Product Requirements of the Core Access Assurance Suite

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

Table of Contents

This document describes the product requirements for the Access Assurance Suite including the Web server, database server, and supported data sources for PasswordCourier Classic and ProfileCourier Classic ticketing and authentication.

For requirements that are specific to the Access Insight Solution, refer to the manual *Access Insight Solution*.

Access Assurance Suite Server Hardware and Software Requirements

Table 1 describes the Access Assurance Suite server requirements. These requirements apply to each server in a distributed installation with the exception of memory, as noted in the table.

Table 1: Access Assurance Suite Server Requirements

Microsoft Windows Server® 2008 or 2008 R2 or 2012 or 2012 R2 or 2016 (Standard, Enterprise, and Data Center editions) **Note:** For additional Windows Server requirements, refer to *“Roles and Features Required for Windows Server 2008, 2012, and 2016 Servers” on page 8*. **Note:** The Windows Core installation only option is not supported.
Microsoft .NET 3.5 Framework * Microsoft .NET 4.0 Framework * Microsoft. NET 4.7.1 Framework
Microsoft Chart Controls for Microsoft .NET Framework 3.5 *
Microsoft Windows Identity Foundation * #
Microsoft XML 6.0* and Microsoft XML 3.0 *
Microsoft Visual C++ (x86) Redistributable*
Microsoft ASP.NET MVC 3* Microsoft ASP.NET MVC 4*
Microsoft Message Queuing **Note:** If you plan to replicate the server used to host the Access Assurance Suite in your environment using virtualization, after you replicate the server, install Microsoft Message Queuing and then install the Access Assurance Suite.
Apache Tomcat Server 7.0.42 *
Java SE Runtime Environment (Build 1.7.0-b147) *
Enable the Microsoft Distributed Transaction Coordinator (MS DTC) service on any server that hosts one or more of the following: the Connector Framework, the Connector Framework Manager, or the Publisher Service. For information about how to enable MS DTC, refer to: http://technet.microsoft.com/en-us/library/cc753620.aspx
Minimum of 4 GB of memory for single-server or distributed installations (8+ GB recommended)
Minimum of 2.0 GHz processing speed (2.70+ recommended)
Minimum of 2 CPUs (4+ CPUs recommended)
NTFS formatted disk drive, 80 GB minimum

* Included with the Access Assurance Suite installation executable. If not already installed, they are installed at the beginning of the installation process.

In Windows Server 2012, Windows Server 2012 R2, and Windows Server 2016, the Windows Identity Foundation is included as a Windows feature and you need to install it separately. It is not installed automatically while installing the Access Assurance suite.

Notes on Hardware and Software Requirements

Please keep the following in mind as you prepare to install the Access Assurance Suite:

- Insure that ASP and ASP.NET is enabled for IIS support.
- The requirements in this section assume that the Access Assurance Suite is the only application installed on the server. Please adjust the memory, CPU, and disk space requirements if other applications are installed on the server.
- For installations involving a virtual machine, each virtual machine must meet the requirements above. The virtual machine requirement is in addition to the requirements that must be met by the server running the virtual machines.
- The Access Assurance Suite should not be installed on an enterprise-critical server such as a Microsoft SharePoint server, a Microsoft Exchange server, or a domain controller.

Supported Browsers

The Access Assurance Suite supports Microsoft Internet Explorer® versions 8, 9, 10 and 11 and the latest versions of Google Chrome and Mozilla Firefox.

Browser Support for Administration Manager and Workflows

The Administration Manager is supported for use with Internet Explorer. FlowChart View is supported by IE8and IE9. TreeView is supported by IE8, IE9, IE10, and IE11.

To summarize the Web browsers which support each set of provisioning pages, refer to the following table:

Table 2: Browser Support for Modern-Look Provisioning Workflow Pages

	Microsoft IE8	Microsoft IE9	Microsoft IE10	Microsoft IE11	Google Chrome*	Mozilla Firefox*
Provisioning Workflow Pages	Yes	Yes	Yes	Yes	No	No
Modern-Look Provisioning Workflow Pages	Yes	Yes	Yes	Yes	Yes	Yes

* This version of the Web browser does not support the CourLocal control because it is an ActiveX control.

Screen Resolution

The minimum screen resolution required is 1280 x 1024 with a minimum color depth of 16-bit.

Roles and Features Required for Windows Server 2008, 2012, and 2016 Servers

The following sections list the minimum set of roles and features that you need on Windows Server 2008 or 2008 R2 or 2012 or 2012 R2 or 2016 servers (32-bit or 64-bit) for the Access Assurance Suite server, for Connector Framework-only servers, and for Connector Framework Manager-only servers.

Requirements for Connectors and Password Management Modules (PMMs)

Connectors and PMMs may require additional roles and features depending on the connector or PMM.

Application Server Role for the Access Assurance Suite Server

The Access Assurance Suite server requires the Application Server Role with the role services and features shown in Table 3 . The Application Server Role is *not* required for CF-only and CFM-only servers.

Table 3: Application Server Role for the Access Assurance Suite Server

Role Services and Features	Access Assurance Suite Server	CF-Only Server	CFM-Only Server
Application Server Foundation	Yes	No	No
Web Server (IIS) Support	Yes	Yes	Yes
COM+ Network Access	Yes	No	No
Windows Process Activation Service Support HTTP Activation Message Queuing Activation TCP Activation Named Pipes Activation	Yes	No	No

Web Server IIS Role - Access Assurance Suite Server and CF-Only and CFM-Only Servers

The Access Assurance Suite server as well as CF-only and CFM-only servers require the Web Server IIS Role with various role services and features. Table 4 lists these roles services and features and indicates if they apply to the Access Assurance Suite server, a CF-only server, or a CFM-only server.

Table 4: Web Server IIS Role Services and Features

Role Services	Features	Access Assurance Suite Server	CF-Only Server	CFM-Only Server
Common HTTP Features				
	Static Content	Yes	Yes	Yes
	Default Document	Yes	Yes	Yes
	Directory browsing	Yes	Yes	Yes
	HTTP Errors	Yes	Yes	Yes
	HTTP Redirection	Yes	No	No
Application Development				
	ASP.NET	Yes	No	No
	.NET Extensibility	Yes	No	No
	ASP	Yes	No	No
Health Diagnostics				
	HTTP Logging	Yes	Yes	Yes
	Logging Tools	Yes	No	No
	Request Monitor	Yes	Yes	Yes
	Tracing	Yes	No	No
Security				
	Basic Authentication	Yes	No	No
	Windows Authentication	Yes	No	No
	Anonymous Authentication	Yes	No	No
	Digest Authentication	Yes	No	No
	Client Server Mapping Authentication	Yes	No	No
	IIS Client Server Mapping Authentication	Yes	No	No
	URL Authentication	Yes	No	No
	Request Filtering	Yes	No	No
	IP and Domain restrictions	Yes	No	No

Windows Server Features - Access Assurance Suite Server and CF-Only and CFM-Only Servers

The Access Assurance Suite server as well as CF-only and CFM-only servers require various Windows Server features. Table 5 lists these features and indicates if they apply to the Access Assurance Suite server, a CF-only server, or a CFM-only server.

Table 5: Windows Server Features

Feature	Access Assurance Suite Server	CF-Only Server	CFM-Only Server
.NET Framework 3.5 Feature .NET Framework 3.5 WCF Activation HTTP Activation Non-HTTP Activation	Yes	Yes	Yes
.NET Framework 4.7.1	Yes	Yes	Yes
Message Queuing Feature Message Queuing Services Message Queuing Server	Yes	Yes	Yes
Remote Server Administration Tools Feature Role Administration Tools Web Server (IIS) Tools	Yes	No	No
Windows PowerShell Integrated Scripting Environment (ISE)	Yes	No	No
Windows Process Activation Service Feature Process Model .NET Environment Configuration APIs	Yes	Yes	Yes

Web Servers

The Access Assurance Suite requires that the Access Assurance Suite server has one of the following web servers:

Table 6: Access Assurance Suite Web Server Requirements

Operating System	Web Server
Microsoft Windows Server 2008	IIS 7.0
Microsoft Windows Server 2008 R2	IIS 7.5
Microsoft Windows Server 2012	IIS 8.0
Microsoft Windows Server 2012 R2	IIS 8.5
Microsoft Windows Server 2016	IIS 10.0

Notes on Web Servers

- The Access Assurance Suite uses the default port 80 for IIS communication.
- Core Security strongly recommends using HTTPS. As a result, a digital certificate is required to protect information between the web browser and web server. For information on obtaining a digital certificate, refer to the product documentation for your web server.
- The Access Assurance Suite does not support the United States Federal Information Processing Standard (FIPS) algorithm. The Access Assurance Suite does not support running on the Windows Server operating system when it is configured to use the Group Policy setting "System cryptography: Use FIPS compliant algorithms for encryption, hashing, and signing”. For more information, refer to the following Microsoft Knowledge Base article:

  http://support.microsoft.com/kb/811833.

Access Assurance Suite with DIRECT! Access Option

The Access Assurance Suite has the following client requirements when used with DIRECT!

Table 7: Access Assurance Suite with DIRECT!® Access Option

Client	A PC with Microsoft Windows XP

Table 8: Access Assurance Suite with DIRECT! Credential Provider Access Option

Client	A PC with Microsoft Windows Vista, Windows 7, Windows 8, Windows 8.1 or Windows 10

Product-Specific Database Server Requirements

The components of the Access Assurance Suite may have specific database requirements as detailed in Table 9 **.**

Table 9: Product-Specific Database Server Requirements (Sheet 1 of 2)

Core Provisioning™ Solution	Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2014 / 2016 (either Standard, Enterprise or Data Center) is required to use Requester/Approver functionality, and Delegation functionality. The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS.
Core Compliance™ Solution	Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2014 / 2016 (either Standard, Enterprise or Data Center) is required for the Verify action and to use Requester/Approver functionality, and Delegation functionality. The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS. **Note**: The Continuous Policy Monitoring and Governance feature requires the use of the Access Insight (AI). Please refer to the manual *Installing the Access Insight Solution.*
RoleCourier® Role Management Solution	Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2014 / 2016 (either Standard, Enterprise or Data Center) is required to store role definitions and to use Requester/Approver functionality, and Delegation functionality. The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS.
Core Password® Solution	Microsoft SQL Server 2008 / 2008 R2 / 2012 /2014 / 2016 (either Standard, Enterprise or Data Center) is required to use Requester/Approver functionality, Delegation functionality, and Password History. The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS.
ProfileCourier® Profile Management Solution	Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2014 / 2016 (either Standard, Enterprise or Data Center) is required to use Requester/Approver functionality, and Delegation functionality. The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS.
Core Access Solution (**Access Assurance Portal Applications** **Access Request Manager™ Solution** **Identity Mapping™ Solution)**	Microsoft SQL Server 2008 / 2008 R2 / 2012 / 2014 / 2016 (either Standard, Enterprise or Data Center). The SQL Server Collation must be set to SQL_Latin1_General_CP1_CI_AS. **Note:** Core Security recommends Microsoft SQL Server 2016 for new installations.

Table 9: Product-Specific Database Server Requirements (Sheet 2 of 2)

PasswordCourier and PasswordCourier Support Staff Classic	No additional server requirements
ProfileCourier Classic	No additional server requirements

For requirements that are specific to the Access Intelligence Engine or the Access Insight Solution, refer to the manual *Installing the Access Intelligence Engine or the Access Insight Solution*.

Microsoft SQL Server

Core Security strongly recommends that Microsoft SQL Server be installed on a separate machine from the one used for the Access Assurance Suite server.

The requirements in Table 10 assume that the Microsoft SQL Server is dedicated for use by the Access Assurance Suite. If the SQL Server is shared with other applications, please adjust the memory, CPU, and disk space requirements specified in Table 10 accordingly.

Table 10: Microsoft SQL Server Requirements

4 GB of memory (8+ GB recommended)
2.0 GHz processing speed (2.70+ recommended)
Minimum of 2 CPUs (4+ CPUs recommended)
200 GB drive (minimum)

Note: If you install SQL Server on the same machine as the Access Assurance Suite, please adjust the memory, CPU, and disk space requirements accordingly.

XML Access Option

The SPML Automator supports the following SPML 1.0 and 2.0 standards:

- addRequest
- modifyRequest
- deleteRequest
- extendedRequest
- operationalAttributes

The Transparent Synchronization Listener

The Transparent Synchronization Listener runs on each domain controller in any domain where you want to detect password changes and use Transparent Synchronization to synchronize your targets.

Table 11 shows the requirements for the Transparent Sycnhronization Listener on the Domain Controller:

Table 11: Requirements for the Transparent Synchronization Listener

4 GB of memory (8+ GB recommended)
2.0 GHz processing speed (2.70+ recommended)
Minimum of 2 CPUs (4+ CPUs recommended)
200 GB drive (minimum)

Ticketing (Audit) and Authentication on the Classic Platform

PasswordCourier Classic, PasswordCourier Support Staff Classic, and ProfileCourier Classic

See the manual *Using PasswordCourier and PasswordCourier Support Staff Classic* and *Using ProfileCourier Classic* for information about how to configure these applications on the classic platform.

Table 12: Supported Data Sources for PasswordCourier Classic and ProfileCourier Classic Authentication

Help Desks	BMC Remedy Action Request System 3.0
Directories	Sun Java System Directory Server 5.2 Sun ONESystem Directory Server 5 iPlanet™ Directory Server 5.0 Netscape Directory Server 4.11
	Microsoft Windows 2000 Server
	Novell eDirectory™ 8.6.0
Databases	Microsoft SQL Server 2008 with appropriate ODBC driver Microsoft SQL Server 2008 R2 with appropriate ODBC driver Microsoft SQL Server 2012 with appropriate ODBC driver Microsoft SQL Server 2014 with appropriate ODBC driver Microsoft SQL Server 2016 with appropriate ODBC driver
	Oracle8i with appropriate ODBC driver and Required Supported Files (RSF) Oracle9i with appropriate ODBC driver and Required Supported Files (RSF) Oracle Database 10*g* with appropriate ODBC driver and Required Supported Files (RSF) Oracle Database 11i*g* with appropriate ODBC driver and Required Supported Files (RSF)
	Sybase Adaptive Server 11.9.2 with appropriate ODBC driver

Table 13: Supported Data Sources for PasswordCourier Classic and ProfileCourier Classic Ticketing

Help Desks	HP OpenView ServiceCenter (previously known as Peregrine ServiceCenter) 3.0 Service Pack 2b - 4.01
	BMC Remedy Action Request System 3.0
Databases	Microsoft SQL Server 2008 with appropriate ODBC driver Microsoft SQL Server 2008 R2 with appropriate ODBC driver Microsoft SQL Server 2012 with appropriate ODBC driver Microsoft SQL Server 2014 with appropriate ODBC driver Microsoft SQL Server 2016 with appropriate ODBC driver
	Oracle8i with appropriate ODBC driver and Required Supported Files (RSF) Oracle9i with appropriate ODBC driver and Required Supported Files (RSF) Oracle Database 10*g* with appropriate ODBC driver and Required Supported Files (RSF) Oracle Database 11i*g* with appropriate ODBC driver and Required Supported Files (RSF)
	Sybase Adaptive Server 11.9.2 with appropriate ODBC driver

Index