CA Technologies SiteMinder®

Agent for Microsoft® SharePoint®

r12.0

Second Edition

CA Technologies Product References

This document references the following CA Technologies products:

- CA Technologies SiteMinder®

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.

Documentation Changes

The following documentation updates have been made since the last release of this documentation:

- Open the SiteMinder Management UI—Added instructions for opening the <stmdnr> Management UI on a web front-end (WFE) server.
- Protect Applications with the SiteMinder Agent for SharePoint—Added steps for protecting web applications on SharePoint farms (CQ151213).
- Web Agent for SharePoint Does Not Honor PersistantIPCheck Parameter—Added a work-around that skips the persistent IP check for the SPSESSION cookie (CQ126355, CQ145763, CQ143544).

Contents

Chapter 1: SiteMinder and Microsoft SharePoint

This section contains the following topics:

Purpose and Audience

The SiteMinder Agent for SharePoint is an HTTP plug-in that lets you protect resources in your Microsoft SharePoint environment with CA SiteMinder.

This document contains tasks and procedures for the following personnel:

- SharePoint Administrators
- SiteMinder Administrators

SharePoint administrators need working knowledge of the following concepts:

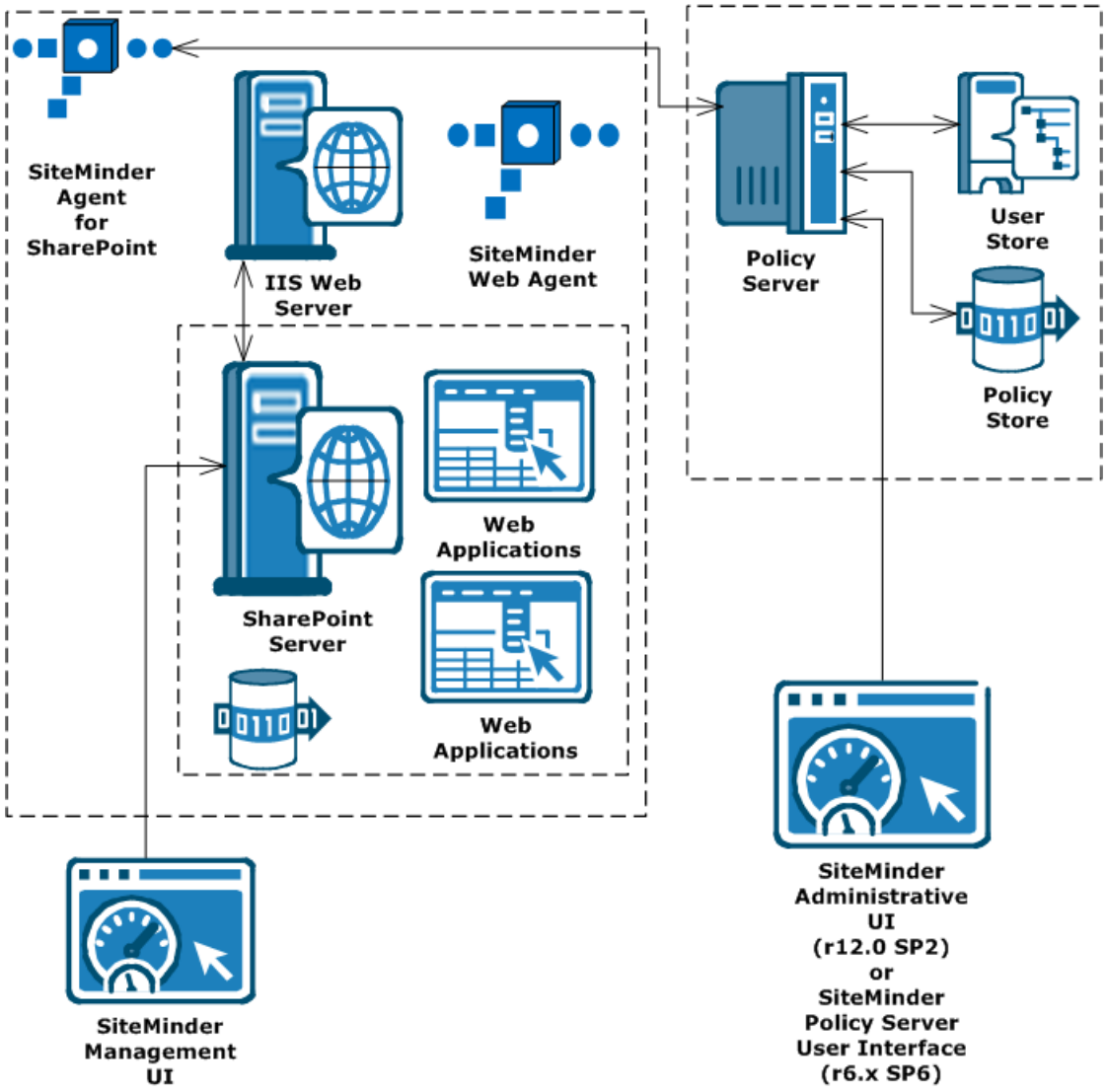
- Creating a SharePoint web application
- Adding SharePoint web applications to site collections
- Managing SharePoint site collection administrators
- Working with web application access policies in SharePoint
- Adding, modifying, or removing files or other content to or from a SharePoint web application
- Managing SharePoint users and user profiles

SiteMinder administrators need working knowledge of the following concepts:

- Installing and configuring SiteMinder Web Agents and Policy Servers
- Creating SiteMinder applications or policies, realms, rules, and responses to protect resources
- Managing SiteMinder user directories

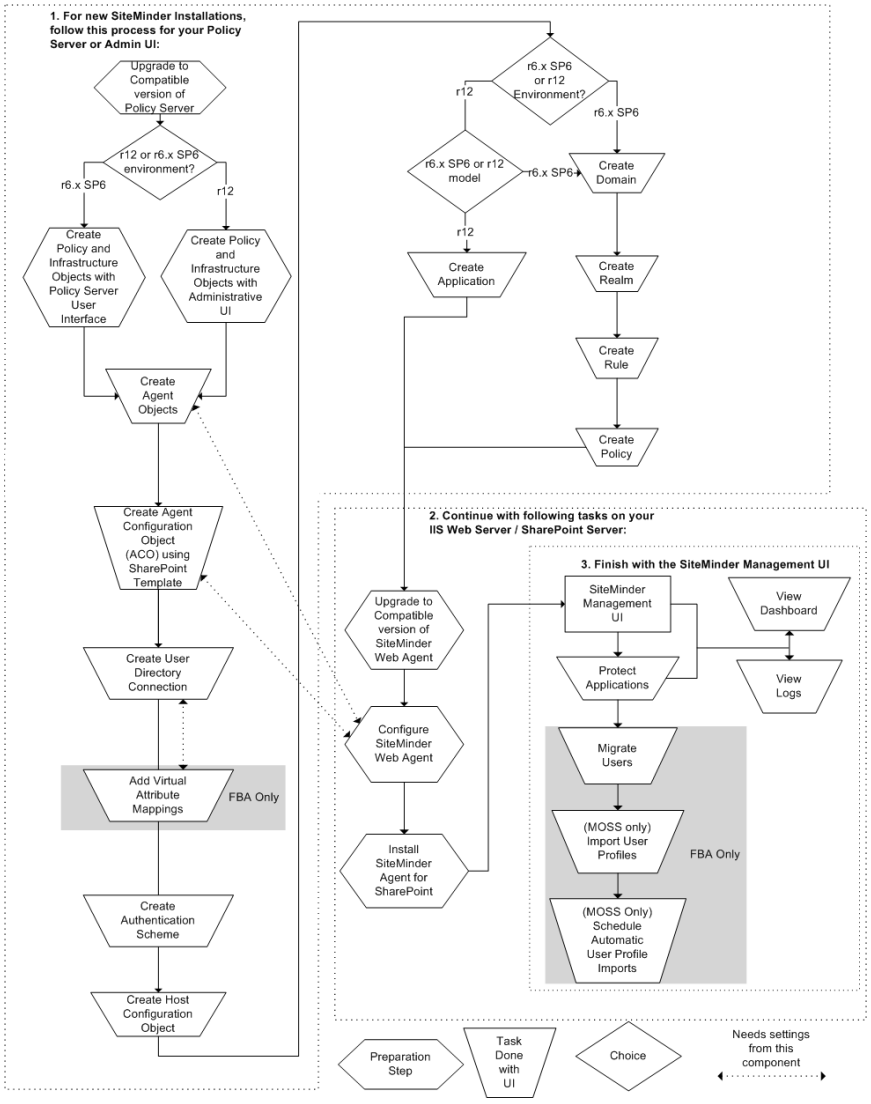
SiteMinder Components used with SharePoint

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



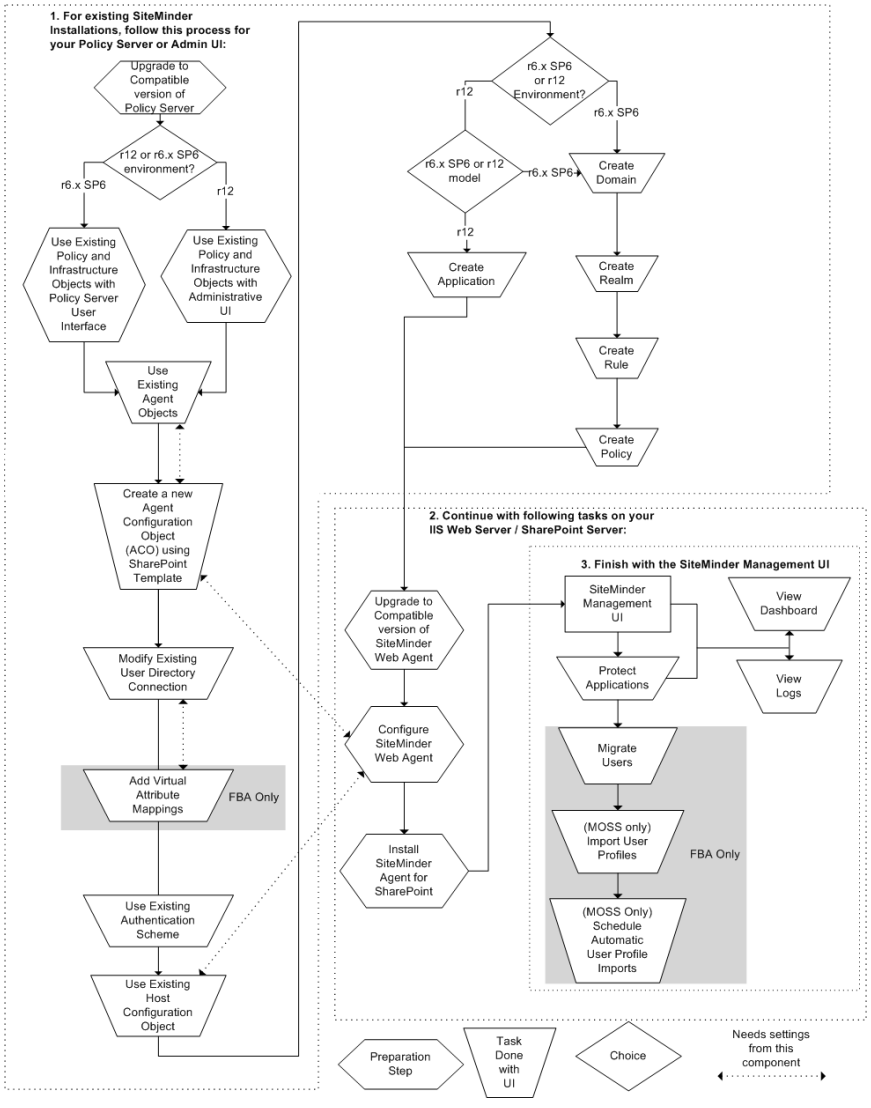
Component and Task Relationships for New Installations

The following illustration describes the typical tasks you perform during new installations of the SiteMinder and SharePoint components:



Component and Task Relationships for Adding the Agent for SharePoint to your Existing SiteMinder Environment

The following illustration describes the typical tasks you perform when adding the Agent for SharePoint to your existing SiteMinder environment:



SiteMinder Agent for SharePoint Authentication Methods and SharePoint Authentication Type Options

The SiteMinder Agent for SharePoint provides the following options by which you can configure SiteMinder protection for one or more SharePoint web applications/zones. You also have the option of leaving one or more SharePoint web applications/zones unprotected in which case CA SiteMinder Agent for SharePoint ignores requests to these SharePoint resources.

Windows (Impersonation)

Used to configure SiteMinder protection along with Windows impersonation for users accessing the SharePoint web application/zone. This option is applicable only when user accounts are stored in Active Directory. Many SiteMinder authentication schemes can be used with this option, including Forms, Basic, and the Windows authentication scheme.

Forms (FBA)

Used to configure SiteMinder protection for users accessing the SharePoint web application/zone. This option can be used with any type of SiteMinder user directory, but it is not used when the user accounts are in Active Directory. The Agent for SharePoint configures the SharePoint web application/zone to use ASP.NET Forms Based authentication. Together, with the SiteMinder Membership and role provider, retrieves the user and group information from the user directory. Many SiteMinder authentication schemes can be used with this option, including Forms and Basic.

Note: For more information about restrictions or workarounds involving SiteMinder authentication schemes, see the SiteMinder Agent for SharePoint Release Notes.

More information:

Office Client Integration without a Persistent Cookie (see page 204)

Chapter 2: Prerequisites

This section contains the following topics:

Microsoft Prerequisites

The SiteMinder Agent for SharePoint requires the following Microsoft products:

- *One* of the following:
  - Microsoft Office SharePoint Server (MOSS) 2007
  - Microsoft Windows SharePoint Services 3.0
- .NET Framework 3.0 (minimum)

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 Platform Support Matrix (see page 195)

SiteMinder Component Prerequisites for the Agent for SharePoint

Your SiteMinder environment needs a minimum of the following components and versions specified to use the SiteMinder Agent for SharePoint:

- One of the following Policy Server versions:
  - r12.0 SP2 (for r12.0 environments)
  - r6.x SP6 (for r6.x environments)
- One of the following Web Agent versions:
  - r12.0 SP2 (for r12.0 environments)
  - r6.x SP6 (for r6.x environments)

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

Upgrade any SiteMinder components in your environment that do not meet the minimum versions shown in the previous list.

More information:

Locate the SiteMinder Platform Support Matrix (see page 195)

SiteMinder Component Settings Required Following Policy Server Upgrades (SharePoint)

If you had to upgrade your SiteMinder Policy Server to use the Agent for SharePoint, change the following settings in your SiteMinder environment:

- Upgrade to *one* of the following SiteMinder policy store versions:
  - r12.0 SP2 (for r12.0 environments)
  - r6.x SP6 (for r6.x environments)
- (Optional) If you plan to use Office Client Integration, update your SiteMinder Web Agent type to include the following settings:
  - Head
  - Options

    Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

Upgrade your Policy Store

The SiteMinder Agent for SharePoint uses specific Agent configuration parameters to manage the protected resources in your SharePoint environment. The following Agent Configuration Object template contains these parameters:

`SharePointDefaultSettings`

If you had to upgrade your Policy Server to use the SiteMinder Agent for SharePoint in your existing SiteMinder environment, upgrade your policy store to add the previous template.

Note: For more information about upgrading your policy store, see the *SiteMinder Upgrade Guide*.

More information:

Create an Agent Configuration Object for your SharePoint Resources (r12.0 SP2) (see page 42)
Create an Agent Configuration Object for your SharePoint Resources (r6.x SP6) (see page 61)

Update the SiteMinder Agent Types for your SharePoint Resources (r12.0 SP2)

In addition to the default HTTP methods monitored by the SiteMinder Web Agents, the SiteMinder Agent for SharePoint also requires the following HTTP methods to protect your SharePoint resources:

- Head
- Options

Update the SiteMinder Agent type settings for your SharePoint resources

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 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 group box, 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:

   `Options`

7. Scroll to the bottom of the Actions group box, and then click Create.

   A new action field appears at the end of the list.

8. Highlight the text in the New Action field, and then enter the following:

   `Head`

   Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

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.

    Note: If you plan to reuse any application resources or domain rules from your existing SiteMinder r12.0 SP2 environment with the Agent for SharePoint, add the HEAD and OPTIONS actions to each application resource or domain rule you want to reuse.

More information:

Add HEAD and OPTIONS Actions to your Resources in an Existing SiteMinder Application (r12.0 SP2) (see page 208)
Add HEAD and OPTIONS Actions to Existing SiteMinder Rules (r12.0 SP2) (see page 209)

Update the SiteMinder Agent Types for your SharePoint Resources (r6.x SP6)

In addition to the default HTTP methods monitored by the SiteMinder Web Agents, the SiteMinder Agent for SharePoint also requires the following HTTP methods to protect your SharePoint resources:

- Head
- Options

To update the SiteMinder Agent type settings for your SharePoint resources

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select View, Agent Types.

   The Policy Server places a checkmark in the View menu to the left of the menu selection and Agent Types appear in the System tab of the SiteMinder Administration window.

   Note: If there is already a check next to Agent Types in the View menu, selecting the option again removes Agent Groups from the System tab.
3. From the System tab, select Agent Types to display the Agent Types List in the right pane.
4. Click the Web Agent entry then right-click.
5. Select Properties of Agent Type.
6. The Agent Type Properties dialog opens.
7. Click Create.

   The New Agent Action dialog opens.
8. Enter the following text and click OK:

   `Options`
9. Click Create.

   The New Agent Action dialog opens.
10. Enter the following text and click OK:

    `Head`

    Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.
11. Click OK.

    The Agent type settings for your SharePoint resources are updated.

    Note: If you plan to reuse any rules from your existing SiteMinder r6.x SP6 environment with the Agent for SharePoint, add the HEAD and OPTIONS actions to each rule you want to reuse.

More information:

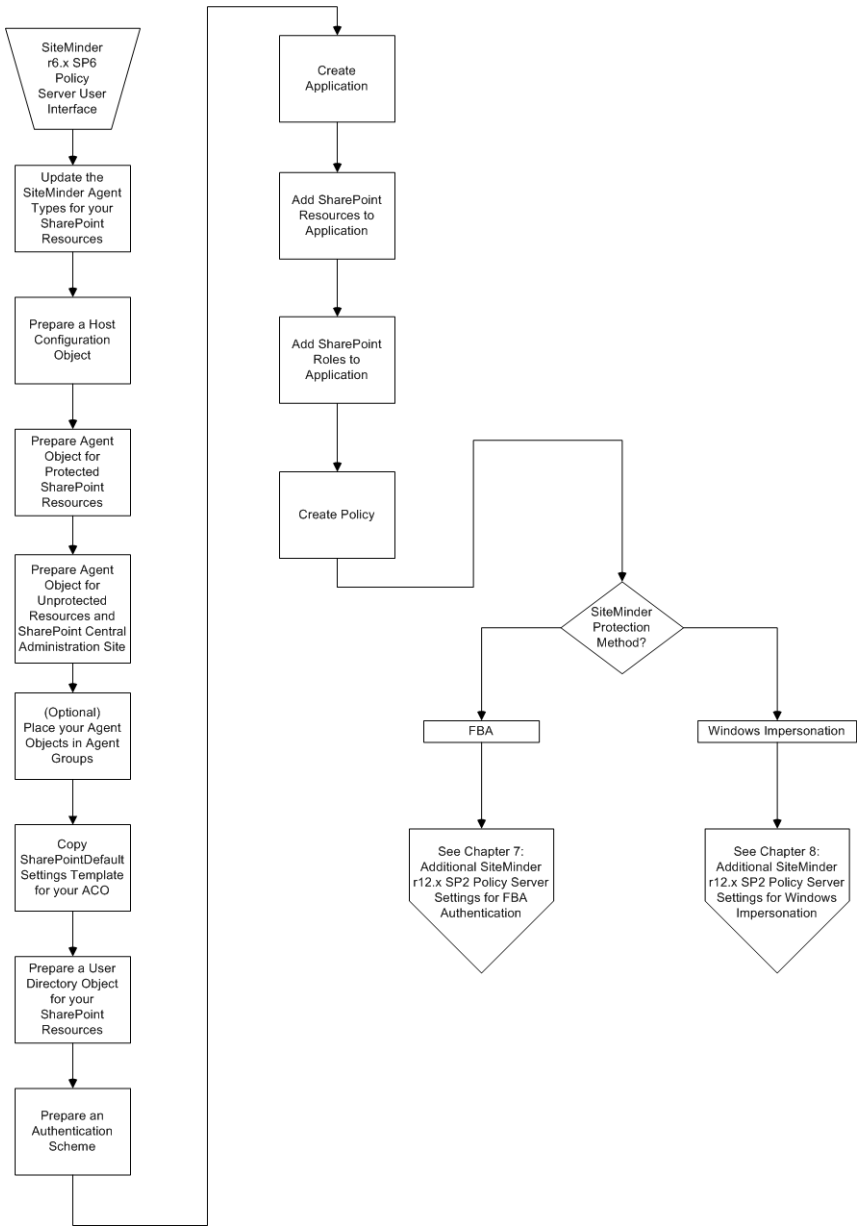
Add HEAD and OPTIONS Actions to Existing SiteMinder Rules (r6.x SP6) (see page 210)

Chapter 3: Configuring the SiteMinder Policy Server

This section contains the following topics:

Protecting SharePoint Resources with SiteMinder r12.0 SP2 Roadmap

Protecting resources on your SharePoint system using SiteMinder r12.0 SP2 requires several separate procedures. The entire protection process is described in the following illustration:



More information:

Set the Web Agent Parameters for Impersonation (r12.0 SP2) (see page 44)

Create or Reuse a Host Configuration Object (r12.0 SP2)

When a SiteMinder Web Agent starts, it uses use a Host Configuration object to make an initial connection to a SiteMinder Policy Server. You need a Host Configuration object to operate the Agent for SharePoint. This section describes how to create a Host Configuration object, but if you are an experienced SiteMinder user, you can also reuse an existing Host Configuration object instead.

To create a host configuration object

1. Click Host Configuration, Create Host Configuration.

   The Create Host Configuration: Host Configuration Search Screen appears.

2. Click Create a copy of an object of type Host Configuration, and then click Submit.

   The Create Host Configuration: dialog appears.

3. Enter a distinctive name and an optional description.

4. Click Add, and then enter the IP Address or fully qualified domain name of the computer which hosts the Policy Server.

5. Click Submit.

   The confirmation screen appears.

6. Click OK.

   The Host Configuration Object is created.

Create Agent Objects for your SharePoint Resources (r12.0 SP2)

The SharePoint resources in your organization need at least two different Agent objects defined in the SiteMinder Administrative UI:

- One Agent object for the SharePoint resources you want to protect.
- One Agent object for the *unprotected* SharePoint resources, such as the SharePoint Central Administration web site.

To create Agent objects for your SharePoint resources

1. Click Infrastructure, Agent, Create Agent.

   The Create Agent dialog appears.

2. Verify that Create a new object of type Agent is selected, and then click OK.

   The Create Agent: Dialog appears.

3. Click the Name field, and enter a distinctive name for the Agent.

   We recommend using a name that you can easily associate with the corresponding SharePoint resources. For example, an Agent object associated with the protected SharePoint resources could be named "SP_Protected", and an Agent Object associated with the unprotected SharePoint resources, could be named, "SP_Unprotected."

4. (Optional) Click the Description field, and enter a description.

5. Click Submit.

   The Agent object is created and the confirmation screen appears.

6. Click OK.

7. Repeat Steps 1 through 6 to create the second Agent object.

Place your Agent Objects in an Agent Group (r12.0 SP2)

If you have many Agent objects, we recommend using Agent Groups because several Agent objects can be added or removed from a policy at the same time. For example, you can create one Agent group for your protected resources and another for your unprotected resources. This section describes how to create Agent Groups, but if you are an experienced SiteMinder user, you can use existing Agent Groups instead.

To place your Agent Objects in an Agent Group

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

   The Create Agent dialog appears.

2. Verify that Create a new object of type Agent Group is selected, and then click OK.

   The Create Agent Group: Dialog appears.

3. Click the Name field, and enter a distinctive name for the Agent group.

4. Click Add/Remove

   The Agent Group Members dialog appears.

5. 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.

6. Click Submit.

   The Agent group is created and the confirmation screen appears.

7. Click OK.

8. Repeat Steps 1 through 7 to create additional Agent groups as needed.

Modify a User Directory Connection for your SharePoint User Directories in the SiteMinder Policy Server (r12.0 SP2)

The SiteMinder Policy Server communicates with your existing user directories to authenticate users. Each user directory needs a connection in the SiteMinder Administrative UI. This section describes how to modify an existing user directory connection for use with the Agent for SharePoint, but you can also create one if you want. For more information about creating a user directory connection, see the *Policy Server Configuration Guide*.

To modify a user directory connection for your SharePoint user directories in the SiteMinder Policy Server

1. Click Infrastructure, Directory, User Directory, Modify User Directory.

   The Modify User Directory search pane appears.

2. Click the option button of the directory you want, and then click Select.

   The Modify Directory: *name* pane appears.

3. Verify the following settings:

   - The Use authenticated user's security context option is *not* set.
   - The Require Credentials Option is set, and that the following fields are completed:
     - Username
     - Password
     - Confirm Password

     Note: Consult the administrator of your directory server for more information about the proper settings to use in your environment.

4. Click Submit.

   The Modify User Directory task is submitted for processing, and the confirmation screen appears.

5. Click OK.

Create Virtual Attribute Mappings to your SharePoint User Directories (r12.0 SP2)

SiteMinder uses virtual attribute mappings for the FBA authentication method to preserve some SharePoint features that are lost when the Agent for SharePoint performs authorization and authentication (instead of the SharePoint environment). For example, the DisplayName attribute mapping allows SiteMinder to add the first and last names of the user to the upper right corner of the browser window. If the DisplayName mapping is not set, SiteMinder uses the login ID of the user instead. Use these mappings for each directory in your SharePoint environment.

The SiteMinder Agent for SharePoint contains the following attribute mappings:

UniversalID

Specifies the directory attribute that contains the user name from a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Examples: (Sun Java System) UniversalID=uid *or* UniversalID=cn

Examples: (Microsoft Active Directory) UniversalID=cn *or* UniversalID=sAMAccountName

Example: (DB2) UniversalID=Name

Email

Specifies the directory attribute that contains the email address of a user within a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Example: (Sun Java System) Email=mail

Example: (Microsoft Active Directory) Email=mail

Example: (DB2) Email=EmailAddress

GroupID

Specifies the directory attribute that contains the group or role to which a user belongs within a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Example: (Sun Java System) GroupID=cn

Example: (Microsoft Active Directory) GroupID=cn

Example: (DB2) GroupID=Name

DisplayName

Specifies the directory attribute that contains the user name you want to display from a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint. The value of this virtual attribute appears in the upper right corner of the browser window after SiteMinder authenticates the user to SharePoint.

Example: (Sun Java System) DisplayName=cn

Example: (Microsoft Active Directory) DisplayName=displayName

Example: (DB2) DisplayName=Name

The names and the attributes to which they are mapped in the previous list are the default values. For r12.0 SP2, change them according to your needs. Use the same names and mappings in both the directory entry on the Policy Server and the related Web Agent Configuration Object.

You must employ the following procedure for each of the listed attributes:

1. UniversalID
2. Email
3. GroupID
4. DisplayName

To create attribute mappings for your SharePoint user directories

1. Click Infrastructure, Directory, User Directory, Modify User Directory.

   The User Directory search screen appears.
2. Search for the directory instance you created, and then click Select.

   Modify User Directory: screen appears.
3. Scroll down to the Attribute Mapping List group box, and then click Create.

   The Create Attribute Mapping screen appears.
4. Verify that Create a new object of type Attribute Mapping is selected, and then click OK.

   The Create Attribute Mapping: screen appears.
5. Enter a distinctive name for your attribute mapping that you are creating, and an (optional) description. For example, enter the UniversalID mapping and description.
6. Click the Definition field, and then enter the attribute name from your user directory that you want to associate with the UniversalID mapping.

   Note: If you are using a SharePoint server (MOSS), and you plan to Import User Profiles, record the value of the UniversalID mapping for future reference.
7. Click OK.

   The Create Attribute Mapping: screen closes.
8. Repeat these steps for each attribute.

More information:

Update the Agent Configuration Parameters for your Agent for SharePoint (see page 99)

(FBA Only) Create a Custom Mapping to Filter Items with a Particular Object Class Attribute from your Search Results (r12.0 SP2)

If you are using the Active Directory or LDAP namespaces in your SiteMinder connection to your user directory, you can define a virtual attribute mapping to a specific object class attribute in that directory. These mappings can help narrow your searches. For example, if your directory schema contains an object class attribute named "computer," you can create a virtual attribute to exclude items containing the "computer" attribute from your search results in the people picker.

To create a custom mapping to filter items with a particular Object Class attribute from your search results

1. Click Infrastructure, Directory, User Directory, Modify User Directory.

   The User Directory search screen appears.

2. Search for the directory instance you created, and then click Select.

   The Modify User Directory: screen appears.

3. Verify that the *one* of the following namespaces is used:

   `AD:`

   `LDAP:`

4. Under the Attribute Mapping list, click Create.

   The Create Attribute Mapping screen appears.

5. Verify that the Create a new object of type Attribute Mapping option button is selected, and then click OK.

6. Enter the following name:

   `FilterClass`

7. (Optional) Enter a description.

8. Click the Definition field, and then type the name of the Object Class attribute which you want to exclude from your results. For example, if the name of your object class attribute is "computer," add the following:

   `computer`

9. Click OK.

   The Create Attribute Mapping screen closes and the Modify User Directory: screen appears.

10. Click Submit.

    The Modify User Directory task is submitted for processing, and the confirmation screen appears.

11. Click OK.

Create or Reuse Authentication Scheme for your SiteMinder Agent for SharePoint (r12.0 SP2)

The SiteMinder Agent for SharePoint supports the CA Technologies SiteMinder Authentication Schemes. The SiteMinder Agent for SharePoint needs an Authentication Scheme defined in the Administrative UI. This section describes how to create an authentication scheme, but if you are an experienced SiteMinder user, you can reuse an existing authentication scheme instead.

To create an authentication scheme for your SiteMinder Agent for SharePoint

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

   The Create Authentication Scheme pane appears.

2. Make sure the Create a new object of type Authentication Scheme radio button is selected, and then click OK.

   The Create Authentication Scheme: pane appears.

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

4. Click the Authentication Scheme Type: drop-down list, and then select the type of Authentication Scheme that you want.

   The options for your chosen Authentication Scheme appear.

5. Complete the fields for your Authentication Scheme.

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

6. Click Submit.

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

7. Click OK.

Create an Application to protect your SharePoint Resources (r12.0 SP2)

To protect your SharePoint resources with the SiteMinder Agent for SharePoint, create an application with the Administrative UI.

To create an application to protect your SharePoint resources

1. Click Policies, Applications, Application, Create Application.

   The Create Application: screen appears.

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

3. Verify that Web Agent appears in the Agent Type drop-down list.

4. Click the ellipsis button next to the Agent field.

   The Select Agent or Agent Group pane appears.

5. Click the button next to the Web Agent Group you created for the SharePoint resources you want to protect, and then click OK.

   Important! Do not add the URL or FQDN for your SharePoint Central Administration web site to any SiteMinder Agent groups, applications, or policies that protect resources. Leave the SharePoint Central Administration web site unprotected (by SiteMinder).

   The Create Application: *Name* pane reappears showing the name of your Web Agent object.

6. Click the Authentication Scheme drop-down list and select the authentication scheme you created for your SharePoint resources.

7. In the User Directories Group, click Add/Remove.

   The Choose User Directories dialog appears.

8. In the Available Members list, click the name of your SharePoint directory, and then click the right arrow.

   Your SharePoint user directory object appears in the Selected Members list.

9. Click OK.

   The Create Application: *Name* pane reappears showing the name of your Directory object.

10. Click Submit.

    The Create Application task is submitted for processing. A confirmation screen appears.

11. Click OK.

Add your SharePoint Resources to your Application (r12.0 SP2)

Define the SharePoint resources in your environment in a SiteMinder Policy before protecting them.

To add SharePoint resources to your application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add Resources to the application by doing the following:
   a. Click the Resource tab, and then click Create.

      The Create Application Resource: pane appears.

   b. Enter a distinctive name for the resource.

   c. Verify that the effective resource field contains the following:

      /*

   d. Under the Action group box, make sure that the Web Agent Actions radio button is selected, and then Control-click the following actions:

      - Get
      - Post
      - Put
      - Options
      - Head

      Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

   e. Click OK.

      The Create Application Resource: pane closes, and the Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation screen appears.
4. Click OK.

   The SharePoint resources are added to your SiteMinder Application.

Add a Role to your SiteMinder Application (r12.0 SP2)

To protect your SharePoint resources with SiteMinder, the SiteMinder application you create requires a role associated with the groups of users who are allowed to access those protected SharePoint resources.

To add a role to your SiteMinder application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add a Role to your Application by doing the following:
   a. Click the Roles Tab, and then click Create.

      The Create Role tab appears.

   b. Make sure the Create a new object of type Role radio button is selected, and then click OK.

      The Create Role: pane appears.

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

   d. Click the Expression field, and then type the following:

      ```
      (TRUE)
      ```

   e. Click OK.

      The Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation window appears.
4. Click OK.

   The role is added to your SiteMinder application.

Create a Policy for your SiteMinder Application (r12.0 SP2)

Your SiteMinder application requires a policy which grants the access rights with the associated SharePoint resources and the user role.

To create a policy for your application

1. Open the Application you created to protect your SharePoint resources by doing the following:

   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.

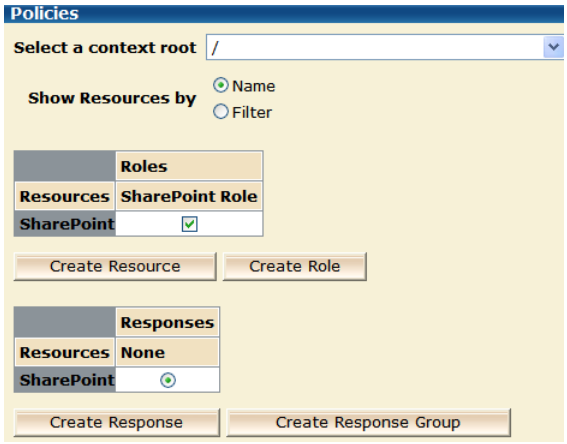
2. Click the Policies tab.

   The Policies screen appears.

3. Verify the following:

   - The Select a context root drop-down list shows the root level (/).
   - The Show Resources by Name option button is selected.

4. Locate the table that shows your SharePoint resources and roles, and then select the check box to grant access to the resources, as shown in the following illustration:



   Note: The drop-down list mentioned previously only appears when you have multiple resource items defined in the Administrative UI

5. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation pane appears.

6. Click OK.

   The policy for your SiteMinder application is created.

Add the Impersonation Response to your Existing SiteMinder Application (r12.0 SP2)

To impersonate users, your SiteMinder applications require a response for impersonation.

To add the impersonation settings to your existing SiteMinder application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Click the Responses tab.

   The Responses screen appears.
3. Click Create Response.

   The Create Application Response screen appears.
4. Click the Name field, and enter a distinctive name.
5. Click Create Response Attribute.

   The Attribute Type screen appears.
6. Define the attribute type by doing the following tasks:
   a. Click the Attribute drop-down list and select the following:

      `WebAgent-HTTP-Header-Variable`

   b. Click the User Attribute option button.

   c. Click the Variable Name field and enter the name for the the response variable. Record the name for future reference when you configure the Web Agent.

      Important! Use the same name for the response variable in both the SiteMinder response and for the value of the SPImpersonateResponseVarName parameter in the Agent Configuration Object.

   d. Click the Attribute Name field and enter the following Active Directory attribute:

      `userprincipalname`

   e. Click OK.

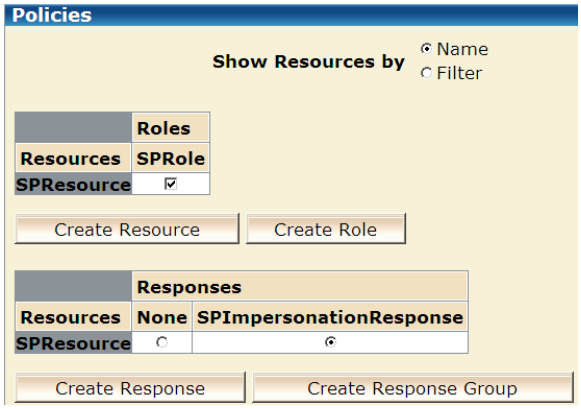
      The Attribute Type screen closes and the Create Application Response screen appears.
7. Click OK.

   The Responses tab appears.

8. Click the Policies tab.

   The Policies screen appears.

9. Locate the name of the response you created in Step 4, and then click its option button, as shown in the following illustration:



10. Click Submit.

    The Modify Application task is submitted for processing, and then a confirmation pane appears.

11. Click OK.

    The impersonation response is added to your SiteMinder application.

How to configure your SiteMinder Agent for SharePoint (r12.0 SP2)

The SiteMinder Agent for SharePoint operates together with a SiteMinder Web Agent. The SiteMinder Web Agent contains the configuration parameters and intercepts HTTP traffic to the web server; while the SiteMinder Agent for SharePoint provides a SiteMinder Management UI that helps you configure the protection for your SharePoint resources.

The SiteMinder Web Agent authenticates your SharePoint resources using any of the following methods:

- The Windows Impersonation authentication method used by the SiteMinder Agent for SharePoint, provides full functionality for the supported versions of Microsoft SharePoint. The SiteMinder Agent for SharePoint uses the value of the UserPrincipalName attribute (obtained from an Active Directory server) to authenticate users to SiteMinder.
- Forms based authentication (FBA) works with Microsoft directory servers, or LDAP directory servers from several vendors. See the *SiteMinder Agent for SharePoint Release Notes* for more information about the limitations of the FBA method.

The SiteMinder Web Agent configuration settings are different for each method used. To configure the SiteMinder Web Agent, use the following process:

1. Create an Agent Configuration object for your SiteMinder Web Agent (a single Agent Configuration Object can contain settings for either authentication method).
2. Change the parameter settings in the previous Web Agent Configuration object to match the authentication methods you want to use with the following procedures:
    - Set the Web Agent parameters for Windows impersonation
    - Set the Web Agent parameters for forms based authentication

Create an Agent Configuration Object for your SharePoint Resources (r12.0 SP2)

The SiteMinder Agent for SharePoint uses its own type of Agent Configuration Object to protect the SharePoint resources. This SharePoint Agent Configuration Object contains the settings used by SiteMinder to manage your SharePoint protection. To properly protect and allow access to your SharePoint resources, this Agent Configuration object requires the following settings:

- The value of the DefaultAgentName parameter contains the name of the Agent Object associated with the *protected* SharePoint resources.
- The value of the AgentName parameter contains the name of the Agent Object associated with the *unprotected* SharePoint resources.

To create an Agent Configuration Object for your SharePoint resources

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

   The Create Agent Configuration: Agent Configuration Search Screen appears.

2. Click the following buttons:

   - Create a copy of an object of type Agent Configuration
   - SharePointDefaultSettings

   Note: If the SharePointDefaultSettings object is missing, upgrade your policy store.

3. Click OK.

   The Create Agent Configuration: dialog appears.

4. Enter a distinctive name and an optional description.

5. Add the Agent object name for your SharePoint Central Administration site by doing the following:

   a. Click the Edit button next to the following parameter:

      `#AgentName`

      The Edit Parameter dialog appears.

   b. Enable the parameter by removing the # character.

   c. Click the Value field, and then enter the following:

      `sharepoint_unprotected_agent_name``,`*`host_name.domain_name.domain_extension`*`:`*`web_site_port_number`*

      For example, if your SharePoint Central Administration site has a Web Agent named, sp_un, running on myhost.example.com using port 99999, enter sp_un,myhost.example.com:99999.

   d. Click Add.

      The Agent appears in the list.

   e. Click OK.

The Edit parameter dialog closes, and then the Modify Agent Configuration: dialog appears.

f. Click the Edit button next to the following parameter:

```
#DefaultAgentName
```

The Edit Parameter dialog appears.

g. Enable the parameter by removing the # character.

h. Click the Value field and enter the name of the Agent Object that you created for the resources you want to protect.

i. Click OK.

The Edit parameter dialog closes, and then the Modify Agent Configuration: dialog appears.

j. Click OK.

The Edit parameter dialog closes, and then the Modify Agent Configuration: dialog appears.

6. Click Submit.

The changes to the Agent Configuration Object are saved and the confirmation screen appears.

7. Click Submit.

The changes to the Agent Configuration Object are saved and the confirmation screen appears.

8. Click OK.

The Agent Configuration object is created.

More information:

Upgrade your Policy Store (see page 19)

Set the Web Agent Parameters for Impersonation (r12.0 SP2)

The SiteMinder Web Agent requires the following parameters to control Windows Impersonation:

SPEnableImpersonation

Lists the URLs of the SharePoint web applications for which Windows impersonation is used.

Example: *server_name.domain_name:port_number*

Default: None (Windows Impersonation *not* used).

SPImpersonateResponseVarName

Specifies the name of a Response variable created in SiteMinder which is mapped to a UserPrincipalName attribute of the user in an Active directory server and assigned as a response to the SiteMinder policy.

Default: None

To set the Web Agent parameters for impersonation

1. Click Infrastructure, Agent Configuration, Modify Agent Configuration.

   A list of Agent Configuration objects appears.

2. Click the configuration object for your SiteMinder Agent for SharePoint, and then click Select.

   The Modify Agent Configuration screen appears.

3. Click the edit button (to the left) of the following parameter:

   `#SPEnableImpersonation`

   The Edit Parameter screen appears.

4. Set the parameter using the following steps:

   a. Click the name field and then remove the # character.

   b. Click the value field, and then enter the URLs of the web applications for which you want to enable impersonation. You must include the port number (even if it is the default 80 or 443).

   c. Click OK.

      The Edit Parameter screen closes.

5. Click the edit button (to the left) of the following parameter:

   `#SPImpersonateResponseVarName`

   The Edit Parameter screen appears.

6. Set the parameter using the following steps:

   a. Click the name field and then remove the # character.

b. Click the value field, and then type the name you want to use for a response variable.

Important! Use the same name for the response variable in both the SiteMinder response and for the value of the SPImpersonateResponseVarName parameter in the Agent Configuration Object.

c. Click OK.

The Edit Parameter screen closes.

7. Click Submit.

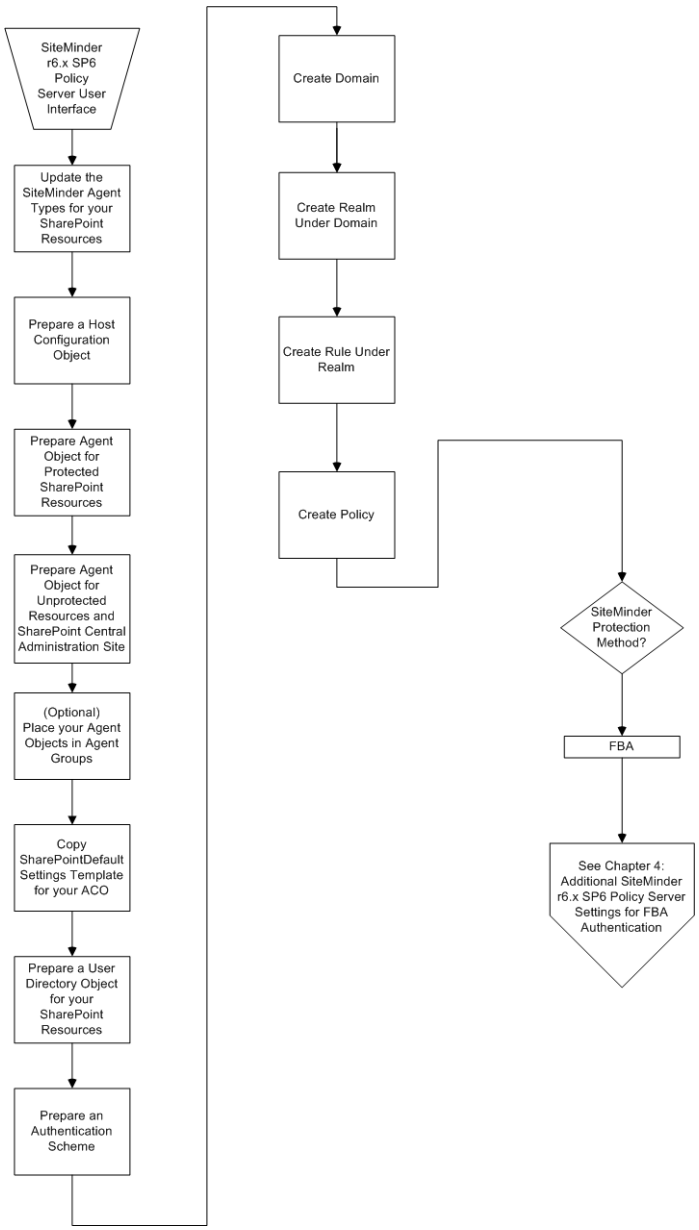
The Modify Agent Configuration screen closes and a confirmation screen appears.

8. Click OK.

The Web Agent parameters are set.

Protecting SharePoint Resources with SiteMinder (r6.x SP6) Roadmap

Protecting resources on your SharePoint system using SiteMinder r6.x SP6 requires several separate procedures. The entire protection process is described in the following illustration:



Create or Reuse a Host Configuration Object (r6.x SP6)

When a SiteMinder Web Agent starts, it uses use a Host Configuration object to make an initial connection to a SiteMinder Policy Server.

You need a Host Configuration object to operate the Agent for SharePoint. This section describes how to create a Host Configuration object, but if you are an experienced SiteMinder user, you can also reuse an existing Host Configuration object instead.

To create a host configuration object

1. Open the Policy Server User Interface.
2. In the System tab, select Host Conf Objects to display the Host Conf Object List in the right pane.
3. In the List pane, select the object you want to duplicate and right-click.
4. Select Duplicate Configuration Object.

   The Host Configuration Object Properties dialog opens.
5. In the Host Configuration Object Properties dialog, enter a distinctive Name and an optional description.

   Note: This name cannot be the same as the name of an existing Agent object.
6. In the Configuration Values list, verify that the value of the PolicyServer parameter is the IP Address or fully qualified domain name of the computer which hosts the Policy Server. If not, do the following:
   a. Click the PolicyServer entry and click Edit.

      The Edit Parameter dialog opens.
   b. If applicable, remove the pound sign (#) prefix in the Parameter Name field to make the parameter active.
   c. In the Value field, enter the IP address or fully qualified domain name of the computer which hosts the Policy Server (replacing the existing value or "<IP Address>" placeholder variable).
7. Click OK to save the new object.

   The Host Configuration Object is created.

Create an Agent Object for each SharePoint Resource (r6.x SP6)

The SharePoint resources in your organization need at least two different Agent objects defined in the SiteMinder Policy Server User Interface:

- One Agent object for the SharePoint resources you want to protect.
- One Agent object for the SharePoint resources that need to remain unprotected, such as the SharePoint Central Administration web site.

To create Agent objects for your SharePoint resources

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select Edit, System Configuration, Create Agent.

   The SiteMinder Agent dialog opens.
3. Click the Name field and enter a distinctive name for the Agent.This value is case-insensitive, and must be 7-bit ASCII characters in the range 32-127.
4. We recommend using a name that you can easily associate with the corresponding SharePoint resources. For example, an Agent object associated with the protected SharePoint resources could be named "SP_Protected", and an Agent Object associated with the unprotected SharePoint resources, could be named, "SP_Unprotected."
5. (Optional) Click the Description field, and enter a description.
6. Verify that the Support 4.x agents check box is unchecked.
7. In the Agent Type group box, verify that the following options are set correctly:
   - SiteMinder option button is selected.
   - Web Agent is selected in the drop-down list.
8. Click OK.

   The Agent object is created.
9. Repeat Steps 2 through 8 to create the second Agent object.

Place your Agent Objects in Agent Groups (r6.x SP6)

If you have many Agent objects, we recommend using Agent Groups because several Agent objects can be added or removed from a policy at the same time. For example, you can create one Agent group for your protected resources and another for your unprotected resources.

To place your Agent Objects in an Agent Group

1. Log into the Policy Server User Interface.
2. From the menu bar of the SiteMinder Administration window, select View, Agent Groups.

   The Policy Server places a checkmark in the View menu to the left of the menu selection and Agent Groups appear in the System tab of the SiteMinder Administration window.

   Note: If there is already a check next to Agent Groups in the View menu, selecting the option again removes Agent Groups from the System tab.
3. From the menu bar of the SiteMinder Administration window, select Edit, System Configuration, Create Agent Group.
4. The Agent Group Properties dialog opens.
5. Click the Name field and enter a distinctive name for the Agent group.
6. Click Add/Remove.

   The Agent Group Items dialog opens.
7. Select the name of an Agent you want to add to the Agent group from the Available Members list.
8. Click the Left Arrow button to move the selected Agent to the Current Members list.
9. Repeat steps 7 and 8 for all Agents you want to add to the Agent group.

   If the list of Agents is long and the Agent you want to add to the Agent group is not displayed in the Available Members list, you can look for Agents using the search feature. The search feature is similar to the one that is available in the SiteMinder Administration window.

Important! Do not add the URL or FQDN for your SharePoint Central Administration web site to any SiteMinder Agent groups, applications, or policies that protect resources. Leave the SharePoint Central Administration web site unprotected (by SiteMinder).

10. Click OK to save the member additions.

    The Group Members group box in the SiteMinder Agent Group dialog displays the Agents you selected for the Agent group.

11. Click OK in the SiteMinder Agent Group dialog to save the Agent group and return to the SiteMinder Administration window.

12. Repeat Steps 3 through 11 to create additional Agent groups as needed.

Modify a User Directory Connection for your SharePoint Directories in the SiteMinder Policy Server (r6.x SP6)

The SiteMinder Policy Server communicates with your existing user directories to authenticate users. Each user directory needs a connection in the SiteMinder Policy Server User Interface. This section describes how to modify an existing user directory connection for use with the Agent for SharePoint, but you can also create one if you want. For more information about creating a user directory connection, see the *Policy Design Guide*.

To create entries for your SharePoint user directories in the SiteMinder Policy Server

1. From the menu bar of the SiteMinder Administration window, select Edit, System Configuration, Modify User Directory.

   The SiteMinder User Directory Dialog opens.

2. Click the Credentials and Connections tab, and then verify the following settings:

   a. Select the Require Credentials check box and then complete the following fields:

   - Username
   - Password
   - Confirm Password

   Note: Consult the administrator of your directory server for more information about the proper settings to use in your environment.

3. Verify that the following check box is *clear*:

   - Run in Authenticated User's Security Context

4. Click OK

   The User Directory is modified.

Edit the User Attribute Mapping File to Configure Virtual Attribute Mappings to your SharePoint User Directories (r6.x SP6)

SiteMinder uses virtual attribute mappings for the FBA authentication method to preserve some SharePoint features that are lost when the Agent for SharePoint performs authorization and authentication (instead of the SharePoint environment). For example, the DisplayName attribute mapping allows SiteMinder to add the first and last names of the user to the upper right corner of the browser window. If the DisplayName mapping is not set, SiteMinder uses the login ID of the user instead. Use these mappings for each directory in your SharePoint environment.

Use the following file to configure virtual attribute mappings for r6.x SP6:

policy_server_home\config\UserAttrMapping.txt

policy_server_home

Specifies the installation directory where your SiteMinder Policy Server is installed. The *%NETE_PS_ROOT%* environment variable points to this directory.

Default: (Windows) C:\Program Files\CA

To configure virtual attribute mappings (r6.x SP6)

1. Open the UserAttrMapping.txt file with a text editor.
2. Locate the section containing the mappings that apply to the type of directory server you are using for your SiteMinder user store. The following example shows the mappings for a Sun Java System server:

```
UserDirName=ldap-sunone
GroupID=cn
Email=mail
UniversalID=uid
DisplayName=cn
```

3. Replace the ldap-sunone in the first line of the previous example with the name of the user directory connection defined in the Policy Server User Interface. For example, if your user directory connection is named, SP_UserD, then change the line to match the following:

```
UserDirName=SP_UserD
```

4. Locate the following the attribute names, and then change their values (on the right of the equals signs) to match the physical attributes in your user directory:

UniversalID

Specifies the directory attribute that contains the user name from a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Examples: (Sun Java System) UniversalID=uid *or* UniversalID=cn

Examples: (Microsoft Active Directory) UniversalID=cn *or* UniversalID=sAMAccountName

Example: (DB2) UniversalID=Name

Note: If you are using a SharePoint server (MOSS), and you plan to Import User Profiles, record the value of the UniversalID mapping for future reference.

Email

Specifies the directory attribute that contains the email address of a user within a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Example: (Sun Java System) Email=mail

Example: (Microsoft Active Directory) Email=mail

Example: (DB2) Email=EmailAddress

GroupID

Specifies the directory attribute that contains the group or role to which a user belongs within a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint.

Example: (Sun Java System) GroupID=cn

Example: (Microsoft Active Directory) GroupID=cn

Example: (DB2) GroupID=Name

DisplayName

Specifies the directory attribute that contains the user name you want to display from a SiteMinder directory that contains your SharePoint users to the SiteMinder Agent for SharePoint. The value of this virtual attribute appears in the upper right corner of the browser window after SiteMinder authenticates the user to SharePoint.

Example: (Sun Java System) DisplayName=cn

Example: (Microsoft Active Directory) DisplayName=displayName

Example: (DB2) DisplayName=Name

5. Repeat steps 2 though 4 for any other SiteMinder user stores associated with your Policy Server that you want to use with your Agent for SharePoint environment. Add more sections if necessary.
6. (Optional) Remove (or comment out) the other example sections in the file that you do not apply to your environment. If you are *not* using a DB2 user store, for example, you can remove the following section:

   ```
   # mappings for "DB2-userstore"
   ```

7. Save the UserAttrMapping.txt file and close the text editor.

   The virtual attribute mappings are configured.

More information:

Update the Agent Configuration Parameters for your Agent for SharePoint (see page 99)

Create a Custom Mapping to Filter Items Containing a Particular Object Class Attribute from your Search Results (r6.x)

If you are using the Active Directory or LDAP namespaces in your SiteMinder connection to your user directory, you can define a virtual attribute mapping to a specific object class attribute in that directory. These mappings can help narrow your searches. For example, if your directory schema contains an object class attribute named "computer," you can create a virtual attribute to exclude items containing the "computer" attribute from your search results in the people picker.

To create a custom mapping to filter items containing a particular Object Class attribute from your search results

1. Open the following file with a text editor:

   `policy_server_home\config\UserAttrMapping.txt`

   policy_server_home

   Specifies the installation directory where your SiteMinder Policy Server is installed. The *%NETE_PS_ROOT%* environment variable points to this directory.

   Default: (Windows) C:\Program Files\CA

2. Locate the section that contains the name of your directory connection and any of the attribute mappings you added previously. The following example shows the default settings for a Sun Java System server:

   ```
   UserDirName=ldap-sunone
   GroupID=cn
   Email=mail
   UniversalID=uid
   DisplayName=cn
   ```

3. Add the following line to the bottom of the section that applies to your directory connection:

   `FilterClass=object_class_attribute_name`

   For example, if the name of your object class attribute is "computer," add the following:

   `FilterClass=computer`

4. Save the UserAttrMapping.txt file and close the text editor.

   The virtual attribute mappings are configured.

Create or Reuse an Authentication Scheme for your SiteMinder Agent for SharePoint (r6.x SP6)

The SiteMinder Agent for SharePoint supports the Authentication Schemes used by CA Technologies SiteMinder. The SiteMinder Agent for SharePoint needs an Authentication Scheme defined in the Policy Server User Interface. This section describes how to create an authentication scheme, but if you are an experienced SiteMinder user, you can reuse an existing authentication scheme instead.

To create an authentication scheme for your SiteMinder Agent for SharePoint

1. From the menu bar of the SiteMinder Administration window, select Edit, System Configuration, Create Authentication Scheme.

   The SiteMinder Authentication Scheme Dialog opens.

2. Enter a distinctive name, and (optional) description.
3. Click the Authentication Scheme Type drop-down list, and then select the type of Authentication Scheme that you want.

   The options for your chosen Authentication Scheme appear.

4. Complete the fields for your Authentication Scheme.

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

5. Click OK.

   The Authentication Scheme is created.

Create a Domain for your SharePoint Resources (r6.x SP6)

Define a Domain in the Policy Server User Interface that contains the SharePoint resources that you want to protect with the SiteMinder Agent for SharePoint.

To create a domain for your SharePoint resources

1. Click the Domains tab.
2. Right-click the top-level Domains item, and then select, Create Domain.

   The SiteMinder domain dialog appears.

3. Enter a distinctive name, and (optional) description.
4. Click the drop-down list and locate the directory connection you want. Click Add.

   The directory appears under the User Directories tab.

5. Click OK.

   The SiteMinder domain dialog closes and the domain is created.

Create a Realm for your SharePoint Resources (r6.x SP6)

Create a realm under your SharePoint domain for the resources that you want to protect with the SiteMinder Agent for SharePoint.

To create a realm for your SharePoint resources

1. Click the Domains tab.

   The domain you created for your SharePoint resources appears.

2. Expand the domain.

   The following icons appear:

   - Realms
   - Responses
   - Policies

3. Right-click Realms, and then select Create realm.

   The SiteMinder realm dialog appears.

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

5. In the Resource tab, do the following:

   - Click Lookup and then add Agent Group you created for your protected SharePoint resources to the realm.
   - Click the drop-down list and then select the authentication scheme you created.

6. Click OK.

   The SiteMinder realm dialog closes and the realm is created.

Create a Rule under your Realm (r6.x SP6)

Your top-level SharePoint realm needs a rule which fires when a user requests access to a protected SharePoint resource.

To create a rule under your SharePoint realm

1. Click the Domains tab, and then expand your SharePoint domain.
2. Right-click your SharePoint realm, and then select Create Rule Under Realm.

   The Rule Properties dialog appears.
3. Enter a distinctive name, and (optional) description.
4. In the Action field, Control-click the following:
   - Get
   - Post
   - Put
   - Head
   - Options

     Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

   The web agent actions are selected.
5. Verify the following settings:
   - The Resource field contains an asterisk (*).
   - The Allow Access option button is selected.
   - The Enabled check box is selected.
6. Click OK.

   The Rule Properties Dialog closes and the new rule appears in the list.

Create a Policy under your Realm (r6.x SP6)

You need a SiteMinder policy associated with your SharePoint domain that defines relationships between the users, the SharePoint resources, and access rights in your organization.

To create a policy for your SharePoint resources

1. Click the Domains tab, and then expand your SharePoint domain.

   A list of objects appears.

2. Right-click Policies, and select Create Policy.

   The Policy Properties dialog appears showing the Users tab.

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

4. Click Add/Remove.

   The Users/Groups dialog appears.

5. Move the groups, users (or any combination of either) that you want to add from the Available Members list to the Current Members list, and then click OK.

   The users or groups are added to the policy.

6. Click the Rules tab, and then click Add/Remove Rules.

   The Available Rules dialog appears.

7. Move your SharePoint rule from the Available Members list to the Current Members list, and then click OK.

   The rule is added to the policy.

8. Click OK.

   The Policy Properties dialog closes and the policy is saved.

Create a SiteMinder Response for Windows Impersonation (r6.x SP6)

The Windows Impersonation authentication method used by the SiteMinder Agent for SharePoint requires a SiteMinder response, which you configure in the Policy Server User Interface.

Create a SiteMinder response for Windows impersonation

1. Click the Domains tab.

   The domain you created for your SharePoint resources appears.

2. Expand the domain.

   The following icons appear:

   - Realms
   - Responses
   - Policies

3. Right-click Responses, and then select Create Response.

   The SiteMinder response dialog appears.

4. Enter a distinctive name, and (optional) description.
5. Verify that SiteMinder Web Agent appears in the Agent Type drop-down list.
6. Click Create.

   The Response Attribute dialog appears.

7. Create the response by doing the following:

   a. Verify that the following appears in the Attribute drop-down list:

      `WebAgent-HTTP-Header-Variable`

   b. Click the User Attribute option button.

   c. Click the Variable Name field and enter the name for the response variable. Record the name for future reference when you configure the Web Agent.

      Important! Use the same name for the response variable in both the SiteMinder response and for the value of the SPImpersonateResponseVarName parameter in the Agent Configuration Object.

   d. Click the Attribute Name field and enter the following Active Directory attribute:

      `userprincipalname`

   e. Click OK.

      The Response Attribute dialog closes.

8. Click OK.

   The SiteMinder response dialog closes.

9. Add the response to your policy by doing the following:
   a. In the Policy list, right-click your SharePoint Policy, and then select Properties of Policy.

      The SiteMinder Policy dialog appears.

   b. Click the Rules tab, and then click the rule for your SharePoint policy.

   c. Click Set Response.

      The Set Response dialog appears with a list of available responses.

   d. Click the response you created, and then click OK.

      The Set Response dialog closes. The Rule in the list now shows the response.

10. Click OK.

    The SiteMinder Policy Dialog closes and the response for Windows Impersonation is created.

How to Configure your SiteMinder Agent for SharePoint (r6.x SP6)

The SiteMinder Agent for SharePoint operates together with a SiteMinder Web Agent. The SiteMinder Web Agent contains the configuration parameters and intercepts HTTP traffic to the web server; while the SiteMinder Agent for SharePoint provides a SiteMinder Management UI that helps you configure the protection for your SharePoint resources.

The SiteMinder Web Agent authenticates your SharePoint resources using any of the following methods:

- The Windows Impersonation authentication method used by the SiteMinder Agent for SharePoint, provides full functionality for the supported versions of Microsoft SharePoint. The SiteMinder Agent for SharePoint uses the value of the UserPrincipalName attribute (obtained from an Active Directory server) to authenticate users to SiteMinder.
- Forms based authentication (FBA) works with Microsoft directory servers, or LDAP directory servers from several vendors. See the *SiteMinder Agent for SharePoint Release Notes* for more information about the limitations of the FBA method.

The SiteMinder Web Agent configuration settings are different for each method used. To configure the SiteMinder Web Agent, use the following process:

1. Create an Agent Configuration object for your SiteMinder Web Agent (a single Agent Configuration Object can contain settings for either authentication method).
2. Change the parameter settings in the previous Web Agent Configuration object to match the authentication methods you want to use with the following procedures:
    - Set the Web Agent parameters for Windows impersonation
    - Set the Web Agent parameters for forms based authentication

Create an Agent Configuration Object for your SharePoint Resources (r6.x SP6)

The SiteMinder Agent for SharePoint uses its own type of Agent Configuration Object to protect the SharePoint resources. This SharePoint Agent Configuration Object contains the settings used by SiteMinder to manage your SharePoint protection. To properly protect and allow access to your SharePoint resources, this Agent Configuration object requires the following settings:

- The value of the DefaultAgentName parameter contains the name of the Agent Object associated with the *protected* SharePoint resources.
- The value of the AgentName parameter contains the name of the Agent Object associated with the *unprotected* SharePoint resources.

To create an Agent Configuration Object for your SharePoint resources

1. Click the System tab, and then click Agent Conf Objects.

   A list of Agent Configuation Objects appears.

2. Right-click SharePointDefaultSettings, and then select Duplicate Configuration Object.

   Note: If the SharePointDefaultSettings object is missing, upgrade your policy store.

   The SiteMinder Agent Configuration dialog appears.

3. Enter a distinctive name, and an optional description.
4. Add the information for your Central Configuration web site by doing the following:
   a. In the parameter name list, click the following parameter:

      `#AgentName`

   b. Click Edit.

      The Edit Parameter dialog appears.

   c. Enable the parameter by removing the # character.

   d. Click the Value field, and then enter the following:

      `sharepoint_unprotected_agent_name,host_name.domain_name.domain_extension:web_site_port_number`

      For example, if your SharePoint Central Administration site has a Web Agent named, sp_un, running on myhost.example.com using port 99999, enter sp_un,myhost.example.com:99999.

   e. Click OK.

      The Edit Parameter dialog closes.

5. Add the name of the Agent Object associated with your protected SharePoint resources by doing the following:
   a. Scroll down the parameter list, and then click the following parameter:

      `#DefaultAgentName`

b. Click Edit.

   The Edit Parameter dialog appears.

c. Enable the parameter by removing the # character.

d. Click the Value field and enter the name of the Agent Object that you created for the resources you want to protect

e. Click OK.

   The Edit Parameter dialog closes.

f. Click OK.

   The SiteMinder Agent Configuration dialog closes and new Agent Configuration Object is created.

More information:

Upgrade your Policy Store (see page 19)

Set the Web Agent Parameters for Windows Impersonation (r6.x SP6)

The SiteMinder Web Agent requires the following parameters to control Windows Impersonation:

SPEnableImpersonation

Lists the URLs of the SharePoint web applications for which Windows impersonation is used.

Example: *server_name.domain_name:port_number*

Default: None (Windows Impersonation *not* used).

SPImpersonateResponseVarName

Specifies the name of a Response variable created in SiteMinder which is mapped to a UserPrincipalName attribute of the user in an Active directory server and assigned as a response to the SiteMinder policy.

Default: None

To set the Web Agent parameters for Windows impersonation

1. Open the Policy Server User Interface
2. From the System tab, select Agent Conf Objects to display the Agent Conf Object List in the right pane.

3. From the List pane, right-click the Agent Configuration Object for your SiteMinder Agent for SharePoint.
4. Select Properties of Configuration Object.

   The Agent Configuration Object Properties dialog opens.
5. Highlight the following parameter and click Edit:

   `#SPEnableImpersonation`

   The Edit Parameter Dialog opens.
6. Set the parameter using the following steps:
   a. Click the Multi-value option button.
   b. Click the Parameter Name field and then remove the # character.
   c. Click the Enter Single value field, and then enter the information for a resource you want to protect with Windows Impersonation, as shown in the following example:

      server_name.domain_name:port_number
   d. Click Add.

      The resource appears in the Multiline display list.
   e. Repeat Steps 6c and 6d for each resource you want to protect with Windows Impersonation.
   f. Click OK.

   The Edit Parameter Dialog closes and you return to the Agent Configuration Object Properties dialog.
7. Highlight the following parameter and click Edit:

   `#SPImpersonateResponseVarName`

   The Edit Parameter Dialog opens.
8. Set the parameter using the following steps:
   a. Click the Parameter Name field and then remove the # character.
   b. Click the Value field, and then type the name you want to use for a response variable.

      Important! Use the same name for the response variable in both the SiteMinder response and for the value of the SPImpersonateResponseVarName parameter in the Agent Configuration Object.
   c. Click OK.

   The Edit Parameter Dialog closes and you return to the Agent Configuration Object Properties dialog.
9. Click OK to exit the Agent Configuration Object Properties dialog.

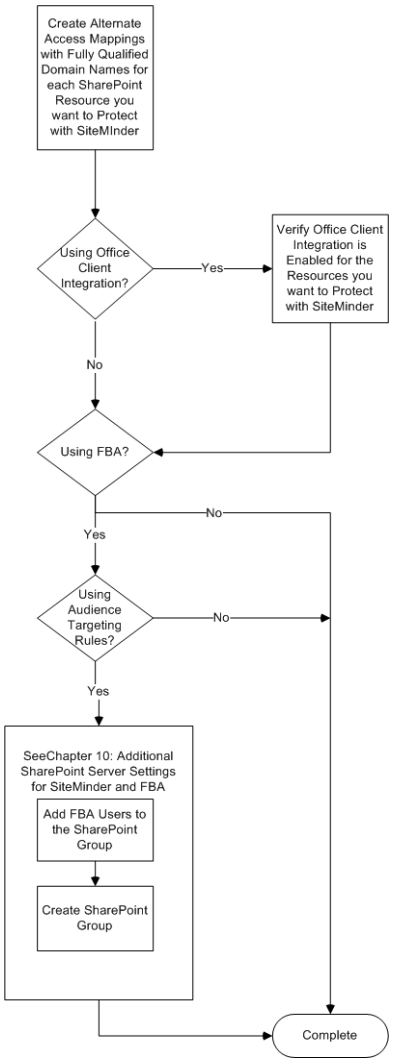
   The Web Agent parameters are set.

Chapter 4: Preparing your Web Server

This section contains the following topics:

Preparing your SharePoint Server Roadmap

Preparing your SharePoint server for the SiteMinder Agent for SharePoint equires several separate procedures. The entire preparation process is described in the following illustration:



Use Fully-Qualified Domain Names for All your SharePoint Sites

All the SharePoint sites that you want to protect with CA Technologies SiteMinder require fully qualified domain names.

To set your SharePoint sites to use a fully qualified domain names

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The Central Administration page appears.

2. Click the Operations tab.

   A list of tasks appears.

3. In the Global Configuration section, click Alternate Access Mappings.

   A list of web sites appears.

4. Locate your SharePoint site. Examine the URL listed in the Public URL for Zone column on the right and verify that it uses a fully qualified domain name.

   Note: *my_web_site*.example.com is an example of a fully qualified domain name.

5. If the URL in Step 3 does *not* use a fully qualified domain name, do the following:

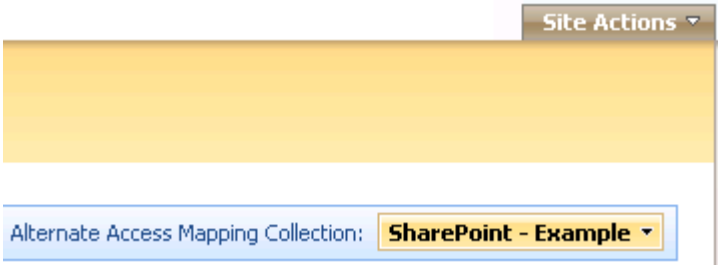
   a. Click the Alternate Access Mapping Collection drop-down list, and then select Change Alternate Access Mapping Collection.

      A list of Alternate Access Mapping Collections appears.

   b. Click the link for your SharePoint site.

      The Alternate Access Mappings screen shows only those sites in your collection.

   c. Verify the name of the SharePoint site you want to protect appears in the drop-down list, as shown in the following example:



d. Click Edit Public URLs.

   The Edit Public Zone URLs screen appears.

e. Edit the URLs to include a fully qualified domain name.

f. Click Save.

The URL shown in the Public URL for Zone column appears with a fully qualified domain name.

6. Repeat Steps 2 thorough 5 for each SharePoint web site you want to protect with SiteMinder.

Verify your Office Client Integration Settings

The SiteMinder Agent for SharePoint supports the Office Client Integration feature of Microsoft SharePoint. Unless your SharePoint server is behind a reverse proxy server, the Agent for SharePoint automatically determines whether or not Office Client Integration is allowed according to the setting in the SharePoint Central Administration UI. For reverse proxy servers, you must add the web applications you want to protect to the Agent Configuration object manually.

When Office Client Integration is allowed, the Agent for SharePoint places a persistent cookie, named SPSESSION on the hard disk of the user. This cookie allows users to access Office documents on the SharePoint server without challenging them for their credentials again (until the SiteMinder session associated with the SPSESSION cookie expires).

Note: If the security policy of your organization prohibits persistent cookies, you can still use Office Client Integration with the SiteMinder Agent for SharePoint in some limited situations.

To verify your office client integration settings

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The Central Administration screen appears.

2. Click Application Management.

   The Application Management screen appears.

3. Click Authentication Provider.

   The Authentication Providers screen appears.

4. Verify that the URL of the web application for which you want to enable Office Client Integration appears in the Web Application: drop-down list (upper-right corner).

5. Under the zone column, click the name of the zone associated with the web application you want.

   The Edit Authentication screen appears.

6. In the Client Integration section, verify that the Yes option button is selected, as shown in the following illustration:

7. Do *one* of the following tasks:
   - If the Enable Client Integration was *already* set to yes, then click Cancel.
   - If you *changed* the Enable Client Integration setting from no to yes, then click Save.
8. Repeat Steps 4 through 7 for all other web applications for which you want to allow Office Client Integration.

More information:

Office Client Integration without a Persistent Cookie (see page 204)
Enable Office Client Integration for a Reverse Proxy (see page 107)

Create SharePoint Groups to Add FBA Users to Audience Targeting Rules

Users who authenticate using FBA cannot be added to audience targeting rules in SharePoint. As a workaround, you can create a SharePoint group that contains those FBA users and then add the group to any audience targeting rules.

Create SharePoint groups to add FBA users to audience targeting rules

1. Open the SharePoint Central Administration UI.

   The Central Administration screen appears.
2. Click Site Actions (in the upper right corner), and then click Site Settings.

   The Site Settings screen appears.
3. Click People and Groups.

   The People and Groups screen appears.
4. Click New, New Group.

   The New Group screen appears.
5. Complete the form to create a group with the settings you want, and then click Create.

   The People and Groups: *your_group_name* screen appears.
6. Click New, Add Users.

   The Add Users screen appears. The name of your group appears in the Give Permission section.
7. Use the Add Users section to add the FBA users you want.
8. Click OK.

   The People and Groups: *your_group_name* screen appears. The group is created.

How to Perform the Manual Configuration Steps for IIS 6.0

To perform the manual configuration steps for an IIS 6.0 web server, use the following process:

1. Change the port number of the default IIS web site.

Change the Port Number of the Default IIS 6.0 Web Site

We recommend changing the port number of the default IIS 6.0 web site.

To change the port number for the default IIS 6.0 web site

1. Open the IIS Manager.
2. Expand the web server, and then expand Web Sites.

   A list of web sites appears.
3. Right-click the default web site (at the top of the list), and select Properties.

   The Properties dialog appears.
4. Click the Web Site tab.
5. In the TCP port field, enter the number of an available port that you want to use, and then click OK.

   The Properties dialog closes and the changes are saved.
6. Start the default web site.
7. Verify the change by opening a browser window access a web page on the new port.

   The port number for the default IIS 6.0 web site is changed.

How to Perform the Manual Configuration Steps for an IIS 7.0 Web Server

To perform the manual configuration steps for an IIS 7.0 web server, use the following process:

1. Change the port number of the default IIS web site.
2. Change the Windows authentication settings for your SharePoint central administration site.

Change the Port Number of the Default IIS 7.0 Web Site

We recommend changing the port number of the default IIS 7.0 web site.

To change the port number for the default IIS 7.0 web site

1. Open the IIS Manager.
2. Expand the web server, and then expand the Sites folder.

   A list of web sites appears.
3. Click Bindings.

   The Site Bindings dialog appears.
4. Click the site on port 80, and then click Edit.

   The Edit Site Binding dialog appears.
5. In the Port field, enter the number of an available port that you want to use, and then click OK.

   The Edit Site Binding dialog closes.
6. Click Close.

   The Site Bindings dialog closes. The port number for the default IIS 7.0 web site is changed.
7. Click Start.

   The default IIS 7.0 web site starts on the new port.

Change the Windows Authentication Settings for your SharePoint Central Administration Site

When the SiteMinder Agent for SharePoint runs on an IIS 7.0 web server, change the Windows authentication settings to disable kernel mode authentication. The SiteMinder Agent requires this setting.

To change the Windows authentication settings for your SharePoint central administration site

1. Click Start, Programs, Administrative Tools, IIS Manager.

   The Internet Information Services (IIS) Manager opens.

2. Expand the web server.

   A list of sub folders appears.

3. Expand the Sites folder.

   A list of web site folders appears.

4. Click the folder for your Central Administration web site, and then, in the right pane, double-click the Authentication icon.

   A list of authentication methods appears.

5. Right-click Windows Authentication, and then select Advanced Settings.

   The Advanced Settings dialog appears.

6. Clear the Enable-Kernel mode authentication check box, and then click OK.

   The Advanced Settings dialog closes. The Windows authentication settings for your SharePoint Central Administration site have been changed.

How to Prepare Your Web Server for Windows Impersonation

To prepare your web server to use Windows impersonation with the SiteMinder Agent for SharePoint, use the following process:

1. Verify the user account for the related application pool has the sufficient privileges.

Verify that the User Account for the Related Application Pool has Sufficient Privileges

The account that runs the application pool associated with the SharePoint resource you want to access as an impersonated user requires certain privileges on the related web server.

To verify that the user account has sufficient privileges

1. Click Start, Programs, Administrative Tools, Local Security Policy.

   Note: The exact menu names differ according to the role of your computer. For example, Domain Controllers possibly have different menus.

   The Local Security Settings dialog appears.

2. Under Security Settings, expand Local Policies, and then expand User Rights Assignment.

   A list of policies appears.

3. Locate the Act as part of the operating system policy, and then verify that the account that runs the application pool appears in the Security setting column. If the account does *not* appear, do the following steps:

   a. Double-click Act as part of the operating system.

      A dialog appears.

   b. Click Add User or Group.

      The Select Users, Computers or Groups dialog appears.

   c. Add the name of the account you want, and then click OK. For example, if your application pool runs on the Network Service account, then assign the privileges to the Network Service account.

   d. Click OK twice.

      Both dialogs close. The account appears in the Security Setting column for the policy.

Chapter 5: Configuring the Web Agent and the Agent for SharePoint

This section contains the following topics:

How to Configure your SiteMinder Web Agent

The SiteMinder Agent for SharePoint requires a SiteMinder Web Agent on the same web server. To configure your SiteMinder Web Agent, use the following process:

1. Gather the configuration information for your SiteMinder Web Agent (see page 75).
2. Run the Web Agent configuration wizard (see page 77).

Gather Web Agent Configuration Information

To configure a SiteMinder Web Agent, you need to collect information about the following items on your SiteMinder Policy Server:

Admin User Name

Specifies the name of an administrator who is allowed to register the host with the Policy Server. Before a trusted host can be registered, this administrator must be defined in the Policy Server, and have permission to register trusted hosts.

Default: siteminder

Admin Password

Specifies the password for the administrator who can register trusted Hosts with the Policy Server.

Enable Shared Secret Rollover

Specifies if the shared secret that encrypts the communication between the trusted host and the Policy Server will be changed periodically.

The Key Rollover feature must already be enabled at the Policy Server. To change this setting at a later time, you must do the following:

- Re-register the trusted host with the Policy Server
- Use the Policy Management API to change the setting.

Trusted Host Name

Specifies any unique name that represents your trusted host on the Policy Server. This name does *not* have to match the name of physical system you are registering.

Example: mytrustedhost

Limits: Must differ from any other existing trusted host name or existing Web Agent name.

Host Configuration Object

Specifies the name of an object that contains connection settings used between the trusted host and the Policy Server. This object must be defined in the Policy Server before you can configure a Web Agent.

Default: DefaultHostSettings

Policy Server IP Address

Specifies the host name or IP address of the Policy Server with which you are registering your trusted host. Specify a port number only if you want to use a *non-default* port.

Example: 192.168.1.100:*non_default_port_number*

Agent Configuration Object

Specifies the name of an Agent Configuration object on the Policy Server that contains the parameter settings that you want your Agent for SharePoint to use. Copy the SharePointDefaultSettings template to create an Agent Configuration Object for your Agent for SharePoint. This template contains specific configuration parameters to manage your SharePoint resources.

Default: AgentObj

Example: SharePointDefaultSettings

Run the Web Agent Configuration Wizard

Run the SiteMinder Web Agent configuration wizard to establish a connection from your IIS web server to the SiteMinder Policy Server. Use the information on the Web Agent Configuration worksheet to complete the items in the wizard.

To run the Web Agent configuration wizard

1. Click Start, Programs, CA, SiteMinder, Web Agent Configuration Wizard.

   The Web Agent Configuration wizard starts.

2. In the Host Registration screen, verify that yes is selected, and then click Next.

   The Admin Registration screen appears.

3. Complete the wizard using the information on your worksheet to complete the fields.

How to Install your SiteMinder Agent for SharePoint

To install the SiteMinder Agent for SharePoint on your web server, use the following process:

1. Gather the the installation information for your SiteMinder Agent for SharePoint. (see page 78)
2. Install the SiteMinder Agent for SharePoint (see page 80).
3. Start the SiteMinder Web Agent (see page 81).

Gather the Installation Information for your SiteMinder Agent for SharePoint

The installation wizard for the SiteMinder Agent for SharePoint requires the following information:

Application Port

Specifies an available port number on the web server that hosts your SiteMinder Agent for SharePoint. The SiteMinder Management UI uses this port.

Default: None

Farm Administrator

Specifies the domain and user name of a user account that has the following privileges:

- SharePoint administrator (for installation on a stand-alone SharePoint server)
- SharePoint server farm administrator (for installation on a SharePoint server farm)
- Administrator on the local computer

Example: *domain_name**user_name*

Password

Specifies the password associated with *one* of the following types of user accounts on the web server:

- SharePoint administrator (of a single SharePoint server).
- SharePoint server farm administrator.

Email ID

Specifies an email address associated with the SharePoint server administrator or SharePoint server farm administrator. A properly formatted email address is required for user profile imports.

Database server

Specifies the name of the SharePoint database server detected by the installer and the following types of database authentication that you can use:

Windows Authentication

Uses Windows authentication to connect to the database server associated with your SharePoint deployment.

SQL Authentication

Uses SQL authentication to connect to the database server associated with your SharePoint deployment. SQL authentication requires the following:

- SQL administrator account

- SQL administrator account password

Default: Windows Authentication

More information:

SiteMinder Agent for SharePoint Installation Worksheet (see page 198)
Protect Applications with the SiteMinder Agent for SharePoint (see page 86)

Install the SiteMinder Agent for SharePoint

The SiteMinder Agent for SharePoint requires that a SiteMinder Web Agent is installed on each web server where SharePoint operates.

If you are installing the SiteMinder Agent for SharePoint on a SharePoint server farm, note the following:

- Verify that all servers in the server farm are running.
- Start by installing the Agent for SharePoint on the primary server in the farm first.
- Continue by installing the Agent for SharePoint on all the secondary servers in the farm.

To install the SiteMinder Agent for SharePoint

1. Gather the information required by the installation wizard.
2. Verify that the following (Windows) service is running on your web server:

   `Windows SharePoint Services Administration`
3. Copy the following file to your web server:

   `ca-sp-`*`version-operating_environmentprocessor_type`*`.exe`

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates an abbreviation that represents the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   processor_type

   Indicates a two-digit number that corresponds the type of processor that is compatible with the file.

   Example: 32 corresponds to 32-bit processors

   Note: Some products (such as the SiteMinder Web Agent) have separate files for the 32-bit and 64-bit versions of the product. Other products (such as the SiteMinder Agent for SharePoint) use a single file labeled 32-bit for *both* the 32-bit and 64-bit versions. See the Platform Support matrix on http://ca.com/support to determine if your product supports a 64-bit operating environment.
4. Double-click the file.

   The installation wizard starts.

Important! Do not click Cancel after the installation process starts (while the progress indicator appears in the wizard). If you decide to change a setting, wait for the wizard to finish. Remove the Agent for SharePoint, and then install the Agent for SharePoint again.

5. Follow the prompts from the wizard to complete the installation.

   The SiteMinder Agent for SharePoint is installed.

Start the Web Agent

Configure your Web Agent parameters and then enable the Web Agent to protect the resources on the web server.

- **Note:** *No* resources are protected until you also define policies in the SiteMinder Policy Server.

To start the web agent

1. Open the following file with a text editor:

   web_agent_home\bin\IIS\WebAgent.conf

   web_agent_home

   Specifies the directory where the SiteMinder Web Agent is installed.

   Default: (r6.x SP6): C:\Program Files\netegrity\webagent

   Default: (r12.0 SP2): C:\Program Files\CA\webagent

2. Locate the EnableWebAgent parameter, and then change its value to yes.
3. Save and close the WebAgent.conf file.
4. Restart the IIS web server (the server itself, *not* the computer on which it operates).

   The web agent starts and the resources on the web server are protected.

Chapter 6: Protect SharePoint Resources and Manage Users

This section contains the following topics:

Privileges required for SiteMinder Management UI Tasks

The following list describes the types of privileges required to perform tasks with the SiteMinder Management UI:

Dashboard

Access to the dashboard tab of the SiteMinder Management UI requires the following privileges:

- Member of the SharePoint Server Farm Administrator group.
- Member of the group allowed to access the protected SharePoint resources in the SiteMinder Policy.

Application Protection

Access to the application protection tab of the SiteMinder Management UI requires the following privileges:

- Member of the SharePoint Server Farm Administrator group.
- Member of the group allowed to access the protected SharePoint resources in the SiteMinder Policy.
- Member of Administrators group.

User Migration

Access to the User Migration tab of the SiteMinder Management UI requires the following privileges:

- Member of the SharePoint Server Farm Administrator group.
- Member of the group allowed to access the protected SharePoint resources in the SiteMinder Policy.
- Member of Administrators group.
- Member of the group granted Personalization Services Permissions to Manage User Profiles

User Profile Import

Access to the User Profile Import tab of the SiteMinder Management UI requires the following privileges:

- Member of the SharePoint Server Farm Administrator group.
- Member of the group allowed to access the protected SharePoint resources in the SiteMinder Policy.
- Member of Administrators group.
- Member of the group granted Personalization Services Permissions to Manage User Profiles

Open the SiteMinder Management UI

The SiteMinder Management UI lets you do the following tasks:

- View the number of SharePoint applications protected by SiteMinder.
- View the status of User Profile Imports.
- Protect SharePoint applications with SiteMinder.
- Migrate your SharePoint users into SiteMinder.
- Import the user profiles of your SharePoint users from SiteMinder.

You can open the Management UI from the SharePoint central administration server or a web front-end (WFE) server.

1. Pick *one* of the following options:
   - To open the Management UI from your SharePoint Central Administration server follow these steps:
     a. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

        The Central Administration page appears.

     b. Click the SiteMinder Management tab.
   - To open the Management UI from a WFE server, open a web browser and then navigate to the following URL:

     `http://server_name:application_port`

     server_name

     Specifies the name of the SharePoint Central Administration server or web front-end (WFE) server on which you want to start the SiteMinder Management UI.

     Application Port

     Specifies an available port number on the web server that hosts your SiteMinder Agent for SharePoint. The SiteMinder Management UI uses this port. This port was defined when you installed the Agent for SharePoint on your SharePoint Central Administration server or web front-end (WFE) server.

     Default: None

Protect Applications with the SiteMinder Agent for SharePoint

The SiteMinder Management UI configures SiteMinder protection for most of your SharePoint applications. Some other SharePoint applications, such as the Shared Services Provider (SSP) or My Sites applications, need to be protected separately using different procedures.

Note: If you are protecting applications on a SharePoint farm, perform this procedure on the following systems:

- Your SharePoint Central Administration server (do this server first).
- *Each* web front-end (WFE) server in your SharePoint 2007 environment (do these servers next, in any order)

Follow these steps:

1. Open the Management UI (see page 85), and then click the Application Protection tab.

   A list of your SharePoint applications appears. The list contains the following information for each application:

   - The Authentication type by which each application is protected.
   - The description field of the web application (the default is the name and port number of the SharePoint application, but your setting could vary).
   - The zone of the SharePoint application.
   - Which version of the SiteMinder Agent for SharePoint is protecting the SharePoint application.
2. Select the check boxes of the SharePoint applications you want to protect.
3. Click the drop-down list for the application you want to protect, and then select one of the following authentication types:

   Forms (FBA)

   Used to configure SiteMinder protection for users accessing the SharePoint web application/zone. This option can be used with any type of SiteMinder user directory, but it is not used when the user accounts are in Active Directory. The Agent for SharePoint configures the SharePoint web application/zone to use ASP.NET Forms Based authentication. Together, with the SiteMinder Membership and role provider, retrieves the user and group information from the user directory. Many SiteMinder authentication schemes can be used with this option, including Forms and Basic.

   Important! The FBA authentication method that the Agent for SharePoint uses is different from SiteMinder forms-based authentication. SiteMinder forms based authentication uses a forms credential collector (FCC).

   Windows (Impersonation)

Used to configure SiteMinder protection along with Windows impersonation for users accessing the SharePoint web application/zone. This option is applicable only when user accounts are stored in Active Directory. Many SiteMinder authentication schemes can be used with this option, including Forms, Basic, and the Windows authentication scheme.

Important! Verify your selections before continuing. Once a web application is protected with the Management UI, it cannot be removed.

4. Click Protect.

   A confirmation message appears at the top of the list. The check boxes of the protected applications are disabled.

5. For SharePoint farms, repeat Steps 1 through 4 for on *each* WFE server for *all* the web applications that you want to protect using SiteMinder.

More information:

How to Protect the SharePoint SSP with SiteMinder r12.0 SP2 and FBA (see page 110)
How to Protect My Sites with SiteMinder (all versions) (see page 142)
Gather the Installation Information for your SiteMinder Agent for SharePoint (see page 78)

User Migration

User migration transfers any users associated with your existing SharePoint environment into SiteMinder, so that you can manage all of your users with SiteMinder. Consider the following when planning your user migration:

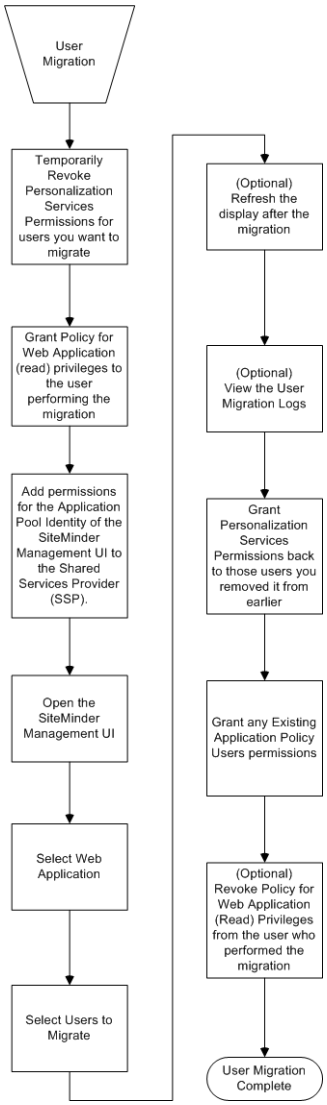
- Administrators who migrate users need the following permissions for each web site from which they want to migrate users:
  - SPBasePermissions
  - EnumeratePermissions

  Note: For more information, see your Microsoft documentation, or go to http://support.microsoft.com/

  Without the previous permissions, the users associated with the web site cannot be migrated.
- The following users cannot be migrated
  - The SHAREPOINT\system user.
  - Any SharePoint Farm Administrators (Farm Administrators lose access to the SharePoint Central Administration UI after migration).
- Reverse migration using the SiteMinder Management UI is *not* supported. After users have been migrated using the SiteMinder Management UI, they *cannot* be migrated back to SharePoint.

User Migration from SharePoint into SiteMinder Roadmap

Migrating users from your SharePoint environment into SiteMinder requires several separate procedures. The entire migration process is described in the following illustration:



Temporarily Revoke Personalization Services Permissions of any Users you want to Migrate

TheSiteMinder SiteMinder Management UI cannot currently migrate users who have personalization services permissions. Use the SharePoint Central Administration UI to revoke permissions for those users temporarily before migrating them.

To temporarily revoke personalization services permissions of any users you want to migrate

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the link for your Shared Services Provider.

   The Shared Services Administration screen appears.

3. Click Personalization Services Permissions.

   The Manage Permissions: Shared Service Rights screen appears, with a list of users and their respective permissions.

   Note: We recommend recording these settings for future reference before removing them.

4. Select the check boxes for all users, and then click Remove selected users.

   A confirmation dialog appears.

5. Click OK.

   The users and their permissions are removed.

Grant Policy for Web Application Privileges to the SharePoint Administrator

To migrate users, the SharePoint Administrator (or the person who uses the SiteMinder Management UI to migrate users) needs read privileges in the SharePoint Policy for Web Application to which the migrated users belong. For example, if you want to migrate users from a web application called webapp1, the person using the SiteMinder Management UI to migrate those users needs read permissions in the Policy for Web Application of webapp1.

To grant policy for web application privileges to the SharePoint administrator

1. Open the SharePoint Central Administration UI.
2. Click Policy for web application.

   The Policy for Web Application screen appears.
3. Verify that the application with the users you want to migrate appears in the Web application drop-down list (in the upper-right corner).
4. Click Add users.

   The Add Users screen appears.
5. Click the Zones drop-down list and then select the zone of the application.
6. Click Next.

   The Choose Users and Choose Permissions sections appear.
7. Enter the name of the SharePoint Administrator in the Choose Users section. Use the buttons to verify the name or to search for the user you want.
8. Select the Full Read - Has full read-only access check box.
9. Click Finish.

   The Policy for Web Application page appears, and the SharePoint Administrator appears in the list of users.

Open the SiteMinder Management UI

The SiteMinder Management UI lets you do the following tasks:

- View the number of SharePoint applications protected by SiteMinder.
- View the status of User Profile Imports.
- Protect SharePoint applications with SiteMinder.
- Migrate your SharePoint users into SiteMinder.
- Import the user profiles of your SharePoint users from SiteMinder.

You can open the Management UI from the SharePoint central administration server or a web front-end (WFE) server.

1. Pick *one* of the following options:
   - To open the Management UI from your SharePoint Central Administration server follow these steps:
     a. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

        The Central Administration page appears.

     b. Click the SiteMinder Management tab.
   - To open the Management UI from a WFE server, open a web browser and then navigate to the following URL:

     `http://server_name:application_port`

     server_name

     Specifies the name of the SharePoint Central Administration server or web front-end (WFE) server on which you want to start the SiteMinder Management UI.

     Application Port

     Specifies an available port number on the web server that hosts your SiteMinder Agent for SharePoint. The SiteMinder Management UI uses this port. This port was defined when you installed the Agent for SharePoint on your SharePoint Central Administration server or web front-end (WFE) server.

     Default: None

Select a Web Application

Select a web application from which you want to migrate the users.

To select a Web Application

1. Click the User Migration tab.

   The User Migration screen appears.

2. Use the following drop-down lists to select a web application that contains the users you want to migrate.

   Web Application

   Specifies the name of the SharePoint web application from which you want to migrate users.

   Example: SharePoint

   Zone

   Specifies the zone of the SharePoint web application that you want to import. Only those zones which currently contain SharePoint web applications appear in the list.

   Examples: Default, Intranet

   User Prefix

   Defines *one* of the following directory attributes by which you can limit your search for users within the specified Zone:

   - *domain_name* (for Windows authentication)
   - *membership_provider_name* (for Forms authentication). The SharePoint Management UI retrieves the membership provider name in the web.config file of the application you want to protect.

   Example: (Windows authentication) example.com

   Example: (Forms authentication) CAMembershipProvider

   Choose Directories to Search

   Specifies the SiteMinder directories to search for a matching user in SharePoint.

3. Click Match Users.

   A list of users appears.

Select Users to Migrate

After you select a web application from which to migrate users, select the specific users you want to migrate.

Note: All users from all zones associated with the protected web application appear in the list, but only those users that also exist in the SiteMinder directory you select are migrated.

To select users to migrate

1. Select a web application.
2. (Optional) Use the Search field and drop-down to filter the list of users.
3. Select the check boxes of the users you want to migrate.
4. Click Migrate.

   The User Migration Status screen appears and displays the results.

User Migration Status

After you migrate users into SharePoint, the User Migration Status page displays the following information:

Migration Started At

Indicates the time the user migration started.

Migration Completed At

Indicates the time the user migration finished.

Number of Users Selected for Migration

Indicates the number of users migrated during the current operation.

Number of Migration Attempts

Indicates the number of users for which migration has been attempted.

Number of Successful Migrations

Indicates the number of successful migrations for the SiteMinder Agent for SharePoint.

Number of failed migrations

Indicates the number of times that a migration by the SiteMinder Agent for SharePoint.

View log messages

Displays a link to the log file of the latest migration.

To refresh the user migration status, click Refresh.

View User Migration Logs

Log files are created during each user migration. After a migration starts, you can view the associated log file.

To view the user migration logs from the user migration status screen, click the log messages link.

Grant Permissions for SharePoint Users Which previously had Access through a Policy for the Web Application

Any SharePoint users who were granted permissions as part of a policy were migrated by the SiteMinder Management UI, but their permissions from the policy were *not* migrated. The previous permissions of the user must be granted again.

To grant permissions for SharePoint users which previously had access through a policy

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The Central Administration page appears.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Policy for web application.

   The Policy for Web Application page appears.

4. Click Add Users.

   The Add Users wizard appears.

5. Use the wizard to grant permission to the users you want.

   Note: For web applications protected by the SiteMinder Agent for SharePoint, searches of user directories only return exact matches. For example, searching for user1 returns user1, but not user11 or user111. Use a wildcard (user1*) to include user11 and user111 in your search results.

   The permissions are granted.

Grant Personalization Services Permissions back to the Users you temporarily Revoked it from after the Migration

After migrating the users, use the SharePoint Central Administration UI to grant the personalization services permissions you temporarily revoked to accomplish the migration.

To grant personalization services permissions back to the users you temporarily revoked it from after the migration

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the link for your Shared Services Provider.

   The Shared Services Administration screen appears.

3. Click Personalization Services Permissions.

   The Manage Permissions: Shared Service Rights screen appears.

4. Click Add Users/Groups.

   The Add Users/Groups: Shared Service Rights screen appears.

5. Click the Users/Groups field of the People Picker, and then type the name of a user that you removed before migration. Use the buttons to verify the name or to browse for the user.

   Note: For web applications protected by the SiteMinder Agent for SharePoint, searches of user directories only return exact matches. For example, searching for user1 returns user1, but not user11 or user111. Use a wildcard (user1*) to include user11 and user111 in your search results.

6. Select the check boxes of the permissions you want to grant.

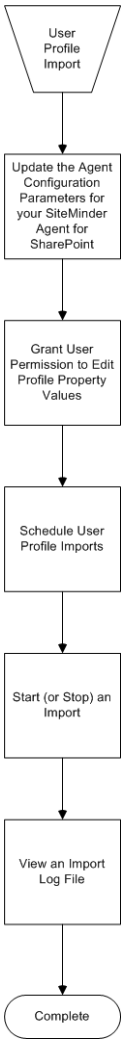
7. Click Save.

   The Manage Permissions: Shared Service Rights screen appears, the user appears in the list.

8. Repeat steps 4 through 7 until all of the users and permissions you temporarily revoked before the migration have been restored.

How to Import User Profiles

Importing user profiles from your SharePoint system into SiteMinder requires several separate procedures. The entire protection process is described in the following illustration:



Update the Agent Configuration Parameters for your Agent for SharePoint

The following tasks require updating the Agent Configuration parameters for your SiteMinder Agent for SharePoint:

- Adding, changing or removing properties from a user profile.
- Importing user profiles.

To update the Agent Configuration parameters for your Agent for SharePoint

1. Open one of the following:
   - (r6.x SP6) Policy Server User Interface
   - (r12.0 SP2) Administrative UI
2. Open the Agent configuration object associated with your SiteMinder Agent for SharePoint.
3. Verify that the value of your Universal ID user attribute from your user directory connection in the Policy Server is also set as the value for the following parameter:

   SPSortVirtualAttribute

   Specifies the name of the Virtual attribute defined in the user directory connection of the SiteMinder Policy Server. Set this attribute before importing or modifying user profiles.

   Default: UniversalID

   Example: (Active Directory) sAMAccountName
4. Verify that the username attribute setting of the following parameter also matches the value of your Universal ID user attribute:

   SPVirtualAttributeMapList

   Contains a group of virtual user attributes which are mapped to existing user attributes in the user directory connection defined in the SiteMinder Policy Server. The following attributes are available:
   - group = *group_name_attribute*
   - email = *email_address_attribute*
   - username = *user_name_attribute*
   - displayname = *display_name_attribute*

   Default: email=Email group=GroupID username=UniversalID displayname=DisplayName
5. Save any changes to your Agent Configuration object.

   The agent configuration parameters are updated.

More information:

Create Virtual Attribute Mappings to your SharePoint User Directories (r12.0 SP2) (see page 31)
Edit the User Attribute Mapping File to Configure Virtual Attribute Mappings to your SharePoint User Directories (r6.x SP6) (see page 51)
Modify a User Directory Connection for your SharePoint User Directories in the SiteMinder Policy Server (r12.0 SP2) (see page 30)
Modify a User Directory Connection for your SharePoint Directories in the SiteMinder Policy Server (r6.x SP6) (see page 50)

Grant User Permission to Edit Profile Property Values

Use the SharePoint Central Administration UI to grant user permission to edit the values of the profile properties you want to import. For example, if the profiles you want to import include the Name property, grant user permission to edit the name property.

To grant user permission to edit the profile property values

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the link for your Shared Services Provider.

   The Shared Services Administration screen appears.

3. Click User Profiles and Properties.

   The User Profiles and Properties screen appears.

4. Click View Profile Properties.

   The View Profile Properties page appears, with a list of properties.

5. Grant permissions for the properties you want by doing the following steps:

   a. Click a property you want, and then select Edit from the drop-down list.

      The Edit User Profile Property screen appears.

   b. Click the Allow Users to Edit Values for this property option button.

   c. Click OK.

      The changes are saved and the View Profile Properties page appears.

   d. Repeat Steps 5a through 5c until all the properties you want have permissions.

   User permission to edit profile property values is granted.

Schedule User Profile Imports

Your SiteMinder Agent for SharePoint can import user profiles from SiteMinder user directories to the databases used by your SharePoint Server.

To schedule user profile imports

1. Click the User Profile Import tab.

   The Configure SiteMinder User Profile Import page appears.

2. If you are using more than one SSP, verify that the one you want appears in the Shared Services Providers drop-down list.

3. Click one of the following in the User Profile and Import Settings section:

   - The link on the right side of the Import Schedule row.
   - Configure profile import

   The Full Import Schedule dialog appears.

4. Choose the settings you want in the dialog, and then click OK.

   The import settings are saved and the Configure SiteMinder User Profile Import page appears.

View SharePoint User Profiles

The SiteMinder Management UI provides a link for viewing SharePoint user profiles.

To view SharePoint user profiles

1. Click the User Profile Import tab.

   The Configure SiteMinder User Profile Import page appears.

2. Click View user profiles.

   The SharePoint user interface opens in a new browser window.

3. Use the SharePoint user interface to view the profiles you want.

   Note: For more information, see the online help for SharePoint.

Start or Stop an Import

The SiteMinder Management UI lets you start an import anytime, or cancel an import that is in progress.

To start or stop an import

1. Click the User Profile Import tab.

   The Configure SiteMinder User Profile Import page appears.

2. Click *one* of the following links:

   Start full import

   Imports all of the user profile items.

   Stop import

   Cancels an import operation that is already in progress.

   The link changes back to the opposite state. For example, if you cancel an import, the link changes to Start full import.

View an Import Log File

Each import operation produces a log file.

To view an import log file

1. Click the User Profile Import tab.

   The Configure SiteMinder User Profile Import page appears.

2. Click View import log.

   The View Import Log screen appears.

Add a Property to a User Profile

The SiteMinder Management UI provides a link for adding a new user property to a SharePoint user profile.

To add a property to a SharePoint user profile

1. Click the User Profile Import tab.

   The Configure SiteMinder User Profile Import page appears.

2. Click Add profile property.

   The SharePoint user interface opens in a new browser window.

3. Use the SharePoint user interface to add the profiles you want.

   Note: For more information, see the online help for SharePoint.

View or Change User Profile Properties

To view or change the user profile properties associated with SharePoint users in SiteMinder, do either of the following tasks:

- View the User Profile properties
- Change the User Profile properties

Change a User Property Mapping

Change the mapping between the properties of the users in your directory and the SiteMinder virtual attributes used in your SiteMinder policies.

To change a user property mapping

1. Click the User Profile Import tab.

   The User Profiles and Properties screen appears.

2. (Optional) If you have multiple Shared Service Providers, click the Shared Service Providers drop-down list to select and display the user properties for another SSP.

3. Click View Profile Properties.

   Note: If the link is not active, enable User Profile Imports.

   A list of properties, and the attributes to which they are mapped appears.

4. To change the mapping of a property, do the following:

   a. Click the link of the property with the mapping that you want to update.

      The Remap user profile property screen appears.

   b. Click Virtual Attributes drop-down list and select the virtual attribute to which you want to map.

   c. Click OK.

   d. The Remap user profile property screen closes and the list of properties appears.

5. Repeat Step 4 to change the mappings for other properties.

View SiteMinder Virtual Attribute Mappings

The SiteMinder Management UI shows the virtual attribute mappings that are configured on your SiteMinder Policy Server. View the mappings to confirm they are correct.

To view the virtual attribute mappings

1. Click the User Profile Import tab.

   The User Profiles and Properties screen appears.

2. (Optional) If you have multiple Shared Service Providers, click the Shared Service Providers drop-down list to select and display the mappings for another SSP.

3. Click View SiteMinder Virtual Attributes.

   Note: If the link is not active, enable User Profile Imports.

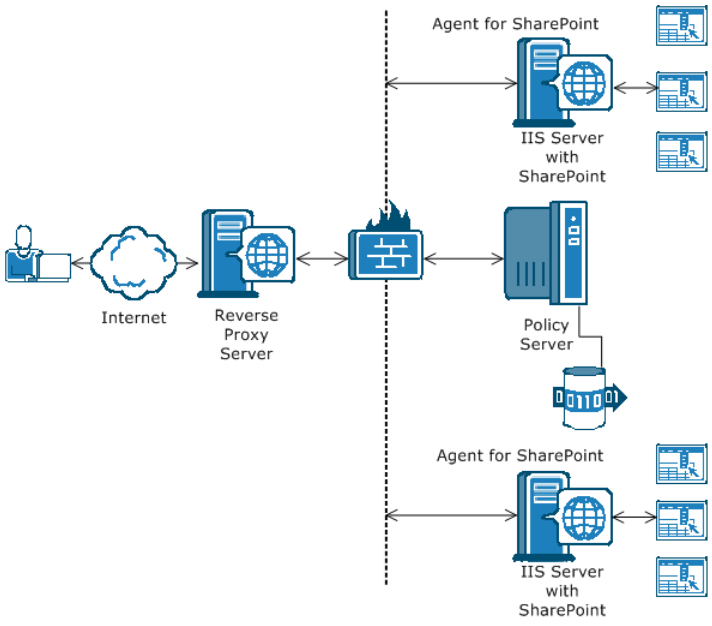
   The current virtual attribute mappings appear.

Chapter 7: Using the SiteMinder Agent for SharePoint with a Reverse Proxy Server

This section contains the following topics:

Reverse Proxy Server Deployment with the Agent for SharePoint

The following illustration shows a reverse proxy server routing traffic to IIS web servers running the SiteMinder Agent for SharePoint behind a firewall:



How to Configure a Reverse Proxy Server for your Agent for SharePoint Environment

To configure a reverse proxy server for your Agent for SharePoint environment, use the following process:

1. Verify that SiteMinder supports the reverse proxy server you want to use.

   Note: For more information about which specific reverse proxy servers SiteMinder supports, see the platform support matrix.

2. Install (if necessary) and configure your reverse proxy server. See the documentation from your reverse proxy server vendor for specific instructions.

3. Install a SiteMinder Web Agent on your reverse proxy server, and then configure the Web Agent to act as a reverse proxy.

   Note: For more information, see the *Web Agent Configuration Guide*.

4. For each web server behind the reverse proxy, set the value ProxyTrust parameter to yes.

5. To enable office client integration, add a list of request URLs to the value of the SPClientIntegration parameter on your reverse proxy server.

More information:

Locate the SiteMinder Platform Support Matrix (see page 195)

Enable Office Client Integration for a Reverse Proxy

In most situations, the SiteMinder Agent for SharePoint automatically determines whether Office Client Integration is allowed for a particular SharePoint resource according to the setting in the SharePoint Central Administration UI.

However, if you are using a SiteMinder Agent for SharePoint with a reverse proxy (such as a SiteMinder Secure Proxy Server, or another vendor's reverse proxy solution), add the request URLs to the value of the following Agent Configuration parameter for your reverse proxy server:

SPClientIntegration

Specifies a list of protected SharePoint resources where Office Client Integration is enabled. In most situations, the settings for this parameter are determined automatically from the setting in the SharePoint Central Administration UI.Each URL in this parameter *requires* a port number (even for a default port such as 80 or 443).

If you are protecting your SharePoint resources using the SiteMinder Secure Proxy Server or an Apache Reverse Proxy server, add the request URLs to this parameter manually. For deployments of the Agent for SharePoint on a Reverse Proxy server, the port numbers are *not* required.

Example: *host_name*:*port_number*

Limits: Port numbers required for typical Agents. Omit port numbers for reverse proxy deployments.

To enable office client integration with a reverse proxy solution, add the request URLs to the value of the SPClientIntegration parameter for your reverse proxy server.

More information:

Verify your Office Client Integration Settings (see page 69)

Chapter 8: Protect the SharePoint Shared Services Provider (SSP) and My Sites with FBA

This section contains the following topics:

The SharePoint Shared Services Provider and SiteMinder

Extend the SharePoint SSP web site on each SharePoint server if you want to implement any of the following functions:

- Allow existing SharePoint users who authenticate with the forms-based authentication (FBA) method to access the following features such as the following:
  - User profiles and properties
  - Profile services policies
  - My Site settings
  - Audiences
- Protect the SSP web site with FBA and any SiteMinder authentication scheme.

How to Protect the SharePoint SSP with SiteMinder r12.0 SP2 and FBA

If you are using a SharePoint server in your organization and you want to protect the SSP with SiteMinder, use the following process:

Note: Not required if you are using Windows SharePoint Services instead of a Microsoft Office SharePoint server.

1. Verify the port numbers of the following SharePoint web sites (see page 112):
   - The Central Administration web site
   - The Default SSP web site
2. Extend the default SSP web site to another zone. (see page 113)
3. Change the alternate access mapping of the extended SSP web site to use a fully qualified domain name (FQDN). (see page 114)
4. Do *one* of the following tasks:
   - Add the SiteMinder ISAPI filter to the IIS 6.0 web site for your Extended SSP. (see page 115)
   - Add the SiteMinder ISAPI filter to the IIS 7.x web site for your Extended SSP (see page 117), and then add the Handler Mapping for the IIS 7.x web site for your Extended SSP. (see page 118)
5. Edit the web.config file of your extended SSP web site to include the following items (see page 119):
   - CA Membership provider
   - CA Role provider
   - HTTP Session Manager Provider
   - Forms Authentication settings

   Note: The CA in the Agent for SharePoint code for the web.config files stands for CA Technologies. In these examples, it does *not* mean SharePoint Central Administration. The related procedures explain where to add the code.
6. Do *one* of the following tasks:
   - Add the SiteMinder ISAPI filter to the IIS 6.0 web site for your default SSP. (see page 121)
   - Add the SiteMinder ISAPI filter to the IIS 7.x web site for your default SSP, and then add the Handler Mapping for the IIS 7.x web site for your default SSP. (see page 123)
7. Edit the web.config file of your default SSP web site to include the following items: (see page 136)
   - CA Membership provider

- CA Role provider
- HTTP Session Manager Provider
- Forms Authentication settings

8. Use the SharePoint Central Administration UI to do the following tasks:
   a. Change the Authentication provider of your default SSP site to Forms. (see page 124)
   b. Change the alternate access mapping of the default SSP web site to use a fully qualified domain name (FQDN). (see page 125)
   c. Add a SiteMinder user under personalization permissions. (see page 126)
   d. Make the SiteMinder user from the previous step a site collection administrator for the default SSP site. (see page 127)
9. Use the Administrative UI to create an application and policy to protect the SSP URL. (see page 127)
10. Use the SharePoint Central Administration UI to change the Authentication provider of your default SSP site to Forms. (see page 138)
11. Rename the following sections in the web.config file of your extended SSP web site:
    - CA Membership provider (see page 139)
    - CA Role provider (see page 140)
12. Use the SharePoint Central Administration UI to change the names of the items in Step 12 on the Authentication provider page of your extended SSP site. (see page 141)

More information:

SiteMinder Agent for SharePoint SSP Protection Worksheet (see page 198)
How to Protect My Sites with SiteMinder (all versions) (see page 142)
Protect Applications with the SiteMinder Agent for SharePoint (see page 86)

Verify the Location of your SharePoint SSP Files

A SharePoint server creates several virtual directories on an IIS web server. Because the SSP files are edited manually before protecting them with SiteMinder, identifying the correct files to modify is critical. The virtual SharePoint sites created on the IIS web server use folders with the corresponding port number. The port number can help you confirm the location of the proper files.

To verify the port numbers of your SharePoint web sites

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Configure your web browser to display the address bar.

3. Note the port number in the URL, as shown in the following example:

   `http://host_name.domain_name.domain_extension:port_number/default.aspx`

4. Mouse-over the shared services link in the left pane (below the Shared Services Administration heading).

5. The URL of the Shared Services Administration web site appears in the status bar, as shown in the following example:

   `http://host_name.domain_name.domain_extension:port_number/ssp/admin/default.aspx`

6. Record these port numbers for future reference. Your SharePoint web site configuration files are in the corresponding subdirectory of the VirtualDirectories folder on the IIS web server. For example, if the port number from Step 4 is 55600, then your SSP files would be in the following location:

   `C:\Inetpub\wwwroot\wss\VirtualDirectories\55600`

   The port numbers of your SharePoint SSP web sites verified.

Extend the Default SSP Web Site to another Zone

Extend the default SSP web site into a different zone. Verify that the zone to which you extend your default SSP web site is the same zone that contains the following resources:

- User profiles and properties
- Profile services policies
- My Site settings
- Audiences

Extend the default SSP web site to another zone

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Create or Extend Web Application.

   The Create or Extend Web Application page appears.

4. Click Extend an existing Web Application.

   The Extend Web Application to Another IIS Web Site page appears.

5. Select your default SSP web site by doing the following tasks:

   a. Click the Web Application drop-down list, and then select Change Application.

      The Select Web Application -- Web Page dialog appears.

   b. From the Name list, click the link that corresponds to your default SSP Web Site.

      The Select Web Application -- Web Page dialog closes and your default SSP Web Site appears in the Web Application drop-down list. The other fields and drop-down lists are automatically populated.

      Note: Record the port number of this web site for future reference.

6. Verify that the Zone drop-down list contains the correct zone.

7. Click OK.

   The default SSP Web Site is extended. The Application Management page appears.

Create an Alternate Access Mapping for your Extended SSP Web Site

The SiteMinder Web Agent requires URLs with fully qualified domain names. Use the SharePoint Central Administration UI to specify a fully qualified domain name for the URL of your extended SSP web site by creating an alternate access mapping.

To create an alternate access mapping of your extended SSP web site

1. Click Start, Programs, Microsoft Office Server, SharePoint v3.0 Central Administration.

   The Central Administration screen appears.

2. Click the Operations tab.

   The Operations screen appears.

3. Click Alternate Access Mappings.

   The alternate access mappings screen appears.

4. Click the link for your extended SSP web site.

   The Edit internal URLs screen appears.

5. Change the URL in the field to include a fully qualified domain name, and then click OK.

   The alternate access mappings screen appears. The URL of your extended SSP web site appears in the list showing a fully qualified domain name.

Add the SiteMinder ISAPI Filter to the IIS 6.0 Web Site for your Extended SSP

The following SharePoint resources need a SiteMinder ISAPI filter installed on the corresponding virtual web site on the IIS web server:

- SharePoint Central Administration site.
- Any SharePoint web sites protected by SiteMinder.
- The Default and Extended SSP sites (optional).
- My Site web sites (optional).

To add the SiteMinder ISAPI filter to your SharePoint resources on an IIS 6.0 web server

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

   The Internet Information Services (IIS) Manager window opens.

2. In the left pane, expand your web server, and expand Web Sites folder.

   A list of web sites appears.

3. Right-click the SharePoint Central Administration v3 web site, and then select Properties.

   The Properties dialog appears.

4. Add the ISAPI filter by doing the following tasks:

   a. Click the Home Directory tab, and then click Configuration.

      The Application Configuration dialog appears.

   b. Click Insert.

      The Add/Edit Application Mapping dialog appears.

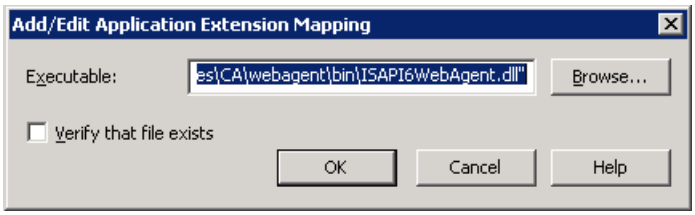
   c. Click Browse, and then locate the following file:

      `web_agent_home\bin\ISAPI6WebAgent.dll`

   d. Click Open.

      The ISAPI6WebAgent.dll file appears in the Executable field of the Add/Edit Application Mapping dialog.

   e. *Clear* the Verify that file exists check box as shown in the following illustration:



f. Click OK.

The Add/Edit Application Mapping dialog closes and the ISAPI6WebAgent.dll file appears in the Wildcard application maps (order of implementation) list.

g. Click Move Up until the ISAPI6WebAgent.dll file is at the top of the list.

h. Click OK.

The Inheritance Overrides dialog appears with a list of child nodes.

i. Click Select All, and then Click OK.

The Inheritance Overrides dialog and the Application Configuration dialogs close.

j. Click OK.

The Properties dialog closes. The SiteMinder ISAPI filter is added to the corresponding SharePoint web site on your IIS 6.0 web server.

5. Choose *one* of the following tasks:

- Right-click the web site folder of another SharePoint resource you want to protect, and then repeat Steps 4a through 4j, until all of the the following SharePoint sites you want to protect have the ISAPI filter installed.
  - Default SSP web site.
  - Extended SSP web site.
  - My Site web site.
- Stop after you have added the ISAPI filter to all the previous types of SharePoint sites.
-

Add the SiteMinder ISAPI Filter to the IIS 7.0 Web Site for your Extended SSP

To run a SiteMinder Web Agent for SharePoint on IIS 7.0, add a SiteMinder ISAPI filter to each SharePoint resource you want to protect on the IIS 7.0 web server. This filter executes the Web Agent ISAPI scripts and other files. Place it before any other ISAPI filters on the web server.

To add the Agent ISAPI filter

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   A Sites folder appears.

3. Expand the Sites folder, and then click the SharePoint web site you want to protect with SiteMinder.

4. Under the IIS section, double-click the ISAPI Filters icon.

   A list of the installed ISAPI Filters appears.

5. In the Actions pane, click Add.

   The Add ISAPI Filter dialog appears.

6. In the Filter Name field, type a name for the ISAPI Filter. We recommend using a name that is easy to recognize, such as "SiteMinder ISAPI Filter."

7. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgentDLL

   web_agent_home

   Specifies the directory where the SiteMinder Web Agent is installed.

   Default: (r6.x SP6): C:\Program Files\netegrity\webagent

   Default: (r12.0 SP2): C:\Program Files\CA\webagent

9. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add ISAPI Filter dialog.

10. Click OK.

    The Add ISAPI Filter dialog closes and the ISAPI filter appears in the list.

11. In the Actions pane, click View Ordered List.

12. Right-click the SiteMinder ISAPI filter in the list, and then select Move up. Repeat this step until the SiteMinder ISAPI filter is at the top of the list.

    The Agent ISAPI filter is added.

13. Repeat Steps 3 through 12 for each SharePoint web site you want to protect with SiteMinder.

Add a Handler Mapping to your IIS 7.0 Web Site for your Extended SSP

The IIS 7.0 web site associated with your extended SSP site requires a handler mapping.

To add a handler mapping to your IIS 7.0 web site for your extended SSP

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   A Sites folder appears.

3. Expand the Sites folder, and then double-click the site of the extended SSP that you want to protect with SiteMinder.

4. Under the IIS section, double-click Handler Mappings.

   A list of handler mappings appears.

5. Under the Actions pane, click Add wildcard script map...

   The Add Wildcard Script Map dialog appears.

6. Click the ellipsis button (to the right of the Executable field).

   An Open dialog appears.

7. Navigate to the following file:

   `web_agent_home\bin\ISAPI6WebAgent.dll`

8. Click Open.

   The Open dialog closes and the location of the file appears in the Executable field of the Add Wildcard Script Map dialog.

9. Click the Name field, and type a name for the handler mapping. We recommend using a name that is easy to recognize, such as SiteMinderHandlerMapping.

10. Click OK.

    A confirmation dialog appears.

11. Click Yes.

    The Add Wildcard Script Map dialog closes and the handler mapping appears in the list.

Manually Update the web.config file for your Extended SSP Web Site

The web.config file that corresponds to your extended SSP web site in your SharePoint server needs the following sections that contain SiteMinder settings:

- Membership provider
- Role provider
- Session Management (HTTP) module
- Forms Authentication Settings

To manually update the web.config file for your extended SSP web site

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

   The Internet Information Services (IIS) Manager opens.

2. Expand the Web Sites folder, and then locate your extended SSP Web Site.
3. Right-click your extended SSP Web Site, and select Stop.

   The extended SSP Web site stops.

4. Right-click your extended SSP Web site, and select Open.

   A new Explorer window opens.

5. Create a backup copy of the existing web.config file.
6. Locate the web.config file and open it with a text editor.

   Important! Do not use Notepad, Wordpad (or any other text editor with line-length limitations) to edit the .config (XML) files. A text editor that is designed for writing programming source code typically does not have such line-length limitations. For more information, see the documentation or online help for your respective editor.

7. Locate the following tags:

   ```
   <system.web>
   <securityPolicy>
   ```

8. Insert the following syntax between the previous tags:

   ```
   <membership defaultProvider="CAMemberProvider">
   <providers>
   <clear />
   <add name="CAMemberProvider"
   type="CA.SMMemberRoleProvider.SMMemberProvider,CA.SiteMinder.MemberRoleProvid
   er, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   </providers>
   </membership>
   <roleManager enabled="true" defaultProvider="CARoleProvider">
   <providers>
   ```

```
<add name="CARoleProvider"
type="CA.SMMemberRoleProvider.SMRoleProvider,CA.SiteMinder.MemberRoleProvider
, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
</providers>
</roleManager>
```

9. Locate the following line:

```
<add name="PublishingHttpModule"
type="Microsoft.SharePoint.Publishing.PublishingHttpModule,
Microsoft.SharePoint.Publishing, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />
```

10. Insert a new line after the previous line, and then add the following syntax:

```
<add name="SessionMgmtModule" type="CA.SPWebModule.SessionMgmtModule,
CA.SiteMinder.SPWebModule, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=29f091c10dd5f4a0" />
```

11. Locate the following tag:

```
<authentication mode="Windows" />
```

12. In the previous line do the following:
    - Replace the word "Windows" with the word "Forms".
    - Delete the closing slash and the extra white space.
13. Add the lines shown in the following example:

```
<forms loginUrl="/_layouts/SPlogin.aspx" />
</authentication>
```

    The authentication section should match the following example:

```
<authentication mode="Forms">
<forms loginUrl="/_layouts/SPlogin.aspx" />
</authentication>
```

14. Save the web.config file and close the text editor.
15. Close the Explorer window.
16. Right-click your extended SSP Web Site in the IIS Manager, and select Start.

    The web config file for your extended SSP Web Site is updated.

Add the SiteMinder ISAPI Filter to the IIS 6.0 Web Site for your Default SSP Site

The following SharePoint resources need a SiteMinder ISAPI filter installed on the corresponding virtual web site on the IIS web server:

- SharePoint Central Administration site.
- Any SharePoint web sites protected by SiteMinder.
- The Default and Extended SSP sites (optional).
- My Site web sites (optional).

To add the SiteMinder ISAPI filter to your SharePoint resources on an IIS 6.0 web server

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

   The Internet Information Services (IIS) Manager window opens.

2. In the left pane, expand your web server, and expand Web Sites folder.

   A list of web sites appears.

3. Right-click the SharePoint Central Administration v3 web site, and then select Properties.

   The Properties dialog appears.

4. Add the ISAPI filter by doing the following tasks:

   a. Click the Home Directory tab, and then click Configuration.

      The Application Configuration dialog appears.

   b. Click Insert.

      The Add/Edit Application Mapping dialog appears.

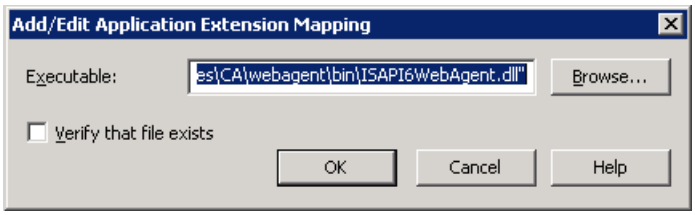
   c. Click Browse, and then locate the following file:

      `web_agent_home\bin\ISAPI6WebAgent.dll`

   d. Click Open.

      The ISAPI6WebAgent.dll file appears in the Executable field of the Add/Edit Application Mapping dialog.

   e. *Clear* the Verify that file exists check box as shown in the following illustration:



f. Click OK.

The Add/Edit Application Mapping dialog closes and the ISAPI6WebAgent.dll file appears in the Wildcard application maps (order of implementation) list.

g. Click Move Up until the ISAPI6WebAgent.dll file is at the top of the list.

h. Click OK.

The Inheritance Overrides dialog appears with a list of child nodes.

i. Click Select All, and then Click OK.

The Inheritance Overrides dialog and the Application Configuration dialogs close.

j. Click OK.

The Properties dialog closes. The SiteMinder ISAPI filter is added to the corresponding SharePoint web site on your IIS 6.0 web server.

5. Choose *one* of the following tasks:

- Right-click the web site folder of another SharePoint resource you want to protect, and then repeat Steps 4a through 4j, until all of the the following SharePoint sites you want to protect have the ISAPI filter installed.
  - Default SSP web site.
  - Extended SSP web site.
  - My Site web site.
- Stop after you have added the ISAPI filter to all the previous types of SharePoint sites.
-

Add the SiteMinder ISAPI Filter to the IIS 7.0 Web Site for your Default SSP Site

To run a SiteMinder Web Agent for SharePoint on IIS 7.0, add a SiteMinder ISAPI filter to each SharePoint resource you want to protect on the IIS 7.0 web server. This filter executes the Web Agent ISAPI scripts and other files. Place it before any other ISAPI filters on the web server.

To add the Agent ISAPI filter

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   A Sites folder appears.

3. Expand the Sites folder, and then click the SharePoint web site you want to protect with SiteMinder.

4. Under the IIS section, double-click the ISAPI Filters icon.

   A list of the installed ISAPI Filters appears.

5. In the Actions pane, click Add.

   The Add ISAPI Filter dialog appears.

6. In the Filter Name field, type a name for the ISAPI Filter. We recommend using a name that is easy to recognize, such as "SiteMinder ISAPI Filter."

7. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgentDLL

   web_agent_home

   Specifies the directory where the SiteMinder Web Agent is installed.

   Default: (r6.x SP6): C:\Program Files\netegrity\webagent

   Default: (r12.0 SP2): C:\Program Files\CA\webagent

9. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add ISAPI Filter dialog.

10. Click OK.

    The Add ISAPI Filter dialog closes and the ISAPI filter appears in the list.

11. In the Actions pane, click View Ordered List.

12. Right-click the SiteMinder ISAPI filter in the list, and then select Move up. Repeat this step until the SiteMinder ISAPI filter is at the top of the list.

    The Agent ISAPI filter is added.

Repeat Steps 3 through 12 for each SharePoint web site you want to protect with SiteMinder.

Change the Authentication Provider of your Default SSP Web Site to Forms

Use the SharePoint Central Administration page to change the authentication provider used by your extended SSP web site.

Change the SharePoint authentication provider for your extended SSP web site using the SharePoint server

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Authentication Providers.

   The Authentication Providers page appears.

4. Verify that the URL of your extended SSP site appears in the drop-down list on the right.

5. Click the link that corresponds to the zone to which you extended your extended SSP web site. For example, if you extended the Default SSP web site to the Intranet zone, then click the Intranet link.

   The Edit Authentication page appears.

6. Click Forms.

7. Click the Membership Provider field and then enter the following:

   ```
   CAMemberProvider
   ```

8. Click the Role Manager field, and then enter the following:

   ```
   CARoleProvider
   ```

9. Click Save.

   The Authentication Providers page appears. The zone of your extended SSP web site shows the updated membership provider name in the list.

Create an Alternate Access Mapping for your Default SSP Web Site

The SiteMinder Web Agent requires URLs with fully qualified domain names. Use the SharePoint Central Administration UI to specify a fully qualified domain name for the URL of your default SSP web site by creating an alternate access mapping.

To create an alternate access mapping of your default SSP web site

1. Click Start, Programs, Microsoft Office Server, SharePoint v3.0 Central Administration.

   The Central Administration screen appears.

2. Click the Operations tab.

   The Operations screen appears.

3. Click Alternate Access Mappings.

   The alternate access mappings screen appears.

4. Click the link for your default SSP web site.

   The Edit internal URLs screen appears.

5. Change the URL in the field to include a fully qualified domain name, and then click OK.

   The alternate access mappings screen appears. The URL of your default SSP web site appears in the list showing a fully qualified domain name.

Add a SiteMinder user to the Personalization Permissions

Adding a SiteMinder user to the personalization permissions grants access to the protected SSP sites.

To add a SiteMinder user to the personalization permissions

1. Click Start, Programs, Microsoft Office Servers, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page appears.

2. Click the link for SharedServices in the left pane.

   The Shared Services Administration page appears.

3. Click Personalization Services Permissions.

   The Manage Permissions: Shared Service Rights screen appears.

4. Click Add Users/Groups.

   The Add Users/Groups screen appears.

5. Enter the users and groups you want. Use the buttons under the dialog to check names, or browse for a user.

6. Check the boxes of the permissions you want for each user or group.

7. Click Save.

   The Add Users/Groups screen closes. The user is added.

Make the SiteMinder user a Site Collection Administrator for your Default SSP Site

The SiteMinder user to which you granted personalization permissions also requires site collection administration privileges for your default SSP site.

To make the SiteMinder user a site collection administrator for your default SSP site

1. Click Start, Programs, Microsoft Office Servers, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the Application Management tab.

   The Application Management screen appears.

3. Click Site Collection Administrators.

   The Site Collection Administrators screen appears.

4. Verify that your default SSP site appears in the Site Collection drop-down list (in the upper right corner) and change it if necessary.

5. Add the SiteMinder user as a primary or secondary site collection administrator. Use the buttons to check the user name or browse for a user. and then click OK.

   The SiteMinder user becomes a site collection administrator.

How to protect your Default SSP Web Site with SiteMinder (r12.0 SP2)

To protect your Default SSP web site with SiteMinder, use the Administrative UI to complete following process:

1. Create a new Application to protect your Default SSP site with the following steps:
   a. Add your existing directory connection and authentication scheme for the new application. (see page 128)
   b. Add the following items as resources of your application (see page 129).
      - Add the Default SSP site as the resource of your Application.
      - Add the Agent Object or Agent Group that represents your protected SharePoint resources to the application.
   c. Add a role to your Application (see page 130).
   d. Create a Policy for your Application (see page 131).

Create a SiteMinder Application to Protect your SSP Sites

To protect your SharePoint SSP sites with the SiteMinder Agent for SharePoint, create an application with the Administrative UI.

To create an application to protect your SharePoint SSP sites

1. Click Policies, Applications, Application, Create Application.

   The Create Application: screen appears.

2. Enter a distinctive name, and (optional) description.
3. Verify that Web Agent appears in the Agent Type drop-down list.
4. Click the ellipsis button next to the Agent field.

   The Select Agent or Agent Group pane appears.

5. Click the button next to the Web Agent Group you created for the SharePoint SSP sites that you want to protect, and then click OK.

   Important! Do not add the URL or FQDN for your SharePoint Central Administration web site to any SiteMinder Agent groups, applications, or policies that protect resources. Leave the SharePoint Central Administration web site unprotected (by SiteMinder).

   The Create Application: *Name* pane reappears showing the name of your Web Agent object.

6. Click the Authentication Scheme drop-down list and select the authentication scheme you created for your SharePoint resources.
7. In the User Directories Group, click Add/Remove.

   The Choose User Directories dialog appears.

8. In the Available Members list, click the name of your SharePoint directory, and then click the right arrow.

   Your SharePoint user directory object appears in the Selected Members list.

9. Click OK.

   The Create Application: *Name* pane reappears showing the name of your Directory object.

10. Click Submit.

    The Create Application task is submitted for processing. A confirmation screen appears.

11. Click OK.

Add Resources to your Application

Define the SharePoint resources in your environment in a SiteMinder Policy before protecting them.

To add SharePoint resources to your application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add Resources to the application by doing the following:
   a. Click the Resource tab, and then click Create.

      The Create Application Resource: pane appears.

   b. Enter a distinctive name for the resource.

   c. Verify that the effective resource field contains the following:

      /*

   d. Under the Action group box, make sure that the Web Agent Actions radio button is selected, and then Control-click the following actions:

      - Get
      - Post
      - Put
      - Options
      - Head

      Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

   e. Click OK.

      The Create Application Resource: pane closes, and the Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation screen appears.
4. Click OK.

   The SharePoint resources are added to your SiteMinder Application.

Add Roles to your Application

To protect your SharePoint resources with SiteMinder, the SiteMinder application you create requires a role associated with the groups of users who are allowed to access those protected SharePoint resources.

To add a role to your SiteMinder application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add a Role to your Application by doing the following:
   a. Click the Roles Tab, and then click Create.

      The Create Role tab appears.

   b. Make sure the Create a new object of type Role radio button is selected, and then click OK.

      The Create Role: pane appears.

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

   d. Click the Expression field, and then type the following:

      ```
      (TRUE)
      ```

   e. Click OK.

      The Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation window appears.
4. Click OK.

   The role is added to your SiteMinder application.

Create a Policy for your Application

Your SiteMinder application requires a policy which grants the access rights with the associated SharePoint resources and the user role.

To create a policy for your application

1. Open the Application you created to protect your SharePoint resources by doing the following:

   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.

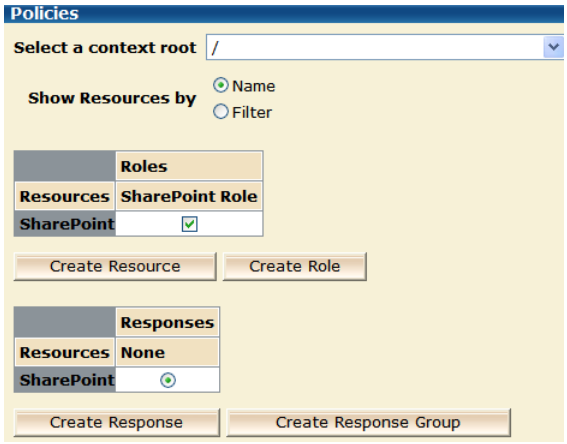
2. Click the Policies tab.

   The Policies screen appears.

3. Verify the following:

   - The Select a context root drop-down list shows the root level (/).
   - The Show Resources by Name option button is selected.

4. Locate the table that shows your SharePoint resources and roles, and then select the check box to grant access to the resources, as shown in the following illustration:



   Note: The drop-down list mentioned previously only appears when you have multiple resource items defined in the Administrative UI

5. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation pane appears.

6. Click OK.

   The policy for your SiteMinder application is created.

How to protect your Default SSP Web Site with SiteMinder (r6.x SP6)

To protect your Default SSP web site with SiteMinder, use the Policy Server User Interface to complete following process:

1. Create a domain, and then create the following items under that domain:
   - A realm
   - A rule
   - A policy

Create a SiteMinder Domain to protect your SSP Sites (r6.x SP6)

To protect your SharePoint SSP sites with the SiteMinder Agent for SharePoint, create a domain with the Policy Server User Interface.

To create a domain to protect your SSP sites

1. Click the Domains tab.
2. Right-click the top-level Domains item, and then select, Create Domain.

   The SiteMinder domain dialog appears.
3. Enter a distinctive name, and (optional) description.
4. Click the drop-down list and locate the directory connection you want. Click Add.

   The directory appears under the User Directories tab.
5. Click OK.

   The SiteMinder domain dialog closes and the domain for your SSP sites is created.

Create a Realm under your Domain to protect your SSP Sites (r6.x SP6)

Create a realm under your SharePoint domain for the SSP sites that you want to protect with the SiteMinder Agent for SharePoint.

To create a realm for your SSP sites

1. Click the Domains tab.

   The domain you created for your SharePoint resources appears.

2. Expand the domain.

   The following icons appear:

   - Realms
   - Responses
   - Policies

3. Right-click Realms, and then select Create realm.

   The SiteMinder realm dialog appears.

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

5. In the Resource tab, do the following:

   - Click Lookup and then add Agent Group you created for your protected SharePoint resources to the realm.
   - Click the drop-down list and then select the authentication scheme you created.

6. Click OK.

   The SiteMinder realm dialog closes and the realm for your SSP sites is created.

Create a Rule Under your Realm to protect your SSP Sites (r6.x SP6)

Your top-level SharePoint realm needs a rule which fires when a user requests access to a protected SSP site.

To create a rule under your SSP realm

1. Click the Domains tab, and then expand the domain you created for your SSP sites.
2. Right-click your SharePoint realm, and then select Create Rule Under Realm.

   The Rule Properties dialog appears.
3. Enter a distinctive name, and (optional) description.
4. In the Action field, Control-click the following:
   - Get
   - Post
   - Put
   - Head
   - Options

   The web agent actions are selected.
5. Verify the following settings:
   - The Resource field contains an asterisk (*).
   - The Allow Access option button is selected.
   - The Enabled check box is selected.
6. Click OK.

   The Rule Properties Dialog closes and the new rule for your SSP sites appears in the list.

Create a Policy under your Realm to protect your SSP Sites (r6.x SP6)

You need a SiteMinder policy associated the domain for your SSP site that defines relationships between the users, the SSP sites, and access rights in your organization.

To create a policy for your SharePoint resources

1. Click the Domains tab, and then expand your SharePoint domain.

   A list of objects appears.

2. Right-click Policies, and select Create Policy.

   The Policy Properties dialog appears showing the Users tab.

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

4. Click Add/Remove.

   The Users/Groups dialog appears.

5. Move the groups, users (or any combination of either) that you want to add from the Available Members list to the Current Members list, and then click OK.

   The users or groups are added to the policy.

6. Click the Rules tab, and then click Add/Remove Rules.

   The Available Rules dialog appears.

7. Move your SharePoint rule from the Available Members list to the Current Members list, and then click OK.

   The rule is added to the policy.

8. Click OK.

   The Policy Properties dialog closes and the policy for your SSP sites is saved.

Manually Update the web.config file for your Default SSP Web Site

The web.config file that corresponds to your default SSP web site in your SharePoint server needs the following sections that contain SiteMinder settings:

- Membership provider
- Role provider
- Session Management (HTTP) module

To manually update the web.config file for your default SSP web site

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

   The Internet Information Services (IIS) Manager opens.

2. Expand the Web Sites folder, and then locate your Default SSP Web Site.
3. Right-click your default SSP Web Site, and select Stop.

   The Default SSP Web site stops.

4. Right-click your default SSP Web site, and select Open.

   A new Explorer window opens.

5. Create a backup copy of the existing web.config file.
6. Locate the web.config file and open it with a text editor.

   Important! Do not use Notepad, Wordpad (or any other text editor with line-length limitations) to edit the .config (XML) files. A text editor that is designed for writing programming source code typically does not have such line-length limitations. For more information, see the documentation or online help for your respective editor.

7. Locate the following tags:

   ```
   <system.web>
   <securityPolicy>
   ```

8. Insert the following syntax between the previous tags:

   ```
   <membership defaultProvider="CAMemberProvider">
   <providers>
   <clear />
   <add name="CAMemberProvider"
   type="CA.SMMemberRoleProvider.SMMemberProvider,CA.SiteMinder.MemberRoleProvid
   er, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   </providers>
   </membership>
   <roleManager enabled="true" defaultProvider="CARoleProvider">
   <providers>
   <add name=" CARoleProvider "
   type="CA.SMMemberRoleProvider.SMRoleProvider,CA.SiteMinder.MemberRoleProvider
   , Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   ```

```
</providers>
</roleManager>
```

9. Locate the following line:

```
<add name="PublishingHttpModule"
type="Microsoft.SharePoint.Publishing.PublishingHttpModule,
Microsoft.SharePoint.Publishing, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />
```

10. Insert a new line after the previous line, and then add the following syntax:

```
<add name="SessionMgmtModule" type="CA.SPWebModule.SessionMgmtModule,
CA.SiteMinder.SPWebModule, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=29f091c10dd5f4a0" />
```

11. Save the web.config file and close the text editor.
12. Close the Explorer window.
13. Right-click your Default SSP Web Site in the IIS Manager, and select Start.

    The web config file for your Default SSP Web Site is updated.

Change the Authentication Provider of your Default SSP Web Site to Forms

Use the SharePoint Central Administration page to change the authentication provider used by your default SSP web site.

Change the SharePoint authentication provider for your default SSP web site using the SharePoint server

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Authentication Providers.

   The Authentication Providers page appears.

4. Verify that the URL of your default SSP site appears in the drop-down list on the right.

5. Click the link that corresponds to the zone of your default SSP site. For example, if your Default SSP web site is in the default zone, then click the Default link.

   The Edit Authentication page appears.

6. Click Forms.

7. Click the Membership Provider field and then enter the following:

   ```
   CAMemberProvider
   ```

8. Click the Role Manager field, and then enter the following:

   ```
   CARoleProvider
   ```

9. Click Save.

   The Authentication Providers page appears. The zone of your default SSP web site shows the updated membership provider name in the list.

Rename the Membership Provider in the web.config file for your Extended SSP Site

After configuring your extended SSP site, rename the membership provider in the web.config file of your *extended* SSP site. Choose whatever name you want for the extended SSP site, but use a unique name to avoid membership provider conflicts.

To manually update the web.config file for your extended SSP web site

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

   The Internet Information Services (IIS) Manager opens.

2. Expand the Web Sites folder, and then locate your extended SSP Web Site.
3. Right-click your extended SSP Web Site, and select Stop.

   The extended SSP Web site stops.

4. Right-click your extended SSP Web site, and select Open.

   A new Explorer window opens.

5. Create a backup copy of the existing web.config file.
6. Locate the web.config file and open it with a text editor.

   Important! Do not use Notepad, Wordpad (or any other text editor with line-length limitations) to edit the .config (XML) files. A text editor that is designed for writing programming source code typically does not have such line-length limitations. For more information, see the documentation or online help for your respective editor.

7. Locate the following section:

   ```
   <membership extendedProvider="CAMemberProvider">
   <providers>
   <clear />
   <add name="CAMemberProvider"
   type="CA.SMMemberRoleProvider.SMMemberProvider,CA.SiteMinder.MemberRoleProvid
   er, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   ```

8. Locate and rename the instances of the following membership provider name (within the previous seciton):

   ```
   "CAMemberProvider"
   ```

   For example, rename the membership provider to the following:

   ```
   "ExtSSPMemberProvider"
   ```

   Note: Record this setting for future reference.

9. Save the web.config file and close the text editor.
10. Close the Explorer window.
11. Right-click your extended SSP Web Site in the IIS Manager, and select Start.

The web config file for your extended SSP Web Site is updated.

Change the Membership Provider Name of the Extended SSP Site

After renaming the membership provider in the web.config file, update the name in the SharePoint Central Administration site.

To change the membership provider name of your extended SSP site

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Authentication Providers.

   The Authentication Providers page appears.

4. Verify that the URL of your default SSP site appears in the drop-down list on the right.

5. Click the link that corresponds to the zone of your Extended SSP site. For example, if your Extended SSP web site is in the default zone, then click the Default link.

   The Edit Authentication page appears.

6. Click Forms.

7. Click the Membership Provider field and then enter the new name of the membership provider you added to the web.config file. See the following example:

   ```
   ExtSSPMemberProvider
   ```

8. Click Save.

9. The Authentication Providers page appears. The zone of your extended SSP web site shows the updated membership provider name in the list.

Verify Access to the SSP Resources in SharePoint

Verify your access using CA Technologies SiteMinder, after configuring your SSP protection.

Verify access to the SSP resources in SharePoint

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the link for SharedServices in the left pane.

   A dialog appears and prompts you for credentials.

3. Enter the credentials of the site collection administrator.

   The SSP Administration page appears. Your access is verified.

How to Protect My Sites with SiteMinder (all versions)

To protect the SharePoint My Sites resources with SiteMinder, use the following process:

1. Protect the SSP sites with SiteMinder.
2. Change the URLs on the My Site Settings page to use fully qualified domain names.
3. Add the SiteMinder ISAPI filter to the IIS web site for your SharePoint My Site.
4. Do one of the following tasks:
   - For r12.0 SP2, use the SiteMinder Administrative UI to create an application to protect the My Site URL.
   - For r6.x SP6, use the Policy Server User Interface to create a Domain, realm, rule, and policy to protect the My Site URL.
5. Add the following items to the web.config file of the My Site:
   - CA Membership Provider
   - CA Role Provider
   - HTTP Session Manager Provider
   - Forms Authentication settings
6. Use the SharePoint Central Administration UI to do the following tasks:
   a. Change the authentication provider of your My Site to Forms.
   b. Add a SiteMinder user to your My Site host permissions.
   c. Add the SiteMinder user from Step 6b as a site collection administrator for My Site.
   d. Grant personalization-services permissions to the group name associated with the authenticated SiteMinder users.
   e. Grant policy for web application permissions to the group name associated with the authenticated SiteMinder users.

More information:

How to Protect the SharePoint SSP with SiteMinder r12.0 SP2 and FBA (see page 110)
Protect Applications with the SiteMinder Agent for SharePoint (see page 86)

Change the My Site Settings URLs to Fully Qualified Domain Names

To protect My Site resources with SiteMinder, all My Sites URLs require fully qualified domain names.

To change the My Site Settings URLs to fully qualified domain names

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The Central Administration page appears.

2. Click the link for SharedServices in the left pane.

   A dialog appears and prompts you for credentials.

3. Enter the credentials of the site collection administrator.

   The SSP Administration page appears.

4. Click My Site Settings.

   The My Site Settings page appears.

5. Change the URLs in the following fields to fully qualified domain names:

   - Preferred Search Center
   - Personal site provider

   Note: *my_web_site*.example.com is an example of a fully qualified domain name.

6. Click OK.

   The My Site Settings URLs are changed.

Add the SiteMinder ISAPI Filter to the IIS 6.0 Web Site for the My Site you want to Protect

The following SharePoint resources need a SiteMinder ISAPI filter installed on the corresponding virtual web site on the IIS web server:

- SharePoint Central Administration site.
- Any SharePoint web sites protected by SiteMinder.
- The Default and Extended SSP sites (optional).
- My Site web sites (optional).

To add the SiteMinder ISAPI filter to your SharePoint resources on an IIS 6.0 web server

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

   The Internet Information Services (IIS) Manager window opens.

2. In the left pane, expand your web server, and expand Web Sites folder.

   A list of web sites appears.

3. Right-click the SharePoint Central Administration v3 web site, and then select Properties.

   The Properties dialog appears.

4. Add the ISAPI filter by doing the following tasks:

   a. Click the Home Directory tab, and then click Configuration.

      The Application Configuration dialog appears.

   b. Click Insert.

      The Add/Edit Application Mapping dialog appears.

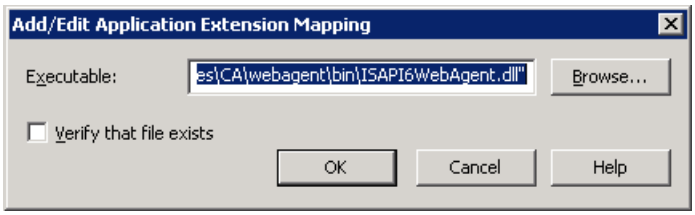
   c. Click Browse, and then locate the following file:

      `web_agent_home\bin\ISAPI6WebAgent.dll`

   d. Click Open.

      The ISAPI6WebAgent.dll file appears in the Executable field of the Add/Edit Application Mapping dialog.

   e. *Clear* the Verify that file exists check box as shown in the following illustration:



f. Click OK.

The Add/Edit Application Mapping dialog closes and the ISAPI6WebAgent.dll file appears in the Wildcard application maps (order of implementation) list.

g. Click Move Up until the ISAPI6WebAgent.dll file is at the top of the list.

h. Click OK.

The Inheritance Overrides dialog appears with a list of child nodes.

i. Click Select All, and then Click OK.

The Inheritance Overrides dialog and the Application Configuration dialogs close.

j. Click OK.

The Properties dialog closes. The SiteMinder ISAPI filter is added to the corresponding SharePoint web site on your IIS 6.0 web server.

5. Choose *one* of the following tasks:

- Right-click the web site folder of another SharePoint resource you want to protect, and then repeat Steps 4a through 4j, until all of the the following SharePoint sites you want to protect have the ISAPI filter installed.
  - Default SSP web site.
  - Extended SSP web site.
  - My Site web site.
- Stop after you have added the ISAPI filter to all the previous types of SharePoint sites.
-

Add the SiteMinder ISAPI Filter to the IIS 7.0 Web Site for the My Site you want to Protect

To run a SiteMinder Web Agent for SharePoint on IIS 7.0, add a SiteMinder ISAPI filter to each SharePoint resource you want to protect on the IIS 7.0 web server. This filter executes the Web Agent ISAPI scripts and other files. Place it before any other ISAPI filters on the web server.

To add the Agent ISAPI filter

1. Open the Internet Information Services (IIS) Manager.

   Note: If the User Account Control dialog appears, click Continue.

2. In the Connections pane, expand the web server.

   A Sites folder appears.

3. Expand the Sites folder, and then click the SharePoint web site you want to protect with SiteMinder.

4. Under the IIS section, double-click the ISAPI Filters icon.

   A list of the installed ISAPI Filters appears.

5. In the Actions pane, click Add.

   The Add ISAPI Filter dialog appears.

6. In the Filter Name field, type a name for the ISAPI Filter. We recommend using a name that is easy to recognize, such as "SiteMinder ISAPI Filter."

7. Click the ellipsis button (to the right of the Executable field).

   The Open dialog appears.

8. Navigate to the following file:

   web_agent_home\bin\ISAPI6WebAgentDLL

   web_agent_home

   Specifies the directory where the SiteMinder Web Agent is installed.

   Default: (r6.x SP6): C:\Program Files\netegrity\webagent

   Default: (r12.0 SP2): C:\Program Files\CA\webagent

9. Click Open.

   The ISAPI6WebAgentDLL.dll file appears in the Add ISAPI Filter dialog.

10. Click OK.

    The Add ISAPI Filter dialog closes and the ISAPI filter appears in the list.

11. In the Actions pane, click View Ordered List.

12. Right-click the SiteMinder ISAPI filter in the list, and then select Move up. Repeat this step until the SiteMinder ISAPI filter is at the top of the list.

The Agent ISAPI filter is added.

13. Repeat Steps 3 through 12 for each SharePoint web site you want to protect with SiteMinder.

Create a SiteMinder Application to Protect your My Site Resources (r12.0 SP2)

To protect your SharePoint My Site resources with the SiteMinder Agent for SharePoint, create an application with the Administrative UI.

To create an application to protect your SharePoint My Site resources

1. Click Policies, Applications, Application, Create Application.

   The Create Application: screen appears.

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

3. Verify that Web Agent appears in the Agent Type drop-down list.

4. Click the ellipsis button next to the Agent field.

   The Select Agent or Agent Group pane appears.

5. Click the button next to the Web Agent Group you created for the SharePoint My Site resources that you want to protect, and then click OK.

   Important! Do not add the URL or FQDN for your SharePoint Central Administration web site to any SiteMinder Agent groups, applications, or policies that protect resources. Leave the SharePoint Central Administration web site unprotected (by SiteMinder).

   The Create Application: *Name* pane reappears showing the name of your Web Agent object.

6. Click the Authentication Scheme drop-down list and select the authentication scheme you created for your SharePoint resources.

7. In the User Directories Group, click Add/Remove.

   The Choose User Directories dialog appears.

8. In the Available Members list, click the name of your SharePoint directory, and then click the right arrow.

   Your SharePoint user directory object appears in the Selected Members list.

9. Click OK.

   The Create Application: *Name* pane reappears showing the name of your Directory object.

10. Click Submit.

    The Create Application task is submitted for processing. A confirmation screen appears.

11. Click OK.

Add Resources to your Application

Define the SharePoint resources in your environment in a SiteMinder Policy before protecting them.

To add SharePoint resources to your application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add Resources to the application by doing the following:
   a. Click the Resource tab, and then click Create.

      The Create Application Resource: pane appears.

   b. Enter a distinctive name for the resource.

   c. Verify that the effective resource field contains the following:

      /*

   d. Under the Action group box, make sure that the Web Agent Actions radio button is selected, and then Control-click the following actions:

      - Get
      - Post
      - Put
      - Options
      - Head

      Note: Add PROPFIND to your list of methods if any of your Microsoft Office applications use the PROPFIND method to make requests to the web server.

   e. Click OK.

      The Create Application Resource: pane closes, and the Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation screen appears.
4. Click OK.

   The SharePoint resources are added to your SiteMinder Application.

Add Roles to your Application

To protect your SharePoint resources with SiteMinder, the SiteMinder application you create requires a role associated with the groups of users who are allowed to access those protected SharePoint resources.

To add a role to your SiteMinder application

1. Open the Application you created to protect your SharePoint resources by doing the following:
   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.
2. Add a Role to your Application by doing the following:
   a. Click the Roles Tab, and then click Create.

      The Create Role tab appears.

   b. Make sure the Create a new object of type Role radio button is selected, and then click OK.

      The Create Role: pane appears.

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

   d. Click the Expression field, and then type the following:

      ```
      (TRUE)
      ```

   e. Click OK.

      The Modify Application: Name pane appears.
3. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation window appears.
4. Click OK.

   The role is added to your SiteMinder application.

Create a Policy for your Application

Your SiteMinder application requires a policy which grants the access rights with the associated SharePoint resources and the user role.

To create a policy for your application

1. Open the Application you created to protect your SharePoint resources by doing the following:

   a. Click Policies, Applications, Application, Modify Application.

      The Modify Application pane appears.

   b. Click the button next to your SharePoint application, and then click Select.

      The Modify Application: *Name* pane appears.

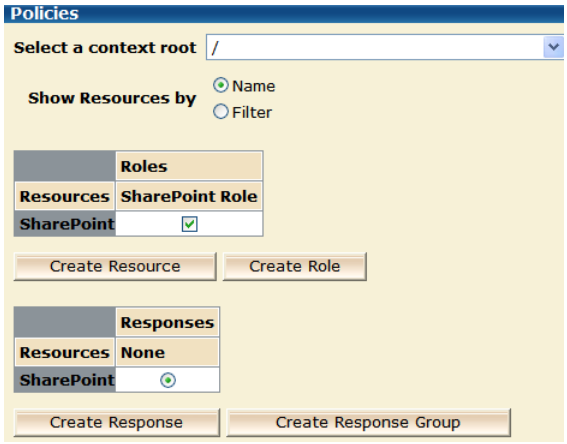
2. Click the Policies tab.

   The Policies screen appears.

3. Verify the following:

   - The Select a context root drop-down list shows the root level (/).
   - The Show Resources by Name option button is selected.

4. Locate the table that shows your SharePoint resources and roles, and then select the check box to grant access to the resources, as shown in the following illustration:



   Note: The drop-down list mentioned previously only appears when you have multiple resource items defined in the Administrative UI

5. Click Submit.

   The Modify Application task is submitted for processing, and then a confirmation pane appears.

6. Click OK.

   The policy for your SiteMinder application is created.

Create a SiteMinder Domain to protect your My Site URL (r6.x SP6)

To protect your My Site URL with the SiteMinder Agent for SharePoint, create a domain with the Policy Server User Interface.

To create a SiteMinder domain to protect your My Site URL

1. Click the Domains tab.
2. Right-click the top-level Domains item, and then select, Create Domain.

   The SiteMinder domain dialog appears.
3. Enter a distinctive name, and (optional) description.
4. Click the drop-down list and locate the directory connection you want. Click Add.

   The directory appears under the User Directories tab.
5. Click OK.

   The SiteMinder domain dialog closes and the domain for your My Site URL is created.

Create a Realm under your Domain to Protect your My Site URL (r6.x SP6)

Create a realm under your SharePoint domain for the My Site URL that you want to protect with the SiteMinder Agent for SharePoint.

To create a realm for your My Site URL

1. Click the Domains tab.

   The domain you created for your My Site URL appears.

2. Expand the domain.

   The following icons appear:

   - Realms
   - Responses
   - Policies

3. Right-click Realms, and then select Create realm.

   The SiteMinder realm dialog appears.

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

5. In the Resource tab, do the following:

   - Click Lookup and then add Agent Group you created for your protected SharePoint resources to the realm.
   - Click the drop-down list and then select the authentication scheme you created.

6. Click OK.

   The SiteMinder realm dialog closes and the realm for your My Site URL is created.

Create a Rule Under your Realm to Protect your My Site URL (r6.x SP6)

Your top-level SharePoint realm needs a rule which fires when a user requests access to a protected My Site URL.

To create a rule under your My Site realm

1. Click the Domains tab, and then expand the domain you created for your My site URL.
2. Right-click your SharePoint realm, and then select Create Rule Under Realm.

   The Rule Properties dialog appears.
3. Enter a distinctive name, and (optional) description.
4. In the Action field, Control-click the following:
   - Get
   - Post
   - Put
   - Head
   - Options

   The web agent actions are selected.
5. Verify the following settings:
   - The Resource field contains an asterisk (*).
   - The Allow Access option button is selected.
   - The Enabled check box is selected.
6. Click OK.

   The Rule Properties Dialog closes and the new rule for your My Site URL appears in the list.

Create a Policy under your Realm to protect your My Site URL (r6.x SP6)

You need a SiteMinder policy associated the domain for your My Site URL that defines relationships between the users, the My Site URL, and access rights in your organization.

To create a policy under your realm for your My Site URL

1. Click the Domains tab, and then expand your SharePoint domain.

   A list of objects appears.

2. Right-click Policies, and select Create Policy.

   The Policy Properties dialog appears showing the Users tab.

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

4. Click Add/Remove.

   The Users/Groups dialog appears.

5. Move the groups, users (or any combination of either) that you want to add from the Available Members list to the Current Members list, and then click OK.

   The users or groups are added to the policy.

6. Click the Rules tab, and then click Add/Remove Rules.

   The Available Rules dialog appears.

7. Move your SharePoint rule from the Available Members list to the Current Members list, and then click OK.

   The rule is added to the policy.

8. Click OK.

   The Policy Properties dialog closes and the policy for your My Site URL is saved.

Manually Update the web.config file of the My Site Resource

The web.config file that corresponds to your My Site resource in your SharePoint server needs the following sections that contain SiteMinder settings:

- Membership provider
- Role provider
- Session Management (HTTP) module

To manually update the web.config file for your My Site resource

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

   The Internet Information Services (IIS) Manager opens.

2. Expand the Web Sites folder, and then locate your My Site resource.
3. Right-click your My Site resource, and select Stop.

   The My Site resource stops.

4. Right-click your My Site resource, and select Open.

   A new Explorer window opens.

5. Create a backup copy of the existing web.config file.
6. Locate the web.config file and open it with a text editor.

   Important! Do not use Notepad, Wordpad (or any other text editor with line-length limitations) to edit the .config (XML) files. A text editor that is designed for writing programming source code typically does not have such line-length limitations. For more information, see the documentation or online help for your respective editor.

7. Locate the following tags:

   ```
   <system.web>
   <securityPolicy>
   ```

8. Insert the following syntax between the previous tags:

   ```
   <membership defaultProvider="CAMemberProvider">
   <providers>
   <clear />
   <add name="CAMemberProvider"
   type="CA.SMMemberRoleProvider.SMMemberProvider,CA.SiteMinder.MemberRoleProvid
   er, Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   </providers>
   </membership>
   <roleManager enabled="true" defaultProvider="CARoleProvider">
   <providers>
   <add name=" CARoleProvider "
   type="CA.SMMemberRoleProvider.SMRoleProvider,CA.SiteMinder.MemberRoleProvider
   , Version=1.0.0.0, Culture=neutral, PublicKeyToken=e9a76eb29817bc54" />
   ```

```
</providers>
</roleManager>
```

9. Locate the following line:

```
<add name="PublishingHttpModule"
type="Microsoft.SharePoint.Publishing.PublishingHttpModule,
Microsoft.SharePoint.Publishing, Version=12.0.0.0, Culture=neutral,
PublicKeyToken=71e9bce111e9429c" />
```

10. Insert a new line after the previous line, and then add the following syntax:

```
<add name="SessionMgmtModule" type="CA.SPWebModule.SessionMgmtModule,
CA.SiteMinder.SPWebModule, Version=1.0.0.0, Culture=neutral,
PublicKeyToken=29f091c10dd5f4a0" />
```

11. Save the web.config file and close the text editor.
12. Close the Explorer window.
13. Right-click your My Site resource in the IIS Manager, and select Start.

    The web config file for your My Site resource is updated.

Change the Authentication Provider of your My Site Resource to Forms

Use the SharePoint Central Administration page to change the authentication provider used by your My Site resource.

Change the SharePoint authentication provider for your My Site resource using the SharePoint server

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page opens.

2. Click the Application Management tab.

   The Application Management page appears.

3. Click Authentication Providers.

   The Authentication Providers page appears.

4. Verify that the URL of your My site appears in the drop-down list on the right.

5. Click the link that corresponds to the zone of your My Site site. For example, if your My Site resource is in the default zone, then click the Default link.

   The Edit Authentication page appears.

6. Click Forms.

7. Click the Membership Provider field and then enter the following:

   ```
   CAMemberProvider
   ```

8. Click the Role Manager field, and then enter the following:

   ```
   CARoleProvider
   ```

9. Click Save.

   The Authentication Providers page appears. The zone of your My Site resource shows the updated membership provider name in the list.

Add a SiteMinder User to your My Site Host Permissions

Adding a SiteMinder user to the My Site host permissions grants access to the protected My Site resources.

To add a SiteMinder User to your My Site Host Permissions

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration page appears.

2. Click the link for SharedServices in the left pane.

   A dialog appears and prompts you for credentials.

3. Enter the credentials of the site collection administrator.

   The SSP Administration page appears.

4. Click the My Site Host Permissions link in the left pane.

   The My Site page appears.

5. Click Set as My Site Host.

   The SiteMinder user is granted My Site host permissions, and a new My Site is created for the SiteMinder user.

Make the SiteMinder user a Site Collection Administrator for your My Site Resource

The SiteMinder user to which you granted My Site Host permissions also requires site collection administration privileges for your My Site resource.

To make the SiteMinder user a site collection administrator for your My Site resource

1. Click Start, Programs, Microsoft Office Servers, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the Application Management tab.

   The Application Management screen appears.

3. Click Site Collection Administrators.

   The Site Collection Administrators screen appears.

4. Verify that your My Site resource appears in the Site Collection drop-down list (in the upper right corner) and change it if necessary.

5. Add the SiteMinder user as a primary or secondary site collection administrator. Use the buttons to check the user name or browse for a user. and then click OK.

   The SiteMinder user becomes a site collection administrator.

Grant Personalization Services Permissions to the Group Associated with your SiteMinder Authenticated Users

The SiteMinder users who access My Sites in SharePoint need personalization services permissions, so that a My Sites link appears in their browsers. Use the SharePoint Central Administration UI to assign permissions to the group name specified in the value of the following parameter:

SPAuthenticatedGroup

Identifies the group to which SiteMinder users who authenticate using forms-based authentication through the Agent for SharePoint belong.

Default: (value) SMAuthenticatedGroup

Default: (state) Disabled

Note: We recommend confirming the value of this parameter in your Agent Configuration object before continuing.

To grant personalization services permissions to the group associated with your SiteMinder authenticated users

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click the link for your Shared Services Provider that you previously protected with SiteMinder.

   The Shared Services Administration screen appears.

3. Click Personalization Services Permissions.

   The Manage Permissions: Shared Service Rights screen appears.

4. Click Add Users/Groups.

   The Add Users/Groups: Shared Service Rights screen appears.

5. Click the Users/Groups field of the People Picker, and then type the name of the group that is specified in the SPAuthenticatedGroup Web Agent parameter. Use the buttons to verify the name or to browse for the group.

6. Select the following check boxes:

   - Create personal site
   - User personal features

7. Click Save.

   The Manage Permissions: Shared Service Rights screen appears, the group appears in the list.

Grant Policy for Web Application Permissions to the Group Associated with your SiteMinder Authenticated Users

The SiteMinder users who access My Sites in SharePoint need policy for web application permissions, so they can create their own personal site collections using the My Site link. Use the SharePoint Central Administration UI to assign permissions to the group name specified in the value of the following parameter:

SPAuthenticatedGroup

Identifies the group to which SiteMinder users who authenticate using forms-based authentication through the Agent for SharePoint belong.

Default: (value) SMAuthenticatedGroup

Default: (state) Disabled

Note: We recommend confirming the value of this parameter in your Agent Configuration object before continuing.

To grant policy for web application permissions to the group associated with your SiteMinder authenticated users

1. Click Start, Programs, Microsoft Office Server, SharePoint 3.0 Central Administration.

   The SharePoint Central Administration screen appears.

2. Click Application Management.

   The Application Management screen appears.

3. Click Policy for Web Application.

   The Policy for Web Application screen appears.

4. Verify that the URL of the My Site you protected with SiteMinder appears in the Web application drop-down list.

5. Click Add Users.

   The Add Users screen appears.

6. (Optional) Click the Zones drop-down list and select the zone you want.

7. Click Next.

   The following sections appear:

   - Choose users
   - Choose permissions
   - Choose system settings

8. Type the name of the group specified in the value of the SPAuthenticated group parameter in the Users field. Use the buttons to verify the name or browse directly for the group you want.

9. Select the Full Control check box, and then click Finish.

   The Policy for Web Application screen appears and the permissions are granted.

Chapter 9: Upgrade your SiteMinder Agent for SharePoint

This section contains the following topics:

Upgrade your SiteMinder Agent for SharePoint

An upgrade occurs when the installer for the SiteMinder Agent for SharePoint detects that its version of the software is newer than the version that exists on the web server. The existing files on the web server are upgraded. For example, if you previously installed version r12.0.2.100 and you run the installation wizard for version r12.0.3.200 the older version of the SiteMinder Agent for SharePoint is replaced with the newer version.

To upgrade your SiteMinder Agent for SharePoint

1. Download the installation file to a temporary directory on your web server.
2. Run the following file:

   `ca-sp-`*`version-operating_environmentprocessor_type`*`.exe`

   version

   Indicates the version of the SiteMinder component.

   Example: 12.0

   operating_environment

   Indicates the abbreviation for the operating environment on which the file runs.

   Example: win represents Microsoft Windows

   Example: sol represents Solaris

   processor_type

   Indicates the type of processor that is compatible with the file.

   Example: 32 corresponds to 32-bit processors

   Example: 64 corresponds to 64-bit processors

   Note: Some products (such as the SiteMinder Web Agent) have separate files for the 32-bit and 64-bit versions of the product. Other products (such as the SiteMinder Agent for SharePoint) use a single file labeled 32-bit for *both* the 32-bit and 64-bit versions. See the Platform Support matrix on http://ca.com/support to determine if your product supports a 64-bit operating environment.

   The wizard opens.
3. Follow the prompts to complete the wizard.

   Your SiteMinder Agent for SharePoint is upgraded.

Chapter 10: Migrating from Previous SiteMinder SharePoint Solutions to the SiteMinder Agent for SharePoint

This section contains the following topics:

Migration Scenarios

Use migration to change from one of the following SiteMinder products to the SiteMinder Agent for SharePoint:

- SiteMinder and Windows Web Server Identity (WWSI)
- SiteMinder SSO with FBA

Migration differs from an upgrade, which is when a more-recent version of the Agent for SharePoint is installed over an older version on a computer.

How to Migrate from SiteMinder SSO & FBA (r6.x SP5 CRx) to the SiteMinder Agent for SharePoint r6.x SP6

This section provides a high-level overview of the procedures necessary to migrate to the SiteMinder Agent for SharePoint. To migrate from SiteMinder SSO & FBA (r6.x SP5 CRx) to the SiteMinder Agent for SharePoint r6.x SP6, use the following process:

1. Verify that the versions of the following components support the SiteMinder Agent for SharePoint:
   - Policy Server
   - Web Agent
2. If necessary, upgrade the previous components to compatible versions.
3. Add the following actions to the SiteMinder Web Agent type:
   - Head
   - Options
4. Modify the directory connection in your Policy Server to use the proper user attributes.
5. (For FBA only). Configure virtual attribute mappings.to the directory specified in your directory connection.
6. Modify your existing authentication scheme to use any supported method you want. For example, you can change the authentication scheme to use basic authentication to replace the FCC scheme used with the previous SharePoint implementation.
7. Delete the following unprotected realms:
   - _vti_bin
   - _vti_inf
   - _layouts
8. Change the following settings in your Agent Configuration object:
   a. Add the SPVirtualAttributeMapList parameter, and set the value to reflect the virtual attribute mappings.
   b. Set the value of the LogoffURI parameter to the following:

      ```
      /_layouts/SPSignout.aspx /_layouts/SPRedirector.aspx
      ```

   c. Delete the following parameter:

      ```
      autoauthorizeoptions
      ```

9. Install the SiteMinder Agent for SharePoint (which includes the Management UI).
10. Use the SiteMinder Management UI to do the following tasks:
    a. Protect your applications.

b. Migrate Users.

c. Import User Profiles (MOSS only).

How to Migrate from SiteMinder SSO & FBA (r12.0 SP1) to the SiteMinder Agent for SharePoint r12.0 SP2

This section provides a high-level overview of the procedures necessary to migrate to the SiteMinder Agent for SharePoint. To migrate from SiteMinder SSO & FBA (r12.0 SP1) to the SiteMinder Agent for SharePoint r12.0 SP2, use the following process:

1. Verify that the versions of the following components support the SiteMinder Agent for SharePoint:
   - Policy Server
   - Web Agent
2. If necessary, upgrade the previous components to compatible versions.
3. Add the following actions to the SiteMinder Web Agent type:
   - Head
   - Options
4. Modify the directory connection in your Policy Server to include the following:
   - User attributes
   - Virtual attribute mappings
5. Configure virtual attribute mappings.to the directory specified in your directory connection.
6. Modify your existing authentication scheme to use any supported method you want. For example, you can change the authentication scheme to use basic authentication to replace the FCC scheme used with the previous SharePoint implementation.
7. Delete the following unprotected realms:
   - _vti_bin
   - _vti_inf
   - _layouts
8. Change the following settings in your Agent Configuration object:
   a. Add the SPVirtualAttributeMapList parameter, and set the value to reflect the virtual attribute mappings.
   b. Set the value of the LogoffURI parameter to the following:

      ```
      /_layouts/SPSignout.aspx /_layouts/SPRedirector.aspx
      ```

   c. Delete the following parameter:

      ```
      autoauthorizeoptions
      ```
9. Install the SiteMinder Agent for SharePoint (which includes the Management UI).
10. Use the SiteMinder Management UI to do the following tasks:

a. Protect your applications.

b. Migrate Users.

c. Import User Profiles (MOSS only).

How to Migrate from WWSI to the SiteMinder Agent for SharePoint

To migrate from the previous WSS solution to the SiteMinder Agent for SharePoint, use the following process:

1. Remove the WWSIISAPI.DLL file from your IIS web server.
2. Prepare your web server.
3. Install the SiteMinder Agent for SharePoint on your web server.
4. Protect the SharePoint applications on your web server with the SiteMinder Management UI.

Remove the WWSIISAPI.DLL File from your IIS Web Server

Remove the WWSIISAPI.DLL file from your IIS Web Server before installing the SiteMinder Agent for SharePoint.

To remove the WWSIISAPI.DLL file from your IIS Web Server

1. Open the IIS Manager.
2. In the left pane, expand the web server, then expand the Web Sites folder.

   A list of web sites appears.
3. Right click a web Site you want to protect with SiteMinder and select Properties.

   The Properties dialog for the web site appears.
4. Click the Home Directory tab, and then click Configuration.

   The Application Configuration dialog appears.
5. In the Wildcard Application Maps (order of implementation) list, click the following file:

   web_agent_home\bin\WWSIISAPI.DLL
6. Click Remove.

   A confirmation dialog appears.
7. Click Yes.

   The confirmation dialog closes and the WWSIISAPI.DLL file is removed.
8. Restart your IIS web server.

More information:

Preparing your SharePoint Server Roadmap (see page 66)
How to Install your SiteMinder Agent for SharePoint (see page 77)
Protect Applications with the SiteMinder Agent for SharePoint (see page 86)

Chapter 11: Removing the SiteMinder Agent for SharePoint

This section contains the following topics:

Remove the SiteMinder Agent for SharePoint

You can remove the SiteMinder Agent for SharePoint from your web server.

To remove the SiteMinder Agent for SharePoint

1. Click Start, Settings, Control Panel, Add/Remove Programs.

   The Add or Remove Programs list appears.

2. Click the CA Technologies SiteMinder Agent for SharePoint, and then click Change/Remove.

   The wizard starts.

3. Click Uninstall.

   A progress bar appears while the wizard runs.

4. Click Done.

   The wizard closes. The SiteMinder Agent for SharePoint is removed.

   Note: Remove the IIS web site associated with the Management UI if you want to use the port number of the Management UI for another purpose in the future.

Chapter 12: Troubleshooting the SiteMinder Agent for SharePoint

This section contains the following topics:

Web Agent for SharePoint Does Not Honor PersistantIPCheck Parameter

Symptom:

I use The Agent for SharePoint 2007 with an Apache reverse proxy server. The Agent does not honor the PersistantIPCheck ACO parameter with a value of No.

Solution:

Set the value of the PersistentIPCheck parameter to No, and then set the value of the sppersistentipcheck parameter to No. Setting the sppersistentipcheck to No skips persistent IP check for the SPSESSION cookie.

Installation Log Location

Symptom:

I tried to install the Agent for SharePoint, but I received the following error message from the installation wizard:

```
"An error occurred while creating the SharePoint UI solution"
```

Solution:

Examine the following log file to determine the cause and corrective actions:

web_agent_home\sharepoint-agent\install_config_info\SharePointUI.log

web_agent_home

Specifies the directory where the SiteMinder Web Agent is installed.

Default: (r6.x SP6): C:\Program Files\netegrity\webagent

Default: (r12.0 SP2): C:\Program Files\CA\webagent

Access denied

Reason:

The user account which ran the installation wizard does not have sufficient privileges to install the Agent for SharePoint.

Action:

The user account that installs the Agent for SharePoint requires the following privileges:

- SharePoint administrator (for installation on a stand-alone SharePoint server)
- SharePoint server farm administrator (for installation on a SharePoint server farm)
- Administrator on the local computer.

Login failed for user ' '. The user is not associated with a trusted SQL Server connection.

Valid for SQL Authentication

Reason:

The user you entered for SQL Authentication was not recognized by the Microsoft SQL Server.

Action:

Verify that the account you want is has sufficient privileges on the SQL Server .

The password supplied with the username " " was not correct. Verify that it was entered correctly and try again

Reason:

The password associated with the user account was not correct.

Action:

Verify the correct user account name and password and install the Agent for SharePoint.

stsadm.exe Access Denied

Valid on Windows Server 2008

Symptom:

When trying to install or remove the Agent for SharePoint, I see an error that resembles the following:

```
c:\Program Files\Common Files\Microsoft Shared\Web Server
Extensions\12>bin\stsadm.exe

Access denied.
```

Solution:

Run the executable as an administrator.

Users are challenged for Credentials when Office Client Integration is Configured

Symptom:

I configured Office Client integration, but users are still challenged for their credentials when they try to access a Microsoft Office document.

Solution:

Add the following methods to the SiteMinder Web Agent type with the Administrative UI:

- Head
- Options

More information:

Update the SiteMinder Agent Types for your SharePoint Resources (r12.0 SP2) (see page 20)

Changes to Agent Configuration Parameters not seen after Restarting IIS Web Server

Symptom:

I changed a configuration parameter for my SiteMinder Agent for SharePoint, and then restarted my IIS web server, but the behavior of the Agent for SharePoint is not reflecting the change I made.

Solution:

If you have finished setting the configuration parameters for your SiteMinder Agent for SharePoint, apply the configuration changes by restarting the following Windows service on your web server:

```
Windows SharePoint Services Timer
```

To apply Web Agent configuration changes

1. Click Start, Programs, Administrative Tools, Services.

   The Services screen appears.

2. Click the following service:

   ```
   Windows SharePoint Services Timer
   ```

   The Service is selected.

3. Click Restart the service.

   The Windows SharePoint Services Timer service restarts.

Users Challenged Again when Accessing Office Document on SharePoint

Symptom:

Users who previously authenticated using SiteMinder are challenged for their credentials in any of the following situations:

- When they try to access office documents for which they are authorized on the SharePoint server.
- When they are working in an open document for which they are authorized on the SharePoint server.

This behavior usually occurs when using the following SiteMinder authentication schemes:

- Basic authentication
- Windows authentication

With other SiteMinder authentication schemes, the challenge can appear within the Microsoft Office document itself.

Solution:

The users are getting challenged because their session has expired. If you feel these challenges happen too often, you can change the session timeout intervals using either of the following:

- Administrative UI (r12.0 SP2)
- Policy Server User Interface (r6.x SP6)

More information:

Office Client Integration without a Persistent Cookie (see page 204)

CA Technologies SiteMinder Agent for SharePoint is already installed

Symptom:

When I try to install the SiteMinder Agent for SharePoint, the wizard exits with the following error message:

```
CA Technologies SiteMinder Agent for SharePoint is already installed.
```

Solution:

This happens because the installation program detects that the same version of the SiteMinder Agent for SharePoint was previously installed on the computer. The installation program does not currently support re installing the same version of the Agent for SharePoint.

As a workaround, do the following:

1. Remove the SiteMinder Agent for SharePoint.
2. Install the same version of the SiteMinder Agent for SharePoint.

Unexpected Error Screen Appears After Clicking the SiteMinder Management Tab

Symptom:

I installed the SiteMinder Management UI, but when I try to open it from the SharePoint Central Administration UI, I see an error message instead.

Solution:

This happens when a virtual folder with the same port number as the Management UI exists in the following directory:

```
C:\inetpub\wwwroot\wss\VirtualDirectories\
```

For example, if a folder named 65534 exists in the previous directory, and you specify port number 65534 when you install the Agent for SharePoint, the error appears.

Do the following:

1. Remove the Agent for SharePoint.
2. Remove the directory.
3. Re install the Agent for SharePoint.

Problems Following SharePoint Farm Administrator Password Change

Symptom:

The password of the SharePoint farm administrator recently changed, and problems with the SharePoint Central Administration UI and the SiteMinder Management UI are occurring.

Solution:

Add the new SharePoint farm administrator password to any application pools associated with your SharePoint environment.

Add the Updated SharePoint Farm Administrator Password to the Application Pool in IIS 6.0

When the password of the SharePoint farm administrator changes, change it in any application pools associated with your SharePoint environment.

To add the updated SharePoint farm administrator password to the application pool in IIS 6.0

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

   The Internet Information Services (IIS) Manager appears.

2. Expand Application Pools.

   A list of application pools appears.

3. Right-click the application pool you want, and then select Properties.

   The Properties dialog appears.

4. Click the Identity tab.

   The Application pool identity properties appear.

5. Select the password field, type the new password for the SharePoint farm administrator, and then press Enter.

   The Confirm Password dialog appears.

6. Type the new password again and then click OK.

   The Confirm password dialog and the application pool properties dialog close. The password is updated.

7. Repeat Steps 3 though 6 for any other application pools in your SharePoint environment.

Add the Updated SharePoint Farm Administrator Password to the Application Pool in IIS 7.0

When the password of the SharePoint farm administrator changes, change it in any application pools associated with your SharePoint environment.

To add the updated SharePoint farm administrator password to the application pool in IIS 7.0

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

   Note: If the User Account Control dialog appears, click Continue.

   The Internet Information Services (IIS) Manager appears.

2. Expand the web server, and then click Application Pools.

   A list of application pools appears.

3. Right-click the application pool you want, and then select Advanced Settings.

   The Advanced Settings dialog appears, with a table of settings.

4. Under the Process model section, click Identity.

   An ellipsis button appears on the right of the row.

5. Click the ellipsis button.

   The Application Pool Identity dialog appears.

6. Click Set.

   The Set Credentials dialog appears.

7. Enter the user name for the account, the new password, and then confirm the password.

8. Click OK *twice*.

   The Set Credentials and the Application Pool Identity dialogs close.

9. Click OK.

   The Advanced Settings dialog closes.

10. Repeat Steps 3 though 9 for any other application pools in your SharePoint environment.

Agent for SharePoint Configuration Settings Missing

Symptom:

I tried to create an Agent Configuration Object for my Agent for SharePoint, but I do not see the SharePointDefaultSettings item that is mentioned in the instructions.

Solution:

Your policy store was not upgraded. To add the Agent for SharePoint configuration settings, upgrade your policy store to one of the following versions:

- r12.0 SP2 (for r12.0 environments)
- r6.x SP6 (for r6.x environments)

More information:

Upgrade your Policy Store (see page 19)

Error freeing profile buffer message in trace logs when using Windows Impersonation

Symptom:

I configured Windows Impersonation for my Agent for SharePoint, but it is not working. The following message appears in the Agent for SharePoint trace log file:

```
Error freeing profile buffer. Error is Attempt to access invalid address.
```

Solution:

To use Windows Impersonation across multiple domains (such as in an Active Directory forest with two-way trust among the domains), the application pool identity used for Windows impersonation requires a domain account.

LSA required for impersonation has failed to initialize error in trace logs when using Windows Impersonation

Symptom:

I configured Windows Impersonation for my Agent for SharePoint, but it is not working. The following message appears in the Agent for SharePoint trace log file:

```
LSA required for impersonation has failed to initialize. No impersonation is being performed.
```

Solution:

Verify that Integrated Windows Authentication is *disabled* in the IIS Manager for *each* SharePoint Web Application that you want to protect with Windows Impersonation.

IIS 6.0 Changes made by the SiteMinder Management UI

Symptom:

I need to troubleshoot my IIS 6.0 web server. What changes did the Agent for SharePoint make when I protected my web application with the SiteMinder Management UI?

Solution:

The following table shows the changes made to an IIS 6.0 web server when the Management UI protects a SharePoint web application with SiteMinder:

Windows Impersonation	FBA
Enables Anonymous Authentication for the web application. Adds the following wildcard mapping (first in the list) for each web application that is being protected: ■ Absolute path to ISAPI6WebAgent.dll ■ Clears the verify that file exists check box	Enables Anonymous Authentication for the web application. Enables FBA for the web application.
Adds the following wildcard mapping (second in the list) of each web application that is being protected: ■ Absolute path to SPWindowsImpersonation.dll ■ Clears the verify that file exists check box	Adds the following wildcard mapping (first in the list) for each web application that is being protected: ■ Absolute path to ISAPI6WebAgent.dll ■ Clears the verify that file exists check box

Adds the following web service extension:

- Name: SiteMinder Web Agent
- Executable: ISAPI6WebAgent.dll
- Status: Allowed

Adds the following wildcard mapping (second in the list) of each web application that is being protected:

- Absolute path to SPWindowsImpersonation.dll
- Clears the verify that file exists check box

Adds the following wildcard mapping (first in the list) for the SharePoint Central Administration web application:

- Absolute path to ISAPI6WebAgent.dll
- Clears the verify that file exists check box

Adds the following web service extension:

- Name: SiteMinder Web Agent
- Executable: ISAPI6WebAgent.dll
- Status: Allowed

Adds the following wildcard mapping (first in the list) for the SharePoint Central Administration web application:

- Absolute path to ISAPI6WebAgent.dll

Clears the verify that file exists check box

IIS 7.0 Changes made by the SiteMinder Management UI

Symptom:

I need to troubleshoot my IIS 7.0 web server. What changes did the Agent for SharePoint make when I protected my web application with the SiteMinder Management UI?

Solution:

The following table shows the changes made to an IIS 7.0 web server when the Management UI protects a SharePoint web application with SiteMinder:

Windows Impersonation	**FBA**
Enables Anonymous Authentication for the web application	Enables Anonymous Authentication for the web application
Adds the following handler mapping (first in the list) for each web application being protected: ■ Request path: * ■ Executable: absolute path of ISAPI6WebAgent.dll ■ Name: SiteMinder Web Agent	Enables FBA for the web application
Adds the following handler mapping (second in the list) for each web application being protected: ■ Request path: * ■ Executable: absolute path of SPWindowsImpersonation.dll ■ Name: SiteMinder Windows Impersonation	Adds the following handler mapping (first in the list) for each web application being protected: ■ Request path: * ■ Executable: absolute path of ISAPI6WebAgent.dll ■ Name: SiteMinder Web Agent
Adds the following ISAPI filter for each web application being protected: ■ Name: SiteMinder Web Agent ■ Executable: absolute path of ISAPI6WebAgent.dll	Adds the following ISAPI filter for each web application being protected: ■ Name: SiteMinder Web Agent ■ Executable: absolute path of ISAPI6WebAgent.dll
Adds the following handler mapping (first in the list) for the Central Administration web application: ■ Request path: * ■ Executable: absolute path of ISAPI6WebAgent.dll ■ Name: SiteMinder Web Agent	Adds the following handler mapping (first in the list) for the Central Administration web application: ■ Request path: * ■ Executable: absolute path of ISAPI6WebAgent.dll ■ Name: SiteMinder Web Agent

Adds the following ISAPI filter for the Central Administration web application:

- Name: SiteMinder Web Agent
- Executable: absolute path of ISAPI6WebAgent.dll

Disables kernel authentication for the Central Administration web application.

Adds the following ISAPI filter for the Central Administration web application:

- Name: SiteMinder Web Agent
- Executable: absolute path of ISAPI6WebAgent.dll

Disables kernel authentication for the Central Administration web application.

Appendix A: SiteMinder Agent for SharePoint Parameters

This section lists the configuration parameters for the SiteMinder Agent for SharePoint.

SPAuthenticatedGroup

Identifies the group to which SiteMinder users who authenticate using forms-based authentication through the Agent for SharePoint belong.

Default: (value) SMAuthenticatedGroup

Default: (state) Disabled

More information:

Create a Global Policy for your Forms Based SharePoint Users (see page 201)

SPAuthorizeUserAgent

Specifies a list of Microsoft Office user-agents for which the SiteMinder Agent for SharePoint allows access. This list is populated automatically when the Agent for SharePoint starts. Changes to the list made with the Administrative UI (for r12.0 SP2) or Management UI (for r6.x SP6), override the default settings.

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 Front Page, Microsoft Data Access Internet Publishing Provider Protocol Discovery, Test for Web Form Existence

Limits: Multiple values allowed.

SPCacheEntryExpireMinute

Specifies the number of minutes that the user and group information obtained from the SiteMinder Policy Server remains in the cache. When this interval expires, the Agent for SharePoint contacts the SiteMinder Policy Server to obtain the user and group information.

Limit: 1

Default: 30

More information:

Adjust the Agent for SharePoint Cache Settings (see page 202)

SPClientIntegration

Specifies a list of protected SharePoint resources where Office Client Integration is enabled. In most situations, the settings for this parameter are determined automatically from the setting in the SharePoint Central Administration UI.Each URL in this parameter *requires* a port number (even for a default port such as 80 or 443).

If you are protecting your SharePoint resources using the SiteMinder Secure Proxy Server or an Apache Reverse Proxy server, add the request URLs to this parameter manually. For deployments of the Agent for SharePoint on a Reverse Proxy server, the port numbers are *not* required.

Example: *host_name*:*port_number*

Limits: Port numbers required for typical Agents. Omit port numbers for reverse proxy deployments.

More information:

Enable Office Client Integration for a Reverse Proxy (see page 107)

SPDisableClientIntegration

Specifies a list of protected SharePoint URLs where Office Client Integration will be blocked, regardless of the setting in the SharePoint Central Administration UI. Add the port number if you are *not* using a default port (such as 80 or 443).

Use this setting to override the settings of the SharePoint Central Administration UI to prevent SharePoint administrators from circumventing SiteMinder settings regarding Office Client integration.

Example: *host_name*:*port_number*

More information:

Prohibit Office Client Integration with the SiteMinder Agent for SharePoint (see page 204)

SPDisambiguateGroup

Reserved for future use. Do *not* enable or change this parameter.

Default: No

SPDisambiguateGroupRule

Reserved for future use. Do *not* enable or change this parameter.

Default: $groupname{$directoryname}

SPDisambiguateUser

Enables user level disambiguation, which avoids duplicate users, when searching multiple SharePoint directories. The value of the SPDisambiguateUserRule parameter specifies the name of the directory as defined in the SiteMinder Policy Server.

Default: Yes (enabled)

SPDisambiguateUserRule

Specifies the format of the user name and the name of the directory connection defined in the SiteMinder Policy Server that is associated with your SharePoint users. The user name format should follow the convention in your organization. For example, if your user names are a first initial and last name without a space, then use the following:

$*user_first_initalUser_Last_Name*{$*directory_name*}

These settings are used to resolve any users found in multiple directories to the directory you specify. Use any special character such as braces {} except comma (,) semicolon (;) and colon (:) to separate the directory name from the user name.

Default: $*user_name_format*{$*directory_name*}

Example:
$*user_first_initalUser_Last_Name*{$*SharePoint_Directory_Connection_in_SiteMinder*}

Note: If you change the value of this parameter, restart your IIS web server, and then migrate your users again (to retain their profile settings).

SPEnableImpersonation

Lists the URLs of the SharePoint web applications for which Windows impersonation is used.

Example: *server_name.domain_name:port_number*

Default: None (Windows Impersonation *not* used).

More information:

Set the Web Agent Parameters for Impersonation (r12.0 SP2) (see page 44)

SPImpersonateResponseVarName

Specifies the name of a Response variable created in SiteMinder which is mapped to a UserPrincipalName attribute of the user in an Active directory server and assigned as a response to the SiteMinder policy.

Default: None

More information:

Set the Web Agent Parameters for Impersonation (r12.0 SP2) (see page 44)

SPNumCacheItem

Specifies the number user and group items contained in the Agent for SharePoint cache. If this value is too low, the Agent for SharePoint contacts the SiteMinder Policy Server to obtain user and group information instead of placing the items in the cache. If this value is too high, the cache could consume more resources than necessary on the SharePoint system. Changing the value of this parameter to zero disables the cache.

Limit:1

Default: 1000

More information:

Adjust the Agent for SharePoint Cache Settings (see page 202)

SPRequestTimeout

Specifies the ASP.NET request timeout value in seconds. Use this parameter to avoid request time-outs in situations where the SiteMinder Management UI takes a long time to change the configuration of a web application.

Default: Disabled (timeout interval equals twice the value of the ASP.NET timeout)

SPSortVirtualAttribute

Specifies the name of the Virtual attribute defined in the user directory connection of the SiteMinder Policy Server. Set this attribute before importing or modifying user profiles.

Default: UniversalID

Example: (Active Directory) sAMAccountName

SPToolsLogLocation

Specifies the directory for the log and trace files created during the following operations:

- Application Protection
- User Migration
- User Profile Import
- UI Dashboard data population

Default: *web_agent_home*\log

More information:

Specify the Location of your Agent for SharePoint Log Files (see page 203)

SPVirtualAttributeMapList

Contains a group of virtual user attributes which are mapped to existing user attributes in the user directory connection defined in the SiteMinder Policy Server. The following attributes are available:

- group = *group_name_attribute*
- email = *email_address_attribute*
- username = *user_name_attribute*
- displayname = *display_name_attribute*

Default: email=Email group=GroupID username=UniversalID displayname=DisplayName

Appendix B: Platform Support

This section contains the following topics:

Locate the SiteMinder Platform Support Matrix

The SiteMinder Platform Support Matrix contains the latest information about supported operating environments. CA maintains the Platform Support Matrix at http://www.ca.com/support.

Follow these steps:

1. Log on to the support site.
2. Click Support by Product.
3. In the Select a Product page drop-down list, type SiteMinder.

   A link for CA Technologies SiteMinder appears.
4. Click the link.

   The SiteMinder product page appears.
5. Scroll down to the Product Status section, and then click the following link:

   `CA Technologies SiteMinder Platform Support matrices`

   The Platform Support matrices page appears.
6. Locate the version of the SiteMinder Agent for SharePoint you want, and then click the PDF link.

   The Platform Support Matrix for the SiteMinder Agent for SharePoint appears.

More information:

SiteMinder Component Prerequisites for the Agent for SharePoint (see page 18)
Microsoft Prerequisites (see page 17)
How to Configure a Reverse Proxy Server for your Agent for SharePoint Environment (see page 106)

Appendix C: Worksheets

This section contains the following topics:

Web Agent Installation Worksheet

Use this worksheet to gather the required information before running the Web Agent installer.

Information Needed	Your Value
Web Agent installation location (if not using the default)	

SiteMinder Web Agent Configuration Worksheet

Print a copy of the following worksheet to gather the required information before configuring the SiteMinder Web Agent:

Information Needed	Your Value
Admin User Name	
Admin Password	
Enable Shared Secret Rollover (y/n)	
Trusted Host Name (must be unique)	
Host Configuration Object	
Policy Server IP Address	
Policy Server Port Numbers (if not using the defaults)	
SmHost.conf file location (if not using the default)	

SiteMinder Agent for SharePoint Installation Worksheet

Print a copy of the following worksheet to gather the required information before installing the SiteMinder Agent for SharePoint:

Information Needed	Your Value
Application Port	
Farm Administrator	
Password	
Email ID	
Database Server	Windows or SQL Server
(SQL Authentication only) SQL User Name	
(SQL Authentication only) SQL User Password	

More information:

Gather the Installation Information for your SiteMinder Agent for SharePoint (see page 78)

SiteMinder Agent for SharePoint SSP Protection Worksheet

Print a copy of the following worksheet to gather the required information before protecting the SharePoint SSP with SiteMinder:

Information Needed	Your Value
Central Administration Port	
Default SSP Port	
Extended SSP Port	

More information:

How to Protect the SharePoint SSP with SiteMinder r12.0 SP2 and FBA (see page 110)

Appendix D: Optional Agent for SharePoint Configuration Settings

This section contains the following topics:

Create a Global Policy for your Forms Based SharePoint Users

If you want grant the same access to *all* the SharePoint users who authenticate to SiteMinder through forms-based authentication, use the following parameter:

SPAuthenticatedGroup

Identifies the group to which SiteMinder users who authenticate using forms-based authentication through the Agent for SharePoint belong.

Default: (value) SMAuthenticatedGroup

Default: (state) Disabled

To create a global policy for your forms-based SharePoint users

1. Enable the SPAuthenticatedGroup parameter (by removing the # character).
2. (Optional) Change the default value of the SPAuthenticatedGroup parameter.
3. Create a SiteMinder policy with a role for the SharePoint users. Use the value of the SPAuthenticatedGroup parameter as the name of the role.

   The global policy for your forms-based Sharepoint users is created.

Adjust the Agent for SharePoint Cache Settings

The SiteMinder Agent for SharePoint uses a cache to store the user and group information it retrieves from the SiteMinder Policy Server. The Agent for SharePoint searches the cache first, before contacting the Policy Server. You can increase the size of the cache and the number of minutes the information is stored to suit your needs. For example, if you have many users or groups in your organization, a larger cache could help improve search times.

The following parameters control the Agent for SharePoint cache:

SPCacheEntryExpireMinute

Specifies the number of minutes that the user and group information obtained from the SiteMinder Policy Server remains in the cache. When this interval expires, the Agent for SharePoint contacts the SiteMinder Policy Server to obtain the user and group information.

Limit: 1

Default: 30

SPNumCacheItem

Specifies the number user and group items contained in the Agent for SharePoint cache. If this value is too low, the Agent for SharePoint contacts the SiteMinder Policy Server to obtain user and group information instead of placing the items in the cache. If this value is too high, the cache could consume more resources than necessary on the SharePoint system. Changing the value of this parameter to zero disables the cache.

Limit:1

Default: 1000

To adjust the Agent for SharePoint cache settings

1. Enable both of the previous parameters by removing the # symbol.
2. Change the values of both parameters to suit your needs.

   The settings of the Agent for SharePoint cache are adjusted.

Specify the Location of your Agent for SharePoint Log Files

You can specify a location for the log and trace log files created by the Agent for SharePoint with the following parameter:

SPToolsLogLocation

Specifies the directory for the log and trace files created during the following operations:

- Application Protection
- User Migration
- User Profile Import
- UI Dashboard data population

Default: *web_agent_home*\log

To specify the location of your Agent for SharePoint log files

1. Update the value of the SPToolsLogLocation parameter with the directory you want.
2. (Optional) Update any of the other web-agent logging parameters (such as LogFileName, LogFileSize, or LogLocalTime) with the values you want.

   Note: For more information, see the *Web Agent Configuration Guide*.

   The Agent for SharePoint log file location is specified.

Prohibit Office Client Integration with the SiteMinder Agent for SharePoint

The SharePoint Central Administration UI controls whether or not office client integration is allowed for a particular web application. If you want to prevent SharePoint administrators from enabling Office Client Integration regardless of the setting in the SharePoint Central Administration UI, you can use the following parameter:

SPDisableClientIntegration

Specifies a list of protected SharePoint URLs where Office Client Integration will be blocked, regardless of the setting in the SharePoint Central Administration UI. Add the port number if you are *not* using a default port (such as 80 or 443).

Use this setting to override the settings of the SharePoint Central Administration UI to prevent SharePoint administrators from circumventing SiteMinder settings regarding Office Client integration.

Example: *host_name*:*port_number*

To prohibit office client integration with the SiteMinder Agent for SharePoint, add the URLs of the SharePoint sites you want to the SPDisableClientIntegration parameter.

Office Client Integration without a Persistent Cookie

The SiteMinder Agent for SharePoint creates a persistent SPSESSION cookie to enable single sign-on during Office Client Integration. If the security policies of your organization do not allow persistent cookies of any kind, you can still implement the Office Client Integration feature of SharePoint with certain restrictions.

The following table describes the circumstances and required SiteMinder settings where Office Client Integration works with and without the persistent SPSESSION cookie:

User Behavior	Challenge Users?	Use Persistent SPSESSION Cookie?	Office Client Integration Enabled?	Supported SiteMinder Authentication Schemes
Opens an Office Document from a browser.	No	Yes	Yes	Any
Opens an Office Document from a browser.	No	No	No	Any

Opens an Office Document with an Office Application or from Windows Explorer	Yes	No	No	Basic or Windows (NTLM/IWA)
Opens Office Document with Windows Explorer, and later tries to edit or save the document after session timeout interval expires.	Yes	Yes	Yes	Basic or Windows (NTLM/IWA)

More information:

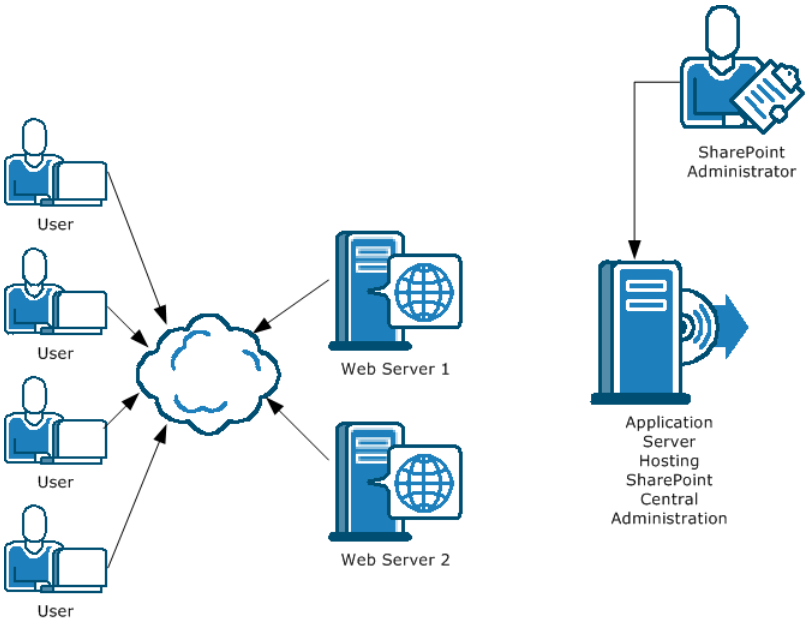
Verify your Office Client Integration Settings (see page 69)
Users Challenged Again when Accessing Office Document on SharePoint (see page 179)

Central Administration Hosted on an Application Server

Hosting your SharePoint Central Administration on an application server offers the following advantages:

- Isolates your central administration functions on a separate computer.
- Preserves bandwidth by allowing your web servers to focus on servicing web-application requests instead of using resources for central administration functions.

The following illustration shows a deployment with the SharePoint central administration site hosted on an application server:



How to Deploy the SiteMinder Agent for SharePoint when an Application Server is Hosting SharePoint Central Administration

To deploy the SiteMinder Agent for SharePoint when an application server is hosting your SharePoint Central Administration site, use the following process:

1. Install and configure a supported version of the SiteMinder Web Agent on each of the following components:
   - The application servers hosting your Central Administration site.
   - The web servers hosting SharePoint resources you want to protect.
2. Install and configure the SiteMinder Management UI on the application servers hosting the SharePoint Central Administration site.
3. Install and configure the SiteMinder Management UI on any web servers hosting SharePoint resources you want to protect.
4. Use the SiteMinder Management UI on each web server to protect the SharePoint applications.

Add HEAD and OPTIONS Actions to your Resources in an Existing SiteMinder Application (r12.0 SP2)

If you want to use the Office Client Integration feature with the SiteMinder Agent for SharePoint, add both of the following Web Agent actions to any existing SiteMinder resources in your SiteMinder Applications:

- HEAD
- OPTIONS

To add HEAD and OPTIONS actions to your resources in an existing SiteMinder application

1. Verify that your Web Agent type is updated with the following:
   - HEAD
   - OPTIONS
2. Click Policies, Application, Modify Application.
3. Click the option button of the application you want, and then click Select.

   The Modify Application: *Name* screen appears.
4. Click the Resources tab.

   The Resources screen appears.
5. Click the Edit button (on the left) of the resource you want.

   The Modify Application Resources: *Name* screen appears.
6. In the Action drop-down list, Control click the following items:
   - HEAD
   - OPTIONS
7. Click OK.

   The Resources screen appears.
8. Repeat Steps 5 through 7 to modify any other resources you want to use.
9. Click Submit.

   The resource is updated, and the confirmation screen appears.
10. Click OK.

More information:

Update the SiteMinder Agent Types for your SharePoint Resources (r12.0 SP2) (see page 20)

Add HEAD and OPTIONS Actions to Existing SiteMinder Rules (r12.0 SP2)

If you want to use the Office Client Integration feature with the SiteMinder Agent for SharePoint, add both of the following Web Agent actions to any existing SiteMinder rules:

- HEAD
- OPTIONS

To add HEAD and OPTIONS actions to existing SiteMinder rules

1. Verify that your Web Agent type is updated with the following:
   - HEAD
   - OPTIONS
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, Control click the following items:
   - HEAD
   - OPTIONS
5. Click Submit.

   The resource is updated, and the confirmation screen appears.
6. Click OK.
7. Repeat Steps 2 through 6 to modify other rules that you want.

More information:

Update the SiteMinder Agent Types for your SharePoint Resources (r12.0 SP2) (see page 20)

Add HEAD and OPTIONS Actions to Existing SiteMinder Rules (r6.x SP6)

If you want to use the Office Client Integration feature with the SiteMinder Agent for SharePoint, add both of the following Web Agent actions to any existing SiteMinder rules:

- HEAD
- OPTIONS

To add HEAD and OPTIONS actions to existing SiteMinder rules

1. Verify that your Web Agent type is updated with the following:
   - HEAD
   - OPTIONS
2. Click the Domains tab, and then expand your SharePoint domain.
3. Expand your SharePoint realm.

   A list of rules under the realm appears.
4. Right-click the rule you want, and then select Properties of Rule.

   The Rule Properties dialog appears.
5. Enter a distinctive name, and (optional) description.
6. In the Action field, Control-click the following:
   - Head
   - Options

   The web agent actions are selected.
7. Verify the following settings:
   - The Resource field contains an asterisk (*).
   - The Allow Access option button is selected.
   - The Enabled check box is selected.
8. Click OK.

   The Rule Properties Dialog closes and the new rule appears in the list.

More information:

Update the SiteMinder Agent Types for your SharePoint Resources (r12.0 SP2) (see page 20)

Index

D

E

G

H

I

L

M

O

P

R

S

T

U

V

W