

## Configuring a Secure Access eTrust SiteMinder Server Instance (NSM Procedure)

Within the Secure Access device, a SiteMinder instance is a set of configuration settings that defines how the Secure Access device interacts with the SiteMinder policy server.

To configure the SiteMinder server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Secure Access device for which you want to configure eTrust SiteMinder server instance.
3. Click the **Configuration** tab and select **Authentication > Auth Servers**. The corresponding workspace appears.



**NOTE:** If you want to update an existing server instance, click the appropriate link in the Auth Server Name box, and perform the Steps 5 through 10.

4. Click the **New** button. The New dialog box appears.
5. In the Auth Server Name list, specify a name to identify the server instance.
6. Select **SiteMinder Server** from the Auth Server Type list.
7. Configure the server using the settings described in Table 1 on page 1.
8. Click one:
  - **OK**—Saves the changes.
  - **Cancel**—Cancels the modifications.
9. Set advanced SiteMinder configuration options (optional) using the settings described in Table 2 on page 8.

**Table 1: Secure Access eTrust SiteMinder Configuration Details**

| Option   | Function  | Your Action   |
|--|---|---|
| <b>SiteMinder Settings &gt; Basic Settings tab</b> |   |   |
| Policy Server                                      | Specifies the name or IP address of the SiteMinder policy server. | Enter a name or IP address.                                       |
| Backup Server(s)                                   | Specifies a list of backup policy servers (optional).             | Enter a comma-delimited list of backup policy servers (optional). |

**Table 1: Secure Access eTrust SiteMinder Configuration Details (continued)**

| Option  | Function   | Your Action   |
|---|--|---|
| Failover Mode?  | Allows the Secure Access device to use the main policy server unless it fails.   | <ul style="list-style-type: none"> <li>■ Select <b>Yes</b> — Secure Access device uses the main policy server unless it fails.</li> <li>■ Select <b>No</b>— Secure Access device load balances among all the specified policy servers.</li> </ul> |
| Agent Name  | Specifies the SiteMinder agent name.   | Enter an agent name.<br><br><b>NOTE:</b> Shared secret and agent name are case-sensitive.   |
| Secret  | Specifies the shared secret.   | Enter a shared secret name.<br><br><b>NOTE:</b> Shared secret and agent name are case-sensitive.  |
| Compatible with   | Specifies a SiteMinder server version. Version 5.5 supports 5.5 and 6.0. Version 6.0 supports only 6.0 of the SiteMinder server API. The default value is 5.5 policy servers.  | Select the server version from the drop-down list.  |
| On logout, redirect to  | Specifies a URL to which users are redirected when they sign out of the Secure Access device (optional). If you leave this field empty, users see the default Secure Access device sign-in page.   | Enter a URL.  |
| Protected Resource  | Specifies a default protected resource. If you do not create sign-in policies for SiteMinder, the Secure Access device uses this default URL to set the user's protection level for the session. The Secure Access device also uses this default URL if you select the Automatic Sign-In option. | Enter a URL.<br><br><b>NOTE:</b> You must enter a forward slash (/) at the beginning of the resource (for example, enter <b>"/live-authentication"</b> ).   |
| <b>Siteminder Settings &gt; SMSESSION cookie settings tab</b> |  |   |

**Table 1: Secure Access eTrust SiteMinder Configuration Details (continued)**

| Option   | Function   | Your Action  |
|--|--|--|
| Cookie Domain                                      | Specifies the cookie domain of the Secure Access device.   | Enter a URL for the cookie domain.<br><br><b>NOTE:</b> <ul style="list-style-type: none"> <li>■ Multiple domains should use a leading period and be comma separated. For example:<br/><b>.sales.myorg.com, .marketing.myorg.com.</b></li> <li>■ Domain names are case-sensitive.</li> <li>■ You cannot use wildcard characters.<br/><br/>For example, if you define “.juniper.net”, the user must access the Secure Access device as “<b>http://secure access device.juniper.net</b>” to ensure that his SMSESSION cookie is sent back to the Secure Access device.</li> </ul> |
| IVE Cookie Domain                                  | Specifies the internet domain(s) to which the Secure Access device sends the SMSESSION cookie using the same guidelines outlined for the Cookie Domain field.                        | Enter a URL.   |
| Protocol   | Sends cookies securely and non securely.   | Select the protocol from the drop-down list: <ul style="list-style-type: none"> <li>■ <b>HTTPS</b>—Sends cookies securely if other Web agents are set up to accept secure cookies.</li> <li>■ <b>HTTP</b>—Sends cookies non securely.</li> </ul>   |
| <b>Siteminder Settings &gt; Authentication tab</b> |  |  |
| Automatic Sign-In                                  | Allows users with a valid <b>SMSESSION</b> to automatically sign in to the Secure Access device.   | Select the <b>Automatic Sign-In</b> option to enable this feature.   |
| Automatic Sign In realm to use                     | Specifies an authentication realm for automatically signed-in users. The Secure Access device maps the user to a role based on the role mapping rules defined in the selected realm. | Select an authentication realm from the drop-down list.  |

**Table 1: Secure Access eTrust SiteMinder Configuration Details (continued)**

| Option                                  | Function   | Your Action   |
|---|--|---|
| If Automatic Sign In fails, redirect to | <p>Specifies an alternate URL for users who sign into the Secure Access device through the Automatic Sign-In mechanism. The Secure Access device redirects users to the specified URL if the Secure Access device fails to authenticate and no redirect response is received from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in to the Secure Access device.</p> <p><b>NOTE:</b> Users who sign in through the sign-in page are always redirected back to the Secure Access device sign-in page if authentication fails.</p> | Enter a URL.  |
| Authentication Type > Custom Agent      | Authenticates using the Secure Access device custom Web agent.   | Select <b>Siteminder Settings &gt; Authentication &gt; Authentication Type &gt; Custom Agent</b> option from the Authentication Type drop-down list.  |
| Authentication Type > Form POST         | Posts user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly.  | Select <b>Siteminder Settings &gt; Authentication &gt; Authentication Type &gt; Form POST</b> option from the <b>Authentication Type</b> drop-down list to allow the Web agent to contact the policy server to determine the appropriate sign-in page to display to the user. |
| Form POST Target                        | <p>Specifies the target URL.</p> <p><b>NOTE:</b> The form post target, form post protocol, form post Webagent, form post port, form post path, and form post parameters field are displayed only when you select <b>Form POST</b> option from the <b>Authentication type</b> drop down list.</p>   | Enter the target URL.   |

**Table 1: Secure Access eTrust SiteMinder Configuration Details (continued)**

| Option               | Function   | Your Action   |
|----------------------|--|---|
| Form POST Protocol   | <p>Allows you to specify the protocol for communication between IVE and the specified Web agent.</p> <p><b>NOTE:</b> This field is displayed only when you select the <b>Form POST</b> option from the Authentication Type drop-down list.</p>       | <p>Select the protocol from the drop-down list:</p> <ul style="list-style-type: none"> <li>■ <b>HTTP</b>—For non secure communication.</li> <li>■ <b>HTTPS</b>—For secure communication.</li> </ul>   |
| Form POST Webagent   | <p>Specifies the name of the Web agent from which the Secure Access device is to obtain SMSESSION cookies.</p> <p><b>NOTE:</b> This field is displayed only when you select <b>Form POST</b> option from the Authentication Type drop-down list.</p> | <p>Enter the name of the web agent.</p>   |
| Form POST Port       | <p>Specifies the port for the protocol.</p> <p><b>NOTE:</b> This field is displayed only when you select the <b>Form POST</b> option from the Authentication Type drop-down list.</p>  | <p>Enter port <b>80</b> for HTTP or port <b>443</b> for HTTPS.</p>  |
| Form POST Path       | <p>Specifies the path of the sign-in page.</p> <p><b>NOTE:</b> This field is displayed only when you select the <b>Form POST</b> option from the Authentication Type drop-down list.</p>   | <p>Enter the path of the Web agent's sign-in page.</p> <p><b>NOTE:</b> The path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent.</p>   |
| Form POST Parameters | <p>Specifies the post parameters to be sent when a user signs in.</p> <p><b>NOTE:</b> This field is displayed only when you select the <b>Form POST</b> option from the Authentication Type drop-down list.</p>                                      | <p>Enter the post parameters.</p> <p>Common SiteMinder variables that you can use include <code>_USER_</code>, <code>_PASS_</code>, and <code>_TARGET_</code>. These variables are replaced by the username and password entered by the user on the Web agent's sign-in page and by the value specified in the Target field. These are the default parameters for login.fcc—if you have made customizations, you may need to change these parameters.</p> |

**Table 1: Secure Access eTrust SiteMinder Configuration Details** (continued)

| Option  | Function   | Your Action  |
|---|--|--|
| Authentication Type ><br>Delegate to a Standard Agent | Delegates authentication to a standard agent. When the user accesses the Secure Access device sign-in page, the Secure Access device determines the FCC URL associated with the protected resource's authentication scheme. The Secure Access device redirects the user to that URL, setting the Secure Access device sign-in URL as the target. After successfully authenticating with the standard agent, an SMSESSION cookie is set in the user's browser and the user is redirected back to the Secure Access device. The Secure Access device then automatically signs in the user and establishes a Secure Access session. | Select <b>Siteminder Settings &gt; Authentication &gt; Authentication Type &gt; Delegate to a Standard Agent</b> option from the Authentication Type drop-down list. |
| <b>Siteminder Settings &gt; Authorization tab</b>     |  |  |
| Authorize requests against SiteMinder policy server   | Uses SiteMinder policy server rules to authorize user Web resource requests. If you select this option, make sure that you create the appropriate rules in SiteMinder that start with the server name followed by a forward slash, such as: "www.yahoo.com/", "www.yahoo.com/*", and "www.yahoo.com/r/f1".   | Select <b>Siteminder Settings &gt; Authorization &gt; Authorize requests against SiteMinder policy server</b> .  |

**Table 1: Secure Access eTrust SiteMinder Configuration Details (continued)**

| Option   | Function  | Your Action   |
|--|---|---|
| If authorization fails, redirect to            | <p>Specifies an alternative URL that users are redirected to if the Secure Access device fails to authorize and no redirect response is received from the SiteMinder policy server. If you leave this field empty, users are prompted to sign back in to the Secure Access device.</p> <p><b>NOTE:</b> If you are using an authorization-only access policy, you must enter an alternative URL in this field regardless of whether the <b>Authorize requests against SiteMinder policy server</b> option is selected. Users are redirected to this URL when an access denied error occurs. See "Defining authorization-only access policies."</p> | Enter a URL.  |
| Resource for insufficient protection level     | Specifies a resource on the Web agent to which the Secure Access device redirects users when they do not have the appropriate permissions.  | Enter a URL.  |
| Ignore authorization for files with extensions | Specifies file extensions corresponding to file types that do not require authorization.  | Enter the extensions of each file type that you want to ignore, separating each with a comma. For example, enter <b>.gif, .jpeg, .jpg, .bmp</b> to ignore various image types. You cannot use wildcard characters (such as *, *.*, or *) to ignore a range of file types. |
| <b>Server Catalog &gt; Expressions tab</b>     |   |   |
| Name   | Specifies a name for the user expression in the SiteMinder user directory.  | Enter a name.   |
| Value  | Specifies a value for the user expression in the SiteMinder user directory.   | Enter a value.  |
| <b>Server Catalog &gt; Attributes tab</b>      |   |   |
| Name   | Specifies the name of the user attribute cookie in the SiteMinder user directory.   | Enter a name.   |

**Table 2: Secure Access eTrust SiteMinder Advanced Configuration Details**

| Option                                       | Function   | Your Action   |
|--|--|---|
| <b>Siteminder Settings &gt; Advanced tab</b> |  |   |
| Poll Interval (seconds)                      | Specifies the interval at which Secure Access device polls the SiteMinder policy server to check for a new key.  | Enter the poll interval in seconds.   |
| Maximum Agents                               | Controls the maximum number of simultaneous connections that the Secure Access device is allowed to make to the policy server.<br><br><b>NOTE:</b> The default setting is 20.  | Enter a number.   |
| Maximum Requests/Agent                       | Controls the maximum number of requests that the policy server connection handles before the Secure Access device ends the connection. If necessary, tune to increase performance.<br><br><b>NOTE:</b> The default setting is 1000.            | Enter a number.   |
| Idle Timeout (minutes)                       | Controls the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before the Secure Access device ends the connection. The default setting of "none" indicates no time limit. | Enter the Idle timeout in minutes.  |
| Authorize while Authenticating               | Specifies that the Secure Access device should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated.  | Select <b>Siteminder Settings &gt; Advanced &gt; Authorize while Authenticating</b> . |

**Table 2: Secure Access eTrust SiteMinder Advanced Configuration Details** (continued)

| Option                                       | Function   | Your Action  |
|--|--|--|
| <b>Siteminder Settings &gt; Advanced tab</b> |  |  |
| Enable Session Grace Period                  | <p>Eliminates the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time.</p> <p>If you do not select this option, the Secure Access device checks the user's SMSESSION cookie on each request.</p> | <p>Select <b>Siteminder Settings &gt; Advanced &gt; Enable Session Grace Period</b> to enable this feature.</p> <p>You can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time. During that period, the Secure Access device assumes that its cached cookie is valid rather than revalidating it against the policy server. Note that the value entered here does not affect session or idle timeout checking.</p> |
| Validate cookie every (seconds)              | Specifies the time period for the Secure Access device to eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Secure Access device should consider the cookie valid for a certain period of time.   | Enter the time period in seconds.  |
| Ignore Query Data                            | Specifies that the Secure Access device does not cache the query parameter in its URLs. Therefore, if a user requests the same resource as is specified in the cached URL, the request should not fail.  | Select the <b>Ignore Query Data</b> option to enable this feature.   |
| Accounting Port                              | Specifies that the value entered in this field must match the accounting port value entered through the Policy Server Management Console in the web UI. By default, this field matches the policy server's default setting of 44441.   | Enter the value.   |

**Table 2: Secure Access eTrust SiteMinder Advanced Configuration Details** (continued)

| Option                                       | Function  | Your Action    |
|--|---|----------------|
| <b>Siteminder Settings &gt; Advanced tab</b> |   |                |
| Authentication Port                          | The value entered in this field must match the authentication port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44442. | Enter a value. |
| Authorization Port                           | The value entered in this field must match the authorization port value entered through the Policy Server Management Console. By default, this field matches the policy server's default setting of 44443.  | Enter a value. |

- Related Topics**
- Configuring a Secure Access Certificate Server Instance (NSM Procedure)
  - Configuring a Secure Access SAML Server Instance (NSM Procedure)
  - Configuring a Secure Access Anonymous Server Instance (NSM Procedure)