Avaya Integrated Management

Job Aid: Applying CA SiteMinder

14-603388
May 2009
Issue 1

Introduction

Avaya Integrated Management (AIM) versions 5.2 and later support CA SiteMinder (SM).

Applying SM to AIM allows users to authenticate against SM and then navigate freely between all AIM applications within this web server.

This application is appropriate for organizations that already employ SM for controlling access to web servers and that wish to integrate AIM in their environment.

This document describes the steps required to apply SM to the AIM server

Note:
This document covers a simple Siteminder use scenario. See the SiteMinder documentation for more information about Siteminder and for more complex configurations and features.

Installing the AIM server on a SiteMinder supported Windows platform

You must install the "SiteMinder Web Agent" on the AIM server host to enable SiteMinder for AIM.

Note the following:

- You must install the AIM server on a Windows Operating System version that the SiteMinder Web Agent supports.
- The SiteMinder Web Agent you installed on the device must be compatible with the ASF Apache web server version, that is included in the AIM server. For example, if the AIM server includes ASF Apache 2.2.11 version, you must install a web agent that supports the Apache web server version.

SiteMinder 6.0 supports the following OS versions are:

- Windows 2000 SP4.
- Windows 2003 SP2 - requires SiteMinder 6.0 QMR5.

See the SiteMinder Support Matrix for more information about supported OS versions and supported web agents.

Assigning a DNS name to the AIM server host

SM requires that you assign a domain name to the AIM server host. The domain name must be published via DNS to allow remote access to the system.

Assign a domain name to the server and change the target of the **Avaya Integrated Management** desktop shortcut:

1. Right-click the shortcut.
2. Select **Properties** to point to the assigned DNS name instead of localhost.

Note:
You must browse SM-enabled web servers with domain names, not IP addresses.

Configuring the SiteMinder Policy Server

This section describes how to configure the Policy Server to apply SM to the AIM server.

Note:
This procedure assumes that a SM Policy Server is installed on a dedicated device and configured with connections to user store and policy store databases/ directories.

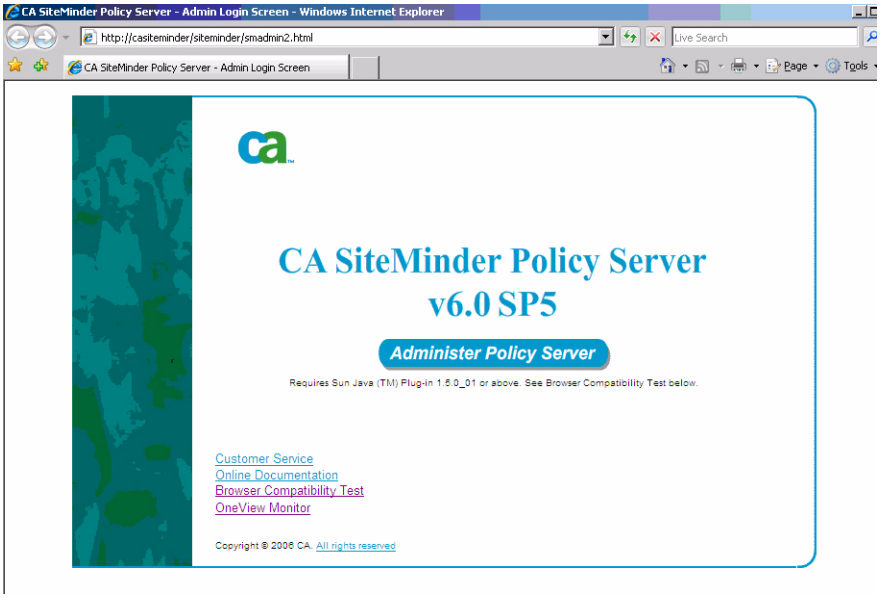
See CA SiteMinder documentation for information about Policy Server installation.

Configure the Policy Server through the SiteMinder 6.0 Administration GUI. Follow these steps to enter the GUI:

1. Click **Start > Programs > SiteMinder > SiteMinder Policy Server User Interface**.

– The following screen opens:

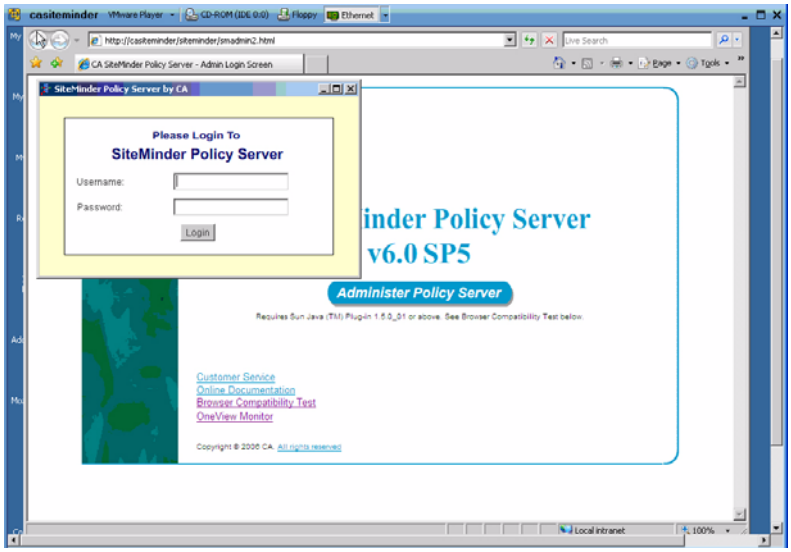
Figure 1: SiteMinder login screen



2. Click **Administer Policy Server**.

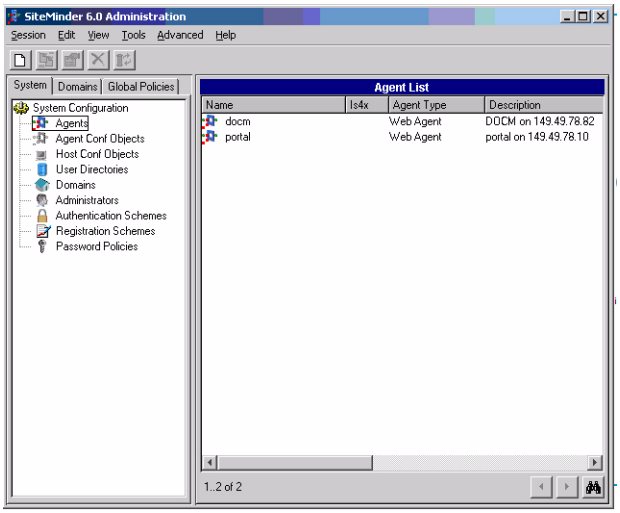
– The following screen opens:

Figure 2: SiteMinder Policy Server login screen



3. Enter the user name and the password.
4. Click **Login**.
   – The SiteMinder Administration GUI opens:

Figure 3: SiteMinder Administration GUI

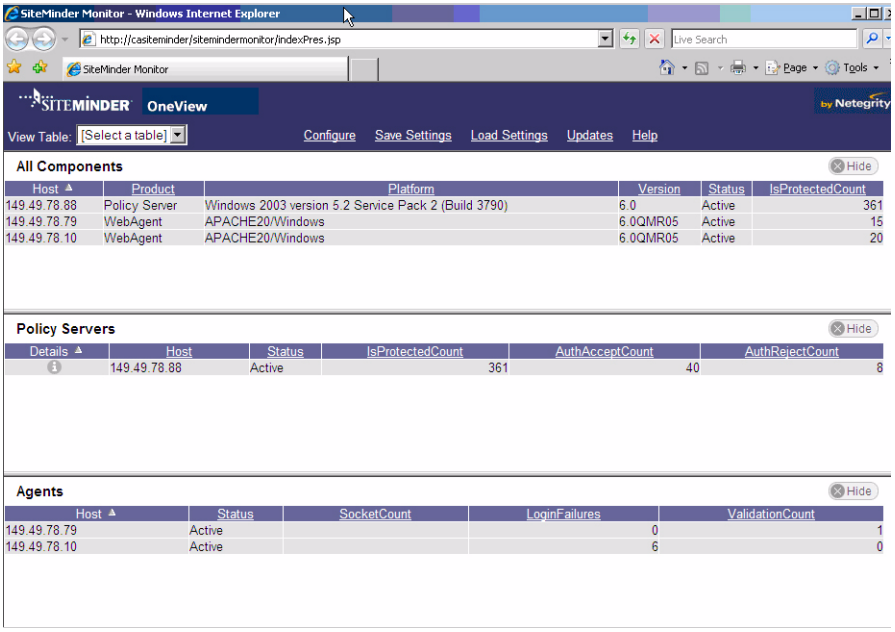


You can start your configuration process.

Tip:

After entering the Admin Login Screen, as mentioned in section 1, you can activate a monitor page, by clicking **OneView Monitor**. The monitor page includes some basic information about the Policy Server and the server's components. This information can be useful. The following screen shows an example:

Figure 4: SiteMinder Monitor screen



5. Create an Agent object for the AIM server host:
   a. Open the **System** tab.
   b. Right-click **Agents**.
   c. Select **Create Agent**.
   d. Select **SiteMinder/Web Agent** as the agent type.
   e. Assign the name docm to the agent.
6. Create an Agent Conf Object for the AIM Web Agent:
   a. Select **Agent Conf Objects**.
   b. Right-click the **ApacheDefaultSettings** agent conf object in the right panel.
   c. Select **Duplicate Configuration Object**.
   d. Assign the name docm to the new object.
   e. Set the parameter values as follows:
      – DefaultAgentName=docm.
      – LegacyVariables=YES.
      – LogoffUri=/SSO/logout.
      – ProxyAgent=YES.

7. Define a Host Conf object to for use by the AIM server host Web Agent:
    a. Open the **System** tab.
    b. Select **Host Conf Objects**.
    c. Right-click the **DefaultHostSettings** host conf object in the right panel.
    d. Select **Duplicate Configuration Object**.
    e. Uncomment the PolicyServer parameter and specify the IP address and ports of the PS.
        – The relevant ports are usually: 44441, 44442 and 44443.
    f. Assign a name for the object, for example docm.
    g. Click **OK**.
8. Define an authentication scheme for AIM login:
    a. Open the **System** tab.
    b. Right-click **Authentication Schemes**.
    c. Select **Create Authentication Scheme**.
    d. Assign the name form-relative to the object.
    e. Select **HTML form template** as the authentication scheme type.
    f. Select **Use Relative Target** in the **scheme setup** tab.
    g. Click **OK**.
9. Create a realm for AIM:
    a. Open the **Domains** tab.
    b. Right-click **Realms**.
    c. Select **Create Realm**.
    d. Assign the name docm to the realm.
    e. Select docm in the **Agent** field.
    f. Enter /SSO/ in the **Resource Filter** field.
    g. Select Unprotected as the **Default Resource Protection**.
    h. In the **Authentication Scheme** field, select the name of an HTML form authentication scheme, by the name: 'form-relative' that you created in step 8.
    i. Click **OK**.
10. Create 2 rules under the docm realm:
    a. Right-click the **docm** realm.
    b. Select **Create Rule under Realm**.
    c. Assign the name docm-login to the rule.

d. Enter cd/login* in the **Resource** field.

e. Select Allow Access and Enabled.

f. Select Web Agent Actions in the **Action** frame.

g. Select GET, POST, and PUT.

h. Click **OK**.

i. Create a second rule by right-clicking the **docm-login** rule and selecting **Duplicate Rule**.

j. Assign the name docm-logout to the new rule.

k. Enter logout In the **Resource** field.

l. Click **OK**.

11. Create a policy for the AIM:

a. Open the **Domains** tab.

b. Right-click **Policies**.

c. Select **Create Policy**.

d. Define the appropriate filter in the **Users** tab:

– Click **Add/Remove…**

– Move the member from **Available Members** in the right panel to **Current Members** in the left panel

– Click **OK**.

e. Add the 2 AIM rules defined in step 10, in the **Rules** tab.

– Click **Add/Remove…**

– Move the member from **Available Members** in the right panel to **Current Members** in the left panel.

– Click **OK**.

f. Select the **Enable** check box.

g. Click **OK**.

Installing and configuring SiteMinder Web Agent on the AIM server host

This section aims to define the steps for installing SiteMinder web agent.

Follow the steps below to install and configure the SM Web Agent on the AIM server host:

1. Run the SM Web Agent installer on the AIM server host.
   - Note that you must run the Web Agent that exactly matches the ASF Apache server installed on the server.
2. Select **Yes. I would like to configure the Agent now** in the installation wizard.
3. Click **Next**.
4. When prompted to register the host, select **Yes**.
5. Click **Next**.
6. Enter the user name and password of the SiteMinder administrator.
7. Click **Next**.
8. Enter the name you want in the **Trusted Host Name** field.
9. Enter the name of the Host Conf object that you defined in step 7 of Configuring the SiteMinder Policy Server in the **Host Configuration Object**.
10. Click **Next**.
11. Enter the IP address and ports of the Policy Server.
    - The relevant ports are usually: 44441, 44442 and 44443.
12. Click **Next**.
13. Select a location for the host configuration file.
14. Click **Next**.
    - The **Select Web Servers** opens.
15. Select the installed ASF Apache server installed on your device.
16. Enter the Agent Configuration Object name that you defined in step 6 of Configuring the SiteMinder Policy Server.
17. Click **Next**.
18. Open the **SSL Authentication** page.
19. Select **No Advanced Authentication**.
20. Click **Next**.
    - The **Self Registration** opens.

21. Select **No**.
22. Click **Next**.
23. Click **Install** to complete the agent configuration.
24. After the installation finishes, click **Finish**.
25. Enable the web Agent. Edit the file <Apache WS home>/conf/WebAgent.conf and change the line EnableWebAgent="NO" to EnableWebAgent="YES".
26. Restart the computer.

Assigning roles to AIM users

By default, when operating in SM mode, authorization of AIM users is based on roles assigned to individual users through the AIM internal user management tool. This means that, unless a user has a record in the AIM user repository (through which a role is assigned to it), that user will not be allowed to access AIM even if SM can authenticate the user. Before enabling SM in AIM, at least one of the SM users (users that have been defined in the SM User Store and can be authenticated by the Web Agent) has to be assigned a role in AIM.

To complete this, follow the steps below:

1. Login into Branch Central Manager as administrator.
2. Select **Utilities/Administrators** in the navigation tree on the left.
3. Use **add** to create a new user record.
4. If this user is going to be authenticated against SiteMinder only, clear the **local** check box. Otherwise, you must assign a password.
5. Select a name for the user. The name must match the name of a SM user.
6. Select a role for the user.
   - To give the user the right to create, delete, and assign roles to other AIM users, select one of the roles 'Security-Administrator' or 'Administrator'. Note that an 'Administrator' is authorized to perform any operation in AIM while a 'Security-Administrator' is restricted to user administration only.
7. Click **save changes**.

When you have authorized an SM user to administer users in AIM, you can enable SM.

Turning on SiteMinder in the AIM server

To turn on SM in AIM:

1. Open the 'sso.properties' configuration file that resides under <Avaya home directory>/private/SSO/
2. Change the line 'cross.domain.sso.enabled=false' to 'cross.domain.sso.enabled=true'.
3. Restart the AIM server using the **stop/start menu** items reachable through the Windows start menu.

How to log in into AIM when SiteMinder Policy Server is inactive or unavailable

Login into AIM directly without needing to authenticate against SM is always possible using the user name and password of a 'local' AIM user (a user that has been assigned a password through the AIM user administration tool).

To log in directly, add the flag 'locallogin' as a parameter to the URL, for example: https://aim.company.com/decm/gui/DOCM.html?locallogin.

You are then be prompted with the native AIM login dialog which allows you to login directly.

This procedure is useful when the SM Policy Server (or the authentication web server) is inactive or unavailable, or if none of the SM users is authorized to access AIM.