

Using Netegrity SiteMinder with AquaLogic SOA Management 2.6

Revised 5/23/2006
Applies to product versions:
AquaLogic SOA Management 2.6

Introduction

AquaLogic SOA Management integrates with Netegrity SiteMinder to provide authentication and access control of your web services. Installation of the Netegrity products and details on the creation of domains, realms, rules and policies in Netegrity is not covered in this document.

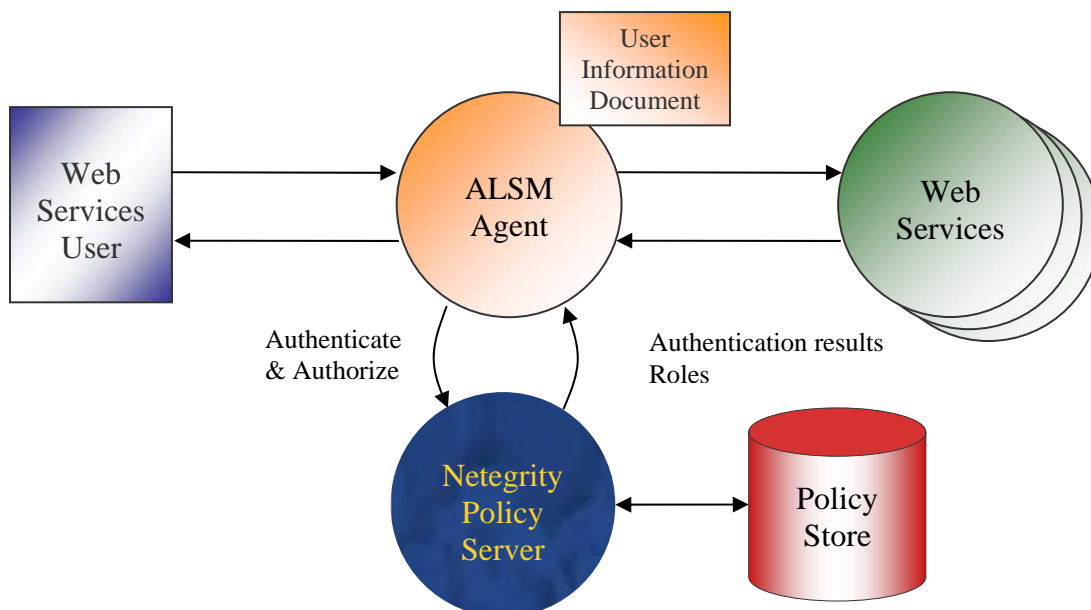
Prerequisites

Before configuring ALSM for use in authentication and/or authorization against Netegrity, please ensure the following are completed:

1. Installation and configuration of Netegrity products:
 - a. Installation of Netegrity Policy Server and SiteMinder Option Pack
 - b. Installation and configuration of a LDAP server with the Policy Server
2. Installation of SOA Management System R5
3. Access to the following Netegrity files and utilities from the machine in which the ALSM is installed:
 - a. smjavaagentapi.jar – Netegrity SiteMinder Java Agent API JAR file found in the Netegrity Policy Server installation or in the Web Agent installation
 - b. smreghost.exe – Netegrity SiteMinder Registration Tool. This is available in the Netegrity Web Agent installation

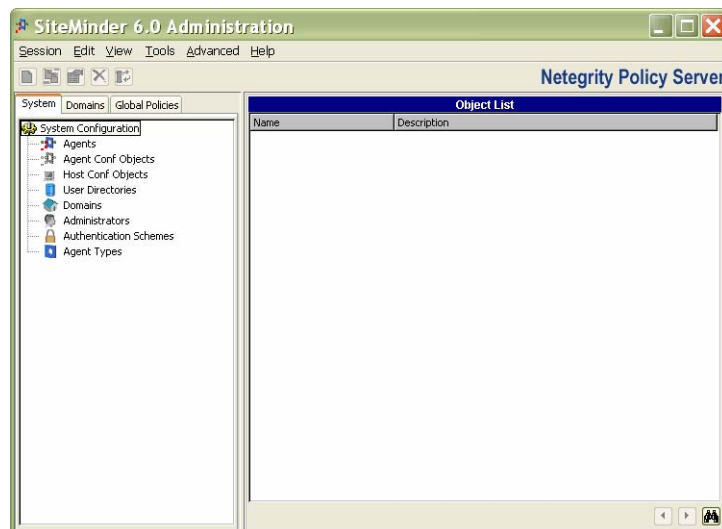
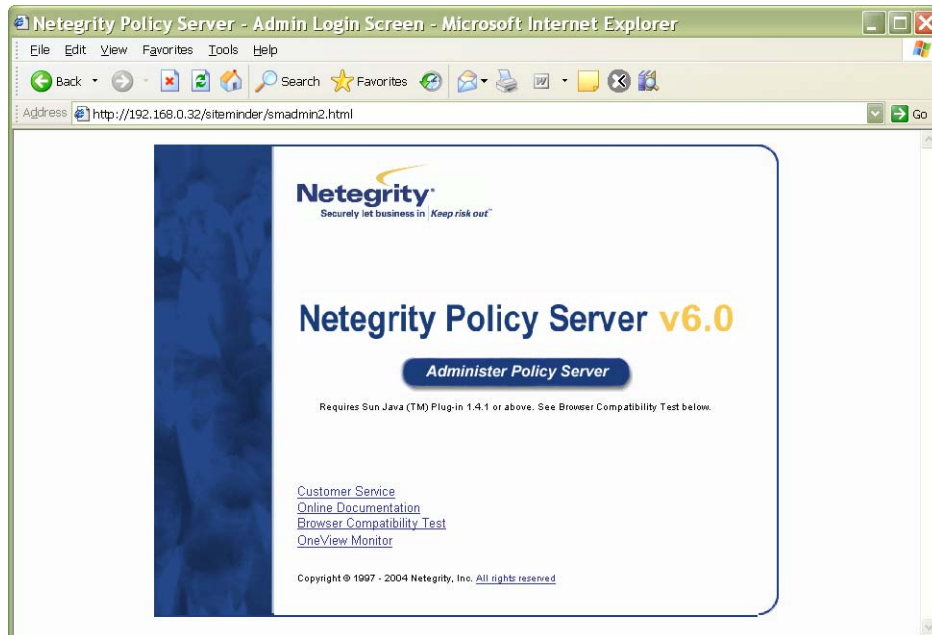
Overview

Integration of the ALSM with Netegrity provides the ability to authenticate users of web services and control access to web services and their operations. The ALSM Agent acts as a Netegrity custom agent and uses the Netegrity SiteMinder Agent API to communicate with Netegrity SiteMinder to enforce security policies. ALSM will create a claimed identity element in the user information document to hold the results of the policy and rules and the role information from Netegrity policy server and store.



Configuring Netegrity

To use ALSM with Netegrity SiteMinder first requires configuring Netegrity to recognize and allow access of the ALSM agent as a Netegrity custom agent. To do this use the Netegrity Policy Server User Interface:

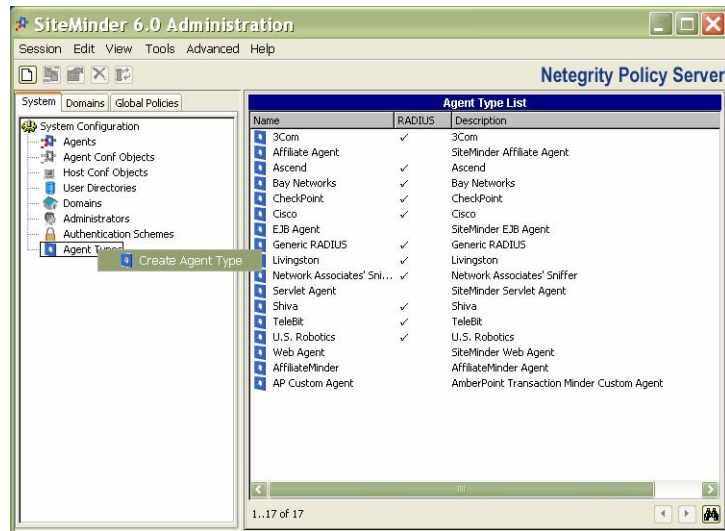


Creating a Netegrity Custom Web Agent for each ALSM Agent

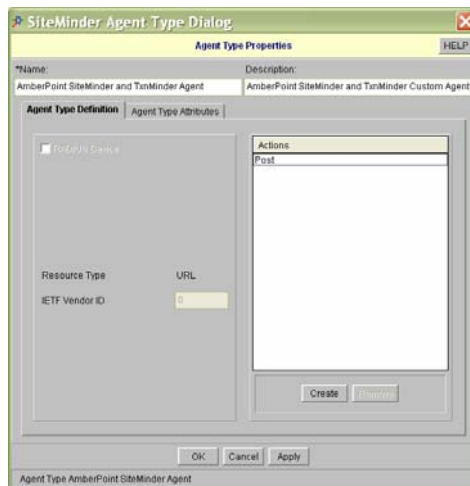
To register the ALSM Agent with the Netegrity Policy Server requires first creating a new custom *Agent Type* in the model of the Netegrity Policy Server and then creating an custom *Agent* of that type in the model.

Custom Agent Type

In the Netegrity Policy Server User Interface, make sure that the Agent Types node is visible in the System Configuration tree by checking View -> Agent Types. Then right mouse click on the Agent Types node and select Create Agent Type:



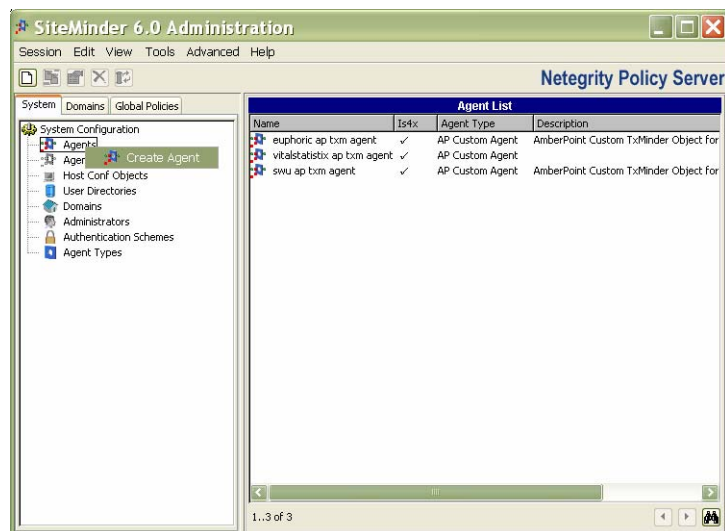
Give the agent type a name such as **ALSM SiteMinder Agent** and enter a description for this custom type. Also, create an action for this custom agent type with the name, **Post**:



Hit the OK or Apply button when done.

Custom Agent

Next create a custom agent for each **ALSM** agent by right clicking on the **Agents** node in the System Configuration tree and selecting **Create Agent**:



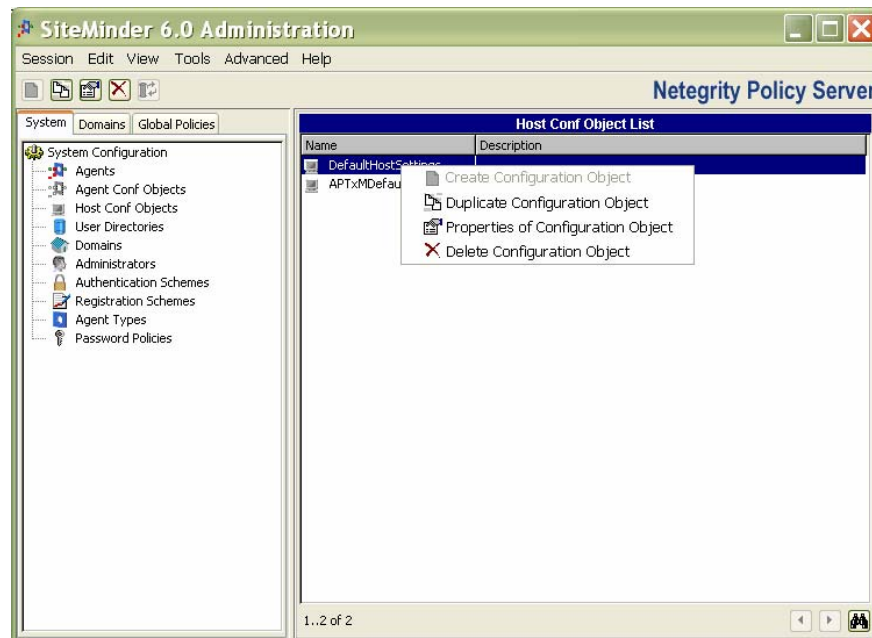
Enter a name and description for the agent. For Agent Type select the type created above. Enter the ip address or host name of the machine running the ALSM agent. Enter a value for Shared Secret which will be used by the ALSM agent to authenticate itself with the policy server.

The SiteMinder Agent Dialog window is titled "SiteMinder Agent Dialog" and has a "HELP" button. It contains the following fields and controls:

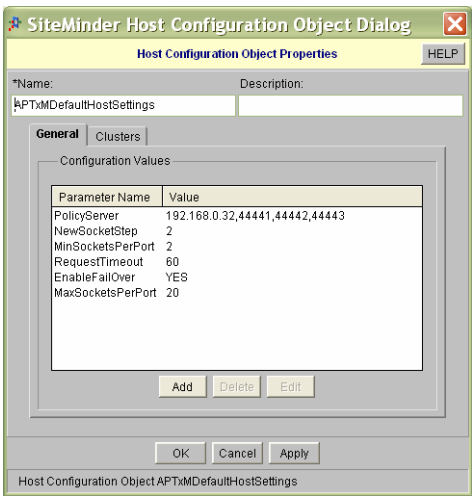
- Agent Properties** section:
 - *Name:** "AmberPoint Agent R5.0 on MyServer80"
 - Description:** "AmberPoint Custom SiteMinder and TmMinder Agent on MyServer"
- Support 4.x agents:** Checked checkbox.
- Agent Type:** Radio buttons for "SiteMinder" (selected) and "RADIUS". A dropdown menu next to "SiteMinder" shows "AmberPoint SiteMinder and TmMinder Agent".
- *IP Address or Host Name:** "10.10.11.120" with a "DNS Lookup" button.
- *Shared Secret:** Two password fields labeled "*Secret:" and "*Confirm Secret:" with masked characters.
- Buttons:** "OK", "Cancel", and "Apply" at the bottom.
- Agent:** A label at the very bottom.

Host Configuration Object for each ALSM Agent

The Host Configuration objects hold parameters for trusted hosts, in this case, the ALSM Agent. The ALSM Agent after connecting to the Policy Server will use these settings. The easiest method to creating a Host Configuration object is to right-mouse click on the DefaultHostSettings line item and selecting Duplicate Configuration Object.



In the Host Configuration Object Dialog, enter in a name for the object.



Double-click on the #PolicyServer line in the table and change the parameter name to PolicyServer by removing the pound sign (#) and enter the IP address of the Netegrity Policy Server. The remaining values are port numbers. Consult the Netegrity Policy Design documentation as to those values. Ensure that the plain radio box is checked.



Generating an Agent Configuration File

Once you have created a custom agent and a host configuration, you can now generate a agent configuration file. This configuration file provides the information needed by a custom agent to initiate a connection to the Netegrity Policy Server. To generate an agent configuraiton file, use the Netegrity command line utility, smregghost.exe in Windows, and smregghost on *linux:

% smregghost.exe -i ipAddress[:port] -u username -p password -hn agentName -sh sharedSecret -hc hostConfigObject [-f filePath]

ipAddress[:port]	IP address of the machine where Policy Server is running. The port specification is optional.
username	Policy Server administrator user name.
password	Policy Server administrator password.
agentName	Name of the Agent object created above.
sharedSecret	Shared secret for the Agent specified above.
hostConfigObject	Name of the Host Configuration Object specified above.
filePath	The relative or absolute path to the agent configuration file to be created. If no file path is specified then by default a configuration file called SmHost.conf will be created in the current directory where the command was issued.

For example:

```
% smreghost.exe -i 298.168.5.12 -u SiteMinder -p password -hn "ALSM Agent" -sh password -hc MyDefaultHostSettings -f C:\Netegrity\SmHost.conf
```

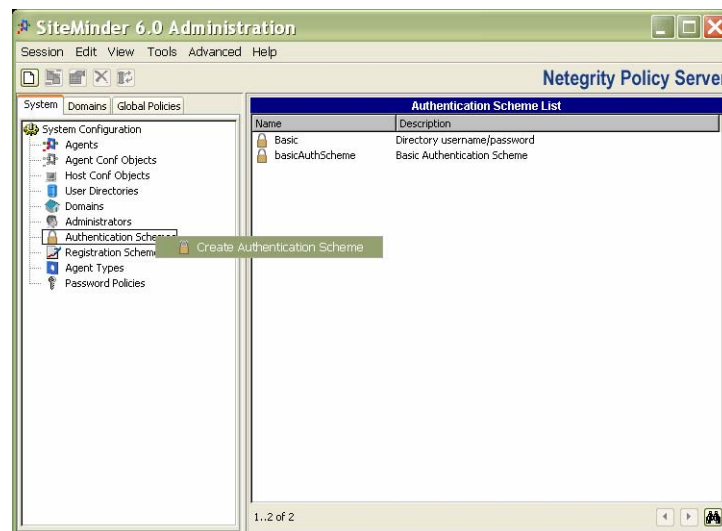
Creating Netegrity Schemes, Domains, Realms, Rules and Policies

The above sections detail the necessary steps to allow the SOA Management System to interact with Netegrity SiteMinder. However, to protect web services domains, realms, rules and policies in Netegrity need to be configured.

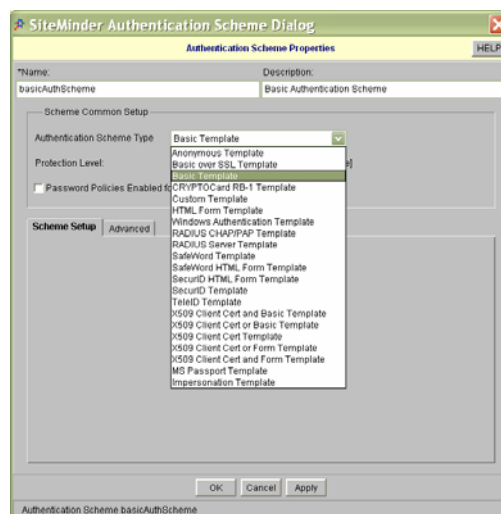
Creating an Authentication Scheme

ALSM supports the SiteMinder Basic Template. The Basic Template expects credentials in the form of a username and password. For Netegrity authentication, ALSM will collect these credentials from the following:

To create a basic authentication scheme, in the System tab, right mouse click on the Authentication Scheme node and select the Create Authentication Scheme menu option.

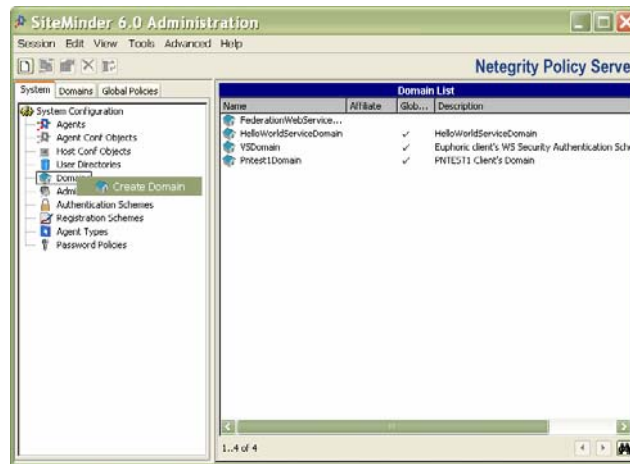


Provide a name and optional description for the scheme. Choose Basic Template as the Authentication Scheme Type. Uncheck the Password Policies Enabled for this Authentication Scheme box. Click OK.

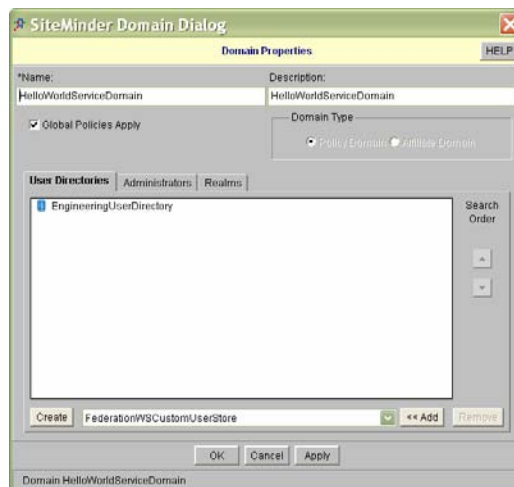


Creating a Policy Domain

As defined by Netegrity, a Policy Domain is a “logical grouping of resources associated with one or more user directories.” For example, one can create a policy domain for each business unit and in that policy domain are the set of realms, rules and policies associated with that unit. To create a Policy Domain, in the System tab, right mouse click on the Domains node and select Create Domain:



Provide a name such as HelloWorldServiceDomain and optional description for the domain.

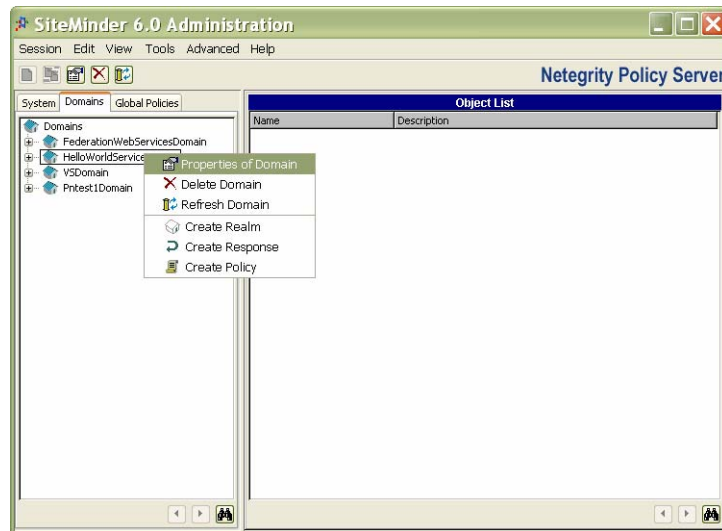


If a user directory has already been configured, then select it and click the Add button. Otherwise, a user directory will need to be configured.

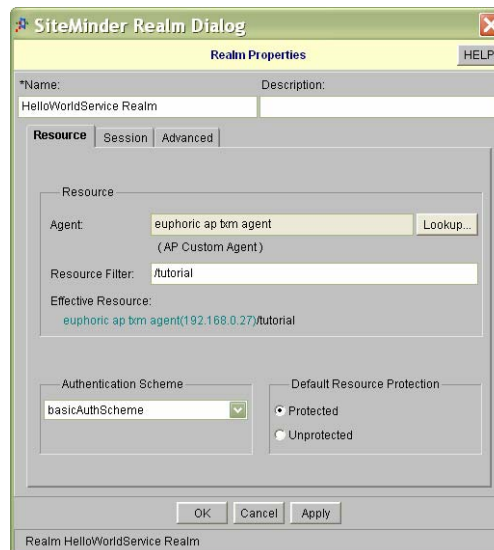
SIT

Creating a Realm

As defined by Netegrity, a Realm is a “cluster of resources within a policy domain grouped together according to security requirements. A realm is usually defined for resources that reside in a common location on your network.” To create a realm, in the Domains tab, right mouse click on the domain created above and select Create Realm:



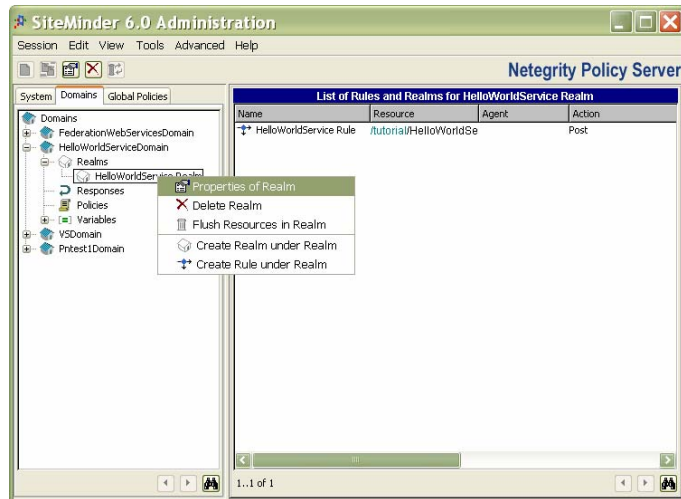
Provide a name such as HelloWorldServiceRealm and optional description. Click the Lookup button in the Resource tab to find the agent(s) created above. Select the agent created above. Enter /tutorial as the Resource Filter for this example. Select as the Authentication Scheme the basic authentication scheme created above. Click OK.



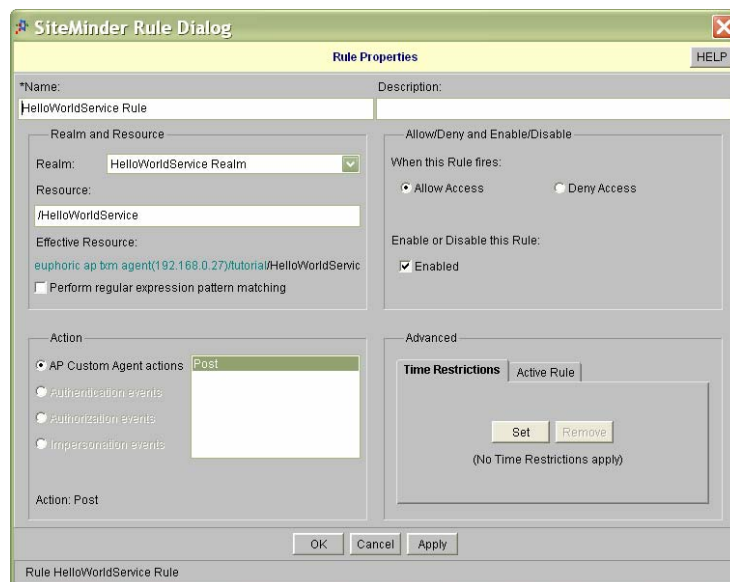
Later to change the authentication scheme to the alternative WS-Security Username Token scheme change the value of the Authentication Scheme in this Realm dialog.

Creating a Rule

As defined by Netegrity, Rules “identify specific resources and either allow or deny access to the resources.” Rules are associated with specific realms and each rule can be associated with all or a subset of the resources in a realm. To create a rule, expand on the domain node created above and right mouse click on the realm created above. Select the Create Rule option:

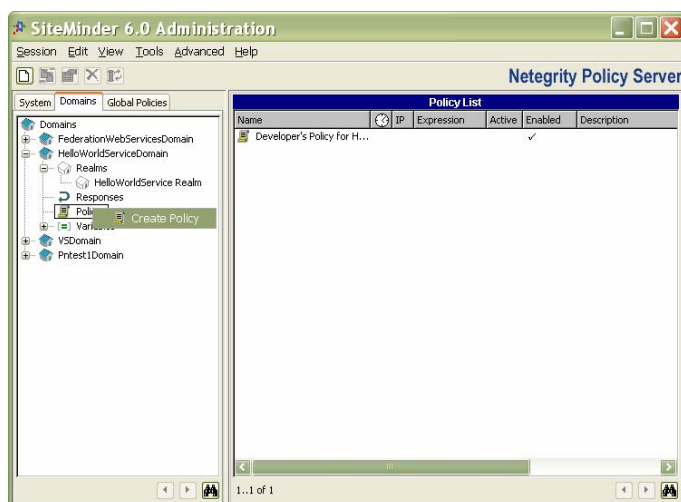


Provide a name and optional description for the Rule. For this example, enter /HelloWorldService for the Resource value. Ensure that the rule is Enabled. Click OK.



Creating a Policy

As defined by Netegrity, Policies “define how users interact with resources.” A policy links together users and rules. To create a policy, right mouse click on the Policies tab and select Create Policy:



SiteMinder Policy Dialog

Policy Properties HELP

*Name: Developer's Policy for HelloWorldService Description:

☒ Enabled

Users Rules IP addresses Time Expression Advanced

EngineeringUserDirectory

Name	User Class
cn=developers,ou=groups,dc=pune,dc=amberpoint,dc=com	groupofuniquenames

Add/Remove... ☐ Allow Nested Groups
(EngineeringUserDirectory is an Authentication and Authorization Directory)

OK Cancel Apply

Policy Developer's Policy for HelloWorldService

Provide a name and optional description. In the Users tab click on the Add/Remove button and add users and groups associated with this policy. Click OK.

Users/Groups HELP

Users/Groups for EngineeringUserDirectory

Current Members

Name	User Class
cn=developers,ou=groups,dc=pune,dc=amberpoint,dc=com	groupofuniquenames

Available Members

Name	User Class
ou=people,dc=pune,dc=amberpoint,dc=com	organizationalperson
ou=groups,dc=pune,dc=amberpoint,dc=com	organizationalgroup
cn=Directory Administrators,dc=pune,dc=amberpoint,dc=com	groupofuniquenames
cn=p4admins,ou=groups,dc=pune,dc=amberpoint,dc=com	groupofuniquenames

1.4 of 4

Exclude

Manual Entry

Entry:

Action: Validate DN Add to Current Members

Expression Editor

Create New Expression ... Edit Search Expression ...

OK Cancel Apply

To add users, move users to the left table

In the Rules tab, click the Add/Remove Rules button and add rules associated with this policy.

SiteMinder Policy Dialog HELP

Policy Properties

*Name: Developer's Policy for HelloWorldService Description:

☒ Enabled

Users **Rules** IP addresses Time Expression Advanced

Rule	Realm	Response
HelloWorldService Rule	HelloWorldService Realm	

Add/Remove Rules... Set Response... Set Global Response... Remove Response

OK Cancel Apply

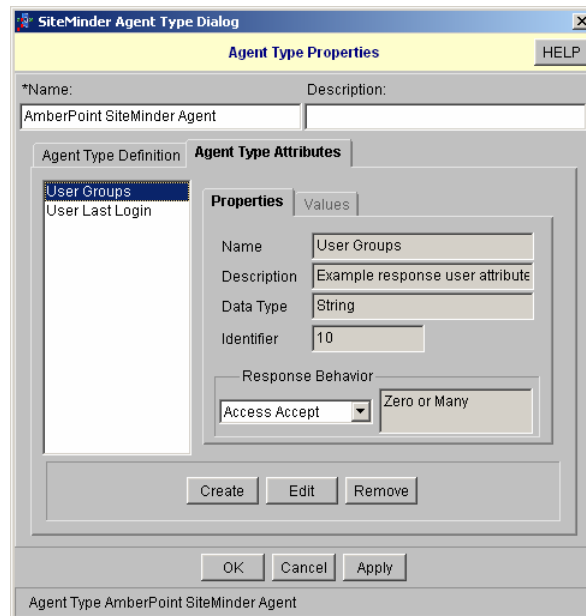
Policy Developer's Policy for HelloWorldService

Configuration Retrieval of User Attributes and Roles

During authentication to Netegrity, user attributes and role information can be retrieved from Netegrity. To retrieve this information requires modifying and adding configurations in the Netegrity Policy Server. The following provides a simple example of how to retrieve the user role information. *Please refer to the Netegrity Policy Design guide for detailed instructions on how to create response attributes.*

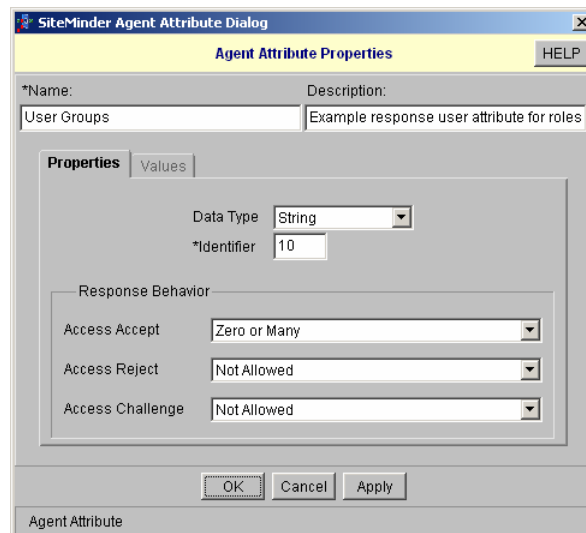
Custom Agent Type Attribute

Configure the custom agent type representing the ALSM agent created above to have an attribute. In this example, the attribute has the name, User Groups, to indicate the groups or roles of the user. Go to the properties dialog for the ALSM custom agent type.



The screenshot shows the 'SiteMinder Agent Type Dialog' with the 'Agent Type Properties' tab selected. The 'Name' field is 'AmberPoint SiteMinder Agent'. The 'Agent Type Definition' list on the left contains 'User Groups' and 'User Last Login'. The 'Properties' tab is active, showing fields for 'Name' (User Groups), 'Description' (Example response user attribute), 'Data Type' (String), and 'Identifier' (10). The 'Response Behavior' section has a dropdown set to 'Access Accept' and a text field set to 'Zero or Many'. At the bottom are 'Create', 'Edit', and 'Remove' buttons, and at the very bottom are 'OK', 'Cancel', and 'Apply' buttons. The status bar at the bottom reads 'Agent Type AmberPoint SiteMinder Agent'.

Go to the Agent Type Attributes tab and click on the Create button.

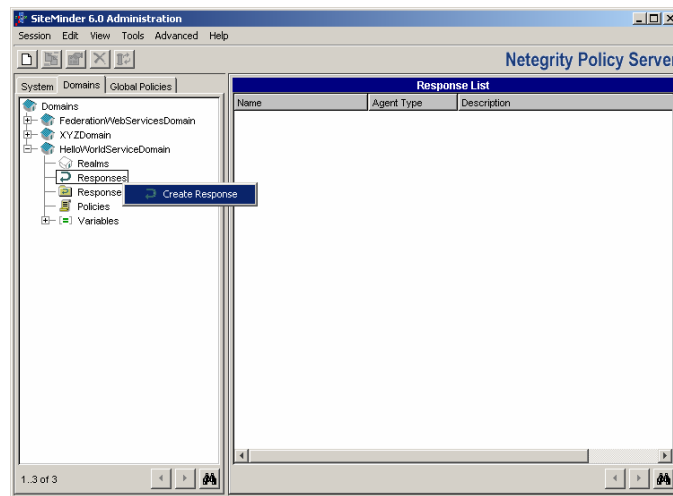


The screenshot shows the 'SiteMinder Agent Attribute Dialog' with the 'Agent Attribute Properties' tab selected. The 'Name' field is 'User Groups' and the 'Description' field is 'Example response user attribute for roles'. The 'Properties' tab is active, showing 'Data Type' (String) and '*Identifier' (10). The 'Response Behavior' section has three dropdowns: 'Access Accept' set to 'Zero or Many', 'Access Reject' set to 'Not Allowed', and 'Access Challenge' set to 'Not Allowed'. At the bottom are 'OK', 'Cancel', and 'Apply' buttons. The status bar at the bottom reads 'Agent Attribute'.

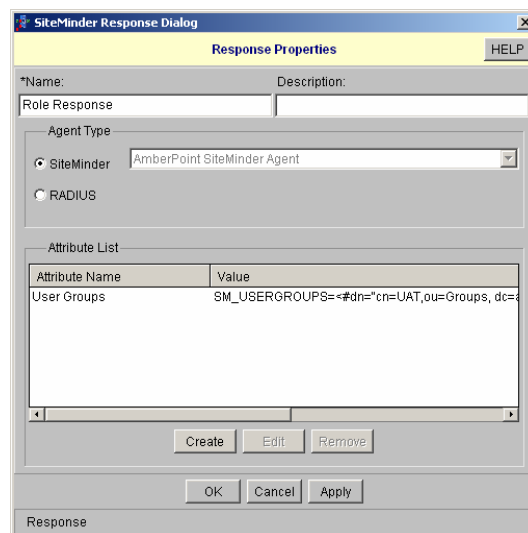
Create the attribute with the above parameters.

Response Attribute

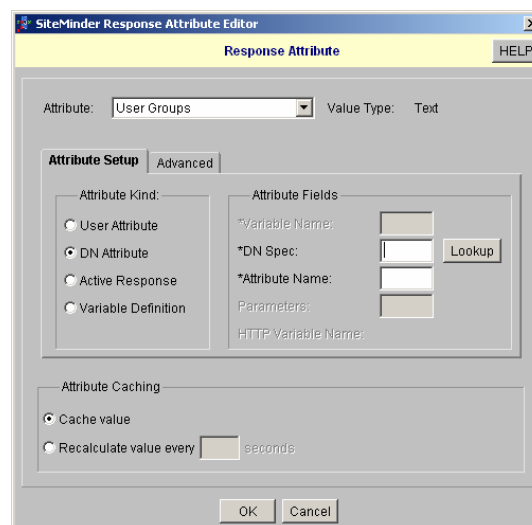
Next, create a response attribute by navigating to the Domains tab in the Netegrity Policy Server window.



For this example create the response with the following name and select the Agent Type as the ALSM agent type created above.



Create an attribute by clicking the Create button. Select the following parameters for the attribute.



In this example, the user groups are specified in the attribute. Enter the following value using the Script field in the Advanced tab:

```
SM_USERGROUPS=<#dn="cn=UAT,ou=Groups,dc=amberpoint,dc=com"
attr="cn"#>^<#dn="cn=SIT,ou=Groups,dc=amberpoint,dc=com" attr="cn"#>.
```

The screenshot shows the 'SiteMinder Response Attribute Editor' dialog box. The title bar reads 'SiteMinder Response Attribute Editor'. The main window has a yellow header bar with the text 'Response Attribute' and a 'HELP' button. Below the header, there is a section for 'Attribute: User Groups' and 'Value Type: Text'. The 'Attribute Setup' tab is selected, and the 'Advanced' sub-tab is active. In the 'Script' field, the following LDAP query is entered: `SM_USERGROUPS=<#dn="cn=UAT,ou=Groups,dc=amberpoint,dc=com" attr="cn"#>^<#dn="cn=SIT,ou=Groups,dc=amberpoint,dc=com" attr="cn"#>.` Below the script field, there is an 'Attribute Caching' section with two radio buttons: 'Cache value' (selected) and 'Recalculate value every' (with a text box for seconds). At the bottom of the dialog are 'OK' and 'Cancel' buttons.

To learn how to configure Netegrity to obtain group information stored in a directory server, see the *Netegrity Policy Design guide*, section *Working with LDAP Directories*.