

Configuring an Infranet Controller eTrust SiteMinder Server Instance (NSM Procedure)

Within the Infranet Controller, an eTrust SiteMinder instance is a set of configuration settings that defines how the Infranet Controller interacts with the eTrust SiteMinder policy server.

To configure an eTrust SiteMinder server instance:

1. In the NSM navigation tree, select **Device Manager > Devices**.
2. Click the **Device Tree** tab, and then double-click the Infranet Controller for which you want to configure an eTrust SiteMinder server instance.
3. Click the **Configuration** tab. In the configuration tree, select **Authentication > Auth Servers**.
4. Add or modify eTrust SiteMinder server settings as specified in Table 1 on page 1.
5. Click one:
 - **OK**—Saves the changes.
 - **Cancel**—Cancels the modifications.

Table 1: Infranet Controller eTrust SiteMinder Configuration Details

Option	Function	Your Action
Auth Server Name	Specifies a name for the auth server.	Enter a name for the auth server.
Auth Server Type	Specifies the auth server type.	Select Siteminder Server .
Siteminder Settings > Basic Settings tab		
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).
Failover Mode?	Specifies that the Infranet Controller can use the main policy server unless it fails.	<ul style="list-style-type: none"> ■ Select Yes — Infranet Controller uses the main policy server unless it fails. ■ Select No— Infranet Controller load balances among all the specified policy servers.
Agent Name	Specifies the SiteMinder agent name.	Enter an agent name. NOTE: Shared secret and agent name are case-sensitive.

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Secret	Specifies the shared secret.	Enter a shared secret name. NOTE: Shared secret and agent name are case-sensitive.
Compatible with	Specifies a SiteMinder server version. Version 5.5 supports versions 5.5 and 6.0. Version 6.0 supports only version 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 Infranet Controller (optional). If you leave this box empty, users see the default Infranet Controller sign-in page.	Enter a URL.
Protected Resource	Specifies a default protected resource. If you do not create sign-in policies for SiteMinder, the Infranet Controller uses this default URL to set the user's protection level for the session. The Infranet Controller also uses this default URL if you select the Automatic Sign-In option.	Enter a URL. NOTE: You must enter a forward slash (/) at the beginning of the resource (for example, "/ive-authentication").
Users authenticate using tokens or one-time passwords	Specifies that the user authentication is done using tokens or one-time passwords.	Select the check box.
Siteminder Settings > SMSESSION Cookie Settings tab		

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Cookie Domain	Specifies the cookie domain of the Infranet Controller.	Enter a URL for the cookie domain. NOTE: <ul style="list-style-type: none"> ■ Multiple domains should use a leading period and be comma separated. For example: .sales.myorg.com, .marketing.myorg.com. ■ Domain names are case-sensitive. ■ You cannot use wildcard characters. For example, if you define “.juniper.net”, the user must access the Infranet Controller as “http://Infranet Controller.juniper.net” to ensure that the SMSESSION cookie is sent back to the Infranet Controller.
IVE Cookie Domain	Specifies the internet domain(s) to which the Infranet Controller sends the SMSESSION cookie using the same guidelines outlined for the Cookie Domain box.	Enter a URL.
Protocol	Specifies that you to send cookies either securely or nonsecurely.	Select the Protocol from the drop down list: <ul style="list-style-type: none"> ■ HTTPS— Sends cookies securely if other Web agents are set up to accept secure cookies. ■ HTTP—Sends cookies nonsecurely.
Siteminder Settings > Authentication tab		
Automatic Sign-In	Specifies that users with a valid SMSESSION automatically sign in to the Infranet Controller.	Select the Automatic Sign-In check box to enable this feature.
Automatic Sign In realm to use	Specifies an authentication realm for automatically signed-in users. The Infranet Controller 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: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
If Automatic Sign In fails, redirect to	Specifies an alternate URL for users who sign into the Infranet Controller through the Automatic Sign-In mechanism. The Infranet Controller redirects users to the specified URL if the Infranet Controller fails to authenticate and no redirect response is received from the SiteMinder policy server. If you leave this box empty, users are prompted to sign back in to the Infranet Controller. NOTE: <ul style="list-style-type: none"> ■ Users who sign in through the sign-in page are always redirected back to the Infranet Controller sign-in page if authentication fails. 	Enter a URL.
Authentication Type > Custom Agent	Specifies that authentication can be done using the Infranet Controller custom Web agent.	Select Siteminder Settings > Authentication > Authentication Type > Custom Agent .
Authentication Type > Form POST	Specifies to post user credentials to a standard Web agent that you have already configured rather than contacting the SiteMinder policy server directly.	Select Siteminder Settings > Authentication > Authentication Type > Form POST to contact the policy server to determine the appropriate sign-in page to display to the user.
Form POST Target	Specifies the target URL. NOTE: The form post target, form post protocol, form post Webagent, form post port, form post path, and form post parameters boxes are displayed only when you select the Form POST option from the Authentication Type drop-down list.	Enter the target URL.

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Form POST Protocol	<p>Specifies the protocol for communication between the IVE and the specified Web agent.</p> <p>NOTE: This box is displayed only when you select the Form POST 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"> ■ HTTP—For nonsecure communication. ■ HTTPS—For secure communication.
Form POST Webagent	<p>Specifies the name of the Web agent from which the Infranet Controller is to obtain SMSESSION cookies.</p> <p>NOTE: This box is displayed only when you select the Form POST 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>NOTE: This box is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter port 80 for HTTP or port 443 for HTTPS.</p>
Form POST Path	<p>Specifies the path of the sign-in page.</p> <p>NOTE: This box is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter the path of the Web agent’s sign-in page.</p> <p>NOTE: The path must start with a backslash (/) character. In the Web agent sign-in page URL, the path appears after the Web agent.</p>

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Form POST Parameters	<p>Specifies the post parameters to be sent when a user signs in.</p> <p>NOTE: This box is displayed only when you select the Form POST option from the Authentication Type drop-down list.</p>	<p>Enter the post parameters.</p> <p>Common SiteMinder variables that you can use include USER PASS and Target. 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 box. These are the default parameters for login.fcc—if you have made customizations, you may need to change these parameters.</p>
Authentication Type > Delegate to a Standard Agent	<p>Specifies that you can delegate authentication to a standard agent. When the user accesses the Infranet Controller sign-in page, the Infranet Controller determines the FCC URL associated with the protected resource's authentication scheme. The Infranet Controller redirects the user to that URL, setting the Infranet Controller 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 Infranet Controller. The Infranet Controller then automatically signs in the user and establishes an Infranet Controller session.</p>	<p>Select SiteMinder Settings > Authentication > Authentication Type > Delegate to a Standard Agent.</p>
SiteMinder Settings > Advanced tab		
Poll Interval (seconds)	<p>Specifies the interval at which Infranet Controller polls the SiteMinder policy server to check for a new key.</p>	<p>Enter the poll interval in seconds.</p>

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Maximum Agents	<p>Specifies the maximum number of simultaneous connections that the Infranet Controller is allowed to make to the policy server.</p> <p>NOTE: The default setting is 20.</p>	Enter a number.
Maximum Requests/Agent	<p>Specifies the maximum number of requests that the policy server connection handles before the Infranet Controller ends the connection. If necessary, tune to increase performance.</p> <p>NOTE: The default setting is 1000.</p>	Enter a number.
Idle Timeout (minutes)	<p>Specifies the maximum number of minutes a connection to the policy server may remain idle (the connection is not handling requests) before the Infranet Controller ends the connection. The default setting of "none" indicates no time limit.</p>	Enter the Idle timeout in minutes.
Authorize while Authenticating	<p>Specifies that the Infranet Controller should look up user attributes on the policy server immediately after authentication to determine if the user is truly authenticated.</p>	Select Siteminder Settings > Advanced > Authorize while Authenticating .

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
<p>Enable Session Grace Period</p>	<p>Specifies that users can eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Infranet Controller should consider the cookie valid for a certain period of time.</p> <p>If you do not select this option, the Infranet Controller checks the user's SMSESSION cookie on each request.</p>	<p>Select Siteminder Settings > Advanced > Enable Session Grace Period 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 Infranet Controller should consider the cookie valid for a certain period of time. During that period, the Infranet Controller 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>
<p>Validate cookie every (seconds)</p>	<p>Specifies the time period for the Infranet Controller to eliminate the overhead of verifying a user's SMSESSION cookie each time the user requests the same resource by indicating that the Infranet Controller should consider the cookie valid for a certain period of time.</p>	<p>Enter the time period in seconds.</p>
<p>Ignore Query Data</p>	<p>Specifies the query parameter in the URL as specified in the cached URL.</p> <p>The Infranet Controller 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. For example, if you enable the Ignore Query Data option, both of the following URLs are considered the same resource:</p> <p>http://foo/bar?param = value1</p> <p>http://foo/bar?param = value2</p>	<p>Select the Ignore Query Data option to enable this feature.</p>

Table 1: Infranet Controller eTrust SiteMinder Configuration Details (continued)

Option	Function	Your Action
Accounting Port	Specifies that the value entered in this box matches the accounting port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44441.	Enter the value for the accounting port.
Authentication Port	Specifies that the value entered in this box matches the authentication port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44442.	Enter a value for the authentication port.
Authorization Port	Specifies that the value entered in this box matches the authorization port value entered through the Policy Server Management Console. By default, this box matches the policy server's default setting of 44443.	Enter a value for the authorization port.
Server Catalog > Expressions tab		
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.
Server Catalog > Attributes tab		
Name	Specifies a name for the user attribute cookie in the SiteMinder user directory.	Enter a name.

- Related Topics**
- Configuring an Infranet Controller Certificate Server Instance (NSM Procedure)
 - Configuring an Infranet Controller Anonymous Server Instance (NSM Procedure)

