CA SiteMinder®

Agent for SharePoint Guide

r12.0 SP3 for SharePoint 2010

Third Edition

CA Technologies Product References

This document references the following CA Technologies products:

- SiteMinder®
- [assign the value for dlp in your book] Content classification service

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction

This section contains the following topics:

Purpose and Audience

The SiteMinder Agent for SharePoint is a gateway or a proxy server-based solution that lets you protect resources in your Microsoft SharePoint environment with SiteMinder.

This guide describes how to install and configure the SiteMinder Agent for SharePoint so you can protect resources stored on SharePoint. This guide is intended for the following SiteMinder and SharePoint personnel:

- SharePoint Administrators
- SiteMinder Administrators

This guide assumes that SharePoint administrators can perform the following tasks:

- Create a SharePoint web application
- Add SharePoint web applications to site collections
- Manage SharePoint site collection administrators
- Work with web application access policies in SharePoint
- Add, modify, or remove files or other content to a SharePoint web application
- Manage SharePoint users and user profiles

This guide assumes that SiteMinder administrators can perform the following tasks:

- Install and configure SiteMinder Agent for SharePoint and Policy Servers
- Create SiteMinder policies, realms, rules, and responses to protect resources
- Manage SiteMinder user directories

New Architecture to Support SharePoint 2010

The SiteMinder Agent for SharePoint 2010 features a new architecture designed to protect your SharePoint 2010 resources. This new architecture is based on industry standards and uses a proxy model to streamline enterprise deployments of the Agent for SharePoint, while supporting future growth.

This agent also includes a new SharePoint connection wizard which simplifies the process of creating connections between your SiteMinder objects and SharePoint resources. This wizard creates the SiteMinder objects you need on the Policy Server and generates a PowerShell script that properly configures your SharePoint central administration server.

Major Differences between Agent for SharePoint Releases

The following table describes the major differences between the Agent for SharePoint releases:

Agent for SharePoint 2007	**Agent for SharePoint 2010**
Required installation of the following on each SharePoint 2007 server: ■ A SiteMinder Web Agent ■ A SiteMinder Agent for SharePoint	Deployed as a proxy-server based solution in front of SharePoint 2010 for more centralized configuration and management.
Used one of two SharePoint 2007 authentication methods: ■ Windows Impersonation ■ ASP.NET Forms-based authentication (FBA)	Uses the new SharePoint 2010 claims-based authentication option, which is based on industry-standard protocols (WS-Federation / SAML 1.1).
Used a SiteMinder Management UI, installed into SharePoint, to configure protection of SharePoint resources. Included a Role and Membership Provider to facilitate People Picker access to SiteMinder user directories.	Configuration and administration enhancements include: ■ New Connection Wizard to automate the configuration of required SiteMinder objects and simplify the creation of a Trusted Identity Provider inside SharePoint 2010. ■ Farm-wide configuration of various aspects of the SiteMinder integration using the new SharePoint 2010 PowerShell interface. ■ Improved People Picker usability through a new Claims Provider component.

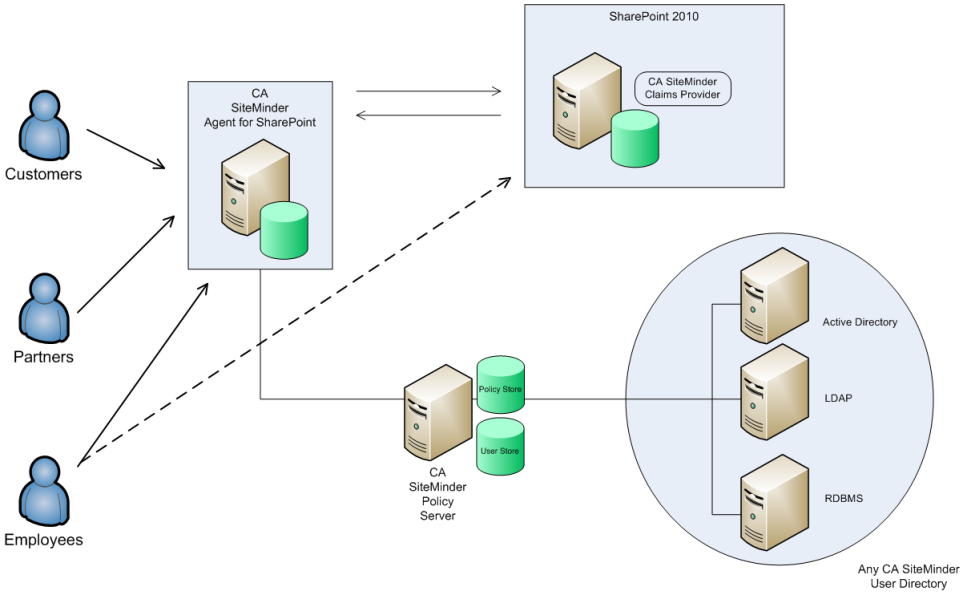
SiteMinder and Microsoft SharePoint

The SiteMinder Agent for SharePoint integrates Microsoft SharePoint 2010 into the SiteMinder web access management environment.

An access control solution uses policy decision points and policy enforcement points. The SiteMinder Agent for SharePoint uses a gateway or proxy server policy enforcement point to protect resources in a Microsoft SharePoint environment. In the network topology, these enforcement points are physically placed between the user and the resource on SharePoint server.

SiteMinder Agent for SharePoint Components and Microsoft SharePoint

The following illustration shows the relationship between the SiteMinder components and the SharePoint server.



In the previous illustration, customers, partners, and employees request resources from SharePoint. The requests must pass through the SiteMinder Agent for SharePoint. The agent provides authentication, policy enforcement, and federated single sign-on capabilities. The SiteMinder Policy Server acts as the policy decision point for authentication. The SiteMinder Policy Store which is connected to the Policy Server stores policies and other configuration objects. This solution enables external users to access protected SharePoint resources and internal users to access SharePoint resources.

SiteMinder Components used with SharePoint

The SiteMinder Agent for SharePoint solution contains the following SiteMinder components in a specific configuration designed to protect SharePoint resources.

Policy Server

The Policy Server acts as the Policy Decision Point (PDP). The Policy Server evaluates and enforces access control policies, for requests made to resources protected by agents, such as the SiteMinder Agent for SharePoint.

Agent for SharePoint

The Agent for SharePoint is a stand-alone server that provides a proxy-based solution for access control. The agent acts as the policy enforcement point (PEP), standing in the network topology physically between the user and the resource on the SharePoint server.

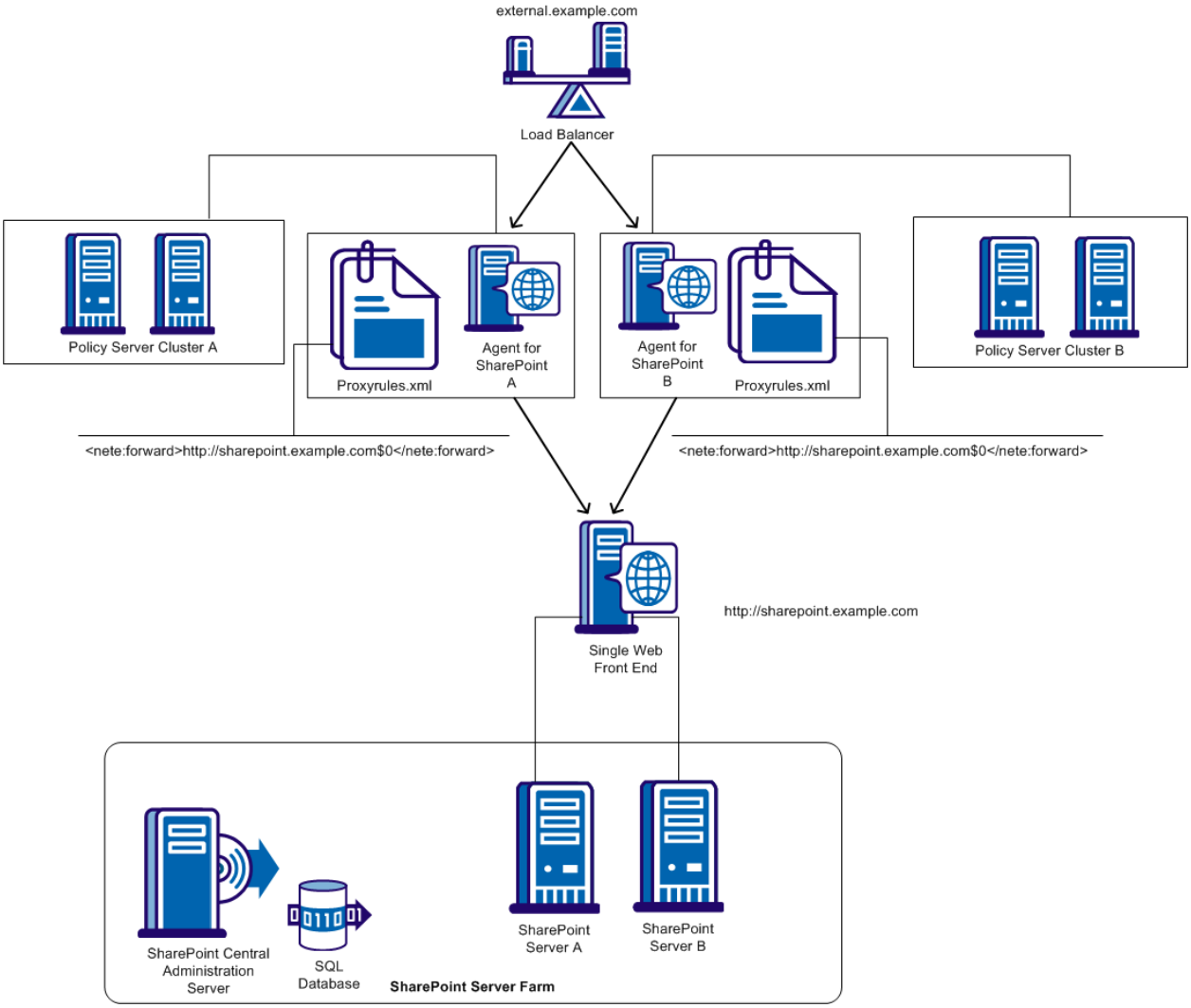
Claims Provider

The SiteMinder Claims Provider is used for configuring particular claim values to grant permissions to SharePoint resources. The Claims Provider is packaged as a SharePoint solution (WSP file) with its feature receiver.

Note: Upgrade any SiteMinder components in your environment that do not meet the minimum versions.

Example SharePoint Farm Deployment with Single Web Front End

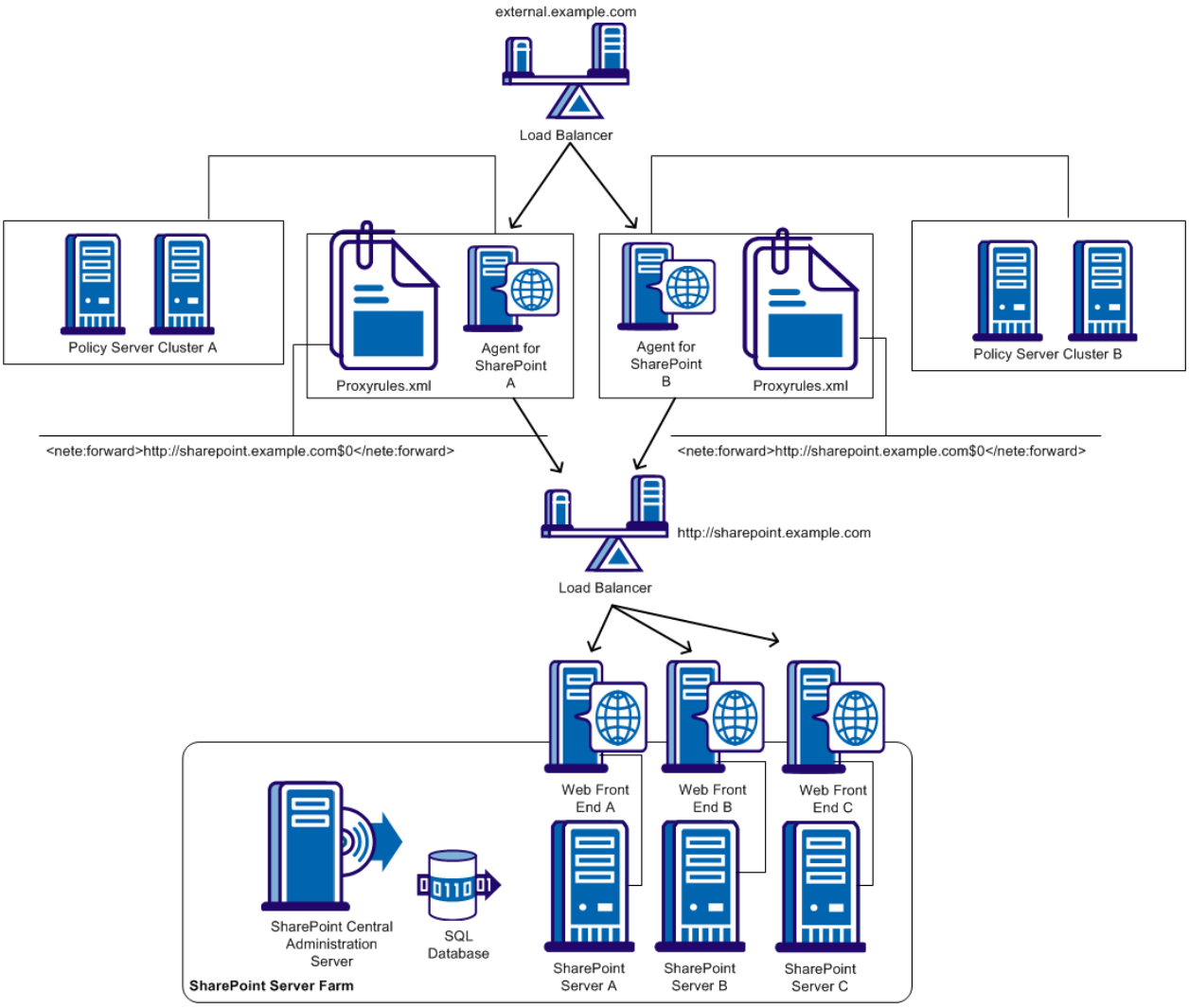
If the servers in your SharePoint farm are associated with a single web front end (WFE) server, the following illustration provides one possible deployment scenario:



In the previous example, your setting in the proxyrules.xml file is <nete:forward>http://sharepoint.example.com$0</nete:forward>

Example SharePoint Farm Deployment with Multiple Web Front Ends and Load Balancing

If your SharePoint farm has servers associated with a multiple web front end (WFE) servers, the following illustration provides one possible deployment scenario:



In the previous example, your setting in the proxyrules.xml file is <nete:forward>http://sharepoint.example.com$0</nete:forward>

Load Balancers and Session Affinity

Load balancers that use session affinity dynamically select the best-performing server to when establishing a session. The load balancers send subsequent requests for the same session back to the same server.

Configuring session affinity helps your load balancers operate more efficiently because the SiteMinder caches are used to their full potential. For example, sessions are stored in the Web Agent cache when they are created. Since the session is cached, subsequent requests for resources during the same session are validated using the information from the Web Agent cache. The Policy Server is not contacted, and efficiency is increased.

Chapter 2: Federation and Claims-based Authentication

Enterprise applications and services are increasingly distributed across organizations. They have customers and partners who reside outside of the enterprise that need access to SharePoint applications within the enterprise. As a result, the need for secure but seamless access to SharePoint resources has increased.

SiteMinder Agent for SharePoint lets you protect your SharePoint resources using SiteMinder web access management capabilities. The federation capabilities allow partnering organizations to trust and share digital identities and attributes of employees, customers, and suppliers across trust domains. These trust domains can exist within one organization or between different organizations.

These federation capabilities also provide single sign-on across partner sites. The Agent for SharePoint provides a custom SiteMinder solution which issues claims and packages claims into security tokens, used to validate and access SharePoint resources.

The following section gives an overview about federation and claims-based authentication used in this solution.

Claims-based Authentication Overview

Claims-based authentication enables applications to authenticate users with the minimum required information. Claims-based authentication allows applications to verify and validate user claims.

The following list explains the fundamental concepts of Claims-based authentication:

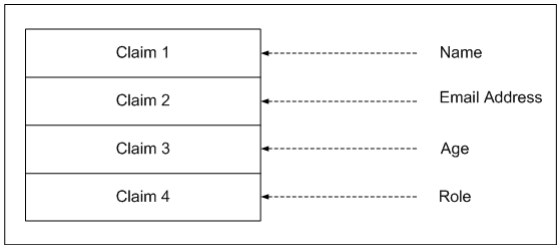
- Claims
- Tokens
- Security Token Service (STS)
- Identity Provider (IdP)
- Claims Provider

Claims

Claims represent any identity information about a user. In some instances, the user can be an application or a computer. A claim enables the user to gain access to multiple resources, such as applications and network resources, without entering credentials multiple times.

A claim is a statement about a user (for example, a name). The bits of identity information include, name, e-mail address, age, or organizational roles and responsibilities. A claim can also include the right of a user to perform something like access a file. Claims can also contain a restrictive right like the financial limit of a user.

A claim is given one or more values and then packaged in security tokens issued by a security token service (STS).



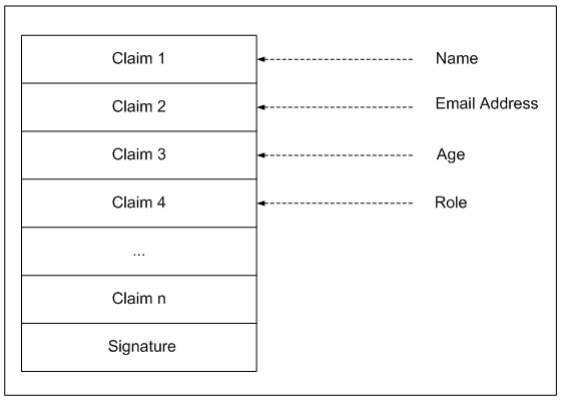
The previous illustration represents a claims token. The illustration shows claim values inside the token.

Tokens

Claims information is transferred in security tokens. Each token contains a set of one or more claims, and contains information about the user to whom this token applies. A security token service (STS) issues the token.

Tokens can be issued in different formats, such as Security Assertion Markup Language (SAML) tokens or WS-Federation (WS-FED) tokens. Security tokens can be signed with an X.509 certificate to protect the contents of the token in transit. The application that receives the token validates it before using the claims.

The Agent for SharePoint uses WS-FED tokens and X.509 certificates to protect its content.



The previous illustration represents a security token. This token contains claim values and a digital signature.

Security Token Service (STS)

The STS (Security Token Service) is a web service that issues, manages, and validates security tokens. STS makes assertions based on the evidence that it trusts, whoever trusts it.

Identity Provider (IdP)

An identity provider is a system that creates, maintains, and manages identity information and asserts identities to other service providers within a federation. For example, a user Adam, has an email address of adam@example.com and authenticated to this domain using a password mechanism.

An identity provider is also known as a SAML authority, asserting party, trusted identity provider, or source site, and is often abbreviated as IdP.

In the SiteMinder Agent for SharePoint solution, the Agent for SharePoint is the IdP STS. The identity provider owns the STS and affirms the tokens created by the STS.

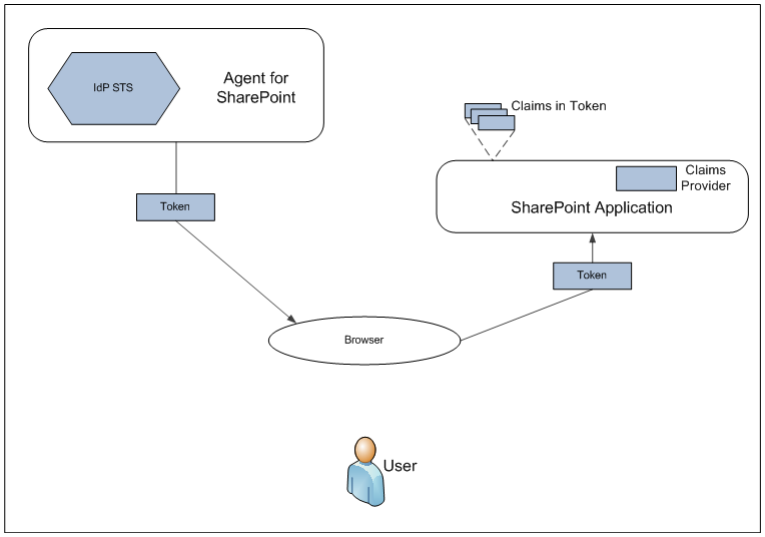
Claims Provider

A SiteMinder claims provider uses virtual attribute mappings in your SiteMinder directories to support searches of your SiteMinder users with the SharePoint people picker.

The claims provider finds and selects user, group, and role-based claim values.

Example Federation and Claims-based Authentication Scenario

The following illustration provides a possible federation and claims-based authentication scenario.



In the illustration, a SharePoint application works on behalf of a user, such as a web browser or another client. This SharePoint application asks an IdP-STS (Agent for SharePoint) for a token containing claims for this user. An HTTP protocol makes the request, the IdP-STS authenticates the user in some way, such as verifying the password of the user. Therefore, the IdP-STS can be certain that the user is authentic.

The request sent to an IdP-STS typically contains a URI identifying the SharePoint application this user wishes to access. The IdP-STS asserts the identity of the user and the application. Once the STS finds account information and other attributes about the user and the application, it generates the token and returns it to the browser.

How the SharePoint Connection Wizard Simplifies Deployment

This release of the Agent for SharePoint includes a connection wizard that automatically creates the Federation objects it requires on your CA SiteMinder Policy Server. The connection wizard also creates a PowerShell script that you modify and run on your SharePoint central administration server. This PowerShell script creates the Trusted Identity provider (IdP).

Chapter 3: Migrating from SharePoint 2007 to SharePoint 2010

This section contains the following topics:

Upgrades to the SiteMinder Agent for SharePoint

No direct upgrade path exists for moving from the SiteMinder Agent for SharePoint with SharePoint 2007 to the SiteMinder Agent for SharePoint with SharePoint 2010. As discussed in the Overview chapter, the agent used with SharePoint 2010 uses a claims-based authentication model supported by SharePoint 2010. The previous agent for use with SharePoint 2007 used different authentication models.

How to Migrate the SiteMinder Agent for SharePoint from SharePoint 2007 to SharePoint 2010

Your organization decides to move from a SharePoint 2007 environment to a SharePoint 2010 environment. You can repurpose your SharePoint 2007 hardware when you migrate to SharePoint 2010. If you decide to do so, consider the steps outlined in this topic.

To migrate the SiteMinder Agent for SharePoint from SharePoint 2007 to SharePoint 2010 complete, the following steps:

1. Uninstall the SiteMinder Agent for SharePoint running on the SharePoint 2007 system. The uninstall procedure is documented in the CA SiteMinder Agent for Microsoft SharePoint Guide r12.0.
2. Upgrade the SharePoint environment to SharePoint 2010.
3. Install the SiteMinder Agent for SharePoint r12.0 SP3 as described in this guide.

Note: You may be able to reuse some of the sites from your SharePoint 2007 deployment in your SharePoint 2010 deployment. See Microsoft.com and SharePoint 2010 documentation for SharePoint migration recommendations, including the migration of existing user identities to the claims format.

Chapter 4: Prerequisites

This section contains the following topics:

Policy Server Prerequisites

The SiteMinder Policy Server requires the following prerequisites to operate with the Agent for SharePoint:

- *One* of the following SiteMinder Policy Server releases:
  - r12 SP3 CR05 (SharePoint 2010 support) build 443.
  - r12 SP3 CR06.
  - Any subsequent CR release.

  Download this Policy Server build (or any CR release), in the CA SiteMinder Hotfix/Cumulative Release Index page at https://support.ca.com/irj/portal/anonymous/phpdocs?filePath=0/5262/5262_fixindex.html
- SiteMinder Administrative UI r12.0 SP3 (any CR)
- SharePoint2010DefaultSettings ACO Template
- (For Office Client Integration) HTTP methods for WebDAV defined in the SiteMinder Agent type
- An smkeydatabase
- An SSL Certificate
- The following open ports:
  - Ports for accounting, authentication, and authorization requests (44441, 44442, 44443 respectively)
  - Port for Connection Wizard (44444)
  - Ports for directory server connections.

Agent for SharePoint Prerequisites

Release r12.0 SP3 of the Agent for SharePoint is the minimum version required.

The Agent for SharePoint also requires the following:

- A 32-bit Java Development Kit version 1.6.0_16 or higher is required on the SiteMinder Agent for SharePoint system.

  Important! The Agent for SharePoint cannot be installed on a computer that hosts any other web server. The Agent for SharePoint operates as a stand-alone proxy-based solution.

- Open the following ports on the Agent for SharePoint:
  - Port 8009 (ajp13)
  - Port 8005 (Tomcat shutdown)
  - Port for HTTP requests on the embedded Apache web server
  - Port for HTTPS requests on the embedded Apache web server
  - Port for HTTP requests by the Claims search service
  - Port for HTTPS requests by the Claims search service

Agent for SharePoint Prerequisites for Linux Operating Environments

If you want to install your Agent for SharePoint on a Linux operating environment, verify that your computer meets the following prerequisites:

- Required Linux patches (see page 31).
- Required Linux libraries (see page 31).
- Required Linux tools (see page 31).

More information:

Registration Failed with Unknown Error 127 (see page 226)

Required Linux Patches

The following Linux patches are required:

For Linux release 2.1

glibc-2.4.2-32.20 for Linux Application Server 2.1

For Web Agents running on 64-bit Linux systems

- Binutils 2.17
- GCC 4.1.0

Required Linux Libraries

If you are installing or upgrading a Linux version of this component, the following is required on the host system:

`compat–libstdc++–33.3.2.3–`*`patch_version`*`.i386.rpm`

Install this rpm to be sure that you have the appropriate 32-bit C run–time library for your operating system.

Linux Tools Required

Before installing a SiteMinder Web Agent on a Red Hat Apache 2.2 web server running on the Red Hat Enterprise Linux operating environment, install all the items included in the Red Hat Legacy Software Development tools package.

Microsoft Prerequisites

The SiteMinder Agent for SharePoint is designed for Microsoft SharePoint 2010.

Verify that your SharePoint servers have the following prerequisites:

- (For Office Client Integration) use Office 2007 SP2 or higher.
- Open Ports for your SharePoint resources (set during SharePoint installation or configuration)

Note: For more information about specific patches or service packs, and the latest version information, see the Platform Support Matrix.

More information:

Locate the SiteMinder Agent for SharePoint Platform Support Matrix (see page 249)

Verify SharePoint Installation

Use the following process to verify that SharePoint is installed correctly before configuring SharePoint with the SiteMinder Agent for SharePoint.

Follow these steps:

1. Log on to SharePoint 2010 Central Administration and create a SharePoint site with any template.

   Note: Verify that the Windows user has administrator privileges.

2. Log on to the newly created SharePoint site.
3. Perform various actions like uploading documents and adding contacts.

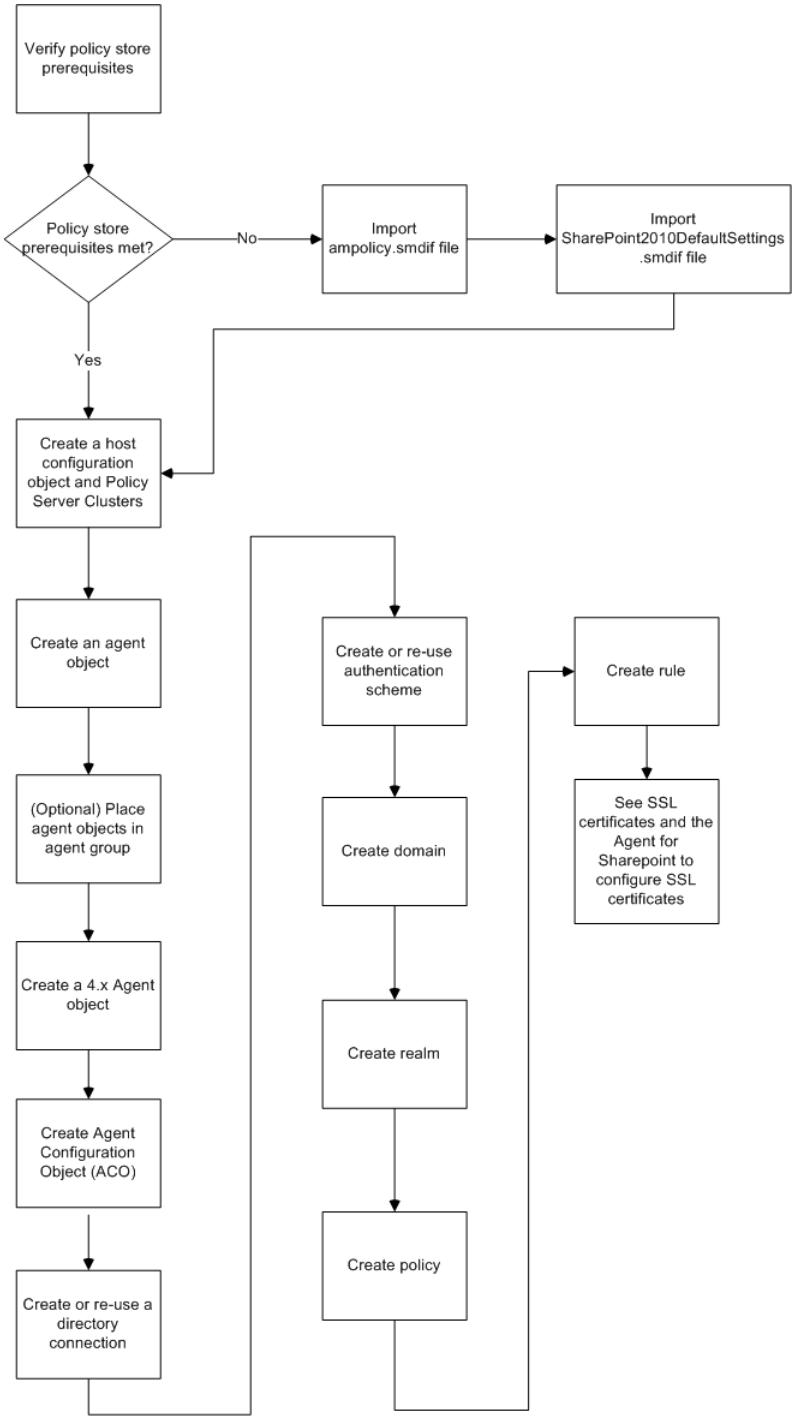
Chapter 5: Configure r12.0 SP3 Policy Server for the Agent for SharePoint

This section contains the following topics:

Policy Server Configuration Overview

The Policy Server authenticates users to your SharePoint environment. The Policy Server stores items you create to define the users in your SharePoint environment and the resources that you want to protect with SiteMinder.

The following illustration describes the tasks you perform to configure the Policy Server for use with the Agent for SharePoint:


Verify policy store prerequisites
Policy store prerequisites met?
No
Import ampolicy.smdif file
Import SharePoint2010DefaultSettings .smdif file
Yes
Create a host configuration object and Policy Server Clusters
Create an agent object
(Optional) Place agent objects in agent group
Create a 4.x Agent object
Create Agent Configuration Object (ACO)
Create or re-use a directory connection
Create or re-use authentication scheme
Create domain
Create realm
Create policy
Create rule
See SSL certificates and the Agent for Sharepoint to configure SSL certificates

How to Configure the r12.0 SP3 Policy Server

Configuring the r12.0 SP3 Policy Server for use with the Agent for SharePoint involves several separate procedures. To configure the Policy Server, perform the following steps:

1. Verify that proper policy store prerequisites exist for the Agent for SharePoint (see page 37).
    a. Import the ampolicy.smdif file to create policy store objects for the Agent for SharePoint (see page 37).
    b. Import the SharePoint2010DefaultSettings.smdif to create an ACO template for the Agent for SharePoint (see page 38).
2. Create a Host Configuration Object and Policy Server Clusters (see page 39).
3. Create an agent object (see page 40).
4. (Optional) Place agent objects in agent groups (see page 41).
5. Create a 4.x agent object for the SharePoint connection wizard (see page 42).
6. Create an agent configuration object (ACO) for the Agent for SharePoint (see page 43).
7. Create or modify a user directory connection (see page 47).
8. Create or reuse an authentication scheme (see page 49).
9. Create domain (see page 50).
10. Create realm (see page 52).
11. Create rule (see page 54)
12. Create policy (see page 55).

Verify that Proper Policy Store Prerequisites Exist for the Agent for SharePoint

To use an existing Policy Server for your SiteMinder Agent for SharePoint, verify that a domain named "FederationWebServicesDomain" exists on each Policy Server.

The FederationWebServicesDomain provide functions for the Agent for SharePoint.

Follow these steps:

1. Open the Administrative UI.
2. Verify that the domain object exists by doing the following steps:
3. Click the Policies tab.
4. Click Domains, Domain, View Domain.

   A list of domains appears.
5. Verify that a domain with the following name appears in the list:

   `FederationWebServicesDomain`
6. If a domain with the previous name does not appear in the list, import the ampolicy.smdif file to all your Policy Servers (see page 37). If the domain appears in the list, the domain prerequisite is met.

   The prerequisite for the policy store is verified.

Import the ampolicy.smdif File to Create Policy Store Objects for the Agent for SharePoint

If your policy store failed to meet the prerequisites for the Agent for SharePoint, import the ampolicy.smdif file to upgrade your policy store. This procedure is only required when you are upgrading an existing Policy Server to use the Agent for SharePoint.

Note: If you have installed the Policy Server in FIPS-only mode, use the **-cf** argument when importing the default policy store objects.

Follow these steps:

1. Run the following command:

   ```
   smobjimport -ipolicy_server_home\db\smdif\ampolicy.smdif
   -dsiteminder_super_user_name -wsiteminder_super_user_password -v -l -c
   ```

   policy_server_home

   Specifies the Policy Server installation path.

   -d*siteminder_super_user_name*

   Specifies the name of the SiteMinder administrator (superuser) account.

   -w*siteminder_super_user_password*

   Specifies the password for the SiteMinder superuser account.

-v

Outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

The policy store objects are automatically imported to the appropriate locations.

Import the SharePoint2010DefaultSettings.smdif to create an ACO template for the Agent for SharePoint

Import the SharePoint2010DefaultSettings.smdif file to upgrade your policy store. This procedure is required when installing a new Policy Server or upgrading an existing Policy Server to use the Agent for SharePoint.

Note: If you have installed the Policy Server in FIPS-only mode, use the -**cf** argument when importing the default policy store objects.

Follow these steps:

1. Run the following command:

```
smobjimport -ipolicy_server_home\db\smdif\SharePoint2010DefaultSettings.smdif
-dsiteminder_super_user_name -wsiteminder_super_user_password -v -l -c
```

policy_server_home

Specifies the Policy Server installation path.

-d*siteminder_super_user_name*

Specifies the name of the SiteMinder administrator (superuser) account.

-w*siteminder_super_user_password*

Specifies the password for the SiteMinder superuser account.

-v

Outputs error, warning, and comment messages in verbose format so that you can monitor the status of the import.

-l

Creates a log file.

-c

Indicates that the smdif input file contains unencrypted data.

The policy store objects are automatically imported to the appropriate locations.

Create a Host Configuration Object and Policy Server Clusters

A host configuration object (HCO) is a configuration object in the Policy Store. The HCO defines the communication settings used by the Agent for SharePoint during an initial connection to a Policy Server. The agent also requires the name of the HCO during the configuration process.

Multiple Policy Servers can function as a cluster to provide load-balancing and high-availability. We recommend deploying Policy Server clusters in your environment.

Follow these steps:

1. Click Infrastructure, Hosts.
2. Click Host Configuration, Create Host Configuration.
3. Click Create a copy of an object of type Host Configuration, and then click OK.

   The Create Host Configuration: Dialog appears.
4. Select DefaultHostSettings template and click OK.

   Important! Do not directly modify and use the DefaultHostSettings object. Always copy this object and then modify it.

   The Create Host Configuration: Copy of DefaultHostSettings page appears.
5. Type the name and a description of the Host Configuration object.
6. Under Configuration Values, specify the Host Configuration settings in the fields.
7. Under Clusters, click Add.

   The Add Cluster dialog opens.
8. Type the IP address and port number of the Policy Server that you are adding to the cluster in the Host and Port fields, respectively.

   Note: To add another Policy Server to the cluster, click Add to Cluster. To delete a Policy Server from the cluster, click the minus sign to its right. To change the sequence of Policy Servers in the cluster, click the up and down arrows.
9. Click OK.

   The cluster is added.

   Note: To modify a cluster, click the right-facing arrow to its left. To delete a cluster, click the minus sign to its right. To add another cluster, click Add, and repeat Steps 7 and 8.
10. Enter a percentage in the Failover Threshold Percent field.

    Note: If the percentage of active servers in a cluster falls below the specified percentage, the cluster fails over to the next available cluster listed.

11. Click Submit.

    The Create Host Configuration task is submitted for processing.

    Important! The Configuration values section specifies a single Policy Server and a simple failover operation used only when no clusters are specified in the Clusters section. If you decide to delete all clusters in favor of a simple failover operation, delete all the Policy Servers from the Clusters section.

Create Agent Object

An agent acts as the policy enforcement point (PEP), by intercepting user requests for SharePoint resources and communicating with the Policy Server. An agent object associates the protected resources on web servers with the SiteMinder policies that protect those resources.

The following agent objects are required:

- An agent object that protects resources (described in the following steps)
- An agent object that supports SiteMinder 4.x functionality (for the SharePoint connection wizard) (see page 42).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.

   The relevant tabs for your administrator privileges appear.

2. Click Infrastructure, Agents, Agent, Create Agent.

   The Create Agent dialog appears.

3. Select Create a new object of type Agent, and then click OK.

   The Create Agent: Dialog appears.

4. Enter a name and an optional description.

   Note: Use a name that you can easily associate with the corresponding SharePoint resources.

5. Select SiteMinder.

6. Select Web Agent from the drop-down list.

7. Click Submit.

   The Create Agent Object task is submitted for processing and the confirmation message appears.

Note: For more information about agent objects, see the *SiteMinder Policy Server Configuration Guide.*

Place your Agent Objects in Agent Groups

Use agent groups if you have many agent objects to simplify administration. Several agent objects can be added or removed from a policy simultaneously. For example, if you have multiple SharePoint and Agent for SharePoint servers then you can create agent groups for different categories and resources. This section describes how to create agent groups, but if you are an experienced SiteMinder user, you can use existing agent groups instead.

Follow these steps

1. Log on to the SiteMinder Administrative UI.

   The relevant tabs for your administrator privileges appear.

2. Click Infrastructure, Agents, Agent Group, Create Agent Group.

   The Create Agent Group pane opens.

3. Click Create a new object of type Agent Group, and then click OK.

   The Create Agent Group: Dialog appears.

   Note: Click Help for descriptions of setting and controls, including their respective requirements and limits.

4. Enter a name and an optional description.
5. Select SiteMinder.
6. Select Web Agent from the drop-down list.
7. Click Add/Remove

   The Agent Group Members dialog appears.

8. Add the Agent Objects you want to the group, and then click OK.

   The Agent Group Members dialog closes and the Create Agent Group dialog appears.

9. Click Submit.

   The Create Agent Group task is submitted for processing and the confirmation message appears.

Note: For more information about agent groups, see the *SiteMinder Policy Server Configuration Guide*.

Create a 4.x Agent Object for the SharePoint Connection Wizard

The following agent objects are required:

- An agent object that protects resources (see page 40).
- An agent object that supports SiteMinder 4.x functionality (described in the following steps).

The SharePoint connection wizard requires an agent object that supports SiteMinder 4.x functionality. Define this agent object on your Policy Servers.

Important: Do not add the 4.x agent object to any agent group, realm, or policy. This agent object exists only to support the internal operations of the Agent for SharePoint.

Follow these steps:

1. Log on to the SiteMinder Administrative UI.

   The relevant tabs for your administrator privileges appear.

2. Click Infrastructure, Agents, Agent, Create Agent.

   The Create Agent dialog appears.

3. Select Create a new object of type Agent, and then click OK.

   The Create Agent dialog appears.

4. Enter a name and an optional description.

   Note: Use a name that you can easily associate with the corresponding SharePoint Connection Wizard.

5. Select SiteMinder.
6. Select Web Agent from the drop-down list.
7. Enable 4.x functionality with the following steps:
   a. Select the Supports 4.x agents check box.

      The trust settings fields appear.

   b. Add the trust settings by completing the following fields:

      IP Address

      Specifies the IP Address of the Policy Server.

      Shared Secret

      Specifies a password that is associated with the 4.x Agent object. The SharePoint Connection Wizard also requires this password.

      Confirm Secret

      Confirms a password that is associated with the 4.x Agent object. The SharePoint Connection Wizard also requires confirmation of this password.
8. Click Submit.

   The Create Agent Object task is submitted for processing and the confirmation message appears.

Create an Agent Configuration Object

An embedded Apache web server is part of the Agent for SharePoint. An Agent Configuration Object (ACO) on the Policy Server contains configuration parameters that control the behavior of the agent running on the embedded web server.

Agents need values in certain parameters to start. For example, all agents need one value in either of the following parameters:

- AgentName
- DefaultAgentName

Other parameters control optional functions that you can set anytime. For example, if you decide to store agent logs on your web server, you can set those parameters later. Agents do not need values in logging parameters to start.

Note: For more information about other parameters in your ACO that are not listed here, see the SiteMinder *Web Agent Configuration Guide*.

Follow these steps:

1. Click Infrastructure, Agent Configuration, Create Agent Configuration.

   The Create Agent Configuration: Search pane opens.

2. Click the following buttons:

   - Create a copy of an object of type Agent Configuration.
   - SharePoint2010DefaultSettings.

   Important! Only copy the SharePoint2010DefaultSettings ACO object. Do not copy any other object in the list.

3. Click OK.

4. Type the name and a description for the agent configuration object.

5. If you have multiple virtual hosts and plan to assign different Agent identities to each virtual host, use the AgentName parameter. Use the DefaultAgentName parameter, if different Agent identities for virtual hosts are not required. Remove any # character in front of the parameter name, and then change the value of *one* of the following parameters (*not* both):

   AgentName

   Defines the identity of the web agent. This identity links the name and the IP address or FQDN of each web server instance hosting an Agent.

   The value of the DefaultAgentName is used instead of the AgentName parameter if any of the following events occur:

   - The AgentName parameter is disabled.
   - The value of AgentName parameter is empty.
   - The values of the AgentName parameter do *not* match any existing agent object.

   Note: This parameter can have more than one value. Use the multivalue option when setting this parameter in an Agent Configuration Object. For local configuration files, add each value to a separate line in the file.

   Default: No default

   Limit: Multiple values are allowed.

   Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. The value is not case-sensitive. For example, the names MyAgent and myagent are treated the same.

   Example: myagent1,192.168.0.0

   Example: myagent,www.example.com

DefaultAgentName

Defines a name that the agent uses to process requests. The value for DefaultAgentName is used for requests on an IP address or interface when no agent name value exists in the AgentName parameter.

If you are using virtual servers, you can set up your SiteMinder environment quickly by using a DefaultAgentName. Using DefaultAgentName means that you do not need to define a separate agent for each virtual server.

Important! If you do not specify a value for the DefaultAgentName parameter, then the value of the AgentName parameter requires every agent identity in its list. Otherwise, the Policy Server cannot tie policies to the agent.

Default: No default.

Limit: Multiple values are allowed.

Limits: Must contain 7-bit ASCII characters in the range of 32-127, and include one or more printable characters. Cannot contain the ampersand (&) and asterisk (*) characters. The value is not case-sensitive. For example, the names MyAgent and myagent are treated the same.

6. Change the value of the following parameter:

   LogOffUri

   Enables full logoff and displays a confirmation page after users are successfully logged off. Configure this page so that it *cannot* be stored in a browser cache. If no logoff occurs because a cached page is used, session hijacking by unauthorized users is possible.

   When SharePoint users click the Sign out link, the following URI is used:

   - /_layouts/SignOut.aspx

   When SharePoint users click the Sign in as another user link, the following URI is used:

   - /_layouts/accessdenied.aspx?loginasanotheruser=true

   If you have multiple SharePoint web sites below a top-level SharePoint website, add the URIs of the lower-level sites to the LogOffURI parameter.

   Note: When the CookiePath parameter is set, the value of the LogOffUri parameter must point to the same cookie path. For example, if the value of your CookiePath parameter is set to example.com, then your LogOffUri must point to example.com/logoff.html

   Default: /_layouts/SignOut.aspx, /_layouts/accessdenied.aspx?loginasanotheruser=true

   Limits: Multiple URI values permitted. Do *not* use a fully qualified URL. Use a relative URI.

   Example: (for a parent site of www.example.com with two lower-level sites named finance and hr respectively) /finance/_layouts/SignOut.aspx, finance/_layouts/accessdenied.aspx?loginasanotheruser=true /hr/_layouts/SignOut.aspx, /hr/_layouts/accessdenied.aspx?loginasanotheruser=true

7. Click OK.

   The new values appear next to the parameters in the list.

8. Click Submit.

   The Create Agent Configuration Task is submitted for processing and the confirmation message appears.

Create or Modify One User Directory Connection

The Policy Server communicates with an existing user directory to authenticate users. The user directory needs a connection defined in the SiteMinder Administrative UI. Create a connection for the directory that contains users who require access to SharePoint resources.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Note: The directory vendors that the Agent for SharePoint supports are limited to the directories SiteMinder supports. For more information about directories that SiteMinder supports, see the Platform Support Matrix at www.support.ca.com.

This section describes the procedure to create a user directory connection.

Follow these steps:

1. Log in to the SiteMinder Administrative UI.

   The relevant tabs for your administrator privileges appear.

2. Click Infrastructure, Directory, User Directory, Create User Directory.

   The Create User Directory pane appears.

3. Enter the Name and an optional description.

4. Select the Directory type from the Namespace list and complete the required connection information under the Directory Setup.

   Note: Enable paging support if you are using the Active Directory as the User Store. The Active Directory Namespace disables paging by default; enable paging support by setting the registry key to one. For more information, see the troubleshooting topic about enabling paging for searches of Active Directory User Stores (see page 222).

5. If your directory server requires credentials for searches, click the Require Credentials check box. Type the user name and password of an authorized account.

   Note: The Require Credentials setting is required for LDAP directories which support anonymous search. This setting supports queries that the SiteMinder Claims Provider makes to the user directory to support the SharePoint People Picker. For more information about these credentials, see the administrator of your directory server.

6. (Optional) Specify the user directory profile attributes that are SiteMinder reserves for its own use in the fields under User Attributes.
7. Click Submit.

   The Create User Directory task is submitted for processing, and the confirmation message appears.
8. Create a virtual attribute mapping for your user claim (see page 148).
9. (Optional) Create additional virtual attribute mappings for group claims (see page 152) or role claims (see page 155).
10. (Optional) Increase the size of the MaxUserAttributeLength setting so that the names of user groups are not truncated when they appear in the claims provider (see page 164).

Note: For more information about creating or modifying a user directory connection, see the *SiteMinder Policy Server Configuration Guide*.

More information:

Locate the SiteMinder Agent for SharePoint Platform Support Matrix (see page 249)

Create an Authentication Scheme for the Agent for SharePoint

SiteMinder uses authentication schemes to collect credentials and determine the identity of a user. During authentication, the agent communicates with the Policy Server to determine the proper credentials to retrieve from a user who is requesting resources.

If you are an experienced SiteMinder user, you can use an existing authentication scheme instead of creating one.

Follow these steps:

1. Click Infrastructure, Authentication, Authentication Schemes, Create Authentication Scheme.

   The Create Authentication Scheme pane appears.

2. Select Create a new object of type Authentication Scheme option, and then click OK.

   The Create Authentication Scheme: Pane appears.

3. Enter a distinctive name, and (optional) description.

4. Select the type of Authentication Scheme from the Authentication Scheme Type list.

   The options for your chosen Authentication Scheme appear.

5. Complete the fields for your Authentication Scheme.

6. Click Submit.

   The Create Authentication Scheme task is submitted for processing and the confirmation screen appears.

Default Location of FCC forms in Administrative UI does not Work

Symptom:

I tried to configure SiteMinder forms-based authentication (FCC), but when I use the following default value shown in the Administrative UI, it does not work:

```
/siteminderagent/forms/login.fcc
```

Solution:

The Agent for SharePoint uses a different directory for forms-based authentication. Do the following:

1. Create the siteminderagent directory in the following location:

   Agent-for-SharePoint_home/proxy-engine/examples/siteminderagent

2. Copy the forms folder from the following directory:

   Agent-for-SharePoint_home/proxy-engine/examples

   To the following directory:

   Agent-for-SharePoint_home/proxy-engine/examples/siteminderagent

   The forms are copied to *Agent-for-SharePoint_home*/proxy-engine/examples/siteminderagent/forms.

Create a Policy Domain

A policy domain is a logical grouping of resources associated with one or more user directories. Policy domains contain realms, rules, responses, and policies (and optionally, rule groups and response groups).

The resources in a policy domain can be grouped in one or more realms. Rules control access to resources, that are associated with the realm that contains the resource. By grouping realms and rules in a policy domain, you can provide a secure domain for your resources.

For example, on a SharePoint site, some resources require a higher level of security than other resources. Define a realm with a higher level of security than uses an authentication scheme such as a certificate-based scheme. Use a realm with basic authentication for the less sensitive resources. For example, a common set of users wants to access both types of resources. You can group both realms in the same policy domain.

Note: The Agent for SharePoint does not support the EPM application policy model. Create domains, realms, rules and policies instead.

Follow these steps:

1. Click Policies, Domains.
2. Click Domain, Create Domain.

   The Create Domain pane opens.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.
3. Type the name and a description of the policy domain.
4. Add User Directories and Realms (see page 52).
5. Click Submit.

   The Create Domain Task is submitted for processing.

Note: For more information about Policy Domains, see the *SiteMinder Policy Server Configuration Guide*.

Assign One User Directory

Add *one* user directory to a policy domain. The Policy Server authenticates users by comparing the credentials to the credentials that are stored in the user directory.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Follow these steps:

1. Under User Directories, click Add/Remove.

   The Choose user directories pane opens.
2. Select a user directory from the list of Available Members, and click the right-facing arrows.

   The user directory is removed from the list of Available Members and added to the list of Selected Members.
3. Click OK.

   The selected user directory is added to the domain.

   Note: To create a user directory and add it to the domain, click New... under User Directories.

Configure a Realm

Realms are groupings of resources in a specific location on your network. SiteMinder <agents> protect the resources in a realm. When users request resources within a realm, the associated Agent for SharePoint authenticates the user. The realm uses the authentication scheme you configured. The SharePoint server authorizes the user.

Because most SharePoint resources are URL-based, define the URLs of your SharePoint resources that you want to protect. Use the following examples as guides:

- http://intranet.example.com
- http://intranet.example.com/finance
- http://intranet.example.com/investors

We recommend creating few realms first during the following types of deployments:

- Testing or evaluation of the Agent for SharePoint
- Initial deployment in your enterprise.

Create a minimum set of realms or rules to enable the Agent for SharePoint to perform basic authentication. A SiteMinder administrator can create additional realms or rules as required. The following are the minimum realms required to enable Agent for SharePoint basic authentication:

- Create a realm to protect access to the authentication URL (/affwebservices/redirectjsp/redirect.jsp).
- Create a realm to allow access to the ClaimsWS (/ClaimsWS/services/WSSharePointClaimsServiceImpl).

  Note: If you intend to protect all resources using the /* rule, then create a realm to allow unprotected access to the ClaimsWS, in addition to the /* realm.

Follow these steps:

1. Click Policies, Domains.
2. Click Realm, Create Realm.

   The Create Realm: Select Domain pane appears.
3. Select the domain you created for your SharePoint resources from the Domain list, and then click Next.

   The Create Realm: Define Realm pane appears.
4. Complete the name and description fields.
5. Click the ellipsis option button.

   The Select an Agent screen appears.

6. Click the option button next to the Agent object you created for your SharePoint resources, and then click OK.

   Important: Do not add the 4.x agent object to any agent group, realm, or policy. This agent object exists only to support the internal operations of the Agent for SharePoint.

7. Click the Resource filter field, and then enter the URL of a SharePoint resource that you want to protect.

   Note: We recommend protecting only URLs on SharePoint systems, not lists, or specific documents.

8. Under rules, create new rules or delete existing rules.
9. Under Sub realms, create new sub realms or delete existing sub realms.
10. Under Session, specify the session properties.
11. Under Advanced, specify the following:
    - Registration schemes.
    - Authorization directory mappings.
    - Types of events you want the realm to process.
12. Click Finish.

    The Create Realm Task is submitted for processing.

Configure a Realm Protected by a SiteMinder Web Agent

You configure a realm to protect a group of resources that users access from a web server.

Note: The following procedure assumes that you are creating an object. You can also copy the properties of an existing object to create an object. For more information, see Duplicate Policy Server Objects.

Follow these steps:

1. Click Policies, Domains.
2. Click Realm, Create Realm.

   The Create Realm: Select Domain pane appears.

3. Select a domain from the Domain list, and click Next.

   The Create Realm: Define Realm pane appears.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.

4. Type the name and a description for the realm.

5. Click the ellipsis button in the Resource section.

   The Select an Agent dialog opens.

6. Select a SiteMinder Web Agent or Agent group, and click OK.
7. Specify the remaining resource properties in the Resource section.
8. Create new rules or delete existing rules.
9. Create new sub realms or delete existing sub realms in the Sub-Realms section.
10. Specify the session properties on the Session section.
11. Specify the registration schemes, authorization directory mappings, and types of events the realm must process in the Advanced section.
12. Click Finish.

    The Create Realm Task is submitted for processing.

Create a Rule for Web Agent Actions

You can create a rule that fires in response to specified Web agent actions. The rule allows or denies access to the resource it is protecting.

To create a rule

1. Click Policies, Domains.
2. Click Rule, Create Rule.

   The Create Rule: Select Domain pane opens.

3. Select a domain from the Domain list, and click Next.

   The Create Rule: Select Realm pane opens.

4. Select the realm that includes the resources that you want the rule to protect, and click Next.

   The Create Rule: Define Rule pane opens.

   Note: If a realm does not exist for the resources that you want to protect, a rule cannot be created to protect those resources.

5. Type the name and a description of the rule in the fields on the General group box.

   Note: Click Help for descriptions of settings and controls, including their respective requirements and limits.

6. Type the resource that you want the rule to protect in the Resource field.

   The Effective Resource updates to include the resource.

7. Specify whether the rules allow or deny access to the protected resource in the Allow/Deny and Enable/Disable sections.

8. Select the Web agent actions option button in the Action section.

   The Action List is populated with HTTP actions.

9. Select one or more HTTP actions from the Action list.
10. (Optional) Specify time restrictions, an active rule, or both in the Advanced section.
11. Click Finish.

    The Create Rule task is submitted for processing.

Create a Policy

You can create a policy by adding it to a new or existing domain. Policies define relationships between users and resources.

Follow these steps:

1. Click the Policies, Domains.
2. Click Domain, Modify Domain.

   The Modify Domain pane opens.

3. Specify search criteria, and click Search.

   A list of domains that match the search criteria opens.

4. Select a domain, and click Select.

   The Modify Domain: *Name* pane opens.

5. Click the Policies tab on the Domain pane.

   The Policies dialog opens.

6. Click Create.

   The Create Policy: *Name* pane opens.

7. Type the name and a description of the policy.
8. Click the Users tab.

   The User Directories dialog opens.

9. Add users, user groups, or both to the policy, and click OK.

   The Modify Domain: *Name* pane reopens.

10. Click Submit.

    The Modify Domain Task is submitted for processing.

Add Users to a Policy

You can add individual users, user groups, or both to a policy and can create a policy binding between the added users and the policy. When a user tries to access a protected resource, the policy verifies that the user is part of its policy binding. Then the policy fires the rules included in the policy to see if the user is allowed to access the resource.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Follow these steps:

1. Click Policies, Domains.

   The Domain pane appears.

2. Click Policy, Modify Policy.

   The Modify Policy page appears.

3. Select the policy to change from the search results and click Select.

   The Modify Policy:*Name* page appears.

4. Click the Users tab on the Policy pane.

   The User Directories pane opens and contains group boxes for each user directory that is associated with the policy domain.

5. Add users or groups from the user directory to the policy.

   In each user directory section, you can select Add Members, Add Entry, Add All. Depending on which method you use to add users to the policy, a dialog opens to let you add users.

   Note: If you select Add Members, the User/Groups pane opens. Individual users are not displayed automatically. Use the search utility to find a specific user within one of the directories.

   You can edit or delete a user or group by clicking the right arrow (>) or minus sign (-), respectively.

6. Select individual users, user groups, or both using whatever method and click OK.

   The User Directories pane reopens and lists the new users for the policy on the section of the user directory. The task of binding users to the policy is complete.

Add Rules to a Policy

Rules indicate the specific resources included in a policy and whether to allow or deny access to the resources when the rule fires. Responses indicate the actions you want to occur when the rule fires.

Note: Add at least one rule or rule group to a policy.

Follow these steps:

1. Click the Rules tab on the Policy pane.

   The Rules dialog opens.

2. Click Add Rule.

   The Available Rules pane opens.

3. Select the individual rules, rule groups, or both that you want to add to the policy, and click OK.

   The Rules section lists the added rules and groups.

4. (Optional) Associate the rule with a response or response group.

   Note: To remove a rule or rule group from a policy, click the minus sign (-) to the right of the rule on the Rules section. To create a rule, click New Rule on the Available Rules pane.

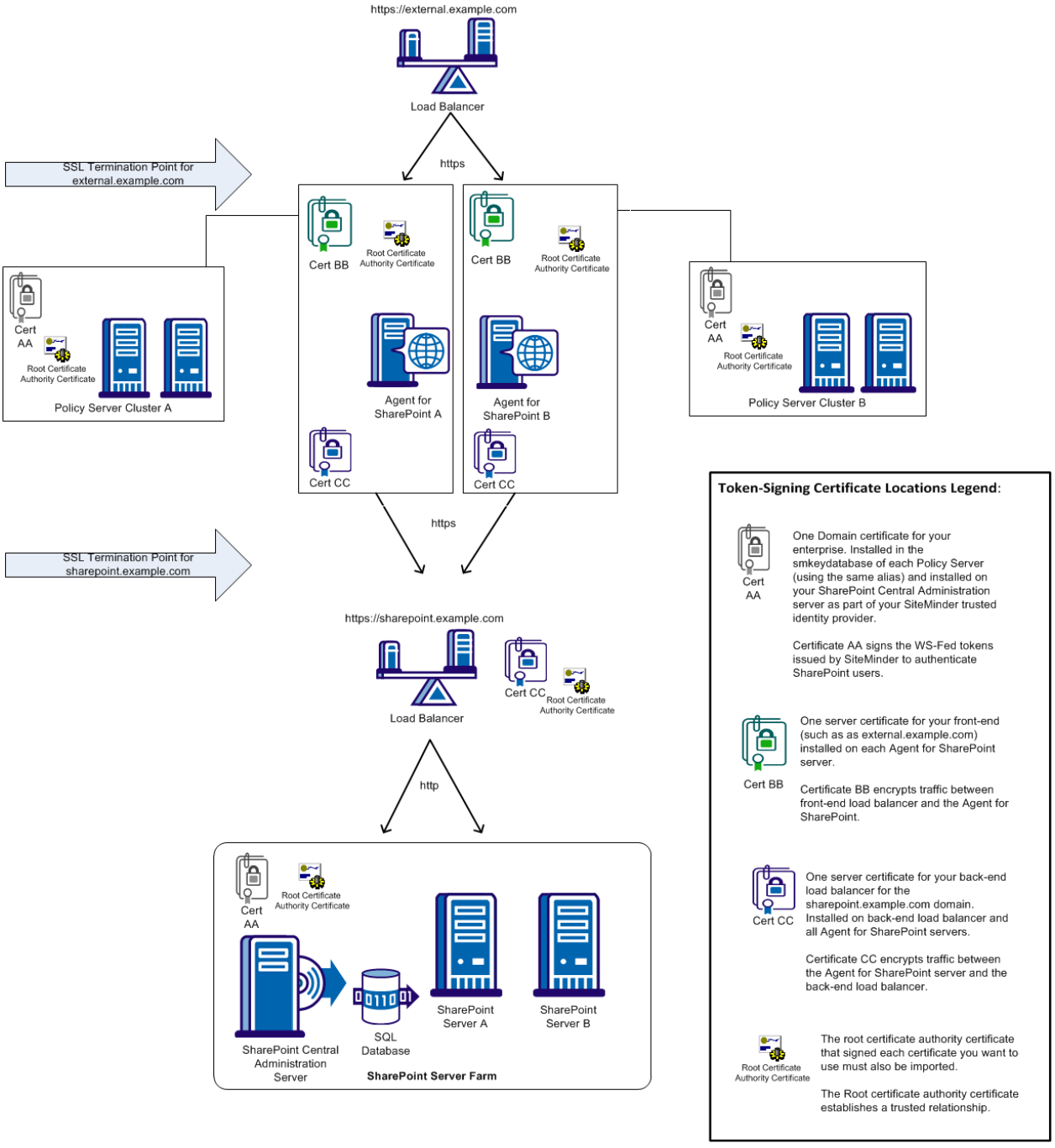
Chapter 6: Token-Signing Certificates Required by the Agent for SharePoint

This section contains the following topics:

Token–Signing Certificate Locations in Your SharePoint Environment

The Agent for SharePoint requires an SSL certificate to transmit the WS-Fed tokens from the Policy Server to the SharePoint server securely.

The following illustration shows the typical locations of the certificates which sign the (WS-Fed) tokens in your SharePoint environment:



How to Request and Install a Policy Server Certificate for the Agent for SharePoint

The Policy Server requires an SSL certificate to sign the WS-Fed token it sends to the SharePoint claims provider.

Requesting and installing a Policy Server signing certificate for the Agent for SharePoint involves several separate procedures. Use the following process as a guide to request and import your own Policy Server signing certificate:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. If you are using a self-signed certificate, start with Step 7.

   Important! Do not use self-signed certificates in production environments. We recommend using self-signed certificates in test environments only.

2. Create a certificate request for a server certificate on an IIS web server (see page 62).
3. Submit your server certificate request to the certificate authority (see page 63).
4. Wait for the Certificate Services administrator to approve your server certificate request (see page 64).
5. Verify your approval and download your server certificate and certificate chain (see page 65).
6. Complete your certificate request (using the same IIS web server and browser from Step 1) (see page 66).
7. Export your server certificate files to the computer hosting the Policy Server (see page 67).
8. Verify certificate support on Policy Servers (see page 68).
9. Configure certificate support on Policy servers (see page 69).
10. Add a certificate to Policy Servers and create a trust file (see page 69).
11. Install the certificate on the Agent for SharePoint system.
12. Install the trust certificate by configuring your identity provider (see page 104).

Create a Certificate Request for a Server Certificate on an IIS Web Server

Requesting a certificate is the first step in the process of creating a Policy Server signing certificate. Any IIS web server in your organization can request a certificate. Using an IIS web server hosted on your Policy Server is more convenient, because it eliminates exporting the certificates to the Policy Server.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Open Internet Information Services (IIS) Manager.
2. Under Connections, click the web server.
3. Double-click Server Certificates.

   A list of certificates appears.
4. Under Actions, click Create Certificate request...

   The Create Certificate wizard appears.
5. Complete the wizard. Save the certificate request to a local file. We recommend using a distinctive name that is easy to remember. For example, ps_wsfed_signing_certificate_request.txt

   The certificate request is created.

Submit Your Certificate Request to a Certificate Authority

After generating your certificate request on an IIS web server, request a certificate from the web server in your organization hosting Active Directory Certificate Services.

Skip this procedure in any of the following situations:

- If you do not use Active Directory Certificate services in your organization.
- You typically submit your certificate requests to an independent, third-party certificate authority.

In any of the previous situations, follow your typical procedures instead.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Open your web browser.
2. Navigate to the following URL:

   `https://fully_qualilfied_domain_name_of_server_running_active_directory_certificate_services/certsrv`

   An example of such a URL is http://certificateauthority.example.com/certsrv.
3. Click Request a certificate.

   The Request a certificate screen appears.
4. Click the advanced certificate request link.
5. Click Submit a certificate request by using a base-64-encoded CMC or PKCS #10 file, or submit a renewal request by using a base-64-encoded PKCS #7 file.

   The Submit a Certificate Request or Renewal Request screen appears.
6. Open the text file containing your certificate request with a text editor. Copy and paste the entire contents of the file into the Saved request field on the screen.
7. Click Submit.

   The certificate pending screen appears.
8. Note the following items for future reference:
   - Your request ID.
   - Use the same browser to verify the status of your request within ten days.

   The request is submitted.

Approve a Certificate Request using Active Directory Certificate Services

Certificate administrators approve or reject certificate requests. Certificate administrator privileges are separate from Administrator privileges. Not all users who have accounts on the computer hosting Active Directory Certificate services have sufficient privileges to approve or reject certificates.

If you have certificate administrator privileges on the web server to which your certificate was submitted, use this procedure. Otherwise, ask the certificate administrator to do this approval for you.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Log in to the web server hosting the Active Directory Certificate services using an account with Certificate administrator privileges.
2. Click Start, Administrative Tools, Certification Authority

   The certsrv snap-in appears.
3. Click the name of the certification authority, and then click the pending request folder.

   A list of pending certificate requests appears.
4. Right-click the request ID associated with the request for the Policy Server Signing certificate.
5. From the context menu, select All Tasks, Issue.

   The certificate is issued.

Verify Your Approval and Download Your Certificate and Certificate Chain

Use the same IIS web server and web browser from which you submitted the request to verify the status of your certificate request. If your certificate is approved, download both the certificate and the certificate chain to your IIS web server.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Open your web browser you used to request your certificate.
2. Navigate to the following URL:

   `https://fully_qualilfied_domain_name_of_server_running_active_directory_certificate_services/certsrv`

   An example of such a URL is http://certificateauthority.example.com/certsrv.
3. Click View the status of a pending certificate request.

   A list of your certificate requests appears.
4. Click the link for your certificate request.

   The Certificate Issued screen appears. If it does not, contact the certificate administrator in your organization for more information.
5. Click the Base 64 Encoded option button.
6. Click all the following links and save the files to your web server:
   - Copy Certificate. (downloads a *.cer file)
   - Copy Certificate Chain (downloads a *.p7b file)

   Your certificate is downloaded.

Complete Your Certificate Request

After downloading your certificate (*.cer) file, complete your certificate request by adding the certificate to your IIS web server. Use the same IIS server from which you originally requested the certificate.

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

Follow these steps:

1. Open Internet Information Services (IIS) Manager.

   The Start page appears.

2. Under Connections, click the web server.

3. Double-click Server Certificates.

   A list of certificates appears.

4. Under Actions, click Complete Certificate Request...

   The Complete Certificate Request wizard appears.

5. Complete the wizard by doing the following tasks:

   a. Navigate to the *.cer file you downloaded previously.

   b. Create a friendly name for the *.cer file.

   The new certificate appears in the list of certificates.

Export Your Policy Server Signing Certificate

Export your Policy Server Signing certificate with IIS manager. This export process creates a certificate file that you add to your Policy Server.

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

Follow these steps:

1. Open Internet Information Services (IIS) Manager.

   The Start page appears.
2. Under Connections, click the web server.
3. Double-click Server Certificates.

   A list of certificates appears.
4. Click your Policy Server signing certificate.

   Your Policy Server signing certificate is selected.
5. Under Actions, click Export.

   The Export Certificate dialog appears.
6. Do the following steps:
   a. Click the ellipsis button and select a directory for your exported certificate.

      A browse dialog appears.
   b. Enter a file name for your exported certificate.
   c. Click Open.

      The browse dialog closes.
   d. Enter a password for the exported certificate and confirm it.

      Note: You need this password to import this certificate into the SiteMinder smkeydatabase used by the Policy Server.
   e. Click OK.

      The Export Certificate dialog closes and the certificate is exported.
7. Close the Internet Information Services (IIS) Manager.
8. If you are using Policy Server clusters, export the certificate to each Policy Server in your environment.

Verify Certificate Support on Policy Servers

SiteMinder uses the smkeydatabase to manage the certificates it uses.

Verify that the smkeydatabase exists on each Policy Server in your SiteMinder environment.

If a smkeydatabase does not exist, create one on each Policy Server to accommodate the certificate used by the Agent for SharePoint.

Follow these steps:

1. On your Policy Server, locate the following directory:

   `policy_server_home\smkeydatabase`

2. Do one of the following steps:

   - If the directory does *not* exist, then create a smkeydatabase on the Policy Server (see page 69).
   - If the directory exists, then add your certificate to the smkeydatabase (see page 69).

3. Repeat Steps 1 and 2 on each Policy Server in your environment.

Configure Certificate Support on Policy Servers

If any of your Policy Servers do not have the smkeydatabase configured, create the smkeydatabase on those Policy Servers. The Agent for SharePoint requires a smkeydatabase on each Policy Server in your environment.

Follow these steps:

1. Log on to your Policy Server.
2. Open a command prompt and navigate to the following directory:

   `policy_server_home`
3. Enter the following command:

   `smkeytool -createDB -password database_password -importDefaultCACerts`

   -createDB

   Creates a smkeydatabase to store keys and certificates.

   -password *smkeydatabase_password*

   Sets a password for the encrypted data in database. The password is encrypted using the policy store key and added to the smkeydatabase.properties file.

   Limits: Length from 6 to 32 characters.

   -importDefaultCACerts

   (Optional) Imports the default Certificate Authority certificates during the creation of the database. These certificates are imported from the cacerts.keystore file, which contains all default Certificate Authority certificates.

   The smkeydatabase is created.
4. Repeat Steps 1 through 4 on each Policy Server in your environment.

Add a Policy Server Signing Certificate to Policy Servers and Create a Trust File

CA SiteMinder requires a certificate to complete signing the WS-Token. CA SiteMinder signs the WS-Token and sends it to SharePoint. To create a certificate for the WS-Token, import an existing certificate that contains both a private and a public key.

This certificate is often in the Public-Key Cryptography Standards #12 (PKCS) format. In the following example, the password protects the PKCS#12 file.

Note: On Windows operating environments, a .pfx file is equivalent to a .p12 file.

Follow these steps:

1. Open the command prompt on the server where the SiteMinder Policy Server is installed.
2. Enter the following command to import the certificate:

   `smkeytool -addPrivKey -alias alias_name -keycertfile certificate_file_name.p12 -password certificate_private_key_password`

   Note: If you want to define aliases for your certificates, the name of the first alias must be defaultenterpriseprivatekey. Subsequent aliases support any name you want. For more information about the smkeytool command, see the *Policy Server Configuration Guide*.

   SiteMinder imports the certificate.
3. If you are using Policy Server clusters, repeat Steps 1 and 2 on *each* Policy Server in your environment.
4. From one Policy Server, enter the following command to create a trust certificate file:

   `smkeytool -export -alias alias_name -outfile exported_certificate_file_name.cer -type cert`

   The trust certificate file that SharePoint requires is created.
5. Copy the trust certificate to a directory on your SharePoint central administration server.
6. Copy any Certificate Authority Certificates in the certificate chain to a directory on your SharePoint central administration server.

   Note: The Powershell script created by the SharePoint connection wizard requires the paths to the following certificates on your SharePoint central administration server:

   - The *exported_certificate_file_name*.cer (certificate) file.
   - Any Certificate Authority certificates in the certificate chain.

More information:

Modify the PowerShell Script (see page 106)

Chapter 7: Install and Configure the SiteMinder Agent for SharePoint

This section contains the following topics:

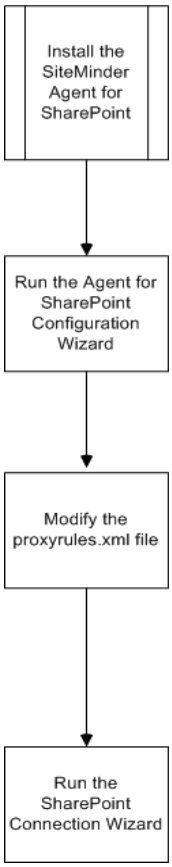
SiteMinder Agent for SharePoint Configuration Overview

The SiteMinder Agent for SharePoint authenticates the identities of users who request access to SharePoint resources using SiteMinder. After SiteMinder authenticates the user, the Agent for SharePoint creates a token, which is forwarded to the SharePoint server. SharePoint then receives and validates the token, it maps the assertions in it to internal SharePoint variables that are used for authorization.

The SiteMinder Claims Provider module lets you search your SiteMinder directories using the SharePoint people picker.

Installing and configuring the Agent for SharePoint involves several separate procedures.

The following illustration describes the tasks you perform when configuring the SiteMinder Agent for SharePoint:



More information:

Install the SiteMinder Agent for SharePoint (see page 73)
Run the Configuration Wizard (see page 78)
Manage SharePoint Connections Using the SharePoint Connection Wizard (see page 83)

FIPS Support Overview

The Agent for SharePoint supports the requirements for cryptographic modules specified in the Federal Information Processing Standards (FIPS) 140-2 standard. When you install the agent, a dialog appears that prompts you to select the level of FIPS support your operating configuration requires.

During a new installation, you can select one of these three FIPS modes:

- COMPAT — Specifies that the installation is not FIPS-compliant. Select this mode when interacting with clients running earlier versions of the Agent for SharePoint.
- MIGRATE — Specifies that the Agent for SharePoint operates both with FIPS-compliant algorithms and algorithms used in earlier version of the agent simultaneously while the data is migrated.
- ONLY — Specifies that the Agent for SharePoint only uses or accepts FIPS-compliant algorithms. When you install in this mode, additional manual configuration is required.

The FIPS mode you select during installation usually is the same as the FIPS mode configured on the Policy Server. When the Policy Server is in Migrate mode, it can operate with the Agent for SharePoint in any mode.

Note: For more information about FIPS, refer the *SiteMinder Policy Server Installation Guide*.

Install the SiteMinder Agent for SharePoint

To use the Agent for SharePoint, the system where you plan to install it must have at least 256 MB of RAM. Other prerequisites differ based on the server system.

For detailed information, see the SiteMinder Agent for SharePoint Support Matrix at http://ca.com/support.

Note: Installation prerequisites pertain to the system on which you run the Agent for SharePoint, not the destination servers to which the Agent for SharePoint routes incoming requests.

The Agent for SharePoint installation consists of two tasks:

1. Install the software.
2. Run the configuration tool.

Note: Throughout the installation instructions, there are references to *Agent-for-SharePoint_home* in directory paths. This variable represents the installation directory of the Agent for SharePoint.

Install the SiteMinder Agent for SharePoint on Windows

The default installation location for the Agent for SharePoint on 32-bit Windows operating environments is: C:\Program Files\CA\Agent-for-SharePoint. On 64-bit Windows operating environments, the default installation location is C:\CA\Agent-for-SharePoint.

Important! The Agent for SharePoint cannot be installed on a computer that hosts any other web server. The Agent for SharePoint operates as a stand-alone proxy-based solution.

To run the Agent for SharePoint Windows installation, the user must be the local Administrator.

Note: We recommend installing the Agent for SharePoint on an NTFS file-system partition system.

Follow these steps:

1. Copy the installation program from the Download location on the CA Support site.
2. Right-click the following executable and select Run as administrator:

   ca-sp2010agent-*version*-win32.exe

   The installation program starts.

   Follow the instructions from the installation wizard.

   Note: The installer displays all java executables installed in the system. Select 32-bit Java Development Kit, Java Runtime Environment, or Java version 1.6.0_16 or higher from the Choose Java Virtual Machine list. If the installer does not detect java executables by default, then browse and select the appropriate path.
3. Restart your system after the installation finishes.

To view the record of the installation, go to the directory *Agent-for-SharePoint_home*\install_config_info and look at this log file:

```
CA_SiteMinder_Agent_for_SharePoint_InstallLog.log
```

Install the SiteMinder Agent for SharePoint on UNIX

This version of the Agent for SharePoint supports installations on Linux and Solaris. For more information about the specific versions supported and any additional patches or RPM updates required, see the SiteMinder platform support matrix.

The default installation location is *user_home*/CA/Agent-for-SharePoint. The folder where you install the Agent for SharePoint requires sufficient permissions (755). Do not install the Agent for SharePoint under the /root folder, because its default permissions (750) are insufficient.

Important! The Agent for SharePoint cannot be installed on a computer that hosts any other web server. The Agent for SharePoint operates as a stand-alone proxy-based solution.

On the Solaris or Linux operating environments, Agent for SharePoint runs as the "nobody" user. If you prefer not to run Agent for SharePoint as this user, create an alternate user and assign the necessary permissions.

Follow these steps:

1. Copy one of the following programs from the download location on the CA Support site to a temporary directory:
   - Solaris: ca-sp2010agent-*version*-sol.bin
   - Linux: ca-sp2010agent-*version*-linux.exe
2. Enter one of the following commands:
   - Solaris: sh ./ca-sp2010agent-*version*-sol.bin
   - Linux: sh ./ca-sp2010agent-*version*-linux.exe
3. Follow the screen prompts provided by the installation wizard.

   Note: The installer displays all java executables installed in the system. Select 32-bit Java Development Kit, Java Runtime Environment, or Java version 1.6.0_16 or higher from the Choose Java Virtual Machine list. If the installer does not detect java executables by default, then browse and select the appropriate path.

To determine whether the installation was successful, go to the directory *Agent-for-SharePoint_home*\install_config_info and look at the following log file:
`CA_SiteMinder_Agent_for_SharePoint_InstallLog.log`

How to Configure the SiteMinder Agent for SharePoint

After you install the Agent for SharePoint, configure the agent for the requirements of your SharePoint environment. Configuring the agent requires several separate procedures, which are described in the following process:

1. Gather the information for your configuration wizard (see page 76).
2. Run the Agent for SharePoint Configuration Wizard (see page 78).
3. Review the following example deployment diagrams:
   - Deployment with a single web front end (farms or stand-alone SharePoint servers) (see page 17).
   - Deployment with multiple web front ends (farms only) (see page 18).
4. Set your proxy rule according to the deployment model you want (see page 81).
5. (Optional) Enable support for dynamic Policy Server clusters (see page 82).
6. Run the SharePoint connection wizard (see page 83).

More information:

Agent for SharePoint Configuration Wizard Information Worksheet (see page 245)
SharePoint Connection Wizard Information Worksheet (see page 246)

Gather SiteMinder Agent for SharePoint Configuration Wizard Information

The Agent for SharePoint configuration wizard helps you register a trusted host, configure the embedded Apache web server

To establish a connection between the Agent for SharePoint and the Policy Server, register a trusted host with the Policy Server. After registration is complete, the registration tool creates the SmHost.conf file. When this file is created successfully, the Agent for SharePoint is allowed to communicate with the Policy Server.

The following lists the required host registration information:

SiteMinder administrator name

Name of a SiteMinder administrator who has privileges to create a trusted host.

SiteMinder administrator password

Password of the SiteMinder administrator.

Trusted host name

Name of the trusted host assigned during configuration.

Note: The name you enter for the trusted host must be unique.

Host Configuration Object

Name of a host configuration object already defined in the Policy Server administrative UI.

Agent Configuration Object

Name of an existing Agent Configuration Object defined in the Policy Server administrative UI.

IP address of the Policy Server where the host is registered

Note: Include a port number for the Policy Server. For example, 121.111.12.11:44442.

Host Configuration File name and location

Identifies the SmHost.conf file, which Web Agents and custom Agents use to act on behalf of the trusted host. Using this file, the host can find a Policy Server and establish a connection. The wizard lists the default location.

Email address of the Agent for SharePoint administrator

The email address for the administrator Default: admin@example.com.

Fully qualified host name of the server

Specifies the hostname of the Agent for SharePoint, this hostname is the address users enter in their web browser:

```
spagent.example.com
```

Port number for HTTP requests

The port listening for HTTP requests Default: 80.

Port number for SSL requests

The port listening for SSL requests Default: 443.

Port number for HTTP Claims web service

The HTTP port used for Claims web service.

Port number for SSL Claims web service

The SSL port used for Claims web service.

Note: No default values are provided for the Claims WS HTTP and SSL Ports. However, use a port that is free, which Tomcat can use to host the web application. For UNIX and Linux, the ports must be greater than 1024. Nobody account works with ports above 1024.

Webagent Enable option

Indicates if the configuration wizard enables (starts) the agent automatically. This setting produces the same results as editing the EnableWebAgent parameter value in the WebAgent.conf file with a text editor.

Default: No (clear check box)

More information:

Agent for SharePoint Configuration Wizard Information Worksheet (see page 245)

Run the Configuration Wizard

After you install the Agent for SharePoint, run the configuration wizard. The configuration wizard registers the Agent for SharePoint with the Policy Server and performs some administrative tasks for the embedded Apache web server.

Before you run the wizard, verify that the required Policy Server objects exist.

Note: Tomcat uses the nobody user by default because it is the least privileged user.

Important! If you have previously run the configuration wizard on your Agent for SharePoint, create a backup copy of your proxyrules.xml file. The configuration wizard creates a default proxyrules.xml file each time it runs on a computer.

Follow these steps:

1. Open a console window and navigate to the directory *Agent-for-SharePoint_home*/
2. Enter one of the following commands:
   - Windows: ca-spagent-config.cmd
   - UNIX or Linux: ca-spagent-config.sh

   The wizard starts. The Host Registration screen appears.

   Note: In Windows, you can alternatively navigate to *Agent-for-SharePoint_home*/install_config_info and double-click ca-spagent-config.exe.
3. Select Yes option to perform host registration if the computer is not registered as a trusted host.

4. As part of the trusted host registration process, respond to the prompts as follows:

   a. Specify the name and password of the SiteMinder administrator and click Next.

      The information you enter must be defined at the Policy Server where the trusted host registers. This screen also includes an optional check box for enabling shared secret rollover.

   b. Specify the name of the Trusted Host and the Host Configuration Object and click Next.

      The name you enter for the trusted host must be unique. The name for the Host Configuration Object must already be defined at the Policy Server where the trusted host is registered.

   c. Enter the IP address of the Policy Server where you want to register the trusted host and click Add. Click Next.

      Note: Include a port number for the Policy Server. For example, 121.111.12.11:44442.

   d. Specify the name and location of the host configuration file, SmHost.conf. The wizard lists the default location. Click Next.

   e. Specify the name of the Agent Configuration Object and click Next. The Agent Configuration Object that you enter must already be defined at the Policy Server where the trusted host is registered.

      Enter the name of the ACO built from the SharePoint2010DefaultSettings ACO template defined in the Policy Server.

   f. Specify the name and location of the Agent Configuration file. The wizard lists the default location. Click Next.

5. Enter the following information for the Apache web server:

   - Server name, in the form *server_name*.example.com.
   - Web server administrator email address, in the form admin@example.com.
   - HTTP port number. The default is 80.
   - HTTPS (SSL) port number. The default is 443.

   Note: On Solaris or Linux, an additional screen prompts for the name of the user under which Tomcat and Apache run. This user cannot be root.

6. Enter the following configuration information for the Claims Search Web Service:Claims WS HTTP Port.

   - Claims WS SSL Port.

   Note: No default values are provided for the Claims WS HTTP and SSL Ports. However, use a port that is free, which Tomcat can use to host the web application. For UNIX and Linux, the ports must be greater than 1024. Nobody account works with ports above 1024.

7. (Optional) Select the check box if you want to enable the Agent for SharePoint.
8. Review the Configuration Summary.
9. Click Install.

   The files are installed.

10. Click Done to exit the wizard.

Note: If you run the Configuration Wizard again for any reason, SSL must be reinitialized. The installer contacts the Policy Server and attempts to register the Trusted Host to create the host configuration file. If trusted host registration does not succeed, the Agent for SharePoint cannot contact the Policy Server and operate properly.

More information:

Gather SiteMinder Agent for SharePoint Configuration Wizard Information (see page 76)
Create a Host Configuration Object and Policy Server Clusters (see page 39)
Agent for SharePoint Configuration Wizard Information Worksheet (see page 245)

Set a Basic Proxy Rule for the Agent for SharePoint

The Agent for SharePoint operates as a proxy-based solution. To protect your SharePoint resources, edit the default proxy rules file so that the Agent for SharePoint points to one of the following locations:

- A hardware load balancer that redirects incoming requests to multiple web front ends associated with multiple SharePoint servers in a SharePoint server farm (see page 18).
- A single web front end associated with multiple SharePoint servers in a SharePoint server farm (see page 17).

Follow these steps:

1. Open the following file on your Agent for SharePoint with a text editor:

   Agent-for-SharePoint_home\proxy-engine\conf\proxyrules.xml

   Important: Do not modify any other configuration files or settings unless explicitly told to do so by CA support personnel.

2. Locate the following line:

   ```
   <nete:forward>http://www.ca.com$0</nete:forward>
   ```

3. Edit the previous line with one of the following values:

   - The URL of your hardware load balancer. This hardware load balancer operates between your Agent for SharePoint server and the SharePoint servers.
   - The URL of your single web front end. In this context, this web front end (WFE) refers a web server that operates in front of your "back end" SharePoint servers.

   If the URL is sharepoint.example.com, edit the line to match the following example:

   ```
   <nete:forward>http://www.sharepoint.example.com$0</nete:forward>
   ```

   Note: The proxyrules.xml file used by the Agent for SharePoint supports redirection to one URL. The Agent for SharePoint does *not* provide any built-in load-balancing functions.

4. Save the file and close your text editor.

   The proxy rule is set.

More information:

Virtual Host Configurations Supported by the Agent for SharePoint (see page 167)

Enable Support for Dynamic Policy Server Clusters for your Agent for SharePoint

The Agent for SharePoint supports dynamic Policy Server clusters. These dynamic Policy Server clusters automatically report when individual Policy Servers are added to or removed from a cluster. A restart of the Agent for SharePoint is not required.

Follow these steps:

1. Use a text editor to open the following file:

   Agent-for-SharePoint_home\proxy-engine\conf\defaultagent\SmHost.conf

2. Locate the following line:

   ```
   enabledynamichco="NO"
   ```

3. Change the previous line to match the following example:

   ```
   enabledynamichco="YES"
   ```

4. Save the file and close the text editor.

5. Restart the Agent for SharePoint.

   Support for dynamic policy servers is enabled. The Agent for SharePoint automatically detects changes to Policy Server clusters.

More information:

How to Start and Stop the Agent for SharePoint (see page 92)

Confirm that the Agent for SharePoint Is Functioning

After you install the Agent for SharePoint, but before changing the proxy rules, you can verify that the server is functioning. You can request index.html file by using the server and port number you specified during installation. For example, if you installed the Agent for SharePoint on server1.example.com and selected port 88 for HTTP communication, you can request the following URL with a browser:

http://server1.example:com:88

If the Agent for SharePoint is working properly, the request redirects to the main CA website (www.ca.com). The default proxy rules file specifies this URL for all redirects.

Assign Permissions for Log Files and Directories on UNIX/Linux

On the UNIX or Linux operating environments, the user account under which the Agent for SharePoint runs requires permissions to create log files.

After running the Agent for SharePoint configuration wizard on a UNIX or Linux operating environment, grant the user account the permissions shown in the following table:

Grant these permissions:	To these directories:
Read, Execute	*Agent-for-SharePoint_home* directory and all subdirectories
Write	*Agent-for-SharePoint_home*/proxy-engine/logs

Manage SharePoint Connections Using the SharePoint Connection Wizard

The SharePoint connection wizard takes you through the process of configuring and managing SharePoint connections with SiteMinder.

Prerequisites for Using the SharePoint Connection Wizard

Before you run the SharePoint Connection Wizard, perform the following steps:

- Verify that you are using a version of the Policy Server that supports the SiteMinder Agent for SharePoint.
- Create a 4.x Agent in the Policy Server Administration UI to enable the Connection Wizard to communicate with the Policy Server.
- The default port number that the SharePoint Connection Wizard uses to contact the Policy Server is 44444. Specify the Administration Service Port number in the Policy Server Management Console if different from the default port number.
- Verify that a policy domain exists on your Policy for the SharePoint resources you want to protect. Verify that the directory containing your SharePoint users is associated with the same policy domain. The SharePoint connection wizard requires the name of the policy domain.
- Identify the required inputs for the SharePoint Connection Wizard by using the Information worksheet.
- Verify that the certificate you want to use for the SharePoint Claims provider is installed on your Agent for SharePoint.

More information:

SharePoint Connection Wizard Information Worksheet (see page 246)
Locate the SiteMinder Agent for SharePoint Platform Support Matrix (see page 249)

Alternate Connection Wizard Method to Help Resolve Firewall Issues

If you experience firewall issues when you try to run the connection wizard, verify that port 44444 is open on your Policy Server.

If your Policy Server uses the *same operating environment* as your Agent for SharePoint, you can copy the SharePoint connection wizard executable file to your Policy Server. Then execute the connection wizard on your Policy Server instead.

Copy the appropriate connection wizard executable file for the operating environment of your Policy Server from the following list:

- (Windows) ca-spconnect-12.0-*version*-win32.exe
- (Solaris) ca-spconnect-*version*-sol.bin
- (Linux) ca-spconnect-*version*-rhel30.bin

More information:

Create a SharePoint Connection (see page 86)
Edit a SharePoint Connection using the SharePoint Connection Wizard (see page 91)
Delete a SharePoint Connection (see page 238)

SAML Autopost Frequency

The following settings determine the frequency at which a SAML autopost operation occurs in your SiteMinder and SharePoint environments:

- Skew time (set in the SharePoint Connection wizard)
- Validity duration (set in the SharePoint Connection wizard)
- Logon Token Cache Expiration window (set in SharePoint)

If these settings create a short interval, pop-up windows related to the autopost operation appear. If these settings create a longer interval, inactive users remain logged in for longer periods than the security policies of your organization prefer.

The following illustration describes the relationships among components that affect how often the SAML autopost occurs:

The following table provides some examples of how changes in the Login Cache Token value on SharePoint change how often the SAML autopost occurs:

SiteMinder				SharePoint	Approximate Time Between SAML Auto Post Operations
Realm Idle Timeout	**Realm Max Timeout**	**Validity Period**	**Skew Time**	**Logon Token Cache Expiration Window**	
1 hour	1 hour	4400 seconds (1 hour 13 minutes)	10 seconds	10 minutes	63 minutes
1 hour	1 hour	4400 seconds (1 hour 13 minutes)	10 seconds	5 minutes	68 minutes

When the Logon Token Cache Expriation Window setting in SharePoint is lower, the SAML autopost operation occurs less often. However, inactive users could possibly remain logged in.

Note: For more information about how to disable FedAuth cookies in SharePoint 2010, go to the technet blogs website, and then search for the following phrase:

"Setting the Login Token Expiration Correctly for SharePoint 2010 SAML Claims Users"

Create a SharePoint Connection

The Agent for SharePoint uses a connection wizard to define the connection parameters used when SiteMinder communicates with your SharePoint server. The connection wizard does following tasks:

- Configures the connection between your Agent for SharePoint and the Policy Server.
- Creates a Windows PowerShell script that you modify and run on your SharePoint central administration server to create a trusted identity provider.

  Important! The SharePoint connection wizard automatically creates federation objects (resource partners) in your Policy Servers. Use only the SharePoint connection wizard to create or manage these objects. If you have a Federation Security Services license, these objects also appear in the FSS Administrative UI. Advise your Federation Security Services Administrator not to modify these objects with the FSS Administrative UI unless explicitly told to do so by CA support personnel.

Follow these steps:

1. Perform the following:
   - (Windows)

   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard

   b. Right-click the executable and select Run as administrator.

   The SharePoint Connection wizard starts.

   - (Unix)

   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard

   b. Enter one of the following commands:
      - Solaris: sh ./ca-spconnect-12.0-sp3-sol.bin
      - Linux: sh ./ca-spconnect-12.0-sp3-rhel30.bin

   The SharePoint Connection wizard starts.
2. Click Next.

   The Login Details screen appears.

3. Enter the following login details to connect to the Policy Server.

   Policy Server Name

   Specifies the Policy Server name or IP address.

   Example: *host_name*:*port_number*

   Note: Specify the Administration port number if the port number is different from the default port number 44444.

   Username

   Specifies the Policy Server administrator username.

   Password

   Specifies the Policy Server administrator password.

   Agent Name

   Specifies the name of the 4.x-compatible Agent object on your Policy Server. The connection with the Policy Server is established using the details given in the Agent Name.

   Shared Secret Key

   Specifies the shared secret key associated with the 4.x-compatible Agent object on your Policy Server.

4. Click Next

   The Select Action screen appears.

5. Select Create a SharePoint connection option.

6. Click Next.

   The SharePoint Connection Properties screen appears.

7. Enter the following details to create a SharePoint connection.

   Select a domain

   Specifies the name of the policy domain you created in the Policy Server to protect your SharePoint resources.

   Name

   Specifies a name for the SharePoint connection. This name is also used as the file name of the PowerShell script that the wizard creates.

   Note: Use a unique name across all Resource Partners and SharePoint connections.

Authentication URL

Specifies the *port number* associated with the predefined protected URL which the SharePoint connection wizard adds automatically. When users try accessing a protected SharePoint resource without a SiteMinder session, they are redirected to the Authentication URL.

If you are using a default port number (such as 80 for HTTP or 443 for HTTPS), delete the CA Portal setting from this field.

Note: We recommend using HTTPS on production environments and pages which handle user credentials, such as login pages.

SharePoint Realm

Specifies a name for a SharePoint realm that uniquely identifies this connection between SiteMinder and SharePoint. This name is used to create the trusted identity provider.

Limits: Unique value across all SharePoint servers, farms and within the SiteMinder environment. This value cannot be used with any other identity providers.

Skew Time

Specifies the number of seconds used as a time difference between the Policy Server (token producer) and the SharePoint server (token consumer). This skew time accommodates for SharePoint connections using clocks that are acting as an account partner but are not synchronized with the Policy Server.

Note: This setting also affects the frequency of the SAML autopost operation (see page 85).

Limits: Positive integers.

Validity Duration

Specifies the number of seconds for which a session remains valid. If the validity duration expires, a logout message is generated, and the user associated with the invalid session is logged out.

Note: This setting also affects the frequency of the SAML autopost operation (see page 85).

Signing Alias

Specifies the alias used by the smkeydatabase to identify the private key associated with the certificate used by your Policy Server to sign the tokens.

Note: We recommended that the private key exists in the key database before you specify its associated alias in this field. Enter the following command on the Policy Server to list all the imported certificates to determine the appropriate Alias:

```
smkeytool -listCerts
```

Protection Level

Specifies the protection level assigned to the resource partner object created by the connection wizard. This protection level setting must be equal to or lower than the protection level assigned to the authentication scheme that protects your SharePoint resources.

Limits: 1-1000 (higher numbers indicate a higher protection level).

8. Click Next

   The Define User Identifier claim screen appears.

9. Complete the following fields:

   Identifier Claim Name

   Specifies name of the attribute mapping in your user directory which identifies the unique value associated with each user.

   Example: useridentifier

   Directory Attribute

   Specifies the directory attribute in your directory that is associated with the specified Identifier Claim name.

   Example: (LDAP directory) uid

   Example: (Active directory) sAMAccountName

10. Click Next

    The Define Additional claims screen appears.

11. Click the drop-down arrows and select the values for any group-based or role-based claims from the following lists:

    Attribute

    Specifies an attribute name for one of the following claim types:

    - Group based
    - Role based

    For multi-valued attributes, prefix *FMATTR:*

    Example: (group-based claim) smusergroups

    Example: (role-based claim) userrole

    Example: (multi-valued attributes) FMATTR:LastName

    Claim Type

    Specifies an attribute value associated with the specified attribute name.

    For group-based claims, use the friendly role of your groups. The people picker in SharePoint displays the description and distinguished name (DN) of the group. Permissions are tied to the DN of the group, not the friendly name.

    Example: (LDAP directory group-based claim) description

    Example: (LDAP directory role-based claim) employeeType

    Example: (Active Directory group-based claim) name

    Example: (Active Directory role-based claim) countryCode

12. Click Add.

    The additional claim is defined.

13. (Optional) Repeat Steps 12 and 13 to add more role-based claims.

14. Click Next.

    The attribute details are saved and the Commit Details screen appears.

15. Click Install.

    The Save Complete screen appears and shows location of your PowerShell script. The PowerShell script is created in the following directory:

    Agent-for-SharePoint_home/sharepoint_connection_wizard/

    The connection wizard uses the connection name you specified (in Step 8) as the name of the PowerShell script. For example, if you specify my_sharepoint_connnection for a connection name in the connection wizard, then name of the PowerShell script is my_sharepoint_connection.ps1.

16. Click Done.

    The connection wizard closes.

More information:

How to Configure the Trusted Identity Provider (see page 104)
SAML Autopost Frequency (see page 85)
Alternate Connection Wizard Method to Help Resolve Firewall Issues (see page 84)

Edit a SharePoint Connection using the SharePoint Connection Wizard

Follow these steps:

1. Perform the following:
   - (Windows)
   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard
   b. Right-click the executable and select Run as administrator.

      The SharePoint Connection wizard starts.
   - (Unix)
   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard
   b. Enter one of the following commands:
      - Solaris: sh ./ca-spconnect-12.0-sp3-sol.bin
      - Linux: sh ./ca-spconnect-12.0-sp3-rhel30.bin

      The SharePoint Connection wizard starts.
2. Click Next.

   The Login Details screen appears.
3. Enter the following login details to connect to the Policy Server.

   Policy Server Name

   Specifies the Policy Server name or IP address.

   Username

   Specifies the Policy Server administrator username.

   Password

   Specifies the Policy Server administrator password.

   Agent Name

   Specifies the Agent-4x. The connection with the Policy Server is established using the details given in the Agent Name.

Shared Secret Key

Specifies the shared secret key associated with the Agent.

4. Click Next

   The Select Action screen appears.

5. Select Edit a SharePoint Connection option.

6. Click Next.

   The SharePoint Connection Properties screen appears.

7. Make the required changes in SharePoint Connection Properties, Name IDs, and Add Attributes screen.

8. Click Install in the Commit Details screen.

   The Save Complete screen appears.

9. Click Done.

   The partnership details are saved, the SharePoint Connection is modified, and the wizard closes.

More information:

SharePoint Connection Wizard Information Worksheet (see page 246)
Alternate Connection Wizard Method to Help Resolve Firewall Issues (see page 84)

How to Start and Stop the Agent for SharePoint

Starting or stopping the Agent for SharePoint involves the following separate procedures:

1. Changing the value of EnableWebAgent in the WebAgent.conf file (see page 93).
2. Changing the state of the related services on the computer running the Agent for SharePoint (see page 94).

Change the Value of the EnableWebAgent Parameter

Change the value of the EnableWebAgent parameter to change the state of the Agent for SharePoint when the related services running on the Agent for SharePoint start or stop.

follow these steps:

1. Open the following file with a text editor:

   ```
   Agent-for-SharePoint_home\proxy-engine\conf\defaultagent\WebAgent.conf
   ```

   Note: On UNIX/Linux operating environments, substitute a forward slash (/) for the backslash in the previous example.

2. Locate the following line:

   ```
   EnableWebAgent="NO"
   ```

3. Change the value inside the quotation marks to *one* of the following:

   - YES to start the Agent for SharePoint after the services start. Your resources are protected.
   - NO to stop the Agent for SharePoint after the services start. Your resources are *not* protected.

4. Change the state of the related services on your Agent for SharePoint (see page 94).

Change the States of the Services on your Agent for SharePoint

You can change the states of the related services on your Agent for SharePoint.

Note: To start or stop your Agent for SharePoint, change the value of the EnableWebAgent parameter first (see page 93).

follow these steps:

1. To change the states of the related services, select *one* of the following procedures:
   - For Windows operating environments, go to Step 2.
   - To *start* the Agent for SharePoint on UNIX operating environments, go to Step 3.
   - To *stop* the Agent for SharePoint on UNIX operating environments, go to Step 4.
2. For Windows operating environments, do the following steps:
   a. From the Windows Start menu navigate to Administrative Tools, Services.

      The Services dialog appears.

   b. Scroll down the list of services and select SiteMinder Agent for SharePoint.

   c. From the Action menu, select All Tasks and select the command you want.

   d. Repeat Step b for SiteMinder Agent for SharePoint Proxy Engine.

      The states of the services and Agent for SharePoint are changed.
3. To start the Agent for SharePoint on UNIX operating environments, do the following steps.
   a. Log on as a root user.

   b. Navigate to the following directory:

      Agent-for-SharePoint_home/proxy-engine

   c. Run the following from a command line:

      ```
      ./sps-ctl start
      ```

      The service and the Agent for SharePoint start. The Agent for SharePoint stops or starts according to the value you set in the EnableWebAgent parameter (see page 93).
4. To stop the Agent for SharePoint on a system running UNIX, do the following steps:
   a. Navigate to the following directory:

      Agent-for-SharePoint_home/proxy-engine

   b. Run the following from a command line:

      ```
      ./sps-ctl stop
      ```

      The service and the Agent for SharePoint stop.

Chapter 8: Configure SharePoint

This section contains the following topics:

How to Configure SharePoint for the Agent for SharePoint

Configuring your SharePoint servers for the Agent for SharePoint involves several separate procedures.

Follow these steps:

1. Configure Alternate Access Mappings (see page 100).
2. Configure the Trusted Identity Provider (see page 104).
3. Configure Authentication Providers (see page 128).
4. Add SiteMinder Users to SharePoint. (see page 130)
5. Manage User Profiles. (see page 131)

Permissions Required for Trusted Identity Provider and Claims Provider

Users who create the trusted identity provider and install or configure the SharePoint claims provider need the following permissions:

User account permissions

User accounts require the following privileges:

- Domain user account.
- Member of Local administrator group on each SharePoint server in the farm (except for the SQL Server and SMTP server)
- Access to the SharePoint 2010 server databases.

Setup User Account

The setup user account requires the following permissions:

- Member of the WSS_ADMIN_WPG Windows security group.
- Member of the IIS_WPG role group.

Database permissions

The following database permissions are required:

- db_owner on the SharePoint Server 2010 server farm configuration database.
- db_owner on the SharePoint Server 2010 Central Administration content database.

PowerShell scripts for Claims Provider

Running the PowerShell scripts for the Claims Provider requires the following permissions:

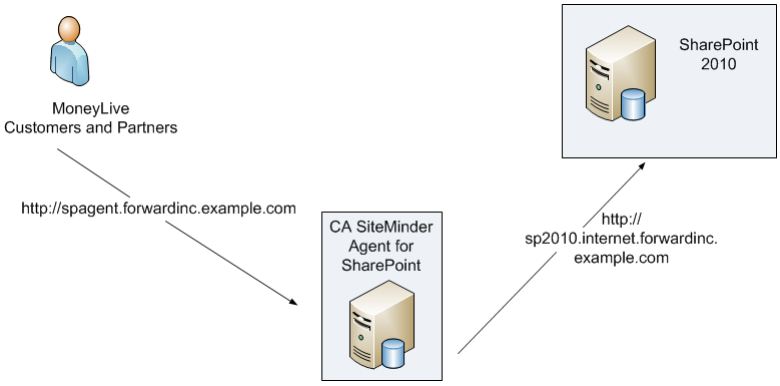
- Local administrator on all SharePoint web front end (WFE) servers.
- Access (read/write) to the configuration database.

Note: The preceding permissions apply when the user is not an Administrator or not part of an Administrator group.

Configure Alternate Access Mapping

ForwardInc is a financial markets data provider. ForwardInc helps financial institutions to use its systems to gather live market and news data to make critical decisions. ForwardInc uses SharePoint 2010 as a web and document management system. ForwardInc requires users (employees, customers, and partners) to access its SharePoint applications.

ForwardInc's SharePoint Administrator created a site to enable customers and partners to access and download daily reports generated by ForwardInc Market Analysts. The SharePoint Administrator must configure alternate access mapping to control the URL address that displays in a web browser.



In the illustration, ForwardInc customers and partners enter a public URL (http://spagent.forwardinc.example.com) in their browsers to access the ForwardInc SharePoint site. The URL (http://spagent.forwardinc.example.com) is what appears in the links on the pages. The request first goes to the Agent for SharePoint, which redirects all authenticated requests to SharePoint, which then sends the user to the SharePoint site.

Follow these steps:

1. Verify if the Zone is associated with Agent for SharePoint (see page 101)
2. Edit Public URL (see page 102)
3. Add Internal URL (see page 103)

Note: This scenario assumes that the SharePoint Administrator has created a web application with the Default zone http://sp2010.default.forwardinc.example.com and the internet zone http://sp2010.internet.forwardinc.example.com.

Alternate Access Mappings

In SharePoint, public URLs are visible to users. Internal URLs identify resources within a particular server or SharePoint server farm. Using alternate access mappings, you can create relationships to between the Public URL and several Internal URLs.

Alternate access mappings create relationships between Public and Internal URLs to perform the following functions:

- Direct users to the correct URLs during their interaction with SharePoint
- Map external requests to the correct web applications and sites within a SharePoint server or server farm.
- Support a SharePoint server or server farm behind a load balancer. The load balancer forwards requests to the Public URL. The SharePoint server uses the alternate access mapping to determine which resources to display for the request.

SharePoint allows each web application to be associated with a collection of mappings between internal and public URLs. The collection of mappings is named a zone.

A zone is a way to map multiple web applications to a single set of content databases. All web applications are initially assigned to the Default zone when first created. You can only assign a different zone when you are extending the web application. Each zone can have a different authentication method.

The five types of zones are as follows:

- Default
- Intranet
- Internet
- Custom
- Extranet

Configure the public URL of the web application zone to the virtual host URL defined in the Agent for SharePoint so the Agent for SharePoint can receive and direct requests to the SharePoint web application.

Before you configure alternate access mapping, note which zone is associated with the Agent for SharePoint. By default, web applications are associated with the default zone which provides Windows Authentication (NTLM).

Verify if Zone is Associated with Agent for SharePoint

Before the SharePoint Administrator configures alternate access mapping, the Administrator must identify the zone which is associated with the Agent for SharePoint. In the ForwardInc scenario, the Default zone uses Windows Authentication (NTLM). The extended internet zone is configured for Claims-based Authentication with the Agent for SharePoint. The web application that Adam must verify is http://sp2010.internet.forwardinc.example.com.

Follow these steps

1. Click Start, Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Central Administration.

   The Central Administration home page appears.

2. Click Application Management.

   The Application Management page appears.

3. Under Web Applications, click Manage web applications.

   The Web Applications page appears.

4. Click the web application http://sp2010.internet.forwardinc.example.com.

   The web application is selected.

5. On the Web Applications ribbon, Click Authentication Providers .

   The Authentication Providers dialog displays the Zone and the Membership Provider Name associated with the web application (http://sp2010.internet.forwardinc.example.com). In the ForwardInc scenario, two zones are displayed Default and Internet. The Internet displays Claims-based authentication.

This procedure verifies that the SharePoint Administrator must configure alternate access mapping for the internet zone.

Edit Public URLs

The SharePoint Administrator must edit the Public URL of the SharePoint web application so that all user requests are routed through the Agent for SharePoint. Two zones are associated with this web application, default zone and internet zone. This procedure aims to edit the Public URL for the internet zone.

Follow these steps

1. Click Start, Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Central Administration.

   The Central Administration home page appears.

2. Click Application Management.

   The Application Management page appears.

3. Click configure alternate access mappings.

   The Alternate Access Mappings page appears with a list of available web applications.

4. Click Edit Public URLs.

   The Edit Public URLs page appears. The Default and the internet zone fields are populated with the URLs http://sp2010.default.forwardinc.example.com and http://sp2010.internet.forwardinc.example.com respectively.

   Note: If the mapping collection that you want to edit does not appear, then select one from the Alternate Access Mapping Collection list.

5. Perform the following tasks in the Public URLs section internet field:

   a. Remove the internet URL (http://sp2010.internet.forwardinc.example.com).

   Note: The internet URL is added as the Internal URL for this zone in add internal URL (see page 103) procedure.

   b. Replace with the Agent for SharePoint URL (http://spagent.forwardinc.example.com)

6. Click Save.

   The Alternate Access Mappings page appears with the saved settings. The following table shows a representation of the alternate access mappings list.

Internal URL	Zone	Public URL for the Zone
http://sp2010.default.forwardinc.example.com	Default	http://sp2010.default.forwardinc.example.com
http://spagent.forwardinc.example.com	Internet	http://spagent.forwardinc.example.com

Note: For more information about Alternate Access Mapping, see www.microsoft.com.

Add Internal URL

This procedure allows the SharePoint Administrator to map the internet zone public URL (http://spagent.forwardinc.example.com) to the SharePoint internal URL (http://sp2010.internet.forwardinc.example.com).

Follow these steps

1. Click Start, Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Central Administration.

   The Central Administration home page appears.

2. Click Application Management.

   The Application Management page appears

3. Click configure alternate access mappings.

   The Alternate Access Mappings page appears with a list of available web applications.

4. Click Add Internal URLs.

   The Add Internal URLs page appears.

   Note: If the mapping collection that you want edit does not appear, then select one from the Alternate Access Mapping Collection list.

5. Enter the internal URL as http://sp2010.internet.forwardinc.example.com in the Add Internal URL section, in the URL protocol, host and port field.

6. Select internet zone for the internal URL, from the Zone list.

7. Click Save.

   The Alternate Access Mappings page appears with the saved settings. The following table shows a representation of the alternate access mappings list.

Internal URL	Zone	Public URL for the Zone
http://sp2010.default.forwardinc.example.com	Default	http://sp2010.default.forwardinc.example.com
http://spagent.forwardinc.example.com	Internet	http://spagent.forwardinc.example.com
http://sp2010.internet.forwardinc.example.com	Internet	http://spagent.forwardinc.example.com

Note: For more information about Alternate Access Mapping, refer to www.microsoft.com.

How to Configure the Trusted Identity Provider

The Windows Identity Framework in SharePoint 2010 supports multiple authentication providers. Create a Trusted Identity Provider in SharePoint to establish runtime integration with SiteMinder Agent for SharePoint. Configuring the Trusted Identity Provider involves the following process:

1. Copy the certificate authority certificate to the SharePoint central administration server (see page 104).
2. Copy the PowerShell script to the SharePoint central administration server (see page 105).
3. Modify the PowerShell script (see page 106).
4. (Optional) Add additional certificate authority certificates to the PowerShell script (see page 112).
5. Create the trusted identity provider (see page 114).
6. (Optional) Verify that the Trusted Identity Provider is registered (see page 115).

More information:

SharePoint 2010 Federation Worksheet (see page 247)

Copy the Policy Server Signing certificate to the SharePoint Central Administration Server

The Policy Server signing certificate you exported from your smkeydatabase on one of your Policy Servers is required to create a trusted identity provider. This certificate lets the SharePoint claims provider verify the authentication claims sent by the Policy Server.

Follow these steps:

1. Navigate to the directory on your Policy Server to which you exported your certificate using the smkeytool command.
2. Locate the Policy Server signing certificate file you exported, and then copy it to a directory on your SharePoint central administration server.

Copy the Powershell Script to the SharePoint Central Administration Server

The PowerShell script created by the SharePoint connection wizard on your Agent for SharePoint host is required to create a trusted identity provider. Copy it from your Agent for SharePoint host to your SharePoint central administration server.

Follow these steps:

1. Navigate to the following directory on your Agent for SharePoint server:

   Agent-for-SharePoint_home\sharepoint_connection_wizard\

2. Locate the PowerShell script created by the SharePoint connection wizard. The script uses the connection name you chose while running the wizard as the file name. For example, if your connection name was my_connection, the name of the script is my_connection.ps1.

3. Copy the PowerShell script to a directory on your SharePoint central administration server.

Modify the PowerShell Script

To create a trusted identity provider on your SharePoint central administration server, edit the PowerShell script to include the following information about your SharePoint environment:

- The full path to the root certificate (typically from a third-party Certificate Authority) that signed your certificate.
- Create a trusted root authority in SharePoint for the certificate authority which signed your certificate.
- The full path to your signing certificate.
- Friendly names for each of the claim mappings.
- The SharePoint realm name (to identify the trusted identity provider).

  Note: This value appears in SharePoint Central Administration under the list of available trusted identity providers.
- A friendly description for the trusted identity provider.

The specific modifications to the PowerShell script vary according to the type of certificates you want to use with your SiteMinder trusted identity provider. The following scenarios exist:

- You are using a certificate that is signed by an external certificate authority, and the certificate authority is *not* trusted by your SharePoint server.
- You are using a self-signed certificate and the certificate authority is *not* trusted by your SharePoint server.
- You are using a certificate, and the certificate authority is trusted by your SharePoint server. Check with your SharePoint administrator to confirm that the proper certificate authority is trusted.

Follow these steps:

1. Use the previous list to determine which scenario applies to your situation.
2. Perform the appropriate procedure from the following list:
   - Modify the PowerShell script for certificates that are signed by an external certificate authority (see page 107).
   - Modify the PowerShell script for un–trusted self-signed certificates (see page 109).
   - Modify the PowerShell script for certificates that are issued by a trusted certificate authority (see page 111).

Modify the PowerShell Script for Certificates Signed by an Un-Trusted External Certificate Authority

If your signing certificate is signed by an external certificate authority, modify the PowerShell script to do the following tasks:

- Import the certificate authority certificate (root certificate) into SharePoint.
- Create a SharePoint trusted root authority that is based on the certificate authority certificate.
- Import the signing certificate.

Follow these steps:

1. Open the PowerShell script with any text editor.
2. Locate the following text:

   ```
   "<full path to Root certificate file>"
   ```

3. Replace the previous text with the full path to your root certificate. For example, if the full path to your certificate is C:\certificates\sharepoint\certificate_authority_certificate.cer, the updated line matches the following example:

   ```
   "C:\certificates\sharepoint\certificate_authority_certificate.cer"
   ```

4. Locate the first occurrence of the following text:

   ```
   <Trusted root authority name>
   ```

5. Replace the previous text with a friendly name for the new trusted root authority in SharePoint. For example, if the name you want is SPCAAuth, the updated line matches the following example:

   ```
   "SPCAAuth"
   ```

6. Locate the following text:

   ```
   "<full path to Signing certificate file>"
   ```

7. Replace the previous text with the full path to your Signing certificate. For example, if the full path to your certificate is C:\certificates\sharepoint\signing_certificate.cer, the updated line matches the following example:

   ```
   "C:\certificates\sharepoint\signing_certificate.cer"
   ```

8. Locate the second occurrence of the following text:

   ```
   <Trusted root authority name>
   ```

9. Replace the previous text with a friendly name for the new trusted root authority in SharePoint. For example, if the name you want is SPSigningAuth, the updated line matches the following example:

   ```
   "SPSigningAuth"
   ```

10. Locate the following text:

    ```
    "<Name of the trusted identity provider>"
    ```

11. Replace the previous text with the name of your SharePoint realm (the realm name follows $realm = in the PowerShell script). For example, if the name of your SharePoint realm is $realm="urn:moss2O1O-wsfed1-casm", the updated line could match the following example:

    ```
    "moss2010-wsfed1-casm"
    ```

12. Locate the following text:

    ```
    "<Description for the Trusted Identity Provider>"
    ```

13. Replace the previous text with a description for your trusted identity provider. For example, if you want to describe the trusted identity provider as "SiteMinder Provider," the updated line could match the following example:

    ```
    "SiteMinder Provider"
    ```

    Note: The LDAP directory and Active Directory charts contain additional examples of possible names.

14. If your certificate chain contains *more than one* certificate authority certificate, add the other certificate authority certificates to the script (see page 112). If your script contains *one* certificate authority certificate, go to the next step.

15. Save your changes and close your text editor.

    The PowerShell script is modified.

16. Create a trusted identity provider (see page 114).

Modify the PowerShell Script for Un-Trusted Self-Signed Certificates

If you are using a self-signed certificate that is issued by a certificate authority which is not explicitly trusted by your SharePoint server, modify the PowerShell script to do the following tasks:

- Import the certificate authority certificate (root certificate) into SharePoint.
- Create a SharePoint trusted root authority that is based on the certificate authority certificate.
- Import the signing certificate.

Follow these steps:

1. Open the PowerShell script with any text editor.
2. Locate the following text:

   ```
   "<full path to Root certificate file>"
   ```

3. Replace the previous text with the full path to your root certificate. For example, if the full path to your certificate is C:\certificates\sharepoint\certificate_authority_certificate.cer, the updated line matches the following example:

   ```
   "C:\certificates\sharepoint\certificate_authority_certificate.cer"
   ```

4. Locate the first occurrence of the following text:

   ```
   <Trusted root authority name>
   ```

5. Replace the previous text with a friendly name for the new trusted root authority in SharePoint. For example, if the name you want is SPCAAuth, the updated line matches the following example:

   ```
   "SPCAAuth"
   ```

6. Locate the following text:

   ```
   "<full path to Signing certificate file>"
   ```

7. Replace the previous text with the full path to your Signing certificate. For example, if the full path to your certificate is C:\certificates\sharepoint\signing_certificate.cer, the updated line matches the following example:

   ```
   "C:\certificates\sharepoint\signing_certificate.cer"
   ```

8. Locate the second occurrence of the following text:

   ```
   <Trusted root authority name>
   ```

9. Replace the previous text with a friendly name for the new trusted root authority in SharePoint. For example, if the name you want is SPSigningAuth, the updated line matches the following example:

   ```
   "SPSigningAuth"
   ```

10. Locate the following text:

    ```
    "<Name of the trusted identity provider>"
    ```

11. Replace the previous text with the name of your SharePoint realm (the realm name follows $realm = in the PowerShell script). For example, if the name of your SharePoint realm is $realm="urn:moss2O1O-wsfed1-casm", the updated line could match the following example:

    ```
    "moss2010-wsfed1-casm"
    ```

12. Locate the following text:

    ```
    "<Description for the Trusted Identity Provider>"
    ```

13. Replace the previous text with a description for your trusted identity provider. For example, if you want to describe the trusted identity provider as "SiteMinder Provider," the updated line could match the following example:

    ```
    "SiteMinder Provider"
    ```

    Note: The LDAP directory and Active Directory charts contain additional examples of possible names.

14. If your certificate chain contains *more than one* certificate authority certificate, add the other certificate authority certificates to the script (see page 112). If your script contains *one* certificate authority certificate, go to the next step.

15. Save your changes and close your text editor.

    The PowerShell script is modified.

16. Create a trusted identity provider (see page 114).

Modify the PowerShell Script for Certificates Issued by a Trusted Certificate Authority

If you are using a certificate signed by a certificate authority that is trusted by the SharePoint server, modify the PowerShell script to do the following tasks:

- Skip the step to import the certificate authority certificate.
- Skip the stop to create a new SharePoint trusted root authority.
- Import only the signing certificate.

Follow these steps:

1. Open the PowerShell script with any text editor.
2. Comment the first two lines in the PowerShell script, as shown in the following example:

```
#$rootcert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("<full
path to Root certificate file>")
#New-SPTrustedRootAuthority -Name "<Trusted root authority name>"
-Certificate $rootcert
```

3. Locate the following text:

```
"<full path to Signing certificate file>"
```

4. Replace the previous text with the full path to your Signing certificate. For example, if the full path to your certificate is C:\certificates\sharepoint\signing_certificate.cer, the updated line matches the following example:

```
"C:\certificates\sharepoint\signing_certificate.cer"
```

5. Locate the second occurrence of the following text:

```
<Trusted root authority name>
```

6. Replace the previous text with a friendly name for the new trusted root authority in SharePoint. For example, if the name you want is SPSigningAuth, the updated line matches the following example:

```
"SPSigningAuth"
```

7. Locate the following text:

```
"<Name of the trusted identity provider>"
```

8. Replace the previous text with the name of your SharePoint realm (the realm name follows $realm = in the PowerShell script). For example, if the name of your SharePoint realm is $realm="urn:moss2O1O-wsfed1-casm", the updated line could match the following example:

```
"moss2O1O-wsfed1-casm"
```

9. Locate the following text:

```
"<Description for the Trusted Identity Provider>"
```

10. Replace the previous text with a description for your trusted identity provider. For example, if you want to describe the trusted identity provider as "SiteMinder Provider," the updated line could match the following example:

    ```
    "SiteMinder Provider"
    ```

    Note: The LDAP directory and Active Directory charts contain additional examples of possible names.

11. Save your changes and close your text editor.

    The PowerShell script is modified.

12. Create a trusted identity provider (see page 114).

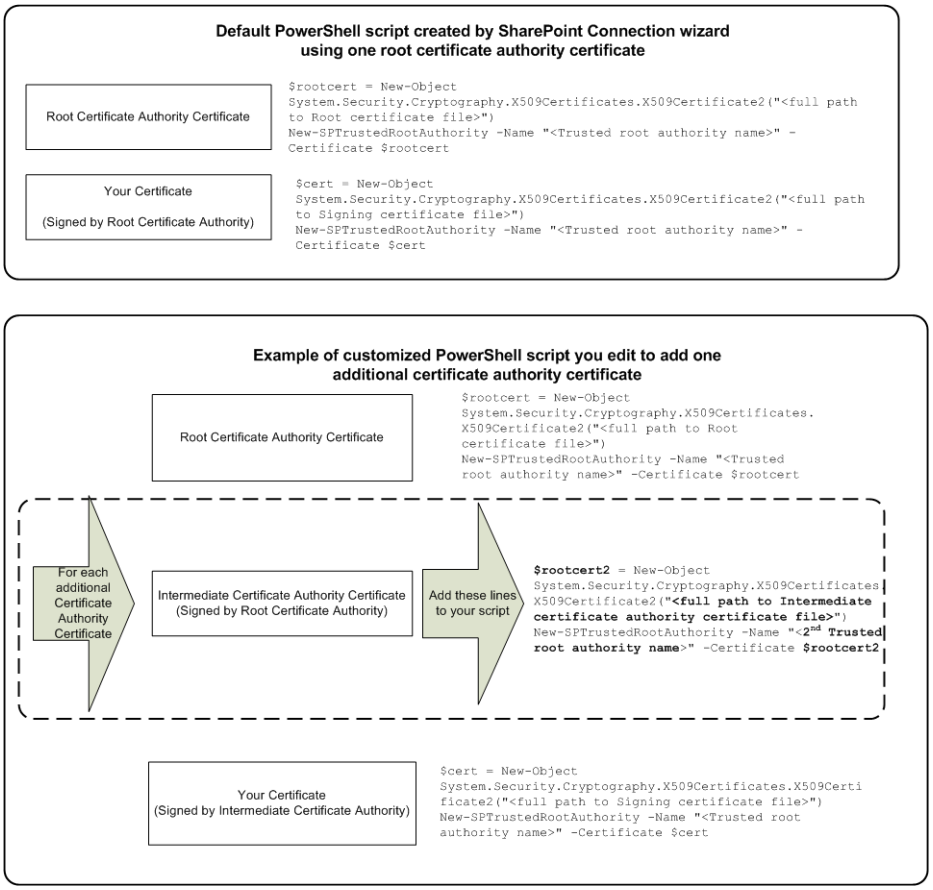
Add Additional Certificate Authority Certificates to the PowerShell Script

The PowerShell script created by the SharePoint connection wizard accommodates the following certificates:

- A certificate authority certificate (also named a root certificate)
- One SSL certificate.

The trusted identity provider requires that all certificates in the certificate chain are included. If an intermediate certificate authority signed your certificate instead, modify the PowerShell script to include both certificate authority certificates.

The following illustration describes the differences between the default PowerShell script, and a PowerShell script that accommodates multiple certificate-authority certificates:



Follow these steps:

1. Copy the following section from your PowerShell script:

   ```
   $rootcert = New-Object
   System.Security.Cryptography.X509Certificates.X509Certificate2("<full path to
   Root certificate file>")
   New-SPTrustedRootAuthority -Name "<Trusted root authority name>" -Certificate
   $rootcert
   ```

2. Copy the following section from your PowerShell script:
3. Add a new line after the section you copied, and then paste the copied into the new line.
4. Edit the pasted section using the changes shown in the following table as a guide:

Change this value:	To this value:
$rootcert	$rootcert2
<full path to Root certificate file>	<full path to additional certificate authority certificate file>
<Trusted root authority name>	Name of the additional trusted root authority

5. To add additional certificate authority certificates, repeat Steps 1 through 4.
6. Save your changes and close your text editor.

   The PowerShell script is modified.

7. Create a trusted identity provider (see page 114).

Run the Powershell Script to Create a Trusted Identity Provider

Run the modified PowerShell script to create a trusted identity provider on your SharePoint central administration server.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell
2. Navigate to the directory containing your edited PowerShell script.
3. Run the script with the following command:

   ```
   .\your_connection_name.ps1
   ```

   For example, if you named your connection "my_sharepoint" when you ran the connection wizard, the command would be .\my_sharepoint.ps1.

   The trusted identity provider is created.

Verify That the Trusted Identity Provider Is Registered

After using the PowerShell command to create your trusted identity provider, verify that it is registered in your SharePoint central administration server.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   The Microsoft PowerShell command prompt appears.

2. Enter the following command:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of the trusted identity providers configured on the SharePoint central administration server appears.

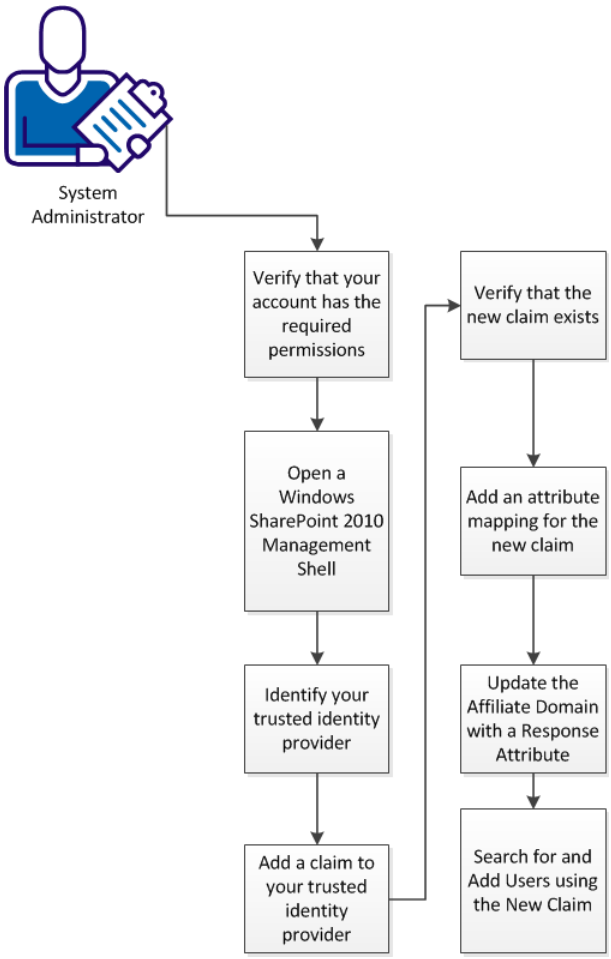
Chapter 9: Adding Claims to Trusted Identity Providers

SharePoint 2010 supports third-party identity providers. These identity providers authenticate and authorize users who request SharePoint resources. A SharePoint administrator configures a trusted identity provider for a SharePoint environment.

Claims are a form of attribute or role, that a user has. Each claim has a name to identify it, and a value that the trusted identity provider verifies by connecting to a user directory.

For example, you can configure claims that correspond to the SamAccountName attribute of an Active Directory server or a uid of an LDAP directory server.

You can add a claim to a SiteMinder trusted identity provider at any time. The following illustration describes the process:



To add a claim to a SiteMinder trusted identity provider, follow these steps:

1. Verify that your account has the required permissions (see page 119).
2. Open a SharePoint 2010 Management Shell window on your SharePoint Central Administration server (see page 119).
3. Identify your SiteMinder trusted identity provider (see page 119).
4. Add a claim to your trusted identity provider (see page 120).
5. Verify that the new claim exists. (see page 120)
6. Add an attribute mapping for the new claim (see page 121).
7. Update the affiliate domain with a response attribute (see page 122).
8. Search for and add users using the new claim (see page 124).

Verify that your Account has the Required Permissions

The user account with which you want to modify the SiteMinder trusted identity provider requires certain permissions. Modify the permissions of your user account if it does *not* meet the following conditions:

- An Administrator account.
- A member of the Administrators group.

Add the following privileges to your account:

- Local administrator on all SharePoint web front end (WFE) servers.
- Read/Write access to the configuration database.

Open a SharePoint 2010 Management Shell Window on your SharePoint Central Administration Server

Add claims to your <stmdnr> trusted identity provider using the SharePoint 2010 Management shell.

Follow these steps:

1. Log in to your SharePoint Central Administration server.
2. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   A SharePoint 2010 management shell command-line window appears.

Identify your Trusted Identity Provider

A SharePoint 2010 environment can have multiple trusted identity providers. Identify your SiteMinder trusted identity provider before modifying any claims that are associated with it.

Follow these steps:

1. Enter the following command to list all of the trusted identity providers:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers appears.
2. Locate your SiteMinder trusted identity provider in the list.

   Your SiteMinder trusted identity provider is identified.

Add a Claim to your Trusted Identity Provider

Adding a claim to your SiteMinder trusted identity provider involves several steps using the SharePoint 2010 Management Console. This example adds a claim for the last name of a user to the SiteMinder trusted identity provider. Use this example as a guide to add any claim you want to your SiteMinder trusted identity provider.

Follow these steps:

1. Enter the following command to assign the name of your <stmdnr> trusted identity provider to a variable:

   ```
   $trutsed_identity_provider_variable_name = Get-SPTrustedIdentityTokenIssuer
   -Identity "name_of_siteminder_trusted_identity_provider"
   ```

2. Enter the following command to add a claim type that is based on the last name of a user:

   ```
   $map2 = New-SPClaimTypeMapping -IncomingClaimType
   "http://schemas.xmlsoap.org/claims/lastname" -IncomingClaimTypeDisplayName
   "role" -LocalClaimType "http://schemas.xmlsoap.org/claims/lastname"
   ```

3. Enter the following command to associate the new claim type with your SiteMinder trusted identity provider:

   ```
   $map2 | Add-SPClaimTypeMapping -TrustedIdentityTokenIssuer
   $trutsed_identity_provider_variable_name
   ```

   The new claim is added to your trusted identity provider.

Verify the New Claim Exists

You can verify the addition of the new claim to your SiteMinder trusted identity provider. This example verifies the addition of a claim for the last name of a user.

Follow these steps:

1. Enter the following command to verify the presence of your new claim:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers appears.

2. Verify that new claim for your SiteMinder trusted identity provider appears.

Add an Attribute Mapping for the New Claim

Add an attribute mapping for the new claim using the SiteMinder Administrative UI. For this example, an attribute mapping links the claim, such as last name, to a specific attribute in your user directory. For both Active Directory servers and LDAP directories, map the Last Name claim to the sn attribute in your directory.

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the name of the new claim. For example, if your new claim is Last Name, as shown in this example, enter the following text:

   `Last Name`
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the directory attribute that you want to associate with the claim you added. For example, if your new claim is Last Name, as shown in this example, enter the following text:

   sn
9. Click OK.

   The Modify User directory page appears.
10. Click Submit.

    The attribute mapping for the new claim is created.

Update the Affiliate Domain with a Response Attribute

Update the affiliate domain with a response attribute for your new claim. This update requires running the SharePoint connection wizard on the computer hosting your SiteMinder Agent for SharePoint.

This procedure adds the mapping of the new claim to your SiteMinder Policy Server.

Follow these steps:

1. Navigate to the following directory:

   `Agent-for-SharePoint_home/sharepoint_connection_wizard`

2. Do *one* of the following procedures:

   - For Windows operating environments, right-click the executable and then select Run as administrator.
   - For Solaris operating environments, enter the following command:

     `Solaris: sh ./ca-spconnect-version-sol.bin`
   - For Linux operating environments, enter the following command:

     `Linux: sh ./ca-spconnect-version-rhel30.bin`

   The wizard starts.

3. Click Next.

   The Login Details screen appears.

4. Complete the following fields with the information from your existing SiteMinder settings:

   Policy Server Name

   Specifies the Policy Server name or IP address.

   Username

   Specifies the Policy Server administrator username.

   Password

   Specifies the Policy Server administrator password.

   Agent Name

   Specifies the Agent-4x. The connection with the Policy Server is established using the details given in the Agent Name.

   Shared Secret Key

   Specifies the shared secret key that is associated with the Agent.

5. Click Next

   The Select Action screen appears.

6. Select Edit a SharePoint Connection option.
7. Click Next.

   The SharePoint Connection Properties screen appears.
8. Click Next until the Add Attributes screen appears.
9. Click the drop-down arrows and select the values for the new claim from the following lists:

   Attribute

   Specifies an attribute name for one of the following claim types:

   - Group based
   - Role based

   For multivalued attributes, prefix FMATTR, as shown in the following example:

   Example: (multivalued attributes) FMATTR:LastName

   Claim Type

   Specifies an attribute value in your directory that is associated with the specified attribute name.

   Example: (Active Directory attribute value for LastName) sn.

   Example: (LDAP Directory role-based claim) sn.
10. Click Add, and then click Next.

    The attribute details are saved and the Commit Details screen appears.
11. Click Install in the Commit Details screen.

    The Save Complete screen appears.
12. Click Done.

    The partnership details are saved, the SharePoint Connection is modified, and the wizard closes.

Search for and Add Users using the New Claim

You can search for users to add to your SharePoint Policy for web application using the new claim. For example, if you added a claim for the Last Name attribute, you can search for users by entering their last names in the SharePoint people picker.

Follow these steps:

1. Click Start, Programs, Microsoft SharePoint 2010 Products.

   The Central Administration home page appears.

2. Click Manage web applications, in the Application Management section.

   The Web Applications Management page appears with a list of available web applications.

3. Click the web application name for which you want to add users.

   The buttons on the ribbon become available.

4. Click User Policy on the ribbon.

   The Policy for Web Application dialog appears.

5. Click Add Users.

   The Select Zone dialog appears.

6. Verify that the Zone you want appears in the drop-down list, and then Click Next.

   The Add Users dialog appears.

7. Click the Browse button, in the Choose Users section, below the Users text box.

   The Select People and Groups – Webpage Dialog appears.

8. Enter a value that corresponds to the new claim. For example, if your new claim is Last Name, enter the last name of a user.

   The right pane displays the search results with a list of users whose attributes match the value on which you searched.

9. Select the user and click Add.

   The selected user is added.

10. (Optional) Repeat steps 8 and 9 to select additional users.

11. Click OK.

    The Add Users dialog appears and displays the selected user.

12. Under Choose Permissions, click the permissions that you want to grant to the users.

13. Click Finish.

    The selected users and permissions are added.

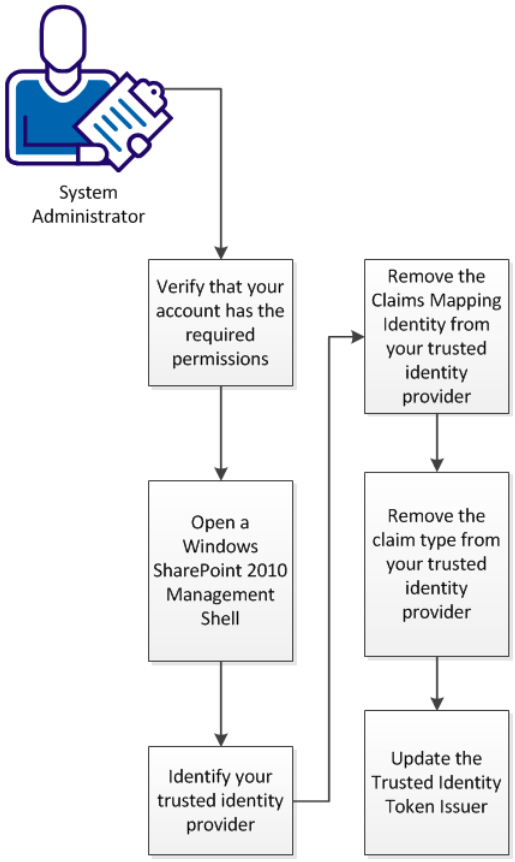
Removing Claims from Trusted Identity Providers

SharePoint 2010 supports third-party identity providers. These identity providers authenticate and authorize users who request SharePoint resources. A SharePoint administrator configures a trusted identity provider for a SharePoint environment.

Claims are a form of attribute or role, that a user has. Each claim has a name to identify it, and a value that the trusted identity provider verifies by connecting to a user directory.

For example, you can configure claims that correspond to the SamAccountName attribute of an Active Directory server or a uid of an LDAP directory server.

You can remove a claim to a SiteMinder trusted identity provider at any time. The following illustration describes the process:



To remove a claim from a SiteMinder trusted identity provider, follow these steps:

1. Verify that your account has the required permissions (see page 119).
2. Open a SharePoint 2010 Management Shell window on your SharePoint Central Administration server (see page 119).
3. Identify your trusted identity provider (see page 119).
4. Remove the claims mapping identity from your trusted identity provider (see page 127).
5. Remove the claim type from your trusted identity provider (see page 128).
6. Update the trusted identity token issuer (see page 128).

Verify that your Account has the Required Permissions

The user account with which you want to modify the SiteMinder trusted identity provider requires certain permissions. Modify the permissions of your user account if it does *not* meet the following conditions:

- An Administrator account.
- A member of the Administrators group.

Add the following privileges to your account:

- Local administrator on all SharePoint web front end (WFE) servers.
- Read/Write access to the configuration database.

Open a SharePoint 2010 Management Shell Window on your SharePoint Central Administration Server

Add claims to your <stmdnr> trusted identity provider using the SharePoint 2010 Management shell.

Follow these steps:

1. Log in to your SharePoint Central Administration server.
2. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   A SharePoint 2010 management shell command-line window appears.

Identify your Trusted Identity Provider

A SharePoint 2010 environment can have multiple trusted identity providers. Identify your SiteMinder trusted identity provider before modifying any claims that are associated with it.

Follow these steps:

1. Enter the following command to list all of the trusted identity providers:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers appears.

2. Locate your SiteMinder trusted identity provider in the list.

   Your SiteMinder trusted identity provider is identified.

Remove the ClaimsMapping Identity from your Trusted Identity Provider

Removing a claim from your SiteMinder trusted identity provider involves several steps using the SharePoint 2010 Management Console. This example removes a claim for the last name of a user from the SiteMinder trusted identity provider. Use this example as a guide to remove any claim you want from your SiteMinder trusted identity provider.

Follow these steps:

1. Enter the following command to assign the name of your <stmdnr> trusted identity provider to a variable:

   ```
   $trutsed_identity_provider_variable_name = Get-SPTrustedIdentityTokenIssuer
   -Identity "name_of_siteminder_trusted_identity_provider"
   ```

2. Enter the following command to verify that the correct item is assigned to the variable:

   ```
   echo $trutsed_identity_provider_variable_name
   ```

3. Enter the following command to remove the claim from the SiteMinder trusted identity provider. The command shown in the following example removes a claim for the last name of a user:

   ```
   Remove-SPClaimTypeMapping -Identity
   "http://schemas.xmlsoap.org/claims/lastname"  -TrustedIdentityTokenIssuer

   $trutsed_identity_provider_variable_name
   ```

4. Repeat Step 1 to refresh the variable for the SiteMinder trusted identity provider.

Remove the Claim Type from your Trusted Identity Provider

Remove the claim type from your SiteMinder trusted identity provider.

Follow these steps:

1. Enter the following command to list the claim types contained in the variable for your SiteMinder trusted identity provider:

   `$trutsed_identity_provider_variable_name.ClaimTypes`

2. From the previous list, locate the claim type that is associated with the claim identity you want to remove.
3. Enter the following command to remove the claim type:

   `$trutsed_identity_provider_variable_name.ClaimTypes.Remove("http://schemas.xmlsoap.org/claims/lastname")`

   For example, the previous command removes the claim type for the last name of a user.

Update the Trusted Identity Token Issuer

Update the SiteMinder trusted identity provider after removing the claim identity and the claim type.

Follow these steps:

1. Enter the following command to update the SiteMinder trusted identity provider:

   `$trutsed_identity_provider_variable_name.Update`

   The trusted identity provider is updated.

Configure the Authentication Providers

You can create a web application that uses Claims-based authentication type by using the SharePoint Central Administration user interface or Windows PowerShell. Use the Central Administration to create a web application.

If you want to automate the task of creating a web application, which is common in enterprises, use Windows PowerShell. You can also modify the authentication type of an existing classic based authentication to claims-based authentication using the PowerShell script.

Modify an Existing Classic Authentication to Claims-based Authentication

You can update a web application that uses classic authentication to claims-based authentication using a PowerShell script. The following procedure helps you migrate existing web applications configured to use classic authentication, to use claims-based authentication.

Important! You cannot reverse this process. After you convert the web application authentication type to a Claims-based authentication, you cannot reconvert the authentication to the previous type.

Follow these steps:

1. Open the SharePoint 2010 Management Shell command prompt.

   The command prompt appears.

2. Enter the following command to change the authentication mode to claims-based authentication:

   ```
   $WebAppName = "http:// yourWebAppUrl"
   $account = "yourDomain\yourUser"
   $wa = get-SPWebApplication $WebAppName

   Set-SPwebApplication $wa -AuthenticationProvider
   (New-SPAuthenticationProvider) -Zone Default
   ```

   The authentication mode is changed to claims-based authentication and the migration prompt is displayed.

   Note: The preceding command modifies an existing classic authentication web application to claims-based authentication. Associate this web application with the Trusted Identity Provider in the SharePoint Central Administration user interface.

3. Click Yes to continue, at the migration prompt.

4. Enter the following command to set the user as an administrator for the site:

   ```
   $wa = get-SPWebApplication $WebAppName
   $account = (New-SPClaimsPrincipal -identity $account -identitytype
   1).ToEncodedString()
   ```

   The user is set as the administrator for the site.

5. Enter the following command to configure the policy to enable the user to have full access:

   ```
   $zp = $wa.ZonePolicies("Default")
   $p = $zp.Add($account,"PSPolicy")
   $fc=$wa.PolicyRoles.GetSpecialRole("FullControl")
   $p.PolicyRoleBindings.Add($fc)
   $wa.Update()
   ```

   The user obtains full access.

6. Enter the following command to configure the policy to perform user migration:

   ```
   $wa = get-SPWebApplication $WebAppName
   $wa.MigrateUsers($true)
   ```

   The user migration process is completed.

7. Start SharePoint 2010 Central Administration from Start, Programs, Microsoft SharePoint 2010 Products.

   The Central Administration Home page appears.

8. Click Manage web applications, in the Application Management section.

   The Web Applications Management page appears with a list of available web applications.

9. Select the web application that has been updated and click Authentication Providers on the ribbon.

   The Authentication Providers dialog shows that the authentication type has been updated to claims-based authentication.

Note: For information about claims-based authentication and for using the Windows PowerShell, see the *SharePoint Server 2010 Deployment Guide* from the Microsoft TechNet website.

Add and Grant Permission to SiteMinder Users

You can add SiteMinder users to SharePoint and assign permission levels depending on the roles. Permission levels allow users to perform a set of related tasks.

Follow these steps:

1. Start SharePoint 2010 Central Administration from Start, Programs, Microsoft SharePoint 2010 Products.

   The Central Administration home page appears.

2. Click Manage web applications, in the Application Management section.

   The Web Applications Management page appears with a list of available web applications.

3. Click the web application name for which you want to add users.

   The buttons on the ribbon become available.

4. Click User Policy on the ribbon.

   The Policy for Web Application dialog appears.

5. Click Add Users.

   The Select Zone dialog appears.

6. Verify that the Zone you want appears in the drop-down list, and then Click Next.

   The Add Users dialog appears.

7. Click the Browse button, in the Choose Users section, below the Users text box.

   The Select People and Groups – Webpage Dialog appears.

8. Browse and select the user group to search for the user.

   The right pane displays the search results with the list of users.

9. Select the user and click Add.

   SharePoint adds the selected user.

10. (Optional) Repeat steps 8 and 9 to select additional users.

11. Click OK.

    The Add Users dialog appears and displays the selected users.

12. Select the required permissions for the users, in the Choose Permissions section.

13. Click Finish.

    SharePoint adds the selected users and assigns the selected permissions to the users.

Manage User Profiles

The SiteMinder Agent for SharePoint [insert SiteMinder version number] does not support User Profile Import or User Migration. However, you can use the Microsoft SharePoint User Profile Synchronization Service to import user information from external directory sources. The User Profile Synchronization Service lets you extract the additional data from the external directory and augments the user records with this data. Data can also be written to the directory source (such as Active Directory or an LDAP directory), provided appropriate permissions are present.

The User Profile Service in SharePoint stores information about users in a central location, that allows multiple SharePoint applications to manage user profiles. Enable the User Profile service using SharePoint Central Administration.

You can configure SharePoint to use the User Profile Synchronization Service to import SiteMinder users. And you can use the SiteMinder Agent for SharePoint solution to protect the web applications.

Note: For more information about User Profile Synchronization, see the *Configure profile synchronization* article from the Microsoft TechNet website.

Chapter 10: Features to Set Up Following Basic Installation and Configuration of the Agent for SharePoint

This section contains the following topics:

Additional SharePoint Configuration Options

Perform any of these additional configuration steps at any time:

- Create a web application that uses claims-based authentication (see page 133).
- Enable SSL on your IIS web server for a web application (see page 134).
- Enable SSL for the web application (see page 135).

Create a New Web Application with Claims based Authentication

Follow these steps:

1. Start SharePoint 2010 Central Administration from Start, Programs, Microsoft SharePoint 2010 Products.

   The Central Administration home page appears.

2. Click Manage web applications, in the Application Management section.

   The Web Applications Management page appears with a list of available web applications.

3. Click New, on the ribbon.

   Create New Web Application dialog appears.

4. Select Claims Based Authentication option, in the Authentication section.
5. Select Yes option for Use Secure Sockets Layer (SSL), in the Security Configuration section.
6. Select the Trusted Identity Provider option, in the Claims Authentication Types.

   Note: This option is already selected if you have set up Trusted Identity Provider authentication in Windows PowerShell.

   Important! Verify that the options for all other authentication types in the Claims Authentication Types section are cleared.
7. Complete the remaining appropriate sections.
8. Click OK.

   A new web application with claims authentication is created.

Note: For information about Claims-based authentication, see www.microsoft.com.

Enable SSL on IIS for the Web Application

A Secure Sockets Layer (SSL) encryption is required for a web application as it provides greater security. When SSL is enabled, remote clients access the web application using URLs that start with https://.

The following procedure describes how to enable SSL on IIS Manager.

Follow these steps:

1. Click Start, Administrative Tools, Internet Information Services (IIS) Manager.

   The IIS Manager dialog appears.
2. Navigate to and select the Windows Claims-based authentication web application site that requires SSL encryption, in the Connections pane.
3. Click Edit Bindings in the Actions pane.

   The Site Bindings dialog appears.
4. Select the https entry, and then click Edit.

   The Edit Site Binding dialog appears.

5. Select the appropriate certificate from the list, in the SSL Certificate field.
6. Click OK.

   The Site Bindings dialog appears.
7. Click Close.

   The web application is enabled for SSL encryption.

Note: If you do not find an appropriate certificate, you cannot bypass the certificate warning screen. If you have a certificate that is issued to the URL, you can import the certificate in to the client to bypass the certificate warning. For more information about configuring a Secure Sockets Layer, refer the *IIS 7 Operations Guide* from www.microsoft.com.

More information:

Create a New Web Application with Claims based Authentication (see page 133)
Enable SSL for the Web Application (see page 135)

Enable SSL for the Web Application

You can configure the web application to use SSL when you create a web application. See *Create a Web Application with Claims-based Authentication* for the procedure to enable SSL when creating a web application. Alternatively, you can extend the SLL capability of a web application by performing the following procedure.

Follow these steps:

1. Click Start, Programs, Microsoft SharePoint 2010 Products, Start SharePoint 2010 Central Administration.

   The Central Administration home page appears.
2. Click Application Management, Configure alternate access mappings section.

   The Central Administration> Alternate Access Mappings page appears with a list of available web applications.
3. Click Add Internal URLs button.

   The Central Administration> Add Internal URLs page appears.

4. Select an Alternate Access Mapping Collection from the Alternate Access Mapping Collection list.
5. Enter the URL with HTTPS in the Add Internal URL field and select a zone.

   For example, enter https://spserver.example.com.
6. Click OK.

   The Central Administration> Alternate Access Mappings page appears with the modified URL.

Note: If you do not find an appropriate certificate, you cannot bypass the certificate warning screen. If you have a certificate that is issued to the URL, you can import the certificate in to the client to bypass the certificate warning. For more information about enabling SSL, for the web application in SharePoint refer www.microsoft.com.

More information:

Create a New Web Application with Claims based Authentication (see page 133)
Enable SSL on IIS for the Web Application (see page 134)

Office Client Integration

Office Client Integration lets users edit and update documents stored on SharePoint with the respective Microsoft Office applications. For example, someone who has Microsoft Word can revise a Word document stored SharePoint.

How to Enable Office Client Integration for the Agent for SharePoint

Enabling support for Office Client Integration involves several separate procedures. To enable support for Office Client Integration, use the following process:

1. Update the SiteMinder Agent Type to include the HTTP methods for WebDAV (see page 137).
2. Add the HTTP Methods for WebDAV to your Existing SiteMinder Rules (see page 138).
3. Update your Agent Configuration Settings for Office Client Integration (see page 139).

Update the SiteMinder Agent Type to include the HTTP methods for WebDAV

To use the Office Client Integration feature, modify the SiteMinder Agent type to include the methods for WebDAV.

Note: To reuse application resources or domain rules from your existing SiteMinder environment, add these WebDAV methods to each respective item that you want to reuse (see page 138).

Follow these steps:

1. Click Infrastructure, Agents, Agent Type, Modify Agent Type.

   The Create Agent Type search pane appears.

2. Highlight the text in the search field, and then type the following:

   Web Agent

3. Click Search.

   The SiteMinder Web Agent type appears in the list.

4. Click Select.

   The Modify Agent Type: *Web Agent* pane appears.

5. Scroll to the bottom of the Actions section, and then click Create.

   A new action field appears at the end of the list.

6. Highlight the text in the New Action field, and then enter the following:

   Head

7. Scroll to the bottom of the Actions section, and then click Create.

   A new action field appears at the end of the list.

8. Repeat Steps 6 and 7 until all of the following methods are added:

   OPTIONS

   PROPFIND

   PROPPATCH

   COPY

   DELETE

   MOVE

   LOCK

   UNLOCK

9. Click Submit.

   The Modify Agent type task is submitted for processing. A confirmation screen appears.

10. Click OK.

    The Agent type settings for your SharePoint resources are updated.

Add the HTTP Methods for WebDAV to your Existing SiteMinder Rules

To use the Office Client Integration feature with the Agent for SharePoint, update the Web agent actions in any rules protecting SharePoint sites.

Follow these steps:

1. Verify that your Web Agent type is updated (see page 137).
2. Click Policies, Domains, Rule, Modify Rule.

   The Modify Rule screen appears.

3. Click the option button of the domain that contains the rule you want, and then click Select.

   Modify Rule: Name screen appears.

4. In the Action drop-down list, press and hold Ctrl and click the following items:

   - HEAD
   - OPTIONS
   - PROPFIND
   - PROPPATCH
   - COPY
   - DELETE
   - MOVE
   - LOCK
   - UNLOCK

5. Click Submit.

   The rule is updated, and the confirmation screen appears.

Update your Agent Configuration Settings for Office Client Integration

The parameter settings in the Agent Configuration Object associated with your Agent for SharePoint control how Office Client Integration operates on your Agent for SharePoint.

follow these steps:

1. Open the Administrative UI.
2. Click Infrastructure, Agent Configuration, Modify Agent Configuration.

   The Modify Agent Configuration: Search pane opens.

3. Specify search criteria that apply to the Agent Configuration Object you are using with the Agent for SharePoint, and then click Search.

   A list of Agent configuration objects that match the search criteria opens.

4. Select an Agent Configuration object for your Agent for SharePoint, and then click Select.

   The Modify Agent Configuration: Name pane opens.

5. Change the values of the following parameters:

SPClientIntegration

Specifies the hostnames of the SharePoint servers protected by the Agent for SharePoint on which you want to permit Office Client Integration. The default parameter is blank and listed as plain. If there are multiple host entries, use the multivalue option button to add multiple hosts.

Add a port number to the value if the Agent for SharePoint operates on a nondefault port (any port except 80 or 443).

To use this parameter, verify that the SharePoint resources protected by SiteMinder also have their Office Client Integration enabled on the SharePoint central administration server.

Client Integration requires a persistent FedAuth cookie, verify that your SharePoint server is not configured to use session cookies. By default, UseSessionCookies in SharePoint is set to NO.

Default: None

Limits: Multiple values allowed. Use fully qualified domain names for all values.

Example: *agent_for_sharepoint_host_name.*example.com (default ports of 80 or 443)

Example: *agent_for_sharepoint_host_name.*example.com:81 (with nondefault port number for HTTP)

Example: *agent_for_sharepoint_host_name.*example.com:4343 (with nondefault port number for HTTPS)

SPDisableClientIntegration

Specifies the hostnames of the SharePoint servers protected by the Agent for SharePoint on which you want to prohibit Office Client Integration. The default parameter is blank and listed as plain. If there are multiple host entries, then switch over to multi-value parameter. The URL in this parameter *requires* a port number (even for a default port such as 80 or 443).

Use this setting to prevent SharePoint administrators from circumventing SiteMinder settings regarding Office Client integration.

Limit: Multiple values allowed.

Example: *agent_for_sharepoint_host_name:port_number*

6. The following parameter describes the user agent values allowed by the Agent for SharePoint:

   SPAuthorizeUserAgent

   Specifies a list of Microsoft Office user-agent strings for which the Agent for SharePoint allows access. This list is populated automatically with the default values when the Agent for SharePoint starts. The user-agent strings in this parameter act as a whitelist. Changes to this parameter override the default settings. Access is denied to clients whose user-agent string does not appear in the list.

   For example, setting the value to Microsoft Office allows access to all versions of Microsoft Office products associated with the respective user agent string. Conversely, setting the value to Microsoft Office/12.0 allows access to only those versions of Microsoft Office products associated with the respective user agent string.

   Default: Microsoft Office, MS FrontPage, MSFrontPage, Microsoft Data Access Internet Publishing Provider Protocol Discovery, Test for Web Form Existence, Microsoft-WebDAV-MiniRedir

   Limits: Multiple values allowed.

7. Examine the default values of the previous parameter. Consult with your SharePoint administrator to determine if additional user agent values are required.
8. Change the value of the CSSChecking parameter to no.

   Note: Because the Agent for SharePoint is a proxy-based solution, this setting is required for Office Client Integration.

9. Click OK.

   The new values appear next to the parameters in the list.

10. Click Submit.

    The Create Agent Configuration Task is submitted for processing and the confirmation message appears.

Claims Provider

The Claims Provider in the Agent for SharePoint is used for configuring particular claim values to grant permissions to SharePoint resources using the SharePoint people picker. The Claims Provider is packaged as a SharePoint solution (WSP file) with its feature receiver.

The Claims Provider requires Directory Attribute Mappings that you configure using the SiteMinder Administrative UI. The Claims Provider uses these mappings to display the results of your searches in the SharePoint people picker.

Using the Claims Provider involves several separate procedures. Use the following process.

1. Create virtual attribute mappings (see page 143).
2. Install the Claims Provider (see page 158).
3. Configure the Claims Provider (see page 159).

Note: The Claims Provider for SharePoint installer supports Windows 64-bit Operating Systems.

Claims Provider Searches and Results

The SharePoint claims provider lets you search your SiteMinder directories with the SharePoint people picker.

The following table describes the relationships between the search criteria you enter in the people picker and the search results that appear:

When you search for this attribute in the SharePoint people picker:	The SharePoint people picker returns the following results:
User identifier or display name.	The user identifier or the display name of the user
Group name	The friendly name associated with the smusergroup attribute
Other attributes (such as claim names based on a role)	The attribute value you associated with the role.

Agent for SharePoint Virtual Attribute Mappings

Virtual attribute mappings create relationships between the attributes from your SiteMinder user directories and the SiteMinder claims provider. These mappings allow SiteMinder to search your user directories for claims, and display the results in the SharePoint people picker.

The following types of claims are supported:

- User claims (one is required)
- Group claims
- Role claims

Note: Configuring this feature requires information from several systems or administrators in your organization. Work with the administrators for your SharePoint environment and with administrators for the user directories in your organization.

Virtual Attribute Mapping Examples for an LDAP Directory

To search the user directory in your SiteMinder environment using the SharePoint people picker, create virtual attribute mappings. The Agent for SharePoint requires at least *one* attribute mapping for claims that are based on the ID of a user. Create additional mappings to accommodate your needs.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Each additional mapping creates another association between a specific attribute in your user directory and the Agent for SharePoint. The people picker in SharePoint uses these associations to search your user directory using the values you specify. For example, you can create an attribute mapping that lets you search by user name, group name or email address.

The following table identifies the typical LDAP directory attribute mappings and describes how they are used in your SiteMinder and SharePoint environments:

For LDAP Directories:	**Create a SiteMinder virtual attribute to search for this claim with the people picker.**		**Create a SiteMinder virtual attribute so the friendly names appear in the people picker next to the corresponding claim values.**		**Enter these corresponding values in the SharePoint Connection wizard.**		**(Optional) Customize the display name for the people picker**
Purpose	**1. Use this name for your virtual attribute.**	**2. Enter the name of the directory attribute you want to use for the claim value.**	**3. Use this name for the SiteMinder virtual attribute.**	**4. Use this name for the directory attribute you want to use as a claim value.**	**5. To define the claim in the connection wizard:**	**6. To define the attribute value for the claim in the connection wizard:**	**7. Replace the string following the -IncomingClaimTypeDisplayName with this value:**
Mandatory User claim that uniquely identifies the user.	useridentifier	uid	smuserdisplayname	displayName	Enter the following value in the Identifier Claim Name field: useridentifier	Enter the following value in the Directory Attribute field: uid	User ID

(Optional) Group-based user-claim that is based on a DN in the directory.	smusergroups	Description (use the friendly name of your groups).	Not required for group-based claims.	Click the Attribute drop-down list and then select the following value: smusergroups	Not required. The connection wizard configures this setting automatically.	Group
(Optional) Role-based user claim	userrole	employeeType	Not supported.	1. Click the Attribute drop-down list and then select the following value: NameValue 2. Click the Claim type drop-down list and select the following value: User Attribute 3. Click the Claim Name field and enter the following value: userrole	Enter the following value in the Directory Attribute field: employeeType	Role

Virtual Attribute Mapping Examples for a Microsoft Active Directory Server

To search the user directory in your SiteMinder environment using the SharePoint people picker, create virtual attribute mappings. The Agent for SharePoint requires at least *one* attribute mapping for claims that are based on the ID of a user. Create additional mappings to accommodate your needs.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Each additional mapping creates another association between a specific attribute in your user directory and the Agent for SharePoint. The people picker in SharePoint uses these associations to search your user directories using the values you specify. For example, you can create an attribute mapping that lets you search by user name, group name or email address.

The following table identifies the typical Microsoft Active Directory attribute mappings and describes how they are used in your SiteMinder and SharePoint environments:

For Active Directories:	**Create a SiteMinder virtual attribute to search for this claim with the people picker.**		**Create a SiteMinder virtual attribute so the friendly names appear in the people picker next to the corresponding claim values.**		**Enter these corresponding values in the SharePoint Connection wizard.**		**(Optional) Customize the display name for the people picker**
Purpose	**1. Use this name for your virtual attribute.**	**2. Enter the name of the directory attribute you want to use for the claim value.**	**3. Use this name for the SiteMinder virtual attribute.**	**4. Use this name for the directory attribute you want to use as a claim value.**	**5. To define the claim in the connection wizard:**	**6. To define the attribute value for the claim in the connection wizard:**	**7. Replace the string following the -Incoming ClaimType DisplayName with this value:**
Mandatory User claim that uniquely identifies the user.	useridentifier	sAMAccountName	smuserdisplayname	displayName	Enter the following value in the Identifier Claim Name field: useridentifier	Enter the following value in the Directory Attribute field: sAMAccountName	User ID

(Optional) A group-based user-claim corresponding to a DN in the directory.	smusergroups	name (use the friendly name of your groups).	Not required for group-based claims.	Click the Attribute drop-down list and then select the following value: smusergroups	Not required. The connection wizard automatically configures this setting.	Group
(Optional) Role-based user claim	userrole	countryCode	Not supported.	1. Click the Attribute drop-down list and then select the following value: NameValue 2. Click the Claim type drop-down list and select the following value: User Attribute 3. Click the Claim Name field and enter the following value: userrole	Enter the following value in the Directory Attribute field: countryCode	Role

User Claims

Integration with SharePoint requires at least one claim that contains an identifier that uniquely identifies the user. These claims often appear in the people picker as cryptic values, such as the following example:

```
uid=e123456
```

Such claims are difficult to associate with the intended user. The Agent for SharePoint uses a special attribute mapping which retrieves the display name of the user. This user name appears next to the related identifier claim in the people picker. After this user mapping is configured, the previous example appears in the people picker like the following one:

uid=e123456 *associated_user_name*

Create an Attribute Mapping for User Claims in an LDAP Directory

The Agent for SharePoint requires an attribute mapping based on an attribute with a unique value for each user. Use the Administrative UI to create a pair of attribute mappings that defines how SiteMinder searches for user claims through the SharePoint people picker.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Note: For more information about the relationships between attribute mappings in an LDAP directory and the other components of your environment, see the LDAP examples chart (see page 144).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   `useridentifier`
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   `uid`
9. Click OK.

   The Modify User directory page appears.
10. To create the second mapping, repeat Steps 4 through 5.
11. Click the name field, and then enter the following name:

    `smuserdisplayname`
12. Verify that the Alias option button is selected, and then click the Definition field.
13. Enter the following definition:

    `displayName`
14. Click OK.

The Modify User directory page appears.

15. Click Submit.

    The attribute mappings are created.

Create an Attribute Mapping for User Claims in a Microsoft Active Directory Server

The Agent for SharePoint requires an attribute mapping that is based on an attribute with a unique value for each user. Use the Administrative UI to create a pair of attribute mappings that defines how SiteMinder searches for user claims through the SharePoint people picker.

Important! The Agent for SharePoint supports only one SiteMinder user directory.

Note: For more information about relationships between attribute mappings in an Active Directory server and other components of your environment, see the Active Directory examples table (see page 146).

Follow these steps:

1. Log in to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   `useridentifier`
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   `sAMAccountName`
9. Click OK.

   The Modify User directory page appears.
10. To create the second mapping, repeat Steps 4 through 5.
11. Click the name field, and then enter the following name:

    `smuserdisplayname`
12. Verify that the Alias option button is selected, and then click the Definition field.
13. Enter the following definition:

    `displayName`
14. Click OK.

The Modify User directory page appears.

15. Click Submit.

    The attribute mappings are created.

Group Claims

You can also configure a claim that uses the groups to which the user belongs. Group mappings assign SharePoint permissions based on groups of users rather than individuals.

Some user directories define the groups of users by including an attribute in the record that contains the distinguished name (DN) of each group. The DN also appears as a cryptic value such as the following example:

```
entryDN=cn=grp12345,ou=Groups,dc=example,dc=com
```

Such claims are difficult to identify the name of the group associated with the value in the people picker.

The Agent for SharePoint uses two attribute mappings and the groups setting you specify in the SharePoint connection wizard to search for groups by their display name. The Agent for SharePoint retrieves both the display name of the group and DN of the group.

Both the display name and the DN of the group then appear in the people picker, for as shown in the following example:

cn=grp12345,ou=Groups,dc=example,dc=com(Sales Managers).

Create Attribute Mappings for Group-based Claims in LDAP Directories

You can also create attribute mappings based on a group of users. Use the Administrative UI to create an attribute mapping that defines how SiteMinder searches for group claims through the SharePoint people picker.

Note: For more information about the relationships between attribute mappings in an LDAP directory and the other components of your environment, see the LDAP examples chart (see page 144).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   ```
   smusergroups
   ```
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   ```
   description
   ```
9. Click OK.

   The Modify User directory page appears.
10. Click Submit.

    The attribute mapping is created.

Create Attribute Mappings for Group-based Claims in Active Directory

You can also create attribute mappings based on a group of users. Use the Administrative UI to create an attribute mapping that defines how SiteMinder searches for group claims through the SharePoint people picker.

Note: For more information about relationships between attribute mappings in an Active Directory server and other components of your environment, see the Active Directory examples table (see page 146).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   ```
   smusergroups
   ```
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   ```
   name
   ```
9. Click OK.

   The Modify User directory page appears.
10. Click Submit.

    The attribute mapping is created.

Role Claims

You can also configure any number of claims in Name=Value format. These name/value pairs are often named *role claims*.

Role claims are found by reading a configurable attribute on the user record in your user directory. You can then assign any name you want for the claim. For example, you can name a claim “userrole” and configure it to point to the “employeeType” attribute in your LDAP directory.

After authentication the Agent for SharePoint creates a name/value pair such as “userrole=manager” for the claim. If the "employeeType" attribute for the authenticated user contains the value named manager, SharePoint allows the user access to the resource.

Create an Attribute Mapping for a Role-based Claims in LDAP Directories

You can also create attribute mappings based on user roles. Use the Administrative UI to create an attribute mapping that defines how SiteMinder searches for role-based claims through the SharePoint people picker.

Note: For more information about the relationships between attribute mappings in an LDAP directory and the other components of your environment, see the LDAP examples chart (see page 144).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   `userrole`
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   `employeeType`
9. Click OK.

   The Modify User directory page appears.
10. Click Submit.

    The attribute mapping is created.
11. (Optional) Create more role-based mappings to suit your needs.

Create an Attribute Mapping for a Role-based Claims in Active Directory

You can also create attribute mappings based on user roles. Use the Administrative UI to create an attribute mapping that defines how SiteMinder searches for role-based claims through the SharePoint people picker.

Note: For more information about relationships between attribute mappings in an Active Directory server and other components of your environment, see the Active Directory examples table (see page 146).

Follow these steps:

1. Log on to the SiteMinder Administrative UI.
2. Click Infrastructure, Directory, User Directory, Modify User Directory.

   A list of user directory connections appears.
3. Click the option button for your user directory, and then click Select.

   The Modify User directory page appears.
4. Click Create.

   The create attribute mapping page appears.
5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.
6. Click the name field, and enter the following name:

   `userrole`
7. Verify that the Alias option button is selected, and then click the Definition field.
8. Enter the following definition:

   `countryCode`
9. Click OK.

   The Modify User directory page appears.
10. Click Submit.

    The attribute mapping is created.
11. (Optional) Create more role-based mappings to suit your needs.

Install Claims Provider

If you are not the user who installed or configured SharePoint, you need one of the following privileges to run the Claims Provider installer:

- Administrator for the local server
- Administrator for the group
- Farm Administrator (for SharePoint farms)

If you are installing your Claims provider on a new SharePoint farm, install the claims provider on your SharePoint central administration server. If you add additional SharePoint servers to your farm later, install the claims provider on each SharePoint server you add.

Follow these steps:

1. Copy the installation program from the download location on the CA Support site.
2. Browse to the Win32 directory in the sp2010-agent-12.0-*version* folder.
3. Right-click the executable and select Run as administrator or double-click ca-sp2010claims-*version*-win64.exe.

   The installation program starts.
4. Follow the instructions from the installation wizard.
5. Restart your system after the installation finishes.

   The Claims provider is successfully installed.

More information:

Locate the SiteMinder Agent for SharePoint Platform Support Matrix (see page 249)
Locate the Installation Media (see page 250)

Verify Claims Provider Installation

Follow these steps:

1. Start SharePoint 2010 Central Administration from Start, Programs, Microsoft SharePoint 2010 Products.
2. Click System Settings.

   The Central Administration>System Settings page appears.
3. Click Manage Farm Solutions, in the Farm Management section.

   The Central Administration>Solution Management page appears and the status of the Claims Provider is shown as Deployed.

How to Configure the Claims Provider

After you install the SiteMinder Claims provider, add the claims search service and update the claims provider of the trusted identity token issuer:

follow these steps:

1. Update the claims provider of the trusted identity token issuer (see page 159).
2. Add the Claims search service (see page 160).

After you add the Claims Search service, you can also configure the Claims Provider to suit your needs with any of the following optional procedures:

- Create SharePoint policies with place holders for expected directory attribute values. (see page 162)
- Change how directory attributes appear in the SharePoint people picker (see page 163).

Update the Claims Provider of the Trusted Identity Token Issuer

The Update-SMTrustedIdentityTokenIssuer command updates the claims provider of a trusted identity token issuer to CASiteMinderClaimProvider.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, the SharePoint 2010 Management Shell.

   The SharePoint 2010 Management Shell command prompt appears.

2. Navigate to the following directory:

   ```
   C:\Program Files\CA\SharePointClaimsProvider\scripts
   ```

3. Enter the update command. This command has the following format:

   ```
   Update-SMTrustedIdentityTokenIssuer.ps1 –TrustedIdentityTokenIssuer
   “<Trusted_Identity_Provider_registered_with_SharePoint>”
   ```

   TrustedIdentityTokenIssuer

   Specifies the name of the SiteMinder trusted identity token issuer (trusted login provider) to update.

   Example:

   ```
   .\Update-SMTrustedIdentityTokenIssuer.ps1 –TrustedIdentityTokenIssuer
   “SiteMinder Federation”
   ```

   SharePoint is updated with the new claims provider of the trusted identity token issuer.

The following conditions apply when you execute the Update-SMTrustedIdentityTokenIssuer command:

- The default trusted claims provider created by SharePoint is removed.
- The SharePoint administrator can use the configured claim provider for searching claims.
- The claims provider of the trusted identity token issuer cannot be empty.
- A new trusted claims provider cannot be created.

Add Claims Search Web Service

Add the claims search web service used in the Agent for SharePoint to specific SharePoint web applications by executing the Add-SMClaimSearchService command. The changes made by this script are reflected across the SharePoint Farm.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, the SharePoint 2010 Management Shell.

   The SharePoint 2010 Management Shell command prompt appears.

2. Navigate to the following directory:

   ```
   C:\Program Files\CA\SharePointClaimsProvider\scripts
   ```

3. Enter the add command. This command has the following format:

   ```
   ADD-SMClaimSearchService.ps1 –WebApplication <URL_of_web_application>
   –claimSearchService <URL_of_claim_search_service_in_spagent>
   ```

   WebApplication

   Specifies the URL of the web application.

   claimSearchService

   Specifies the URL of the claim search service running in Agent for SharePoint.

   Example:

   ```
   .\ADD-SMClaimSearchService.ps1 –WebApplication http://myhostname:1234
   –claimSearchService
   http://spagent.ca.com:2345/ClaimsWS/services/WSSharePointClaimsServiceImp
   l
   ```

   The claims search web service is added to the web.conf file of the web application.

4. Enter the add command again, to add the claims web search service to the web.conf file of the SharePoint Central Administration.

   ```
   ADD-SMClaimSearchService.ps1 –WebApplication <Central_Administration_URL>
   –claimSearchService <URL_of_claim_search_service_in_spagent>
   ```

WebApplication

Specifies the URL of the SharePoint Central Administration website.

claimSearchService

Specifies the URL of the claim search service running in the Agent for SharePoint. Add the port number you specified for the Claims WS of the Agent for SharePoint when you ran the Configuration wizard to the end of the URL.

Example:

```
.\ADD-SMClaimSearchService.ps1 –WebApplication
http://SharePoint_server_name:1221 –claimSearchService
http://spagent.ca.com:2345/ClaimsWS/services/WSSharePointClaimsServiceImp
l
```

The claims search web service is added to the web.conf file of the SharePoint Central Administration.

More information:

Agent for SharePoint Configuration Wizard Information Worksheet (see page 245)

Create SharePoint Policies with Placeholders for Expected Directory Attributes

The Agent for SharePoint lets you create policies in your SharePoint environment using directory attribute values that do not yet exist in your associated user directory.

For example, suppose your directory server contains an attribute named employeeType, and the employeeType attribute uses one of the following values for each user:

- Employee
- Contractor
- Manager
- Executive

For example, suppose you want to create an attribute value for the employeeType attribute named Vendor in your directory servers to use with SharePoint.

If a different group in your organization manages the directory servers, that task is beyond your control. The Claims Provider creates placeholders for the new attribute values using the loopback feature.

In this example, use the loopback feature so that the Vendor attribute value exists in your SharePoint environment it appears in the directory servers. New attribute values let you create SharePoint policies whenever you want, without waiting for your administrator to add the actual attribute values to your directory.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   The management shell command line window opens.

2. Navigate to the following directory:

   ```
   C:\Program Files\CA\SharePointClaimsProvider\scripts
   ```

3. Enter the following command:

   ```
   .\Set-SMClaimProviderConfiguration.ps1 -EnableLoopBackSearch
   ```

   Loopback search is enabled.

4. Use the SharePoint people picker to search the new attribute values you want.

   A placeholder for the new attribute value is added to SharePoint using the loopback search function.

5. Repeat Step 4 to add additional placeholders for more attribute values.

6. (Optional) After adding your placeholders, disable support for the loopback search function by doing the following steps:

   a. Repeat Steps 1 and 2.

b. Enter the following command:

```
.\Set-SMClaimProviderConfiguration.ps1 -DisableLoopBackSearch
```

Loopback search is disabled.

Change How Directory Attributes Appear in the SharePoint People Picker

You can customize how certain directory attributes from your SiteMinder user directories appear in the SharePoint people picker.

Change how directory attributes appear in the SharePoint people picker

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   The management shell command line window opens.

2. Navigate to the following directory:

   ```
   C:\Program Files\CA\SharePointClaimsProvider\scripts
   ```

3. Enter the .\Set-SMClaimProviderConfiguration.ps1 command with one of the following options:

   -UserNameFormat

   Specifies how the user names for which you search appear in the SharePoint people picker. Use one of the following options:

   ValueOnly

   Displays only the value of the identifier claim attribute in your directory server associated with the user. For example, if your uid is user_*number,* then only user_*number* appears in your search results.

   Example: user_0001

   DisplaynameOnly

   Displays only the name of the user, using the format specified in your SiteMinder directory.

   Example: *last_name_of_user*, *first_name_of_user*

   DisplaynameAppended

   Displays the name of the user, and the value of the identifier claim attribute in your directory server associated with the user.

   Example: user_0001 (*last_name_of_user*, *first_name_of_user)*

-GroupNameFormat

Specifies how the group names for which you search appear in the SharePoint people picker. Use one of the following options:

ValueOnly

Displays only the domain name (DN) value of the group claim attribute in your directory server associated with the user.

Example: OU=group_0001, DC=example, DC=COM

DisplaynameOnly

Displays only the name of the group, using the format specified in your SiteMinder directory.

Example: *group_name*

DisplaynameAppended

Displays the name of the group, and the value of the group claim attribute in your directory server associated with the user.

Example: *group_name* OU=group_0001, DC=example, DC=COM

The appearance of the directory attributes is changed.

Increase the size of the MaxUserAttributeLength Setting

Increase the size of the MaxUserAttributeLength setting in your Policy Server if you are creating group-based virtual attribute mappings. In Active Directory servers, the SiteMinder claims provider binds the group name to its associated domain. If the names of the associated domains are too long to fit in the window, the claims provider truncates them. To avoid this truncation, increase the size of the MaxUserAttributeLength setting in your Policy Server.

follow these steps:

1. Open the following file on your Policy Server:

   policy_server_home\config\properties\wsfed.properties

2. Locate the following line:

   com.netegrity.assertiongenerator.wsfed.MaxUserAttributeLength=1024

3. Change the value 1024 (at the end of the line) to a larger number. We recommend using multiples of 1024.

   The size of the MaxUserAttributeLength setting is increased.

Remove Claims Search Web Service

The Remove-SMClaimSearchService command removes the changes made in the web.config file. The script identifies the modifications made by the user from the *CASiteMinderSharePoint2010Agent_ClaimsSearchServiceEndpoint* file.

Follow these steps:

1. Click Start, All Programs, Microsoft SharePoint 2010 Products, the SharePoint 2010 Management Shell.

   The SharePoint 2010 Management Shell command prompt appears.

2. Navigate to the folloiwng directory:

   ```
   C:\Program Files\CA\SharePointClaimsProvider\scripts
   ```

3. Enter the remove command. This command has the following format:

   ```
   Remove-SMClaimSearchService.ps1 –WebApplication <URL_of_web_application>
   ```

   WebApplication

   Specifies the URL of the web application.

   Example:

   ```
   .\Remove-SMClaimSearchService.ps1 –WebApplication http://myhostname:1234
   ```

   The changes made in the web.config file are removed.

Extend Web Applications to Different Zones for CRAWL Service and Search Support

The Agent for SharePoint does not support CRAWL services because the service does not use SiteMinder cookies. The SharePoint CRAWL service uses Windows authentication, and the Agent for SharePoint uses claims authentication. Because the SharePoint CRAWL service cannot respond to the authentication challenge the Agent for SharePoint makes, the Agent for SharePoint denies the request. When this denial occurs, the connection to the CRAWL service or the search times out.

follow these steps:

1. Extend the SharePoint web application with which you want to use the crawl service to a different zone.
2. Configure the extended web application (from Step 1) to use Integrated Windows (IWA or NTLM) authentication.
3. Configure the CRAWL service to use the URL of the extended SharePoint web application (from Step 1).

   Extending the web application to another zone provides protection of the web application with the Agent for SharePoint while supporting the CRAWL service and search functions.

Chapter 11: Advanced Options

This section contains the following topics:

Virtual Hosts with the Agent for SharePoint

The following sections describe using virtual hosts with your Agent for SharePoint.

Virtual Host Configurations Supported by the Agent for SharePoint

The SiteMinder Agent for SharePoint supports virtual hosts. Virtual hosts conserve hardware resources by operating different websites on a single server.

The Agent for SharePoint supports virtual hosts that use the following configuration methods:

Port-based virtual hosts

Indicates a virtual host on your Agent for SharePoint server that operates on a unique port number.

Host-header-based virtual hosts

Indicates a virtual host on your Agent for SharePoint server that uses unique host header values.

Path-based virtual hosts

Indicates a virtual host on your Agent for SharePoint server using unique URI values.

More information:

Set a Basic Proxy Rule for the Agent for SharePoint (see page 81)

Define Virtual Hosts for each Web Application

Virtual hosts are required for each SharePoint web application you want to protect. Define a virtual host for each SharePoint web application on the Agent for SharePoint server. A single virtual host definition on the Agent for SharePoint server accommodates the following types of proxy rules:

- Port-based forwarding
- Host-header-based forwarding
- Path-based forwarding

Follow these steps:

1. Use a text editor to open the following file:

   Agent-for-SharePoint_home\proxy-engine\conf\server.conf

2. Locate the following line:

   hostnames="*default_SharePoint_URL*"

3. Change the value of previous line to include a default URL to which you want to forward any requests that are *not* for your web applications. Any requests that are not for your web applications are forwarded to this default URL. For example, a generic SharePoint page can appear to users who do not request a specific resource.

4. Copy the following section:

```
<VirtualHost name="default">
    #addresses="192.168.1.100"
    hostnames="default_SharePoint_URL"
    defaultsessionscheme="default"

    # specify the block size for request and response in KBs

    requestblocksize="4"

    responseblocksize="4"

    #The defaults can be overriden
    #not only for the Virtual Host
    #but for the WebAgent for that
    #virtual host as well
    #<WebAgent>
    #</WebAgent>
</VirtualHost>
```

5. Add a new line below the </VirtualHost> tag.

6. Copy the section from Step 4 and paste it into the new line you created in Step 5.

7. Do the following steps:

   a. Replace the word default in the <VirtualHost name= tag with a unique name you want.

b. Replace the URL in the <hostnames= tag with the URL of your web application.

8. Save your changes to the file.
9. Repeat Steps 5 through 8 until virtual hosts are defined for all your web applications.

How to Configure Port-based Virtual Hosts

Configuring port-based virtual hosts on your Agent for SharePoint is a process that involves several separate procedures. Some procedures involve different components in your environment. To configure port-based virtual hosts on your Agent for SharePoint server, use the following process:

1. Define a virtual host for each web application (see page 168).
2. Have your network administrator update your DNS server with the virtual host settings (see page 169).
3. Create proxy rules for your port-based virtual hosts (see page 170).
4. On your SharePoint central administration server, do the following (see page 171):
   a. Change the public URL of the web application to the virtual host defined in the Agent for SharePoint.
   b. Change the internal URL of the web application to the actual URL of your SharePoint resource.

Update the DNS Tables with your Port-based Virtual Hosts

The virtual host names defined on your Agent for SharePoint require an association with the IP address of the Agent for SharePoint in the DNS servers of your organization. Have your network administrator update the DNS tables in your organization accordingly.

Create Proxy Rules for your Port-based Virtual Hosts

Port-based virtual hosts require different settings than the default proxy rule file used by the Agent for SharePoint. After defining virtual hosts for your web applications, create proxy rules for your port-based virtual hosts.

Follow these steps:

1. To preserve your current proxy rules, rename your existing proxyrules.xml file in the following directory:

   Agent-for-SharePoint_home\proxy-engine\conf

2. Open the following file with a text editor:

   Agent-for-SharePoint_home\proxy-engine\examples\proxyrules\proxyrules_example1.xml

3. Save a copy of the previous file using the following path and file name:

   Agent-for-SharePoint_home\proxy-engine\conf\proxyrules.xml

4. Locate the following line:

   ```
   <nete:proxyrules xmlns:nete="http://www.company.com/">
   ```

5. Replace the http://www.company.com/ with the name of your virtual host, as shown in the following example:

   ```
   <nete:proxyrules xmlns:nete="http://www.example.com/">
   ```

6. Locate the following line:

   ```
   <nete:case value="banking.company.com:80">
   ```

7. Replace the banking.company:com:80 with the domain name, suffix and port number for your SharePoint web application, as shown in the following example:

   ```
   sharepoint.example.com:8606
   ```

8. Add your other web applications to the proxy rules file by repeating Steps 5 through 7 in the following section:

   ```
   <!-- replace bondtrading.company.com with a virtual host defined in the
   server.conf file -->
         <nete:case value="bondtrading.company.com:80">
         <!-- replace http://server2.company.com with the appropriate destination
   server -->
            <nete:forward>http://server2.company.com$1</nete:forward>
   </nete:case>
   ```

9. Duplicate the previous section and modify it until all your port-based web applications have proxy rules.

10. Locate the following line:

    ```
    <nete:forward>http://home.company.com$1</nete:forward>
    ```

11. Replace the http://home.company.com in the previous line with the URL of a default site you want to use for requests *not* matching your web applications.
12. Save the file and close the text editor.
13. Restart the Agent for SharePoint (see page 92).

Add Public and Internal URLs on your SharePoint Server for your Port-Based Hosts

Port-based proxy rules require the following alternate access mappings on your SharePoint central administration server:

- Set the public URL for the zone to the URL of your virtual host associated with the web application.
- Set the internal URL to the server to which the requests from the virtual host are forwarded.

The following table describes an example of the alternate access mappings for port-based proxy rules:

Internal URL	Zone	Public URL for Zone
http://www.sharepoint.example.com:8606	Default	http://sharepoint.example.com

Follow these steps:

1. Open your SharePoint central administration site.
2. Click Application Management.
3. Under Web Applications, click Configure Alternate Access Mappings.
4. Use the examples in the previous table as a guide to edit your public URLs (see page 102) and Add Internal URLs (see page 103).

How to Configure Host-Header-Based Virtual Hosts

Configuring host-header-based virtual hosts on your Agent for SharePoint is a process that involves several separate procedures. Some procedures involve different components in your environment. To configure host-header-based virtual hosts on your Agent for SharePoint server, use the following process:

1. Define a virtual host for each web application (see page 168).
2. Have your network administrator update your DNS server with the virtual host settings (see page 172).
3. Create proxy rules for your host-header-based virtual hosts (see page 173).
4. On your SharePoint central administration server, do the following (see page 174):
   a. Change the public URL of the web application to the virtual host defined in the Agent for SharePoint.
   b. Change the internal URL of the web application to the actual URL of your SharePoint resource.

Update the DNS Tables with your Host-Header-Based Virtual Hosts

The virtual host names defined on your Agent for SharePoint require an association with the IP address of the Agent for SharePoint in the DNS servers of your organization. Have your network administrator update the DNS tables in your organization accordingly.

Create Proxy Rules for your Host-Header-Based Virtual Hosts

Host-header-based virtual hosts require different settings than the default proxy rule file used by the Agent for SharePoint. After defining your virtual hosts for your web applications, create proxy rules for your host-header-based virtual hosts.

Follow these steps:

1. To preserve your current proxy rules, rename your existing proxyrules.xml file in the following directory:

   Agent-for-SharePoint_home\proxy-engine\conf

2. Open the following file with a text editor:

   Agent-for-SharePoint_home\proxy-engine\examples\proxyrules\proxyrules_example2.xml

3. Save a copy of the previous file using the following path and file name:

   Agent-for-SharePoint_home\proxy-engine\conf\proxyrules.xml

4. Locate the following line:

   ```
   <nete:proxyrules xmlns:nete="http://www.company.com/">
   ```

5. Replace http://www.company.com/ in the previous line with the name of your virtual host, as shown in the following example:

   ```
   <nete:proxyrules xmlns:nete="http://www.example.com/">
   ```

6. Locate the following line:

   ```
   <nete:cond type="header" criteria="equals" headername="HEADER">
   ```

7. Replace HEADER in the previous line with the following:

   ```
   HOST
   ```

8. Locate the following line:

   ```
   <nete:case value="value1">
   ```

9. Replace value1 in the previous line with the value of a host header you want, as shown in the following example:

   ```
   <nete:case value="sharepoint.example.com">
   ```

10. Locate the following line:

    ```
    <nete:forward>http://server1.company.com</nete:forward>
    ```

11. Replace the http://server1.company.com with the URL of the server to which you want to forward requests that use the header value from Step 8. Use the following example as a guide:

    ```
    <nete:forward>http://sharepointserver1.example.com</nete:forward>
    ```

12. Add additional header values and destination servers by repeating Steps 8 through 11 on the following respective lines in the file:

```
<nete:case value="value2">

<nete:forward>http://server2.company.com</nete:forward>
```

13. Locate the following line:

```
<nete:forward>http://home.company.com$1</nete:forward>
```

14. Replace the http://home.company.com in the previous line with the URL of a default site you want to use for requests *not* matching your web applications.
15. Save the file and close the text editor.
16. Restart the Agent for SharePoint (see page 92).

Add Public and Internal URLs on your SharePoint server for your Host-Header-Based Hosts

Host-header-based proxy rules require the following alternate access mappings on your SharePoint central administration server:

- Set the public URL for the zone to the URL of your virtual host associated with the web application.
- Set the internal URL to the server to which the requests from the virtual host are forwarded.

The following table describes an example of the alternate access mappings for host-header-based proxy rules:

Internal URL	Zone	Public URL for Zone
http://www.sharepointserver1.example.com	Default	http://sharepoint.example.com

Follow these steps:

1. Open your SharePoint central administration site.
2. Click Application Management.
3. Under Web Applications, click Configure Alternate Access Mappings.
4. Use the examples in the previous table as a guide to edit your public URLs (see page 102) and Add Internal URLs (see page 103).

How to Configure Path-based Virtual Hosts

If your web applications share the same ports and use host-header values to separate traffic, you can configure path-based virtual hosts.

Configuring path-based virtual hosts on your Agent for SharePoint is a process that involves several separate procedures. Some procedures involve different components in your environment. To configure path-based virtual hosts on your Agent for SharePoint server, use the following process:

1. Define a virtual host for each web application (see page 168).
2. Have your network administrator update your DNS server with the virtual host settings (see page 175).
3. Create proxy rules for your path-based virtual hosts (see page 176).
4. On your SharePoint central administration server, do the following (see page 177):
    a. Change the public URL of the web application to the virtual host defined in the Agent for SharePoint.
    b. Change the internal URL of the web application to the actual URL of your SharePoint resource.

Update the DNS Tables with your Path-based Virtual Hosts

The virtual host names defined on your Agent for SharePoint require an association with the IP address of the Agent for SharePoint in the DNS servers of your organization. Have your network administrator update the DNS tables in your organization accordingly.

Create Proxy Rules for your Path-based Virtual Hosts

Path-based virtual hosts require different settings than the default proxy rule file used by the Agent for SharePoint. After defining your virtual hosts for your web applications, create proxy rules for your path-based virtual hosts.

Follow these steps:

1. To preserve your current proxy rules, rename your existing proxyrules.xml file in the following directory:

   Agent-for-SharePoint_home\proxy-engine\conf

2. Open the following file with a text editor:

   Agent-for-SharePoint_home\proxy-engine\examples\proxyrules\proxyrules_example2.xml

3. Save a copy of the previous file using the following path and file name:

   Agent-for-SharePoint_home\proxy-engine\conf\proxyrules.xml

4. Locate the following line:

   ```
   <nete:proxyrules xmlns:nete="http://www.netegrity.com/">
   ```

5. Replace http://www.netegrity.com/ in the previous line with the name of your virtual host, as shown in the following example:

   ```
   <nete:proxyrules xmlns:nete="http://www.example.com/">
   ```

6. Locate the following line:

   ```
   <nete:case value="/dir1">
   ```

7. Replace the /dir1 in the previous line with the path (URI) for which you want the request redirected. For example, if the path is /sales, all URLs containing /sales are redirected to the resource you specify.

8. Locate the following line:

   ```
   <nete:forward>http://server1.company.com$2</nete:forward>
   ```

9. Replace the http://server1.company.com with the URL of the server to which you want to forward requests that use the path (URI) value from Step 8. Use the following example as a guide:

   ```
   <nete:forward>http://sharepointserver1.example.com</nete:forward>
   ```

10. Add additional header values and destination servers by repeating Steps 6 through 9 on the following respective lines in the file:

    ```
    <nete:case value="/dir2">
    ```

    ```
    <nete:forward>http://server2.company.com$2</nete:forward>
    ```

11. Locate the following line:

    ```
    <nete:forward>http://home.company.com$1</nete:forward>
    ```

12. Replace the http://home.company.com in the previous line with the URL of a default site you want to use for requests *not* matching your web applications.
13. Save the file and close the text editor.
14. Restart the Agent for SharePoint (see page 92).

Add Public and Internal URLs on your SharePoint server for Path-Based Virtual Hosts

Path-based proxy rules require the following alternate access mappings on your SharePoint central administration server:

- Set the public URL for the zone to the URL of your virtual host associated with the web application.
- Set the internal URL to the server to which the requests from the virtual host are forwarded.

The following table describes an example of the alternate access mappings for path-based proxy rules:

Internal URL	Zone	Public URL for Zone
http://www.sharepointserver1.example.com	Default	http://sharepoint.example.com

Follow these steps:

1. Open your SharePoint central administration site.
2. Click Application Management.
3. Under Web Applications, click Configure Alternate Access Mappings.
4. Use the examples in the previous table as a guide to edit your public URLs (see page 102) and Add Internal URLs (see page 103).

How to Protect the Claims WS Service using SSL

The Agent for SharePoint performs user look–ups in the SQL Server database of the SharePoint central administration server using the Claims web service (WS). You can encrypt communications to the Claims WS service with SSL. Protecting the Claims WS service requires that several separate procedures performed on various components in your environment.

To protect the Claims WS service using SSL, use the following process:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

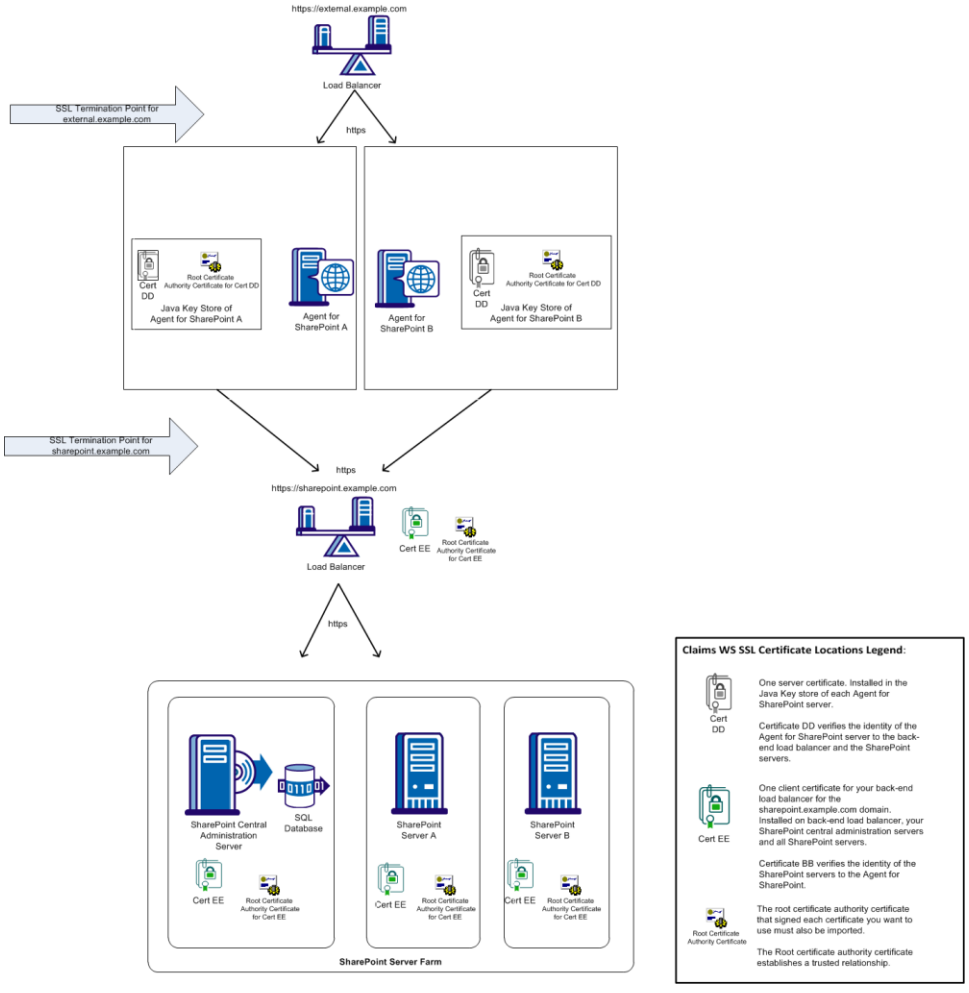
1. Review the certificate locations (see page 179).
2. Perform the following tasks on the computer hosting your Agent for SharePoint:
   a. Verify the prerequisites (see page 180).
   b. Generate a key store file for the Claims Search Service (see page 180).
   c. Extract the certificate from the key store (see page 181).
   d. Edit the server.conf file used by the Agent for SharePoint (see page 182).
   e. Generate the SSLConfig.properties file (see page 183).
3. Add a trusted root authority in your SharePoint farm (see page 184).
4. Configure a mutual trust relationship between the claims search service and the claims provider by performing the following tasks on each SharePoint server in your environment:
   a. Request a client certificate (see page 185).
   b. Have your administrator approve your request for a client certificate (see page 186).
   c. Verify your approval and install your client certificate.
   d. Export your client certificate (see page 189).
   e. Install the client certificate on your SharePoint servers (see page 190).
   f. Grant application pool identity permissions to the certificate (see page 191).
   g. Register the end point for the claims search service (see page 192).
5. Return to the computer hosting your Agent for SharePoint and perform the following tasks:
   a. Create a trusted store for the root certificates (see page 193).

b. Generate an SSLConfig.Properties file for the trusted root certificate store (see page 193).

c. Restart the Agent for SharePoint (see page 92).

Claims WS Service Certificate Locations

The following illustration shows the typical locations of the certificates which encrypt the communications of your Claims web service (WS) in your SharePoint environment:



Verify the Prerequisites

Verify the following prerequisites before protecting the Claims WS service with SSL:

- Farm administrator privileges and local administrator privileges for each SharePoint sever in the farm.
- For Windows environments, verify that the JAVA_HOME in your environment points to the JDK 1.6 installation directory.
- For UNIX/Linux operating environments, verify the following:
  - The Agent for SharePoint environment variables are exported to your environment. Run the following script:

    `Agent-for-SharePoint_home\ca_sps_env.sh`
  - The java_home variable in your environment points to the JDK 1.6 installation directory.

Generate a keystore for the Claims Search Service

The Agent for SharePoint supports only JCEKS key stores. Create a JCEKS key store to protect the claims search service. The keytool application described in this procedure is installed with your Java development kit.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. On the system hosting your Agent for SharePoint, open a command prompt.
2. Run the following command:

   `keytool -genkeypair -keyalg RSA -keystore .\absolute_path_to_key_store -alias alias_name -storetype JCEKS -storepass keystore_password`

   Note: We recommend using an absolute path under the *Agent for SharePoint_home*\SSL\keys directory.

   The keystore is created.

Extract the Certificate from the keystore

After you create the keystore on your Agent for SharePoint, extract the certificate from the keystore.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. On the system hosting your Agent for SharePoint, open a command prompt.
2. Verify the name of the alias associated with the certificate you want to extract by running the following command:

   `keytool -list -v -keystore key_store_file_path -storetype JCEKS`

3. Run the following command:

   `keytool -export -keystore key_store_file_path -alias alias_name -file certificate_file_name.cer -storetype JCEKS`

   The certificate is extracted with the file name you specified.

Edit the server.conf file used by the Agent for SharePoint

Part of protecting the Claims WS service with SSL involves updating the following settings in the server.conf file used by the Agent for SharePoint:

- The local SSL port number.
- The path to the key store on the host of the Agent for SharePoint.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Open the following file:

   Agent-for-SharePoint_home\proxy-engine\conf\server.conf

2. Locate the following section of the file:

   <localapp>

3. In the <localapp> section, locate the following line:

   #local.https.port=*port_number*

4. Remove the # from the beginning of the line. Verify that the port number following the equal sign matches the one you entered for the Claims WS service SSL port in the SharePoint configuration wizard.

5. Locate the following line:

   #local.https.keyStoreFileName="tomcat.keystore"

6. Remove the # from the beginning of the line. Replace the tomcat.keystore with the relative path to the keystore you created to store the keys used for the protection of the Claims WS service.

7. Save and close the file.

8. Restart the Agent for SharePoint (see page 92).

Generate the SSLConfig.properties file for the keystore

Part of the process of protecting the Claims WS service involves generating an SSLConfig.properties file for the keystore. You can generate this file using a script that is installed with the Agent for SharePoint.

The GenerateSSLConfig uses the following syntax:

`GenerateSSLConfig -keystorepass` *`password_to_your_keystore`*

Follow these steps:

1. Open a command-line window with Administrative privileges.
2. Navigate to the following directory:

   `Agent-for-SharePoint_home``\proxy-engine\bin`
3. Run one of the following script files:
   - (Windows) GenerateSSLConfig.Bat
   - (UNIX or Linux) GenerateSSLConfig.sh

   You specify the following parameters when you run the script:

   -keystorepass

   Specifies the password for the keystore.

   If an SSLConfig.properties file exists, an overwrite warning appears.

   A confirmation message confirms the keystore was configured and displays the directory of the keystore you created. The SSLConfig.properties file is generated.

Add a Trusted Root Authority to your SharePoint Farm

Your SharePoint farm requires a new trusted root authority to identify and authenticate the information it receives from the claims service. Create a trusted root authority on your SharePoint 2010 central administration server.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Copy the certificate you created to protect the ClaimsWS service to a directory on your SharePoint central administration server.
2. Open the SharePoint 2010 central administration site.
3. Click Security.
4. Under General Security, click Manage trust.
5. Click New.

   The Create Trusted Relationship dialog appears.
6. Enter a name for the trust relationship.
7. Click the Browse button next to the Root Authority Certificate, and then locate the certificate you copied over in Step 1.
8. Click OK.
9. Repeat Steps 1 through 8 for each Certificate Authority certificate in your certificate chain.

   The trusted root authority is created.

Request a Client Certificate

A mutual trust relationship between the claims search service and the claims provider requires a client certificate.

Several third-party tools are available for creating certificates. This procedure provides one possible example using Active Directory Certificate services and IIS 7.

If your organization uses different tools or procedures to create client certificates, use those tools or procedures instead.

If you already have a client certificate, skip this procedure.

Follow these steps:

1. Open your web browser.
2. Navigate to the following URL:

   `https://fully_qualilfied_domain_name_of_server_running_active_directory_certificate_services/certsrv`

   An example of such a URL is http://certificateauthority.example.com/certsrv.
3. Click Request a certificate.

   The Request a certificate screen appears.
4. Click the advanced certificate request link.
5. Click the Create and submit a request to this CA.

   An Advanced Certificate Request form appears.
6. Complete the form.

   Note: Under type of certificate needed, verify that Client Authentication Certificate appears in the drop-down list.
7. Click Submit.

   A confirmation dialog appears.
8. Click Yes.

   The request is submitted.
9. Note the following items for future reference:
   - Your request ID.
   - Use the same browser to verify the status of your request within ten days.

Have your Administrator Approve your Request for a Client Certificate

Certificate administrators approve or reject certificate requests. Certificate administrator privileges are separate from Administrator privileges. Not all users who have accounts on the computer hosting Active Directory Certificate services have sufficient privileges to approve or reject certificates.

If you have certificate administrator privileges on the web server to which your certificate was submitted, use this procedure. Otherwise, ask the certificate administrator to do this approval for you.

Follow these steps:

1. Log in to the web server hosting the Active Directory Certificate services using an account with Certificate administrator privileges.
2. Click Start, Administrative Tools, Certification Authority

   The certsrv snap-in appears.
3. Click the name of the certification authority, and then click the pending request folder.

   A list of pending certificate requests appears.
4. Right-click the request ID associated with the request for the client certificate.
5. From the context menu, select All Tasks, Issue.

   The certificate is issued.

Verify your Approval and Download your Client Certificate

Use the same IIS web server and web browser from which you submitted the request to verify the status of your certificate request. If your certificate is approved, install the certificate on your computer.

Follow these steps:

1. Open your web browser you used to request your certificate.
2. Navigate to the following URL:

   `https://fully_qualilfied_domain_name_of_server_running_active_directory_certificate_services/certsrv`

   An example of such a URL is https://certificateauthority.example.com/certsrv.
3. Click View the status of a pending certificate request.

   A list of your certificate requests appears.
4. Click the link for your certificate request.

   The Certificate Issued screen appears. If it does not, contact the certificate administrator in your organization for more information.
5. Click the Install Certificate link.

   A confirmation dialog appears.
6. Click Yes.

   The certificate is installed on your computer.

Install the Certificates Snap-in

On the Windows operating environment, install the Certificates snap-in for the Local Computer and my user accounts on the Microsoft Management console to manage your certificates. After you install the snap-in, save the instance of the console containing the Certificates snap-in for your future use.

Note: For other operating environments, use another certificate tool, such as OpenSSL.

Follow these steps:

1. Click Start, Run.

   The Run dialog appears.

2. In the Open field, type mmc and then click OK.

   The Microsoft Management console appears.

3. Click File, Add/Remove Snap-in.

   The Add or Remove Snap-ins dialog appears.

4. In the Available snap-ins list, click Certificates, and then click Add.

   The Certificates snap-in dialog appears.

5. Click the Computer account option button, and then click Next.

6. Click the Local computer option button, and then click Finish.

   The Certificates snap-in dialog closes. The Certificates snap-in appears in the Selected snap-ins list.

7. In the Available snap-ins list, click Certificates, and then click Add.

   The Certificates snap-in dialog appears.

8. Click the My User Account option button.

9. Click OK.

   The Add or Remove Snap-ins dialog closes. The certificates snap-in is added.

10. Save your instance of the console for future use. Otherwise, the snap-in does not appear in the future.

Export your Client Certificate from the Administrator Account Into the Local Computer Account

After installing your client certificate on your system, use the certificates snap-in of the Microsoft Management console to export the certificate from the current user account (Administrator account). Then import the certificate into the Local computer account. The local computer account requires access to the client certificate.

Follow these steps:

1. Click Start, Run.

   The Run dialog appears.

2. In the Open field, type mmc, and then click OK.

   The Microsoft Management console appears.

3. Export the client certificate from the current user account of the Administrator with the following steps:

   a. Expand the console root folder, and then click Certificates — Current User.

      Note: If the proper certificates snap-in does not appear, install it (see page 188).

   b. Expand certificates, and then open the following folders (where the certificate is stored):

      - Personal
      - Certificates

      A list of certificates appears.

   c. Right-click your client certificate, and then select All Tasks, Export.

      The certificate export wizard opens.

   d. Export the certificate using the Base-64 encoded X.509 (.cer) option.

      The client certificate is exported.

4. Import the client certificate to the local user account (on the same computer) with the following steps:

   a. Expand the console root folder, and then click Certificates — Local Computer.

      Note: If the proper certificates snap-in does not appear, install it (see page 188).

   b. Expand certificates, and then double-click the folder to which you want to import the client certificate.

   c. Click Action, All tasks, Import.

      The certificate import wizard opens.

d. Navigate to the file that you created when exporting the certificate in Step 3d, then follow the prompts in the wizard to import the certificate into the local computer account.

   The certificate is imported into the local computer account.

5. Save your changes to the Microsoft Management console, and then close it.

Install the client certificate on your SharePoint Servers

Install the exported client certificate on the following servers in your SharePoint environment:

- Your SharePoint central administration server.
- All web front end (WFE) servers in your SharePoint farm.

Follow these steps:

1. Copy the exported certificate to a directory on your server.
2. Click Start, Run.

   The Run dialog appears.
3. In the Open field, type mmc and then click OK.
4. Expand Certificates — Local Computer.

   Note: If the Certificates snap-in does not appear, install it (see page 188).
5. Expand Personal.
6. The certificates folder appears.

   Right-click the certificates folder, and then click All Tasks, Import.
7. Import the client certificate.

   The certificate appears.
8. Double-click the client certificate. Verify that the General tab is selected.
9. Note the value in the Issued to field. You need this name to register the endpoint for the claims search service.
10. Repeat Steps 1 through 9 on each server in your environment (central administration server and on each WFE server).

Grant Application Pool Identities for SharePoint Web Applications Permissions to the Client Certificate

All application pool identities that are associated with protected SharePoint web applications need read-only permissions to the client certificate. Perform this procedure on all the following servers in your environment:

- Your SharePoint central administration server.
- All web front end (WFE) servers in your SharePoint farm.

Follow these steps:

1. Click Start, Run.

   The Run dialog appears.

2. In the Open field, type mmc and then click OK.

   The Microsoft Management console appears.

3. Expand the console root folder, and then click Certificates — Local Computer.

   Note: If the Certificates snap-in does not appear, install it (see page 188).

4. Locate your client certificate. Right-click your client certificate, and then select All tasks, Manage Private keys.

   The permissions dialog appears.

5. Locate the application pool identity in IIS Manager, Application Pool Section, and then grant that identity read access to the client certificate.

6. Repeat Step 5 for all other application pool identities.

   The permissions are granted.

7. Repeat Steps 1 through 6 on the SharePoint Central administration server and all the web front–end servers in your SharePoint farm.

Register the Claims search service end point on all web front end servers

Registering a new end point for the claims search service associates the secure connection with the client certificate. A PowerShell script installed with the SiteMinder claims provider automates the registration process. Register the new end point for all of the web front end (WFE) servers in your SharePoint environment.

If you previously registered another SiteMinder claims search service, remove it by running the following script first:

SharePointClaimsProvider_directory\scripts\Remove-SMClaimSearchService.ps1

Follow these steps:

1. Gather the following information:

   –WebApplication *url_of_SharePoint_web application*

   Specifies the URL associated with the web application hosted on a SharePoint server.

   -ClaimSearchService *claims_search_service_URL*

   Specifies the URL of the claims search service.

   Limits: If the claim search service uses SSL, specify https: as the protocol in the URL.

   –ClientCertificateName

   Specifies the value in the Issued To: field of your client certificate. This client certificate protects the Claims WS (web service).

2. Open the SharePoint 2010 Management Shell.
3. Navigate to the following directory:

   SharePointClaimsProvider_directory\scripts

4. Enter the following command:

   ```
   .\Add-SMClaimSearchService.ps1 –WebApplication url_of_web_application url
   -ClaimSearchService https://claims_search_service_url
   -EnableSSLClientAuthentication –ClientCertificateName
   name_in_Issued-To:_field_of_Certificate
   ```

   The new end point is registered.

5. Restart your IIS web server.
6. Repeat Steps 1 through 5 on all of the web front end (WFE) servers in your SharePoint environment.

Create a Trusted Store for the Root Certificate Authority Certificate

The server on which your Agent for SharePoint runs also requires a separate trusted store for the root certificate authority certificates. If you use certificates signed by a third-party certificate authority, import the certificate authority certificate signed by the third party into this trusted store. If you are using a self-signed certificate import either the self-signed certificate or the associated public key into this trusted store.

Important! Do not use self-signed certificates in production environments. We recommend using self-signed certificates in test environments only.

Follow these steps:

Note: This procedure provides one possible example of how to configure this feature using third-party tools. CA Technologies did *not* develop nor provide these tools. These tools are subject to change at any time by the third party without notice. Use this procedure as a guide for configuring this feature in your specific environment. The actual steps required in your situation could be different from the steps that are shown here.

1. Copy your certificate to the server on which your Agent for SharePoint runs.
2. Open a Command Prompt window.
3. Create a trusted store with the following command:

   ```
   Keytool –importcert –alias alias_name -file path_to_root_certificate
   -trustcacerts –keystore relative_path_to_trusted_store -storepass
   trusted_store_password -storetype JCEKS
   ```

   Note: We recommend using a relative location under the *Agent-for-SharePoint_home*\SSL\keys directory

Generate a SSLConfig.Properties file for the Trusted Store

Part of the process of protecting the Claims WS service involves generating an SSLConfig.properties file for the trusted store that contains the root certificate. You can generate this file using a script that is installed with the Agent for SharePoint.

The GenerateSSLConfig uses the following syntax:

```
GenerateSSLConfig -keystorepass password_to_your_keystore -truststore
full_path_to_your_trusted_store -truststorepass password_to_your_trusted_store
```

Follow these steps:

1. Open a command line window with Administrative privileges.
2. Navigate to the following directory:

   Agent-for-SharePoint_home\proxy-engine\bin

3. Run one of the following script files:
   - (Windows) GenerateSSLConfig.Bat
   - (UNIX or Linux) GenerateSSLConfig.sh

   You specify the following parameters when you run the script:

   keystorepass

   Specify the password for the keystore you created.

   truststore

   Specify the full path to your trusted store.

   truststorepass

   Specify the password for your trusted store.

   If an SSLConfig.properties file exists, an overwrite warning appears.

   The SSLConfig.properties file is generated.

SSL and the Agent for SharePoint

The following sections describe protecting the Agent for SharePoint communications using SSL.

Keys and Server Certificates Management

The Agent for SharePoint fully supports the Secure Sockets Layer (SSL) protocol. SSL provides secure communication between the client and the server, enabling mutual authentication (using certificates) and private encrypted messages (using keys).

The Agent for SharePoint uses the OpenSSL cryptography toolkit, which implements the SSL v2/v3 and Transport Layer Security (TLS v1) network protocols and related cryptography standards required by these protocols. The OpenSSL toolkit includes the openssl command line tool for generating keys and certificates. The openssl executable image and supporting libraries are located in the <install dir>\SSL\bin folder or corresponding UNIX directory.

Note: To enable SSL on Solaris, you must have patch 127127-11 installed on the same system as the Agent for SharePoint.

To run the openssl command line tool, connect to the appropriate folder or directory. Open a command line Windows or UNIX shell. Use the following syntax as a guideline for entering openssl commands:

openssl *command* [*command_opts*] [*command_args*]

The **openssl** tool provides a large number of commands (*command* in the synopsis above); each one can include numerous options and arguments (*command_opts* and *command_args* in the synopsis). You can find complete documentation for openssl at the following URL:

http://www.openssl.org/docs/apps/openssl.html

Important! When you issue the openssl command, verify that a valid path to the openssl configuration file (openssl.conf) exists using the -config parameter in the command line.

The commands you are most likely to use to perform fundamental SSL tasks are as follows:

- Generating a private key
- Generating a Certificate Signing Request (CSR)
- Generating a certificate by self signing the CSR
- Having a certificate signed by a Certificate Authority (CA)
- Installing a signed certificate
- Decrypting an RSA key
- Encrypting an RSA key
- Changing the password of an RSA key

Review the following important information about private keys and server certificates:

- The server certificate and private key work together. Use the server certificate with the corresponding private key.
- The server certificate should be digitally signed by a Certificate Authority (CA) or self-signed with your own private key (recommended for sites intended exclusively for internal use).
- The SSLCertificateFile and SSLCertificateKeyFile directives in the SSL.conf file must point to the corresponding certificate and key files.
- If you are using Apache's virtual host feature, each virtual host you want to secure must have its own private key and server certificate.

Generate a Private RSA Key

SSL uses keys to encrypt and decrypt messages. Keys come in pairs: public key, and a private key. With OpenSSL, the private key contains the public key information, so you do not generate a public key separately.

Keys use various cryptographic algorithms and key exchange methods. For generating private keys, use the RSA key exchange method with the Date Encryption Standard (DES) cryptographic algorithm. The following is a UNIX example for an openssl command:

```
openssl genrsa -des3 -out server.key
```

The key output file is encrypted in ASCII PEM (from “Privacy Enhanced Mail") format.

Because the file is encrypted, you are prompted for a passphrase to protect it, you can decrypt it later if necessary. Do not use the -des3 argument in the command line, if you do not want your key to be protected.

Important! Do not use the -des3 option if you are running on Windows. The Agent for SharePoint does not start if there is a prompt for a passphrase.

To view the details of this RSA key, enter the following command:

```
openssl rsa -noout -text -in server.key
```

RSA Key Decryption

To remove the encryption from a private key, perform the following procedure.

follow these steps:

1. Make a copy of the encrypted key as a backup, for example:
   cup server.key server.key.org
2. Enter this command:

   ```
   openssl rsa -in server.key.org -out server.key
   ```

If you specify the output file without a preceding encryption option (that is, -des, -des3, or -idea), then the file is written in plain text, without a prompt for a passphrase.

Important! The availability of an unencrypted key on your system makes your system vulnerable to impersonation on the Internet. Verify that this file has the appropriate permissions, that is, readable only by root on UNIX, or Administrator on Windows.

RSA Key Encryption

To encrypt an unencrypted RSA key, enter the following command:

```
openssl dsa -in server.key -des3 -out server.key.new
```

Do not use this command on Windows, because the web server does not start if there is a prompt for a passphrase.

Modify the Passphrase for an RSA Key

To change the password on an existing RSA key, enter the following command:

```
openssl rsa -des3 -in server.key -out server.key.new
```

You are prompted for both the old passphrase and a new passphrase. Rename your newly created key to the old key name.

Create Certificate Signing Request

Certificates are created for authentication. They associate a public key with the identity of a user or server. The next step after generating a private key is to generate a certificate request, or Certificate Signing Request (CSR), using the private key. You can send the CSR to a Certificate Authority for signing into a certificate, or you can create a self-signed certificate.

Note: We recommend you to create a self-signed certificate for testing or internal uses only.

To create a CSR with the RSA server private key, enter the following command:

```
openssl req -config openssl.cnf -new -key server.key -out server.csr
```

You are prompted for several answers to identify the request.

Note: This command presupposes the existence of an openssl configuration file in the present working directory. The file is located at <install dir>\SSL\bin\openssl.cnf. If you change the name, or move it to another location, enter the correct location of openssl.cnf in the command line.

The CSR output file is in an ASCII PEM Privacy Enhanced Mail (PEM) format. You can specify a different format with the -outform option.

To view details about the CSR, use the following command:

```
openssl req -noout -text -in server.csr
```

Create a Self-Signed Certificate

To create a certificate for testing or other internal purposes, use the following command:

```
openssl -req -new -x509 -key server.key -out cert_name.crt
```

To set an expiration time, use the -days flag. For example, when you set -days 365, the certificate expires in one year.

Place the output file in the following directory:

Agent-for-SharePoint_home\SSL\certs

Restart the Agent for SharePoint to enable the certificate.

Obtain Certificate Signed by a CA

To have a certificate signed by a Certificate Authority, go to the CA's website and complete the online submission form. For more information about commercial CAs, you can visit one of these web sites:

- VeriSign
  http://digitalid.verisign.com/server/apacheNotice.htm
- Thawte
  http://www.thawte.com/certs/server/request.html

Allow 5-10 working days for the CA to process your request.

Install a Signed Certificate

You can install a CA-signed certificate by editing the ssl.conf file. Verify that the SSLCertificateFile and SSLCertificateKeyFile directives are pointing to the key file and the certificate file you previously created. The csr file is no longer required.

SSL Configuration for FIPS COMPAT and MIGRATE Modes

The procedure for enabling SSL on the Agent for SharePoint varies slightly depending on the FIPS mode. In a new installation with FIPS in COMPAT or MIGRATE mode, configure SSL with the following steps. With a new installation or migration to FIPS in ONLY mode, additional steps are required.

follow these steps:

1. Enter the following command to generate a Private RSA Key (also referred as the server key):

   ```
   openssl genrsa -des3 -out server.key
   ```

2. To remove the encryption from a private key, follow these steps:

   1. Make a copy of the encrypted key as a backup, for example:

   2. copy server.key server.key.org

3. Enter the following command to remove encryption:

   ```
   openssl rsa -in server.key.org -out server.key
   ```

4. Enter the following command to generate a Certificate Signing Request (CSR):

   ```
   openssl req -config openssl.cnf -new -key server.key -out server.csr
   ```

5. Have the certificate signed by a Certificate Authority (CA).

6. Install the signed certificate.

7. Verify that httpd-ssl.conf file is pointing to correct directives/paths of server key and certs.

8. Enable SSL on the Agent for SharePoint:

   On UNIX:

   Agent-for-SharePoint_home/proxy-engine/sps-ctl startssl

   On Windows:

   Agent-for-SharePoint_home\httpd\bin\configssl.bat -enable

9. Restart the Agent for SharePoint.

   The Agent for SharePoint is configured for SSL.

If at a later time you want to run without SSL, enter this command:

Agent-for-SharePoint_home\httpd\bin\configssl.bat -disable.

SSL Configuration for FIPS ONLY Mode

For an installation of the Agent for SharePoint in FIPS ONLY mode, the required configuration for SSL support is listed in the following procedure.

follow these steps:

1. Verify OPENSSL_FIPS environment variable is set to 1 and that the CA_SM_PS_FIPS140 environment variable is set to ONLY.
2. Generate a server key. Specify the size of key as at least 1024 KB. Be sure that the algorithm (des3 in the example following) is FIPS-compliant. For example:

   ```
   openssl genrsa -des3 -out server.key 1024
   ```

3. Generate a Certificate Signing Request (CSR) as shown in this example:

   ```
   openssl req -config openssl.cnf -new -key server.key -out server.csr
   ```

4. Have the certificate signed by a Certificate Authority (CA).
5. Install the signed certificate.
6. Verify that in the httpd-ssl.conf file the directives/paths of the server key and certs are correct.
7. Verify that the value of the SSLPassPhraseDialog variable in the httpd-ssl.conf file (located in *Agent-for-SharePoint_home*\httpd\conf\extra folder) is set to custom.

8. Verify that the value of the SSLCustomPropertiesFile variable is set to <*Agent-for-SharePoint_home*>/Tomcat/properties/spsssl.properties.
9. Enable SSL on the Agent for SharePoint as follows:

   On UNIX

   1. Enter the following command:

      Agent-for-SharePoint_home/proxy-engine/configssl.sh *passphrase*

      Note: The passphrase is the same one provided to the key in Step 2.

      This command encrypts the passphrase and stores it in spsssl.properties file.

   2. Enter the following command:

      Agent-for-SharePoint_home/proxy-engine/sps-ctl startssl

      SSL is enabled.

   On Windows

   1. Enter the following command:

      Agent-for-SharePoint_home\httpd\bin\configssl.bat –enable *passphrase*

      Note: The passphrase is the one provided to the key in Step2.

      This command encrypts the passphrase and stores it in the spsssl.properties file.

   2. Restart the Agent for SharePoint.

      SSL is enabled.

      Note: If at a later time you want to run without SSL, enter the following command:

      Agent-for-SharePoint_home\httpd\bin\configssl.bat -disable.

Enable SSL for Virtual Hosts

The Apache server supports virtual hosts, which are multiple web hosts that run from a single Apache binary. Apache virtual hosts can be name-based or IP-based. Name-based virtual hosts share a single IP address, while IP-based virtual hosts require a different IP address for each virtual host.

Apache virtual hosts using the SSL protocol must contain the following conditions:

- IP-based due to limitations in the protocol.
- Must have virtual host containers in the Apache configuration file for both secure (HTTPS) and not secure (HTTP) requests.

The following is an example of a secure (HTTPS) virtual host:

```
<VirtualHost 10.0.0.1:443>
DocumentRoot ".../htdocs/site1"
ServerName www.site1.net
ServerAdmin webmaster@site1.net
ErrorLog logs/covalent_error_log_site1
TransferLog logs/...
SSLEngine on
SSLCertificateFile /www.site1.net.cert
SSLCertificateKeyFile /www.site1.net.key
CustomLog logs/cipher_log_site1 \
          "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
</VirtualHost>
```

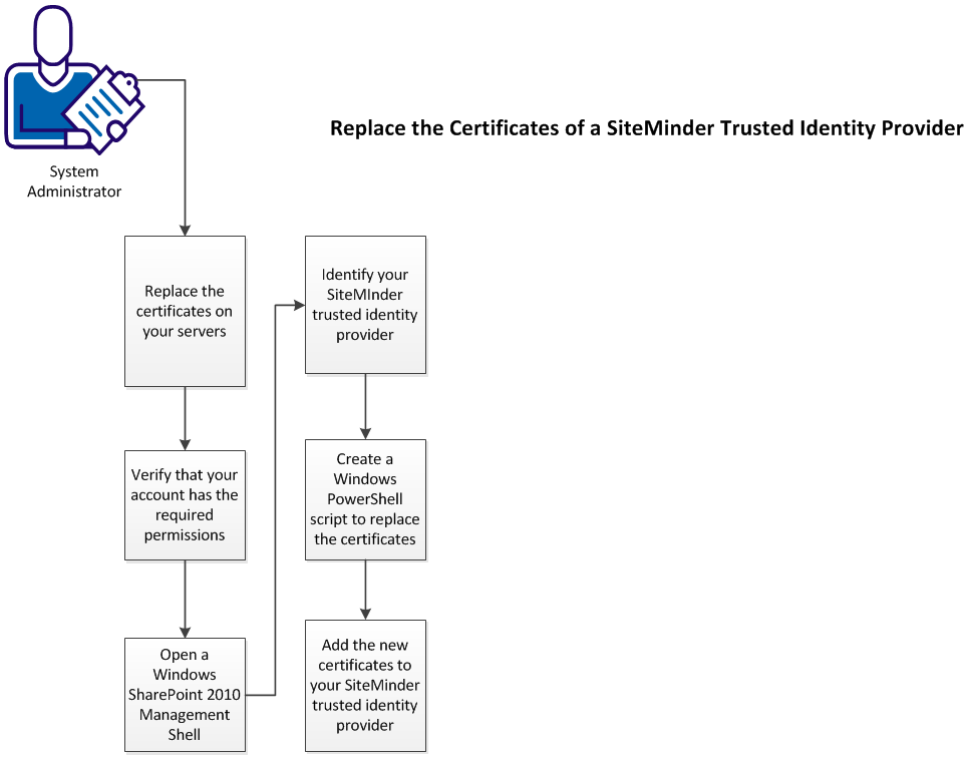
Chapter 12: How to Replace the Certificates for your SiteMinder Trusted Identity Provider

SiteMinder trusted identity providers use the following SSL certificates to encrypt their communications with the SiteMinder Policy Server:

- A certificate authority certificate (CA-certificate or root certificate).
- An x.509 certificate (signing certificate).

When any of the previous certificates expire, you can replace them with valid certificates.

The following illustration describes how to replace the certificates of your SiteMinder trusted identity provider:



To replace the certificates for your SiteMinder trusted identity provider, follow these steps:

1. Replace the certificates on your servers (see page 205).
2. Verify that your account has the required permissions (see page 119).
3. Open a SharePoint 2010 management shell window on your SharePoint central administration server (see page 119).
4. Identify your SiteMinder trusted identity provider (see page 119).
5. Create a Windows PowerShell script to update the certificates (see page 207).
6. Add the new certificates to your SiteMinder trusted identity provider (see page 208).

Replace the Certificates on your Servers

Replace the expired certificates on the following computers:

- The computer hosting your SharePoint central administration server.
- Any computers hosting a web front end (WFE) for your SharePoint environment.

Follow these steps:

1. Perform the following steps on the computer hosting your SharePoint central administration server:
   a. Remove the expired CA-certificate (root certificate) from the computer.
   b. Copy your new CA-certificate (root certificate) to the computer.

      Note: Record this information for future use in your Windows PowerShell script.

   c. Remove the expired signing certificate from the computer.
   d. Copy your new signing certificate to the computer.

      Note: Record this information for future use in your Windows PowerShell script.
2. Perform the following steps on a computer hosting a web front end (WFE) server in your SharePoint environment:
   a. Remove the expired CA-certificate (root certificate) from the computer.
   b. Copy your new CA-certificate (root certificate) to the computer.

      Note: Record this information for future use in your Windows PowerShell script.

   c. Remove the expired signing certificate from the computer.
   d. Copy your new signing certificate to the computer.

      Note: Record this information for future use in your Windows PowerShell script.
3. Repeat Step 2 for all web front end (WFE) servers in your SharePoint environment.

   The certificates on your computers have been replaced.

Verify that your Account has the Required Permissions

The user account with which you want to modify the SiteMinder trusted identity provider requires certain permissions. Modify the permissions of your user account if it does *not* meet the following conditions:

- An Administrator account.
- A member of the Administrators group.

Add the following privileges to your account:

- Local administrator on all SharePoint web front end (WFE) servers.
- Read/Write access to the configuration database.

Open a SharePoint 2010 Management Shell Window on your SharePoint Central Administration Server

Add claims to your <stmdnr> trusted identity provider using the SharePoint 2010 Management shell.

Follow these steps:

1. Log in to your SharePoint Central Administration server.
2. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   A SharePoint 2010 management shell command-line window appears.

Identify your Trusted Identity Provider

A SharePoint 2010 environment can have multiple trusted identity providers. Identify your SiteMinder trusted identity provider before modifying any claims that are associated with it.

Follow these steps:

1. Enter the following command to list all of the trusted identity providers:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers appears.
2. Locate your SiteMinder trusted identity provider in the list.

   Your SiteMinder trusted identity provider is identified.

Create a PowerShell Script to Update the Certificates

Adding the new certificates to your SiteMinder trusted identity provider involves several steps using the SharePoint 2010 Management shell.

We recommend using a PowerShell script that contains all of the commands, such as the one shown in the following example:

```
Remove-SPTrustedRootAuthority CASigningRootCert
Remove-SPTrustedRootAuthority CASigningCert

$rootcert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("full_path_to_updated_certificate_authority_certificate.cer")
$cert = New-Object
System.Security.Cryptography.X509Certificates.X509Certificate2("full_path_to_signing_certificate.cer")
$tip = Get-SPTrustedIdentityTokenIssuer
name_of_siteminder_trusted_identity_provider
$tip.SigningCertificate = $cert
$tip.Update()
New-SPTrustedRootAuthority -Name "CASigningRootCert" -Certificate $cert
New-SPTrustedRootAuthority -Name "CASigningCert" -Certificate $cert
```

Follow these steps:

1. Copy the example script shown previous and save it on your SharePoint central administration server as a .ps1 file.
2. Open the .ps1 file with a text editor.
3. Edit the .ps1 file to suit your environment with the following steps:
   a. Locate the following text:

      full_path_to_updated_certificate_authority_certificate

   b. Replace the previous text with the full path to your new certificate authority (root) certificate.

      Example: C:\exampleserver\certificates\rootcertificate.cer

   c. Locate the following text:

      full_path_to_signing_certificate

   d. Replace the previous text with the full path to your new signing certificate.

      Example:
      C:\exampleserver\certificates\signingcertificates\sharepointsigningcertificate.cer

   e. Locate the following text:

      name_of_siteminder_trusted_identity_provider

   f. Replace the previous text with the name of your SiteMinder trusted identity provider.

      Example: SiteMinder_TIP
4. Save the .ps1 file and close the text editor.

   The Windows PowerShell script is created.

Add the New Certificates to your SiteMinder Trusted Identity Provider

Add the new certificates to your SiteMinder trusted identity provider by running the PowerShell script on your SharePoint Central administration server.

Follow these steps:

1. Change the directory of your SharePoint 2010 Management shell window to the directory that contains your .ps1 file.
2. Execute your .ps1 file with the following command.

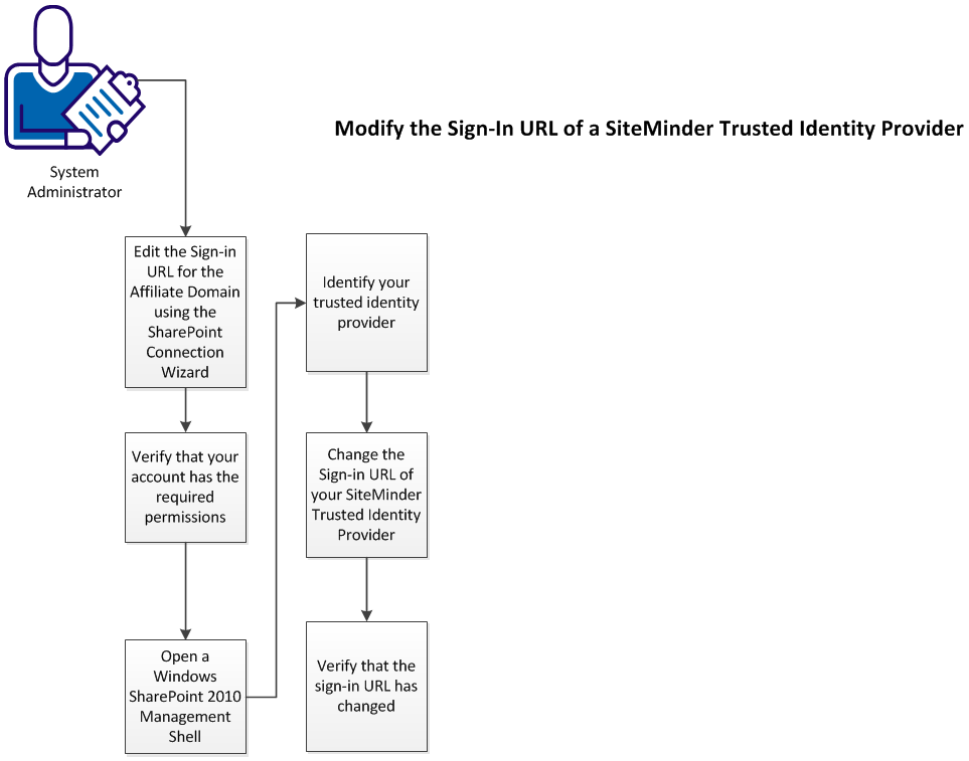
   \.*name_of_your_.ps1_file*.ps1

   The new certificates are added to the trusted identity provider.

Chapter 13: How to Modify the Sign-In URL of your SiteMinder Trusted Identity Provider

This scenario describes changing the sign-in URL of your SiteMinder trusted identity provider of an existing SiteMinder environment. For example, update the URL if you change the protocol of your sign-in URL from HTTP to HTTPS.

The following illustration describes the process of modifying the sign-in URL of your SiteMinder trusted identity provider:



To modify the sign-in URL of your SiteMinder identity provider, follow these steps:

1. Edit the sign-in URL for the affiliate domain using the SharePoint connection wizard (see page 210).
2. Verify that your account has the required permissions (see page 119).
3. Open a SharePoint 2010 Management Shell window on your SharePoint Central Administration server (see page 119).
4. Identify your SiteMinder trusted identity provider (see page 119).
5. Change the sign-in URL of your SiteMinder trusted identity provider (see page 213).
6. Verify that the sign-in URL has changed (see page 214).

Edit the Sign-In URL for the Affilliate Domain using the Sharepoint Connection Wizard

You can update the affiliate domain with a new sign-in URL for your SiteMinder trusted identity provider. This update requires running the SharePoint connection wizard on the computer hosting your SiteMinder Agent for SharePoint.

This procedure adds the new sign-in URL of your SiteMinder trusted identity provider on your SiteMinder Policy Server.

Follow these steps:

1. Navigate to the following directory:

   `Agent-for-SharePoint_home/sharepoint_connection_wizard`

2. Do *one* of the following procedures:

   - For Windows operating environments, right-click the executable and then select Run as administrator.
   - For Solaris operating environments, enter the following command:

     `Solaris: sh ./ca-spconnect-`*`version`*`-sol.bin`

   - For Linux operating environments, enter the following command:

     `Linux: sh ./ca-spconnect-`*`version`*`-rhel30.bin`

   The wizard starts.

3. Click Next.

   The Login Details screen appears.

4. Complete the following fields with the information from your existing SiteMinder settings:

   Policy Server Name

   Specifies the Policy Server name or IP address.

   Username

   Specifies the Policy Server administrator username.

   Password

   Specifies the Policy Server administrator password.

   Agent Name

   Specifies the Agent-4x. The connection with the Policy Server is established using the details given in the Agent Name.

   Shared Secret Key

   Specifies the shared secret key that is associated with the Agent.

5. Click Next

   The Select Action screen appears.

6. Select Edit a SharePoint Connection option.

7. Click Next.

   The SharePoint Connection Properties screen appears.

8. Click Next until the SharePoint Connection Properties screen appears.

9. Locate the following field:

   Authentication URL

   Specifies the *port number that is associated* with the predefined protected URL which the SharePoint connection wizard adds automatically. When users try accessing a protected SharePoint resource without a SiteMinder session, they are redirected to the Authentication URL.

   If you are using a default port number (such as 80 for HTTP or 443 for HTTPS), delete the <port> setting from this field.

   Note: We recommend using HTTPS on production environments and pages which handle user credentials, such as login pages.

10. Change the protocol (such as HTTP or HTTPS) or the port number.

11. Click Next.

    The attribute details are saved and the Commit Details screen appears.

12. Click Install in the Commit Details screen.

    The Save Complete screen appears.

13. Click Done.

    The partnership details are saved, the SharePoint Connection is modified, and the wizard closes.

Verify that your Account has the Required Permissions

The user account with which you want to modify the SiteMinder trusted identity provider requires certain permissions. Modify the permissions of your user account if it does *not* meet the following conditions:

- An Administrator account.
- A member of the Administrators group.

Add the following privileges to your account:

- Local administrator on all SharePoint web front end (WFE) servers.
- Read/Write access to the configuration database.

Open a SharePoint 2010 Management Shell Window on your SharePoint Central Administration Server

Add claims to your <stmdnr> trusted identity provider using the SharePoint 2010 Management shell.

Follow these steps:

1. Log in to your SharePoint Central Administration server.
2. Click Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   A SharePoint 2010 management shell command-line window appears.

Identify your Trusted Identity Provider

A SharePoint 2010 environment can have multiple trusted identity providers. Identify your SiteMinder trusted identity provider before modifying any claims that are associated with it.

Follow these steps:

1. Enter the following command to list all of the trusted identity providers:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers appears.

2. Locate your SiteMinder trusted identity provider in the list.

   Your SiteMinder trusted identity provider is identified.

Change the Sign-in URL of your SiteMinder Trusted Identity Provider

Use the SharePoint 2010 Management Console to Changing the sign-in URL of your SiteMinder trusted identity provider.

Follow these steps:

1. Enter the following command to change the sign-in URL of your SiteMinder trusted identity provider:

   ```
   Set-SPTrustedIdentityTokenIssuer
   "name_of_your_siteminder_trusted_identity_provider" -SignInUrl new_sign-in_URL
   ```

   Example: Changing Sign-in URL

   This example shows how to change a sign-in URL for a trusted identity provider named SMTIP.

   ```
   Set-SPTrustedIdentityTokenIssuer "SMTIP" -SignInUrl
   https://sharepoint.example.com
   ```

   The sign-in URL is changed.

Verify that the Sign-in URL has Changed

You can verify the new sign-in URL for your SiteMinder trusted identity provider.

Follow these steps:

1. Enter the following command to verify the presence the new sign-in URL:

   ```
   Get-SPTrustedIdentityTokenIssuer
   ```

   A list of trusted identity providers and their respective settings appears.
2. Verify that the sign-in URL for your SiteMinder trusted identity provider is correct.

Chapter 14: Troubleshooting

This section contains the following topics:

Attributes Appear Truncated in SharePoint (140548)

Symptom:

I've noticed the following occur:

- My directory attributes appear truncated in SharePoint.
- I see the following message in my log files:

  `[WARNING: Response attribute will be trimmed. [attr = FMATTR:memberOf] [actual attr len = number] [ response attr len = number]]`

Solution:

Do the following:

1. Open the following file on your Policy Server:

   policy_server_home`\config\properties\wsfed.properties`

2. Locate the following line:

   `com.netegrity.assertiongenerator.wsfed.MaxUserAttributeLength=1024`

3. Change the value 1024 (at the end of the line) to a larger number. We recommend using multiples of 1024.

Log Files Show Access Denied Due to BadURLChars Settings

Symptom:

The log files of my Agent for SharePoint show users were denied access to resources because of the settings in the BadURLChars parameter.

Solution:

Follow these steps:

1. Examine the request to determine which character from the URL appears in the list of values for the following parameter:

   BadUrlChars

   Specifies the character sequences that cannot be used in URL requests. The Agent for SharePoint examines the characters in the URL that occur before the "?" character against those characters specified by this parameter. If any of the specified characters are found, the Agent for SharePoint rejects the request.

   You can specify the following characters:

   - a backward slash (\)
   - two forward slashes (//)
   - period and a forward slash (./)
   - forward slash and a period (/.)
   - forward slash and an asterisk (/*)
   - an asterisk and a period (*.)
   - a tilde (~)
   - %2D
   - %20
   - %00-%1f
   - %25 (do *not* add this value to the list if the URLs of your protected SharePoint resources contain blank spaces [%20])

   Separate multiple characters with commas. Do *not* use spaces.

   You can use the bad URL characters in CGI parameters if the question mark (?) precedes the bad URL characters.

   Default: (Agent for SharePoint) //,./,/.,/*,*.,~,\,%00-%1f

   Limits:

   - You can specify characters literally. You can also enter the URL-encoded form of that character. For example, you can enter the letter a, or you can enter the encoded equivalent of %61.

- You can specify a maximum number of 4096 characters (including commas that are used for separating characters).
- You can specify ranges of characters that are separated with hyphens. The syntax is: *starting_character-ending_character*. For example, you can enter a-z as a range of characters.
- Specify quotes (") with the URL-encoded equivalent of %22. Do *not* use ASCII.

2. Remove the character in your URL from the list of values in the previous parameter.

Log Files Show Access Denied Because of SPAuthorizeUserAgent Settings

Symptom:

The trace log files of my Agent for SharePoint show users were denied access to resources because of the settings in the SPAuthorizeUserAgent parameter.

Solution:

Follow these steps:

1. Examine the request shown in the trace log file to determine which User Agent string value was denied access. The following example shows typical trace log file results for this parameter:

```
spauthorizeuseragent=Microsoft Office Protocol Discovery
spauthorizeuseragent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; FDM; .NET CLR 3.5.30729; .NET CLR
3.0.30729; .NET4.0C; .NET4.0E)
spauthorizeuseragent=Mozilla/4.0 (compatible; MSIE 8.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; FDM; .NET CLR 3.5.30729; .NET CLR
3.0.30729; .NET4.0C; .NET4.0E)
spauthorizeuseragent=Mozilla/5.0 (Windows; U; Windows NT 6.1; en-US;
rv:1.9.2.13) Gecko/20101203 Firefox/3.6.13
spauthorizeuseragent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
InfoPath.2; MS-RTC LM8; .NET4.0C)
spauthorizeuseragent=Microsoft Office/12.0
spauthorizeuseragent=Microsoft Office/12.0 (Windows NT 6.1; Microsoft Office
Word 12.0.6545; Pro)
spauthorizeuseragent=Microsoft Office Existence Discovery
spauthorizeuseragent=Mozilla/4.0 (compatible; MSIE 7.0; Windows NT 6.1; WOW64;
Trident/4.0; SLCC2; .NET CLR 2.0.50727; .NET CLR 3.5.30729; .NET CLR 3.0.30729;
InfoPath.2; MS-RTC LM8; .NET4.0C; MSOffice 12)
spauthorizeuseragent=MSFrontPage/12.0
spauthorizeuseragent=Mozilla/4.0 (compatible; MS FrontPage 12.0)
spauthorizeuseragent=Microsoft-WebDAV-MiniRedir/6.1.7600
```

2. Add the user agent string from your trace log to the list of values in the following parameter:

   SPAuthorizeUserAgent

   Specifies a list of Microsoft Office user-agent strings for which the Agent for SharePoint allows access. This list is populated automatically with the default values when the Agent for SharePoint starts. The user-agent strings in this parameter act as a whitelist. Changes to this parameter override the default settings. Access is denied to clients whose user-agent string does not appear in the list.

For example, setting the value to Microsoft Office allows access to all versions of Microsoft Office products associated with the respective user agent string. Conversely, setting the value to Microsoft Office/12.0 allows access to only those versions of Microsoft Office products associated with the respective user agent string.

Default: Microsoft Office, MS FrontPage, MSFrontPage, Microsoft Data Access Internet Publishing Provider Protocol Discovery, Test for Web Form Existence, Microsoft-WebDAV-MiniRedir

Limits: Multiple values allowed.

Enable Search of Custom Object Classes in Your LDAP Directory

Symptom:

My LDAP directory contains custom object classes, but SiteMinder does not find them during searches.

Solution:

Follow these steps:

Note: For UNIX and Linux environments, navigate to the /registry directory, and then locate the previous setting in the sm.registry file.

1. Open the following registry location on each Policy Server:

   `HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\GroupClassFilters`

2. Locate the following key:

   `LDAP:`

3. Change the value of the data to the following:

   `*`

4. Navigate to the following key:

   `HKLM\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\`

   `Ds\ClassFilters`

5. Locate the following key:

   `LDAP:`

6. Change the value of the data to the following:

   `*`

REST API in Excel Services Does Not Work Due to CSSChecking ACO Parameter

Symptom:

REST API in Excel Services does not work when a SharePoint web application using Claims-based Authentication is protected with SiteMinder.

Solution:

The REST API in Excel Services does not work because the CSSChecking ACO parameter is enabled by default. CSSChecking verifies URLs for escaped and unescaped characters defined in the BadCSSChars parameter and returns with an Access Denied message.

Disable the CSSChecking ACO parameter. This change allows the REST API in Excel Services to work when a SharePoint web application using Claims-based Authentication is protected with SiteMinder.

Follow these steps:

1. Log on to the SiteMinder Administrative UI.

   The relevant tabs for your administrator privileges appear.

2. Click Infrastructure, Agents, Agent Configuration, Modify Agent Configuration.

   The Modify Agent Configuration: Search screen opens.

3. Select the Agent Configuration object from the list and click Select.

   The Modify Agent Configuration: ACO_Name dialog appears.

4. Click the Edit button on the CssChecking Parameter.

   The Edit Parameter dialog appears.

5. Enter No in the Value field and click OK.

   The Modify Agent Configuration: ACO_Name dialog appears with the General and Parameters group boxes.

6. Click Submit.

   The Modify Agent Configuration Object task is submitted for processing and the confirmation message appears.

Cannot Log Off Users from Sites and Subsites without Referring LogOffURI ACO (CQ 135854)

Symptom:

I cannot log off from a SharePoint site or a subsite.

Solution:

You cannot log off from a SharePoint site or a subsite because the actual logoff URL is different. Verify the signoff URL for each of the sites and subsites and add them to the LogOffURI ACO parameter.

For example, assume http://example.ca.com/ is the main site and http://example.ca.com/hr and http://example.ca.com/finance are subsites. The logoff URI is different for each of the sites and the subsites. Configure all of the sign-out pages as logoff URIs in the LogOffURI ACO parameter.

Enable Paging for Searches of Active Directory User Stores (32-bit systems)

Valid for Policy Servers that are installed on Windows 32-bit operating environments that are connected to Active Directory servers.

Symptom:

I cannot use the SharePoint people picker to search my Active Directory user store.

Solution:

The Active Directory namespace does not support paging, causing searches of more than 1000 users to fail. To support searches of large numbers of users in the Active Directory namespace, set the EnablePagingADNameSpace registry key to one.

To enable paging for searches on your Windows Policy Server:

1. Open the Windows registry editor.
2. Locate the following registry key:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider\EnablePagingADNameSpace`
3. Set the value of the key to 1.

To enable paging for searches on your UNIX Policy Server:

1. Navigate to *policy_server_installation_directory*/siteminder/registry
2. Open sm.registry in a text editor.
3. Locate the following text in the file:

   `HKEY_LOCAL_MACHINE\SOFTWARE\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider\EnablePagingADNameSpace`
4. Set the value of the key to 1.

Enable Paging for Searches of Active Directory User Stores (64-bit systems)

Valid for Policy Servers that are installed on Windows 64-bit operating environments (using WoW64 mode) that are connected to Active Directory servers.

Symptom:

I cannot use the SharePoint people picker to search my Active Directory user store.

Solution:

The Active Directory namespace does not support paging, causing searches of more than 1000 users to fail. To support searches of large numbers of users in the Active Directory namespace, set the EnablePagingADNameSpace registry key to one.

To enable paging for searches on your Windows Policy Server:

1. Open the Windows registry editor.
2. Locate the following registry key:

   ```
   HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\Netegrity\SiteMinder\CurrentVersion\Ds\LDAPProvider\EnablePagingADNameSpace
   ```

3. Set the value of the key to 1.

Users Cannot Access Office Applications in Internet Explorer 7 when Office Client Integration Is Enabled

Valid for Windows Vista

Symptom:

I cannot access Office applications in Internet Explorer 7 when Office Client Integration is enabled.

Solution:

This error is the result of a known Microsoft issue. Persistent cookies are not shared between Internet Explorer 7 and Office applications in Windows Vista. Internet Explorer 7 has an isolated cache location where files saved by web pages and persistent cookies are saved.

To access Office applications, add the SharePoint site to the list of trusted sites. This change enables the Web to save persistent cookies and temporary files to the regular cache. In this location, persistent cookies and temporary files are available to Office applications.

The following procedure shows how to add the SharePoint site (http://spagent.example:port) to the list of trusted sites in Internet Explorer 7.

Follow these steps:

1. Open Internet Explorer 7 browser.
2. Click Internet Options in the Tools menu.

   The Tools menu opens.
3. Click on the Security tab.

   The Security tab opens.
4. Click on Trusted Sites.

   The Trusted Sites icon is selected and the description appears.
5. Click on the Sites button.
6. Type the SharePoint site http://spagent.example:port into the text box and click the Add button.
7. (Optional) Clear the Require server verification (https://) option.

   Note: Clear the Require server verification (https://) option to add sites to the zone that do not use the https:// protocol. This setting protects your information while it is being transferred to the server that the site is hosted on.
8. Click the Close button.

   The Trusted Sites dialog opens.

9. Click OK.

   The Internet Options dialog opens.

Note: For more information about this issue, see the KB article 932118 on Microsoft Support site.

I Can Only View Read Only Copies of Documents on SharePoint Sites, but the Office Client Integration Is Enabled

Symptom:

My SharePoint servers have the Office Client Integration feature enabled, but I cannot open any of the documents for editing. I can only open read-only files.

Sometimes I also see the following error message:

```
An error (1502) occurred during the action Open File. File not found.
```

Solution:

Verify that the host names in the following Agent for SharePoint configuration parameter do *not* contain port numbers:

SPClientIntegration

Specifies the hostnames of the SharePoint servers protected by the Agent for SharePoint on which you want to permit Office Client Integration. The default parameter is blank and listed as plain. If there are multiple host entries, use the multivalue option button to add multiple hosts.

Add a port number to the value if the Agent for SharePoint operates on a nondefault port (any port except 80 or 443).

To use this parameter, verify that the SharePoint resources protected by SiteMinder also have their Office Client Integration enabled on the SharePoint central administration server.

Client Integration requires a persistent FedAuth cookie, verify that your SharePoint server is not configured to use session cookies. By default, UseSessionCookies in SharePoint is set to NO.

Default: None

Limits: Multiple values allowed. Use fully qualified domain names for all values.

Example: *agent_for_sharepoint_host_name.*example.com (default ports of 80 or 443)

Example: *agent_for_sharepoint_host_name.*example.com:81 (with nondefault port number for HTTP)

Example: *agent_for_sharepoint_host_name.*example.com:4343 (with nondefault port number for HTTPS)

SharePoint FedAuth Cookies and Office Client Integration Behavior

Symptom:

SharePoint stores a persistent FedAuth cookie on the hard drives of authenticated users. I do not want the SharePoint server to use these persistent cookies.

Solution:

You can configure SharePoint so a persistent FedAuth cookie is not stored. However, disabling the persistent FedAuth cookie also disables the single-sign on function of Office Client Integration. Users who try to open files on the SharePoint server are challenged for their credentials.

Note: For more information about how to disable FedAuth cookies in SharePoint 2010, go to the technet blogs website, and then search for the following phrase:

"Setting the Login Token Expiration Correctly for SharePoint 2010 SAML Claims Users"

Registration Failed with Unknown Error 127

Valid on Linux operating environments

Symptom:

I received the following error:

```
Registration Failed: Unknown Error 127
```

Solution:

Verify that your Linux operating environment meets the proper prerequisites.

More information:

Agent for SharePoint Prerequisites for Linux Operating Environments (see page 30)

Chapter 15: Agent for SharePoint Log Files

This section contains the following topics:

Agent for SharePoint Logging

The Agent for SharePoint log files record information about the status of the agent and other events. You can turn on various logs and tracing components to debug and troubleshoot events.

A log is a record of events that occur during program execution. A log consists of a series of log messages, each one describing some event that occurred during program execution. Log messages are written to log files.

A trace file provides detailed information about program operation for tracing and debugging purposes. Trace messages are ordinarily turned off during normal operation. Trace messages are embedded in the source code and cannot easily be localized. Moreover, trace messages can include significant data in addition to the message itself; for example, the name of the current user or realm.

The agent contains the following log files:

- server.log (see page 228)
- webagent.log (see page 229)
- trace.log (see page 229)
- Httpclient.log (see page 229)
- federation.log (see page 231)
- federationtrace.log (see page 232)
- claimswebservice.log (see page 233)
- claimswebservicetrace.log (see page 234)
- SPConnectionWizard.log (see page 235)

Important! We recommend you to enable logging only for debugging. In a production environment, enabling logging can cause performance degradation.

Server Logging

The Server.log file defines the startup and shutdown of the Agent for SharePoint. The <Server> element in the server.conf allows you to specify the logging settings for the Agent for SharePoint. The Web Agent error logging and trace logging configuration is done in the Web Agent configuration file (webagent.conf or localconfig.conf) or the Agent Configuration Object configured at the Policy Server.

Logging is enabled by default in the server.conf file and the log level is set to 2.

The logging section has the following format:

```
# Logging for the server
# 1 - FATAL
# 2 - ERROR
# 3 - INFO
# 4 - DEBUG
loglevel="2"
logconsole="yes"
logfile="yes"
logappend="no"
# Note: If logfilename is specified as a relative file, it
# will be relative to proxy-engine/
logfilename="logs/server.log"
```

loglevel

Sets the log level of the Agent for SharePoint server log. The higher the log level, the greater the detail of information that is recorded in the Agent for SharePoint log.

The log levels are as follows:

1

Indicates the least amount of detail in the log. Only fatal errors are recorded at log level 1.

2

Reports any error messages. Any errors that occur during processing are recorded at log level 2.

3

Indicates that warnings and other informational messages are recorded in the log.

4

Indicates debugging, the highest level of detail in the log.

logconsole

Specifies that the log file is written to the console window.

logfile

Specifies that the log information is written to a file. Set the parameter to yes to write the file to the location specified in the logfilename parameter. Set it to no if you do not want to write the log to a file.

logappend

Indicates that the log information is appended to a log file when the Agent for SharePoint starts. Set this parameter to yes to append data to an existing log file when the Agent for SharePoint restarts. Set this parameter to no if you do not want to append data.

logfilename

Defines the path and filename of the Agent for SharePoint log file. The default location is logs/server.log.

SiteMinder Web Agent Logging

The webagent.log file is a standard (WebAgent) HTTPluggin.dll HLA log file. Webagent.log logs events which monitor the communication between the Agent for SharePoint and the Policy Server. The name and location for this file is defined in the Agent Configuration Object. The logging parameters for this file are configured in the Logfile setting in the Agent Configuration Object.

SiteMinder Trace Logging

The trace.log file is a standard (WebAgent) HTTPPluggin.dll LowLevel trace file. The name and location for this file is defined in the Agent Configuration Object. The logging parameters for this file are configured in the SharePointAgentTrace.conf file. This file is found in the directory *Agent-for-SharePoint_home*/proxy-engine/conf/defaultagent.

HttpClient Logging

You can enable HttpLogging by setting the httpclientlog parameter to "yes". This parameter in located in the <Server> section of the server.conf file. By default, this parameter is set to "no".

We recommend that you enable HttpClient logging only for debugging. In a production environment, enabling logging can cause performance degradation.

Configure HttpClient Logging

You can configure various aspects of HttpClient logging by setting values to parameters in the httpclientlogging.properties file. This file is located in the *Agent-for-SharePoint_home*\Tomcat\properties directory.

Important! Because of potential performance degradation, do not enable HttpClient logging in a production environment.

The httpclientlogging.properties file has the following configurable parameters:

java.util.logging.FileHandler.formatter

Description: Specifies the name of the formatter class

Limits:

java.util.logging.SimpleFormatter — writes brief summaries of log records

java.util.logging.XMLFormatter — writes detailed descriptions in XML format

Default: java.util.logging.SimpleFormatter

java.util.logging.FileHandler.pattern

Description: Specifies the name of the HttpClient log file.

Limits:

Agent-for-SharePoint_home\proxy-engine\logs\httpclient%g.log

%g represents the generation number of the rotated log file.

java.util.logging.FileHandler.count

Description: Specifies the number of output files in a cycle

Default: 10

java.util.logging.FileHandler.limit

Description: Specifies an approximate maximum number of bytes to write to any on log file.

Limits: If set to zero, there is no limit.

Default: 5,000,000

In addition, you can specify the content of the logs with the following parameters:

Note: The value is always FINEST.

org.apache.commons.httpclient.level=FINEST

Specifies context logging only

httpclient.wire.header.level=FINEST

org.apache.commons.httpclient.level=FINEST

Specifies header wire and context logging

httpclient.wire.level=FINEST

org.apache.commons.httpclient.level=FINEST

Specifies full wire (header and content) and context logging

Federation Logging

The federation.log file in the Agent for SharePoint records error messages. The logger.properties file controls the configuration for this log.

The federation logging is disabled by default. You can enable federation logging by performing the following procedure in the LoggerConfig.properties file.

Note: Restart the Agent for SharePoint if you change the LoggerConfig.properties file.

Follow these steps:

1. Open the LoggerConfig.properties file. This file can be found in the directory *Agent-for-SharePoint*_home/Tomcat/webapps/affwebservices/WEB-INF/classes.
2. Set the LoggingOn parameter to Y.
3. Accept the default name and location for the LogFileName setting, which points to the federation.log file.
4. Restart your Agent for SharePoint.

   Error logging in the federation.log is now enabled.

More Information:

How to Start and Stop the Agent for SharePoint (see page 92)

Federation Trace Logging

The federationtrace.log file provides trace for each federation transaction that happens at the FSS layer in the Agent for SharePoint. The federationtrace log file is located in A*gent-for-SharePoint*_home/proxy-engine/logs. The LoggerConfig.properties file controls the configuration for this log.

The federation trace logging is disabled by default. You can enable federationtrace logging by performing the following procedure in the LoggerConfig.properties file.

Note: Restart the Agent for SharePoint if you change the LoggerConfig.properties file.

Follow these steps:

1. Open the LoggerConfig.properties file. This file can be found in the directory *Agent-for-SharePoint*_home/Tomcat/webapps/affwebservices/WEB-INF/classes.
2. Set the TracingOn setting to Y.
3. Accept the default name and location for the TraceFileName setting, which points to the federationtrace.log file.

   Note: Verify that the federationtrace.log file location points to the following directory
   Agent-for-SharePoint_home\\proxy-engine\\conf\\defaultagent\\FederationTrace.conf

   Federation trace logging is now enabled.

More information:

How to Start and Stop the Agent for SharePoint (see page 92)

Configure Federation Trace Logging

To collect federation transaction trace messages for the Agent for SharePoint, configure the federation trace logging.

Follow these steps:

1. Open the federationtrace.conf file. This file can be found in the directory *Agent-for-SharePoint_home*/proxy-engine/conf/defaultagent/federationtrace.conf.
2. Do one of the following:
   - Make a copy of the default template, federationtrace.conf and modify the file to include only the data you want to monitor.
   - Copy one of the preconfigured templates and assign a new name to it.

   Note: Do not edit the template directly.

3. Open the LoggerConfig.properties file in the directory *Agent-for-SharePoint_home*/Tomcat/webapps/affwebservices/WEB-INF/classes, and set the following parameters:
   - Set TracingOn to Yes. This option instructs the trace facility to write messages to a file.
   - Set the TraceFileName parameter to the full path of the trace log file. The default location is in *Agent-for-SharePoint_home*/proxy-engine/logs/federationtrace.log.
   - Set the TraceConfigFile parameter to the full path of the trace configuration file, either the default template, federationtrace.conf or another template. The default location is in *Agent-for-SharePoint_home*/proxy-engine/conf/defaultagent/federationtrace.conf.
4. Optionally, you can format the trace log file, the file that contains the log output. The following parameters are the Web Agent configuration parameters that dictate the format of the trace log file:
   - TraceRollover
   - TraceSize
   - TraceCount
   - TraceFormat
   - TraceDelim

   The LoggerConfig.properties file contains descriptions of all these settings.

   Note: Restart the Agent for SharePoint if you change the LoggerConfig.properties file.

Claims Web Service Logging

The claimswebservice.log records events that take place in the WS layer in the Agent for SharePoint. This file can be found in the directory *Agent-for-SharePoint_home*/proxy-engine/logs. The logging configuration is done in the LoggerConfig.properties file.

The claims web service logging is disabled by default. You can enable claims web service logging by performing the following procedure in the LoggerConfig.properties file.

Note: Restart the Agent for SharePoint if you change the LoggerConfig.properties file.

Follow these steps:

1. Open the LoggerConfig.properties file. This file can be found in the directory *Agent-for-SharePoint_home*/Tomcat/webapps/ClaimsWS/WEB-INF/classes.

2. Set the LoggingOn setting to Y.

   Accept the default name and location for the LogFileName setting, which points to the claimswebservice.log file.

   Claims web service logging is now enabled.

More information:

How to Start and Stop the Agent for SharePoint (see page 92)

Claims Web Service Trace Logging

The claimswebservicetrace.log provides trace for each user lookup that happens at the WS layer in the Agent for SharePoint. This file can be found in the directory *Agent-for-SharePoint_home*/proxy-engine/logs. The logging configuration is done in the FederationTrace.conf file. The FederationTrace.conf file can be found in the directory *Agent-for-SharePoint_home*/proxy-engine/conf/defaultagent.

Claims Web Service Trace logging is disabled by default. You can enable Claims Web Service logging by performing the following procedure in the LoggerConfig.properties file.

Note: Restart the Agent for SharePoint if you change the LoggerConfig.properties file.

Follow these steps:

1. Open the LoggerConfig.properties file. This file can be found in the directory *Agent-for-SharePoint_home*/Tomcat/webapps/ClaimsWS/WEB-INF/classes.
2. Set the TracingOn setting to Y.

   Accept the default name and location for the LogFileName setting, which points to the claimswebservicetrace.log file.

   Claims web service trace logging is now enabled.

More information:

How to Start and Stop the Agent for SharePoint (see page 92)

SharePoint Connection Wizard Logging

The SPConnectionWizard.log generates a log file which records events related to creating, editing, or deleting a SharePoint Connection. The log file reports data that the user has entered for creating or editing a connection, and if the connection was successfully or not. If the connection fails, then it lists the reason for failure.

When a connection has been successfully created or edited, the connection wizard generates a script file. Use this script file to create a trusted identity provider.

The SPConnectionWizard.log file is enabled by default. This file can be found in the directory *Agent-for-SharePoint*_home/sharepoint_connection_wizard/logs.

Note: For more information about creating a trusted identity provider, see the procedure on creating a trusted identity provider.

Configure SSL Logging for the Agent for SharePoint

You can configure SSL logging for the web server which hosts the Agent for SharePoint.

Follow these steps:

1. Open the following file with a text editor:

   ```
   Agent-for-SharePoint_home\httpd\conf\extra\httpd-ssl.conf
   ```

2. Locate the following line in the file:

   ```
   CustomLog logs/ssl_request_log \
       "%t %h %{SSL_PROTOCOL}x %{SSL_CIPHER}x \"%r\" %b"
   ```

3. Verify that all of the previous lines are not commented (They do *not* start with a # character).
4. Save the file and close the text editor.
5. Restart the Agent for SharePoint.

   SSL logging for the Agent for SharePoint is configured.

More information:

How to Start and Stop the Agent for SharePoint (see page 92)

SharePoint 2010 Logs

The Unified Logging Service (ULS Logs) is the primary logging or debugging service in SharePoint 2010. ULS Logs write SharePoint events to the SharePoint Trace Log, and stores them in the file system.

The ULS Logs for SharePoint are by default created under C:\Program Files\Common Files\Microsoft Shared\Web Server Extensions\14\LOGS. ULS logs are also sometimes referred to as Trace Logs.

You can configure logging parameters by modifying the required settings from Monitoring, Reporting, Configure diagnostic logging in Central Administration UI.

Note: For more information about logging in SharePoint, refer *Debugging and Logging Capabilities in SharePoint 2010* article from the Microsoft TechNet website.

Chapter 16: Remove SiteMinder Agent for SharePoint

This section contains the following topics:

How to Remove the SiteMinder Agent for SharePoint

To remove the SiteMinder Agent for SharePoint, complete the following procedures:

1. Remove the Claims Provider from SharePoint (see page 237).
2. Run the SharePoint Connection wizard to delete your SharePoint Connection (see page 238).
3. Perform the following steps on your SharePoint central administration server:
   a. Remove the trusted identity provider from any web applications using it (see page 240).
   b. Remove the Trusted Identity Provider from SharePoint (see page 241).
4. Remove the Agent for SharePoint.
5. (Optional) Remove Policy Server Objects from the Policy Store (see page 242).

Remove Claims Provider

You can remove the Claims Provider from the computer hosting SharePoint Central Administrative by completing the following procedure.

Follow these steps:

1. Select Start, Control Panel, Programs, Uninstall a program.

   The Uninstall or change a program page appears.
2. Select CA SiteMinder Claims Provider for SharePoint.
3. Click Uninstall.
4. Read the confirmation information and click Uninstall.
5. Click Done.

The Claims Provider is removed from your system.

Delete a SharePoint Connection

Follow these steps:

1. Perform the following:
   - (Windows)
   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard
   b. Right-click the executable and select Run as administrator.

      The SharePoint Connection wizard starts.
   - (Unix)
   a. Navigate to the following directory:
   Agent-for-SharePoint_home/sharepoint_connection_wizard
   b. Enter one of the following commands:
      - Solaris: sh ./ca-spconnect-12.0-sp3-sol.bin
      - Linux: sh ./ca-spconnect-12.0-sp3-rhel30.bin

      The SharePoint Connection wizard starts.
2. Click Next.

   The Login Details screen appears.
3. Enter the following login details to connect to the Policy Server.

   Policy Server Name

   Specifies the Policy Server name or IP address.

   Username

   Specifies the Policy Server administrator username.

   Password

   Specifies the Policy Server administrator password.

   Agent Name

   Specifies the Agent-4x. The connection with the Policy Server is established using the details given in the Agent Name.

   Shared Secret Key

   Specifies the shared secret key associated with the Agent.
4. Click Next

   The Select Action screen appears.
5. Select Delete a SharePoint connection option.
6. Click Next.

The Delete from list screen appears.

7. Select the items from the list and click Delete.
8. Click Next.

   The Commit details screen appears.
9. Click Install.

   The Save complete screen appears.
10. Click Done.

    The partnership details are saved, the SharePoint Connection is deleted, and the wizard closes.

More information:

SharePoint Connection Wizard Information Worksheet (see page 246)

Remove the Trusted Identity Provider from any Web Applications Using it

A trusted identity provider cannot be removed from SharePoint while any web applications are using it. Before you remove the trusted identity provider itself, remove the association between the SiteMinder trusted identity provider and any of your web agents using it.

follow these steps:

1. Click Start, Microsoft SharePoint 2010 Products, SharePoint 2010 Central Administration.

   The Central Administration home page opens.

2. Under Application Management, click Manage web applications.

   The web application management page opens.

3. Click the line corresponding to the name of a web application using the SiteMinder trusted identity provider.

   The web application is selected.

4. On the ribbon, click Authentication Providers.

   The Authentication Providers dialog appears.

5. In the Authentication Providers dialog, click the link that corresponds to the zone of your web application. For example, if the web application using the SiteMinder trusted identity provider is in the Intranet zone, click the Intranet link.

   The Edit Authentication page appears.

6. Under Claims Authentication types, clear all Trusted Identity provider check boxes.

7. Click Save.

   The SiteMinder trusted identity provider is removed from the web application in the zone.

8. Repeat Steps 3 through 7 for all web applications and the zones using the SiteMinder trusted identity provider.

   The trusted identity provider is removed from all web applications and their respective zones.

More information:

Alternate Connection Wizard Method to Help Resolve Firewall Issues (see page 84)

Remove Trusted Identity Provider

You can perform the following procedure to remove the trusted identity provider for SharePoint using Windows PowerShell.

Follow these steps:

1. Select Start, All Programs, Microsoft SharePoint 2010 Products, SharePoint 2010 Management Shell.

   The Microsoft PowerShell command prompt appears.

2. Enter following command:

   `Remove-SPTrustedIdentityTokenIssuer -Identity`

   -Identity

   Specifies the name of the identity provider to remove.

   Example: Remove-SPTrustedIdentityTokenIssuer TestSTS

   The trusted identity provider for SharePoint is removed.

Note: If you re-create a Trusted Identity Provider, verify that a hash precedes the 'New-SPTrustedRootAuthority' line in the powershell script. As the certificates (signing, root CA, and intermediate CA) are not removed, modify the powershell script by adding hash to avoid certificate errors.

Remove the Agent for SharePoint from Windows

You can remove the Agent for SharePoint from your Windows system by performing the following procedure.

Follow these steps:

1. Select Start, Control Panel.
2. Select Programs, Uninstall a program.
3. Select SiteMinder Agent for SharePoint *version*.
4. Click Uninstall/Change.

5. Read the confirmation information and click Uninstall.
6. Click Finish.

   The uninstall confirmation screen appears.
7. Select one of the following options:
   - Yes, restart my system
   - No, I will restart my system myself
8. Click Done.

Note: If you have modified any of the Agent for SharePoint files such as server.conf, the uninstall program does not remove these files or their parent folders.

Remove the Agent for SharePoint from UNIX

Use the following procedure to uninstall Agent for SharePoint from a UNIX system.

Follow these steps:

1. Open a console window.
2. Navigate to the root installation directory.
3. Run the following program at the command prompt:

   ./ca-spagent-uninstall.sh

Note: If you have modified any Agent for SharePoint files, such as server.conf, the uninstall program does not remove these files or their parent folders automatically. Remove any files and folders for files you have changed.

(Optional) Delete Policy Store Objects

If you do not intend to use the Policy Store objects after removing the agent, delete the objects using the SiteMinder Administrative UI.

Note: Your administrative privileges determine the objects you can access.

Follow these steps:

1. Click *<tab>*, *<Policy Server category>*.

   Example: Click Infrastructure, Authentication.

2. Click <*Policy Server object*>, Delete <*Policy Server object*>.

   The Delete Object pane opens.

   Example: Click Authentication Scheme, Delete Authentication Scheme.

   The Delete Authentication Scheme pane opens.

3. Specify search criteria, and click Search.

   A list of objects that match the search criteria opens.

4. Select an object from the list, and click Select.

   A confirmation pane opens.

   Note: You can select more than one object at a time.

5. Click Yes.

   The Delete Object task is submitted for processing.

Appendix A: Agent for SharePoint Worksheets

This section contains the following topics:

Agent for SharePoint Configuration Wizard Information Worksheet

Use this worksheet to gather the required information to configure the Agent for SharePoint.

Information Required	Your Value
SiteMinder administrator name	
SiteMinder administrator password	
Trusted host name	
Host Configuration Object	
Agent Configuration Object	
IP address of the Policy Server where the host is registered	
Host Configuration File name and location	
Name and location of the Web Agent configuration file	
Email address of the Apache web server administrator	
Fully qualified host name of the server	
Port number for HTTP requests	
Port number for SSL requests	
Port number for HTTP Claims web service	
Port number for SSL Claims web service	

More information:

Run the Configuration Wizard (see page 78)

SharePoint Connection Wizard Information Worksheet

Use this worksheet to gather the required information to configure the SharePoint Connection Wizard.

Important! The SharePoint connection wizard automatically creates federation objects (resource partners) in your Policy Servers. Use only the SharePoint connection wizard to create or manage these objects. If you have a Federation Security Services license, these objects also appear in the FSS Administrative UI. Advise your Federation Security Services Administrator not to modify these objects with the FSS Administrative UI unless explicitly told to do so by CA support personnel.

Information Needed	Your Value
Policy Server name	
Policy Server administrator username	
Policy Server administrator password	
Agent-4x name	
Shared Secret Key of the Agent-4x	
Domain associated with the SharePoint connection	
Name of the SharePoint connection	
Authentication URL	
SharePoint Realm Name	
Skew Time	
Validity Duration	
Signing Alias	
Protection level	
Identifier Claim Name	
Directory Attribute	
Attribute	(group-based claims) smusergroups (role-based claims) userrole
Claim Type	

More information:

Manage SharePoint Connections Using the SharePoint Connection Wizard (see page 83)

SharePoint 2010 Federation Worksheet

Use this worksheet to gather the required information to configure SharePoint for SiteMinder.

Information Needed	Your Value
Trusted Identity Provider name	
Certificate authority certificate	
Certificate-Authority Certificates	
Claims Mappings	
Claims Identifier	
Realm	
SignInUrl	
UseWReply	
Name ID	
Account Partner ID	
Signing Certificate	
Security Token Consuming Service	

More information:

Configure SharePoint (see page 97)

Appendix B: Platform Support and Installation Media

This section contains the following topics:

Locate the SiteMinder Agent for SharePoint Platform Support Matrix

You can find a comprehensive list of the CA and third–party components supported by SiteMinder on the Technical Support site.

Follow these steps:

1. Log in to the Technical Support site.

   The Support home page appears.

2. Under Support, click Support By Product.
3. In the Select a Product Page field, enter SiteMinder and press Enter.

   The SiteMinder product page appears.

4. Scroll to the Product Status section and click CA SiteMinder Family of Products Platform Support Matrices.

   The CA SiteMinder Platform Support Matrices section appears.

5. Under CA SiteMinder Agent for SharePoint, click the PDF link.

   The CA SiteMinder Agent for SharePoint Platform Support Matrix opens in a new tab.

Locate the Bookshelf

The SiteMinder Agent for SharePoint bookshelf is available on the Technical Support site.

Follow these steps:

1. Log in to the Technical Support site.

   The Support home page appears.

2. Under Support, Under Support, click Documentation.
3. In the Select a Bookshelf field select SiteMinder Agent for SharePoint *version* and click Go.

   The SiteMinder Agent for SharePoint bookshelf page appears.

Locate the Installation Media

You can find a comprehensive list of the SiteMinder installation media on the Technical Support site.

Follow these steps:

1. Log in to the Technical Support site.
2. Under Support, click Download Center, Products.

   The Download Center screen appears.
3. Enter SiteMinder Agent for SharePoint in the Select a Product field.
4. Select a release from the Select a Release list.
5. Select a service pack from the Select a Gen Level list.
6. Click Go.

   The Product Downloads screen appears. All SiteMinder Agent for SharePoint installation executables are listed.

Index

D

E

F

G

H

I

K

L

M

N

O

P

R

S

T

U

V