapping window.
5. In the list of databases, select Courion.
6. DataCollectionUser (or the pre-existing user you specify) should be listed as the db_owner of the Courion database. If it is not, make that change.
7. In the list of databases, select msdb.
8. In the "Database role membership for:" area, select the following roles:
 - f. SQLAgentOperatorRole
 - g. SQLAgentReaderRole
 - h. SQLAgentUserRole
9. Click **OK** to save your changes.
10. In the Object Explorer, go to SQL Server Agent and expand that folder.
11. Select CourionDataCollectionProxy. Open the property window for that proxy.
12. Go to the Principals window.
13. Click **Add**.
14. Add the DataCollectionUser (or the pre-existing user) as SQL Login type.

15. Click **OK**.

Section 3: Create Credentials and Proxy

1. Create a new credential for this domain user who has this privilege for the database server by specifying CourionCredentials as the credential name, and the domain, username, and password.
 - a. Log into Microsoft SQL Server Management Studio as the sa user (or another user with sysadmin privileges).
 - b. Go to SSMS > Security > Credentials-> New Credential ...
 - c. Specify the fields as follows:
 - Credential Name: CourionCredentials
 - Identity: Windows User having account on Database Machine (Ensure you have added this user using the ... option available on the credentials screen)
 - Domain Password
 - Domain Password
2. Click **OK**.
3. In the Object Explorer, go to SQL Server Agent and expand that folder.
4. Create a new proxy as follows:
 - a. Proxy name: CourionDataCollectionProxy
 - b. Credentials: CourionCredentials
 - d. Subsystem: PowerShell

Log Files for Debugging ETL Errors with Data Collection Rules

To troubleshoot errors related to Talend/Tomcat configuration issues, refer to the following log files in the [CoreSecurityInstallPath]\CourionService <Tomcat Install Dir>/logs/ folder:

- tomcat7-stderr.<Date>.log
- tomcat7-stdout.<Date>.log

Problem: "ETL Job Failed" error

This problem can occur because ETL is not properly deployed in Tomcat. Restart the Tomcat service (Apache Tomcat 7) and then run the data collection rule again.

The problem can also occur if the COURION_HOME environment variables is missing or not set correctly. To confirm this cause, search both of the Tomcat logs for the following error:

```
Exception in component tJava_4
java.lang.NullPointerException
at content.ldap_0_1.ldap.tJava_4Process(ldap.java:1190)
```

To resolve the error, do the following:

1. Edit the COURION_HOME system variable and set the value to the location of the Courion installation which is usually c:\Program Files (x86)\Courion Corporation.
2. Restart the Tomcat service.
3. Run the data collection rule.
4. If the error occurs again, restart the system to clear and reset the system variable.

Problem: "Tomcat Server is not accessible" Error

Solution 1

Check the Tomcat log file which is located at <Tomcat dir>/logs/tomcat7-stdout.<Date>.log for the following:

```
System.Reflection.TargetInvocationException: Exception
has been thrown by the target of an invocation. --->
System.ArgumentNullException: valid certificate is
required to instantiate a ServiceClient

Parameter name: clientCertificate
```

This exception indicates that the client certificate is not present under "Trusted People" store.

To resolve this problem, do the following:

1. Import client certificate under "Trusted People" store.
2. Restart IIS.
3. Start the Tomcat service.
4. Re-run the data collection rule.

Solution 2

Check the Tomcat log file which is located at <Tomcat dir>/logs/tomcat7-stdout.<Date>.log for the following:

```
System.Reflection.TargetInvocationException: Exception
has been thrown by the target of an invocation. --->
System.ArgumentNullException: valid certificate is
required to instantiate a ServiceClient

Parameter name: serviceCertificate
```

This exception indicates that the Server certificate is not present under "Trusted People" store.

To resolve this problem, do the following:

1. Import Server certificate under "Trusted People" store .
2. Restart IIS.

3. Start the Tomcat service.
4. Re-run the data collection rule.

Solution 3

Check the Tomcat log file which is located at <Tomcat dir>/logs/tomcat7-stdout.<Date>.log for the following:

```
System.Reflection.TargetInvocationException: Exception
has been thrown by the target of an invocation. --->
System.ServiceModel.Security.SecurityNegotiationException
: SOAP security negotiation failed. See inner exception
for more details. ---> System.ArgumentException: The
certificate 'CN=AccessAssuranceSuiteClient' must have a
private key. The process must have access rights for the
private key.
```

This exception indicates that the client certificate present under "Trusted People" does not have a private key.

To resolve this problem, do the following:

1. Import client certificate with private key (.pfx extension) under "Trusted People" store.
2. Restart IIS.
3. Start the Tomcat service.
4. Re-run the data collection rule.

Solution 4

Check the Tomcat log file which is located at <Tomcat dir>/logs/tomcat7-stdout.<Date>.log for the following:

```
System.Reflection.TargetInvocationException: Exception
has been thrown by the target of an invocation. --->
System.ServiceModel.ServiceActivationException: The
requested service, 'http://<ServerName>/CoreARMS/
DataServices/DataCollectionService.svc' could not be
activated. See the server's diagnostic trace logs for more
information.
```

This exception indicates that the server certificate present under "Trusted People" does not have private key. To resolve this problem, do the following:

1. Import server certificate with private key (.pfx extension) under "Trusted People" store
2. Restart IIS.
3. Start the Tomcat service.
4. Re-run the data collection rule.

Solution 5

Check the Tomcat log file which is located at <Tomcat dir>/logs/tomcat7-stdout.<Date>.log for the following:

```
javax.net.ssl.SSLHandshakeException:
sun.security.validator.ValidatorException: PKIX path
building failed:
sun.security.provider.certpath.SunCertPathBuilderExceptio
n: unable to find valid certification path to requested
target
```

This exception indicates that the Tomcat server is not configured to run in an SSL environment.

To resolve this problem, do the following:

1. Make sure you have the server .cer file available on your server.
2. Open CMD and navigate to JRE bin folder. For example, cd "c:\Program Files\Java\jre7\bin"
3. Run the following command:


```
keytool.exe -import -alias Server -keystore "C:\Program
Files\Java\jre7\lib\security\cacerts" -file
c:\Users\courionadmin\Desktop\ServerCER.cer
```

Note: The -keystore parameter expects the cert location and jre location for your environment. Modify the above command as needed.
4. Restart IIS.
5. Start the Tomcat service.
6. Re-run the data collection rule.

Problem: Tomcat service is not Starting

Solution 1

If the Tomcat service will not start, check to be sure that the following environment variables are set as follows:

%CATALINA_HOME% should be set to the Tomcat installation directory.

%JRE_HOME% should be set to the jre7 installation directory.

To resolve the problem, do the following:

1. Edit the environment variables and set the correct values.
2. Restart IIS.

Solution 2

If solution 1 does not work, continue troubleshooting as follows:

1. Using a command line window, go to the Tomcat installation directory.
2. Go to the Tomcat bin folder.
3. Run the startup.bat file. A new console window should appear containing detailed information.

If the error is similar to the following, the issue relates to 32-bit or 64-bit support:

```
java.lang.UnsatisfiedLinkError: C:\tomcat\apache-tomcat-7.0.42\bin\tcnative-1.dll
```

```
1: Can't load AMD 64-bit .dll on a IA 32-bit platform
```

```
at java.lang.ClassLoader$NativeLibrary.load(Native Method)
at java.lang.ClassLoader.loadLibrary1(Unknown Source)
at java.lang.ClassLoader.loadLibrary0(Unknown Source)
at java.lang.ClassLoader.loadLibrary(Unknown Source)
at java.lang.Runtime.loadLibrary0(Unknown Source)
```

To resolve the issue, confirm that the Windows architecture supports the same bit size that is supported by Tomcat.

Problem: "Job Failed" Error

This error is difficult to debug because there is no specific log file generated by Tomcat. There are multiple possible causes for this error.

A known cause is that the one of the following dll and library files are missing.

- Janet-win64.dll in <Tomcat install dir>/bin
- Janet-win32.dll in <Tomcat install dir>/bin

Or that the following library file is missing:

- janet-java-1.0-SNAPSHOT.jar in <Tomcat install dir>/lib folder

Talend requires the java to .net dll (janet.dll) file to communicate with the dot net component.

Index

triplet 61

W

Windows Authentication 39

A

Access Assurance Portal 7, 11, 12

Access Assurance Suite 7

account ID 61

B

batch 68

Batch ID 79

D

data feed 7, 13, 51

delete

mapped accounts 83

Disabled Account 53

I

ID Admins 12

Inclusion Maps 77

Integrated Windows Authentication 12

J

Job 64

L

log files 95

M

Mapping_Account 68, 78

Mapping_Target 78

O

Overview window 86

P

profile ID 61

Profile table 61

R

Recurrence Pattern 66

reporting 85

rule 57

S

schedule rules 63

Scheduler 64

T

target ID 60

