



FORUM SYSTEMS SENTRY™ VERSION 9 CA™ SITEMINDER INTEGRATION GUIDE



Legal Marks

No portion of this document may be reproduced or copied in any form, or by any means – graphic, electronic, or mechanical, including photocopying, taping, recording, or information retrieval system – without expressed permission from Forum Systems, Inc.

FORUMOS™ Firmware, Forum Systems XMLSec™ WebAdmin, Forum Systems XML Security Appliance™, Forum Sentry™, Forum Presidio™, Forum XWall™, Forum Sentry™ Web Services Gateway, Forum Presidio™ OpenPGP Gateway, Forum FIA Gateway™, Forum XWall Type-PCI™, Forum XWall® Web Services Firewall and Forum XRay™ are trademarks and registered trademarks of Forum Systems, Inc.

All other products are trademarks or registered trademarks of their respective companies.

Copyright © 2002-2024 Forum Systems, Inc. – All Rights Reserved.

Forum Sentry™ Version 9 CA™ SiteMinder Integration Guide, published May 2024.

D-OEM-SE-028154

Table of Contents

INTRODUCTION TO THE CA SITEMINDER INTEGRATION GUIDE.....	1
Audience for the CA SiteMinder Integration Guide.....	1
LOGON TO PRODUCT	2
FORUM SYSTEMS NATIVE CA SITEMINDER INTEGRATION.....	3
Authentication Stage	4
Authorization Stage	4
Session Caching.....	4
Failed Authentication and Authorization.....	5
Sample SiteMinder Host Configuration Object.....	5
Protecting Your Virtual Resources	7
Add a Run-time SiteMinder Policy and Register New Trusted Host on the Policy Server.....	10
Adding a RunTime SiteMinder Policy.....	10
Registering the New Trusted Host on the Policy Server	11
Run-time Access Control and SiteMinder Group Privileges.....	12
Assign Run-time Privilege to SiteMinder Policies.....	13
Add a Design-time SiteMinder Policy	14
Design-time Access Control and SiteMinder Group Privileges	16
Configure a SiteMinder Policy for Advanced Password Services	17
Adding a Filter Expression for SiteMinder Advanced Password Services	17
Removing a Filter Expression for SiteMinder Advanced Password Services	18
Administer the Policy Server	19
SiteMinder Advanced Password Services with Tasks	20
Use Case with SiteMinder APS: Map Attributes To XML Task	20
Add the Map Attributes to XML Task for SiteMinder Policy	20
Generate a cookie using a WS-Security Header Task	22
Use Run Task List to View the SAML Cookie	25
INVALIDATE SESSION COOKIES.....	27
Invalidating Session Cookies - The Logout Task	27
Adding the Logout Task.....	27
APPENDIX	29
Appendix A - Constraints for SiteMinder Policies	29
Appendix B - Specifications of SiteMinder Policies	29
INDEX	30

INTRODUCTION TO THE CA SITEMINDER INTEGRATION GUIDE

Audience for the CA SiteMinder Integration Guide

The *Forum Systems Sentry™ Version 9 CA™ SiteMinder Integration Guide* is for System Administrators who will manage access control with CA SiteMinder versions 5.5 and 6.0 users and policies.

Conventions Used in CA SiteMinder Integration Guide

A red asterisk (*) aligned with a field term means that this field is required. In this and other documentation, the Web Administration Interface is referred to as the WebAdmin and the Forum XML Security Appliance™ is referred to as the 'device', 'product' or 'system'.

In this document, all data or commands that must be entered or selected are displayed in boldface. Example:

User name: **johnsmith**
Password: *********

UI screens which display a STATUS column represent the following states:

- Green status light = enabled policy.
- Yellow status light = a required functional element of this policy is disabled.
- Red status light = disabled policy.

Throughout this and other documents in the Documentation Set, repetitive actions such as:

- View / edit a policy.
- Enable / disable a policy.
- Delete a policy.
- Rename a policy.
- Limit display of policies with Search or Max Results fields.

are not shown. For more information, refer to the Common Operations section of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*.

Customers with plug-in licenses on the system, confirm that your Integration License is visible on the General Info screen under the SUPPORTED FEATURES section.

Assumptions

This document assumes that the reader will review the appropriate chapter before performing the operations listed in this document. This document also assumes that the reader is familiar with CA SiteMinder Policy Server Version 5.5 and 6.0.

LOGON TO PRODUCT

How To Log in to the Product

Log in to the WebAdmin from your browser with an HTTP request to the IP:port configured during installation. By default, the port used is 5050.

https://<IP>:5050



FORUM SYSTEMS LOGIN - PHOENIX	
User Name*:	<input type="text"/>
Password*:	<input type="password"/>
<input type="button" value="Login"/>	

1. With your browser open, enter the **URL** supplied by your IT Administrator to access the WebAdmin UI. A Security Alert message appears with the default SSL certificate.
2. Press **Yes** to accept the certificate. The Login screen appears.
3. The Enter Network Password screen appears.
4. Enter a **User Name** and **Password**, and then click **Login**. The WebAdmin appears, displaying the Getting Started screen.

How To Logout of the Product

Logout of the WebAdmin while on any screen by clicking the LOGOUT button on the lower right of the screen.



FORUM SYSTEMS NATIVE CA SITEMINDER INTEGRATION

Forum Systems provides a native integration with an embedded CA SiteMinder Agent to provide a best-of-breed web services security solution and web services ID management in conjunction with a CA Policy Server deployment. The native SiteMinder Agent resides on the Forum Systems device and communicates directly with the CA Policy Server for Authentication and Authorization decisions. This integration provides a simple means of leveraging existing SiteMinder policy server deployments for Web Services ID management and also provides the ability to use SiteMinder Policy Server as the user store for Administrators of the Forum Systems device.

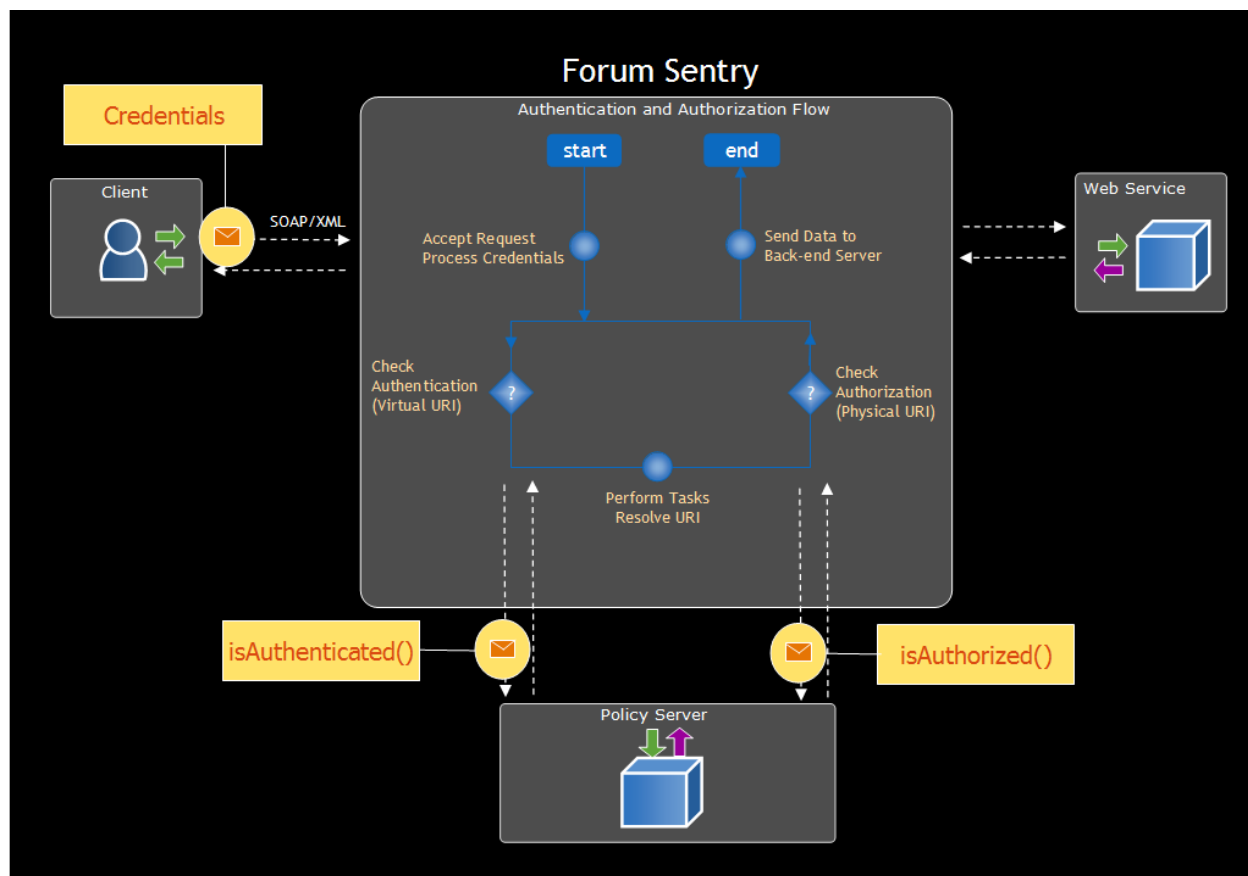


Figure 1: Authentication and Authorization Flow.

Credential Consumption

The Forum device provides a number of protocol and document based credential tasks. The credential consumption tasks that are applicable for the CA Policy Server Integration are: Basic Authentication, SSL X509 Authentication, SiteMinder cookie Authentication, WSS-Username Header, WSS-X.509 Header, XML mapping, digital signature, and SAML.

Run-time Authentication and Authorization

One of the primary use cases for deployed production solutions is having the Forum Systems device placed at the perimeter of Web Services and Web Application access points such that a single point of decision making can be accomplished for Intrusion Detection and Prevention, Web Services Security, and Authentication and Authorization for access to Web Services and Web Application resources within an environment. The ID management and access control portion of this perimeter defense takes place in two stages. The first stage is the Authentication stage, the second is the Authorization stage.

Authentication Stage

The Authentication stage often occurs when the access is first received to the Forum Systems device. The authentication may be in the form of HTTP Basic Authentication, HTTP Digest Authentication, HTTP Form POST Authentication, an existing SiteMinder session cookie, document based SAML assertion, WSS-Username tokens, WSS-X509 tokens, XML mapping, digital signature, or SSL X509 Client Authentication. The Authentication stage of the ID management and access control checks the validity of the incoming user against the SiteMinder policy server domain in which the integrated Forum SiteMinder Agent has been configured to belong. The authentication check verifies if the Virtual URI or Physical URI is configured to be a protected resource in SiteMinder. If the Virtual URI or Physical URI is protected, the credentials are then used to determine whether the user belongs within the domain of allowable users. By default Sentry includes the back-end URL in the authentication check, if the back-end URL is known. Setting the “protect virtual resource” checkbox on a WSDL or XML policy, will cause Sentry to always use the Virtual URI instead of Physical URI for both authentication and authorization for that policy.

Authorization Stage

Once the URL is confirmed to be protected and the credentials for the users are known to be valid, an `isAuthorized()` call will be performed from the Forum SiteMinder Agent to the CA Policy Server which determines whether or not the authenticated user is authorized to access the back-end URL resource. The `isAuthorized()` call includes the protected resource, the method POST, and the IP address of the incoming request. The Policy Server is configured to protect resources by first defining domains, defining realms within those domains, and finally defining rules within those realms. Authorization is required for any resources that are configured to be protected resources within SiteMinder Policy server.

Session Caching

For single sign-on deployments, use of a session caching mechanism, also known as persistent sessions, can be configured on the Policy Server in order to reuse valid session information for subsequent requests without having to re-authenticate. Since Forum Systems integrates directly with a native embedded CA SiteMinder Agent, the session caching capabilities are supported. Each defined protected realm within a Policy Server Domain contains a Session tab where settings include Max Timeout, Max Idle Timeout, Persistent Sessions, and Validation periods.

Sentry caches two different type of responses from the Policy Server: `isProtected` and `login`. Once a request is made to Sentry, the URI is checked against the PolicyServer to see if the resource is protected. The information is kept in the cache for the amount of time configured in the Policy Server. Sentry also caches successful logins, it caches the username, password and any attributes returned by the Policy Server. Subsequent login requests are checked locally without sending a request to the Policy Server. Each Sentry device contains its own copy of the cache. In other words, the cache is not shared among multiple Sentry instances.

Please refer to the CA Documentation Section “Configuring a Realm Protected by a SiteMinder Web Agent” for detailed information about how to configure session caching on the Policy Server. The Forum SiteMinder Agent will use these values to determine cache validity periods for credentials and realms. Once a cached session token expires, credentials must again be submitted to SiteMinder Policy Server to validate and provide new session information. There is no configuration required on the Forum server to support this - all configuration settings for caching are managed on the policy server realm.

Failed Authentication and Authorization

Events that fail Authorization or Authentication checks trigger either the “Authentication Failed” IDP rule, or the “Authorization Failed” IDP Rule. Handling of these events from a logging, enforcement, and notification can be managed within the IDP Policies section of the Forum Web Administration interface. Debugging failed Authentication and Authorization can be accomplished by enabling debug logging on both the Forum server and the CA Policy Server for the Authentication and Authorization services.

The following sections detail the integration steps between Forum Systems and CA SiteMinder Policy server to configure policies to communicate and perform Authentication and Authorization decisions. The integration architecture scenarios presented are designed to function with SiteMinder versions 5.5 and 6.0.

Sample SiteMinder Host Configuration Object

The following graphic displays a sample SiteMinder host configuration object. When creating a new SiteMinder policy on the Forum agent you have the ability to also create a new trusted host entry on the policy server. A host configuration object is required for these steps.

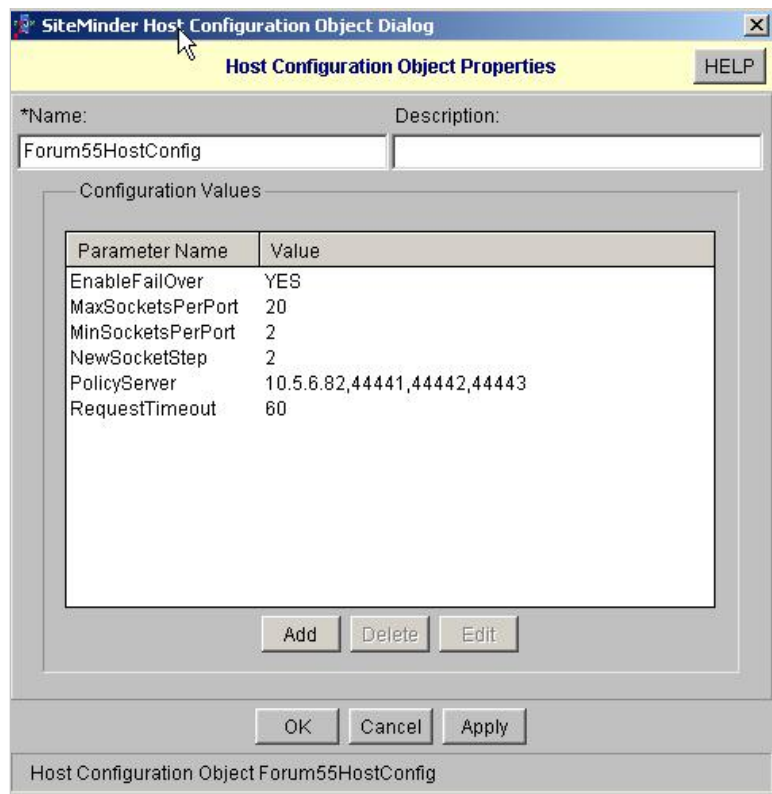


Figure 2: Sample SiteMinder Host Configuration Object.

Overview of SiteMinder Policies

Navigate to the ACCESS category of the WebAdmin UI and select **SiteMinder**. The SITEMINDER POLICY screen displays a summary view of existing policies and allows for creation or editing of policies. In the following example, the SiteMinder policy, SiteMinder-SM100 defines the settings for the CA SiteMinder Host and Web Agent embedded in the Forum device. This population of users allowed access to the protected SiteMinder resources is treated as a group within the Forum device and can have Access Control List privileges associated just as with any other type of group.

<input type="checkbox"/>	POLICY NAME	STATUS	AGENT NAME	ADMIN RESOURCE	POLICY SERVER
<input type="checkbox"/>	SiteMinder_Administration	●	demoagent1	/forum/demo1/auth/auth.htm	10.5.6.82
<input type="checkbox"/>	SiteMinder_RunTime	●	demoagent	/forum/demo/auth/auth.htm	10.5.6.82

SiteMinder Screen Terms

The SiteMinder Policies screen includes a listing of all existing SiteMinder network policies. The following table describes each term and definition on the SITEMINDER screen:

TERM	DEFINITION
POLICY SERVER	
Saved SmHost.conf	Current configuration file with the SiteMinder host name for this device and the IP and Port settings used to communicate with the Policy Server.
SmHost.conf	Configuration file with the SiteMinder host name for this device and the IP and Port settings used to communicate with the Policy Server.
Policy Server Administration URL	The directory for the SiteMinder policy server administration GUI. The default value "/siteminder" matches the SiteMinder default.
Policy Name	Name of the SiteMinder policy on the appliance.
Status	<ul style="list-style-type: none">Green status light = enabled policy.Yellow status light = a required functional element of this policy is disabled.Red status light = disabled policy. <p>SiteMinder policies are automatically enabled upon creation.</p>
Agent Name	The name of this SiteMinder Web Agent requesting services from the SiteMinder Policy Server.
Administration Resource	TheResource Name used for SiteMinder authorization of Forum Systems Sentry™ administrators.
Policy Server	The IP address of the SiteMinder server.

Protecting Your Virtual Resources

Note: When CA SiteMinder is configured, an option on the WSDL and XML policies Setting tab, the Protect virtual resource option, allows configuring authentication and authorization for either the virtual or physical resources.

The screenshot shows the 'Settings' tab for a WSDL policy. The 'Policy Name' is 'QAService'. The 'Protect virtual resource' checkbox is checked.

Services	Task Lists	Settings	IDP Rules	Documents
WSDL POLICY SETTINGS				
Policy Name*:		QAService		
Policy Description:				
Protect virtual resource:		<input checked="" type="checkbox"/>		

- With the **Protect virtual resource** checkbox checked on the Settings tab of a WSDL or XML policy, the system uses the Sentry Virtual Directory when authenticating and authorizing against the back end server.
- With the **Protect virtual resource** checkbox unchecked on the Settings tab of a WSDL or XML policy, the system uses the Sentry physical URI when authenticating and authorizing against the back end server.

Components of the Forum SiteMinder Policy

From the SITEMINDER screen, select **New**, or select the link of an existing policy to view the settings for an existing policy.

The screenshot shows the 'SITEMINDER POLICY CONFIGURATION' screen. The 'Policy Name' is 'SiteMinderRunTime'. The 'Enable privileged access' radio button is set to 'No'. The 'Administration Resource' is '/forum'. The 'Response Variable Identifier' is '224'. The 'Agent Name' is 'demoagent'. The 'OnAccept Text Filter' is '*.will expire.*'. The 'Response Text Mapping' section has two checkboxes, 'FILTER EXPRESSION' and 'REPLACE EXPRESSION', both of which are unchecked.

SITEMINDER > SITEMINDER POLICY CONFIGURATION	
SITEMINDER POLICY	
Policy Name:	SiteMinderRunTime
Enable privileged access:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Restrict Menus:	<input type="checkbox"/>
Role policy:	<input type="text"/>
Administration Resource*:	/forum
Response Variable Identifier*:	224
Agent Name*:	demoagent
ADVANCED PASSWORD SERVICES	
OnAccept Text Filter:	*.will expire.*
Response Text Mapping	
<input type="checkbox"/> FILTER EXPRESSION	REPLACE EXPRESSION
<input type="checkbox"/>	
<input type="button" value="Test"/> <input type="button" value="Remove"/> <input type="button" value="Apply"/> <input type="button" value="Save"/>	

SiteMinder Policy Configuration Screen Terms

When configuring your SiteMinder Policy Server from the SITEMINDER POLICY CONFIGURATION screen, please consider the following:

TERM	DEFINITION
SITEMINDER POLICY	
Policy Name	The name given to this SiteMinder policy. SiteMinder policies may be 1-32 alphanumeric characters.
Enable privileged access	Both options refer to design-time privileges: <ul style="list-style-type: none">• With Yes selected, the users have access to the WebAdmin as a super user.• With No selected, the users have access to the WebAdmin with only the Domain privileges set for the Group associated with this policy.
Restrict Menus	When the SiteMinder Policy grants WebAdmin access this option can be used to restrict the screen the user has access to. This option can only be used if enable privileged access is not enabled, since super users have access to all the screens.
Role Policy	The name of the RolePolicy used to restrict the menus. The RolePolicy consists of a list of all the screens the user has access to.
Administration Resource	The Resource Name used for SiteMinder authorization of Forum Systems Sentry™ administrators.
Response Variable Identifier	The SiteMinder web agent response attribute that is used to send custom attributes from SiteMinder to the Forum product. This value must match the id for custom attributes defined by the SiteMinder administrator. For example, if the SiteMinder web agent response attribute type used is WebAgent-HTTP-Header-Variable, the default attribute identifier for WebAgent-HTTP-Header-Variable attributes configured in SiteMinder is 224. <div>Note: Response Variable Identifier valid values are from 0 to 255. The default is 224.</div>
Agent Name	The name of this Web Agent requesting services from the SiteMinder Policy Server.
Cache timeout (minutes)	How long Sentry will cache information returned from requests to the SiteMinder server.
ADVANCED PASSWORD SERVICES	
OnAccept Text Filter	"OnAccept Text Filter", if specified, denies access when a SiteMinder WebAgent-OnAccept-Text attribute received during APS authentication does not match the specified regular expression filter. The default value ".*will-expire.*" allows access when APS password pre-expiration warnings are received, but not when APS indicates that the password must be changed.
Response Text Mapping	The Response Text Mapping area uses regular expression filter-and-replace expressions to manipulate WebAgent-OnAccept-Text and WebAgent-OnReject-Text messages received during APS authentication. These messages appear in custom SiteMinder attribute values and in Forum-generated SOAP faults. No APS message manipulation is performed by default.

SiteMinder Trusted Host Registration Screen Terms

From the SITEMINDER screen, select Create to view the TRUSTED HOST REGISTRATION screen. The following terms and definitions are presented when registering a trusted host with SiteMinder:

TERM	DEFINITION
REGISTRATION INFORMATION	
Server	SiteMinder policy server IP address.
Port	SiteMinder policy server port.
Name for host to be registered	Name of the trusted host to be created for this physical machine
Name of host configuration object	SiteMinder Host Config object. For more information, refer to the Sample SiteMinder Host Configuration Object section.
Administrator username	SiteMinder administrator username
Administrator password	SiteMinder administrator password

Note: View these terms in the Add a SiteMinder Policy and Register the Forum Product with SiteMinder section, presented later in this document.

SiteMinder Policy Examples

Example configurations for SiteMinder policies include:

- Add a Run-time SiteMinder Policy and Register New Trusted Host on the Policy Server.
- Run-time Access Control and SiteMinder Group Privileges.
- Assign Run-time Privilege.
- Add a Design-time SiteMinder Policy.
- Design-time Access Control and SiteMinder Group Privileges.
- Assign Design-time Privileges.
- Configure a SiteMinder Policy for Advanced Password Services.
- Add a Filter Expression for SiteMinder Advanced Password Services.
- Remove a Filter Expression for SiteMinder Advanced Password Services.
- Administer the Policy Server.

Note: For information on editing / viewing, deleting or enabling / disabling a SiteMinder Policy, refer to the Common Operations of the *Forum Systems Sentry™ Version 9 Web-based Administration Guide*. To rename a SiteMinder policy, delete it, and re-create it.

Add a Run-time SiteMinder Policy and Register New Trusted Host on the Policy Server

While adding a SiteMinder policy to the Forum Systems product, you may also create a SmHost.conf file which provides communication to the host server. This creates a trusted host entry on the Policy Server for this physical machine. You can also load a SMHost.conf file provided to you by your SiteMinder administrator.

Adding a RunTime SiteMinder Policy

Follow these steps to add a SiteMinder policy for run-time.

The screenshot shows the 'SITE MINDER' configuration interface. Under the 'POLICY SERVER' section, there are fields for 'Saved SmHost.conf:' (with a link to 'SmHost.conf'), 'SmHost.conf:', 'Policy Server Administration URL:' (set to '/siteminder'), and buttons for 'Browse...', 'Create', 'Administer', and 'Save'. Below this is a table with columns: 'POLICY NAME', 'STATUS', 'AGENT NAME', 'ADMIN RESOURCE', and 'POLICY SERVER'. The table is currently empty, showing 'No items to display'. At the bottom of the table are buttons for 'Delete', 'Enable', 'Disable', and 'New'.

The screenshot shows the 'SITE MINDER > SITE MINDER POLICY CONFIGURATION' screen. The 'SITEMINDER POLICY' section contains fields for 'Policy Name:' (set to 'SiteMinderRunTime'), 'Enable privileged access:' (radio buttons for 'Yes' and 'No', with 'No' selected), 'Restrict Menus:' (checkbox), 'Role policy:' (dropdown), 'Administration Resource*:' (set to '/forum'), 'Response Variable Identifier*:' (set to '224'), and 'Agent Name*:' (set to 'demoagent'). The 'ADVANCED PASSWORD SERVICES' section includes 'OnAccept Text Filter:' (set to '.*will expire.*') and 'Response Text Mapping' (checkboxes for 'FILTER EXPRESSION' and 'REPLACE EXPRESSION'). At the bottom are buttons for 'Test', 'Remove', 'Apply', and 'Save'.

- From the ACCESS User Policies category of the Navigator, select **SiteMinder** and the SITEMINDER screen appears.
- Select **New**.
- On the SITEMINDER POLICY CONFIGURATION screen, in the Policy Name field, enter a **name** for this SiteMinder policy.

Note: SiteMinder policy names must be unique and may be from 1 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.

- Click **No** for Enable privileged access radio button.
- In the Administration Resource field, add the **Resource Name** used for SiteMinder authorization of Sentry administrators.
- In the Response Variable Identifier field, retain the default value of 224.
- In the Agent Name field, enter the **name** of the Web Agent that is requesting services from the SiteMinder Policy Server.
- If you desire to cache responses from SiteMinder then change the default value of the **Cache timeout** to the desired time in minutes.

- Select **Save** and the SITEMINDER screen refreshes with the message “SiteMinder policy configuration saved” visible at the top of the screen.

Registering the New Trusted Host on the Policy Server

Follow these steps to register the Sentry product.

SITEMINDER

POLICY SERVER

Saved SmHost.conf: [SmHost.conf](#)

SmHost.conf*: Browse... **Create**

Policy Server Administration URL*: /siteminder **Administer**

Save

<input type="checkbox"/>	POLICY NAME	STATUS	AGENT NAME	ADMIN RESOURCE	POLICY SERVER	
<input type="checkbox"/>	SiteMinderRunTime	●	demoagent	/forum/demo/auth/auth.htm	10.5.6.82	Delete Enable Disable New

SITEMINDER > TRUSTED HOST REGISTRATION

REGISTRATION INFORMATION

Server*: 10.5.6.82

Port: 44442

Name for host to be registered*: forumhost300

Name of host configuration object*: Forum61HostConfig

Administrator username*: SiteMinder

Administrator password*: ••••••••

Register

- On the SITEMINDER screen, aligned with the SmHost.conf: field, click **Create**.
- On the TRUSTED HOST REGISTRATION screen, in the Server field, enter the **IP address** of the SiteMinder server.
- In the Port field, retain the default value of 44442.
- In the Name for host to be registered field, enter a **name** that represents the physical machine name to be created as a trusted host on the SiteMinder server.
- In the Name of host configuration object, enter a **name** that represents the SiteMinder Host Config object.
- In the Administrator username field, enter the **SiteMinder administrator username**.
- In the Administrator password field, enter the **SiteMinder administrator password**.
- Click **Register** to run the native smreghost process of creating a trusted host entry on the policy server. The SITEMINDER POLICY CONFIGURATION screen refreshes with the Saved SmHost.conf file from the trusted host registration.

Run-time Access Control and SiteMinder Group Privileges

Access privileges may be set for SiteMinder policy from the User ACLs screen, which can be used to grant the Execute (Run-Time) privilege. The User ACL DETAILS screen displays the privileges enabled for the SiteMinder policies. The Forum SiteMinder policy itself represents a population of users allowed to access the resources protected by SiteMinder. The Forum SiteMinder policy will appear in the User ACLs screen just as a standard group will appear, and Administrators can set Execute (for run-time processing) privilege for the SiteMinder policy. The following graphic displays the relationship between SiteMinder policies and run-time access control:

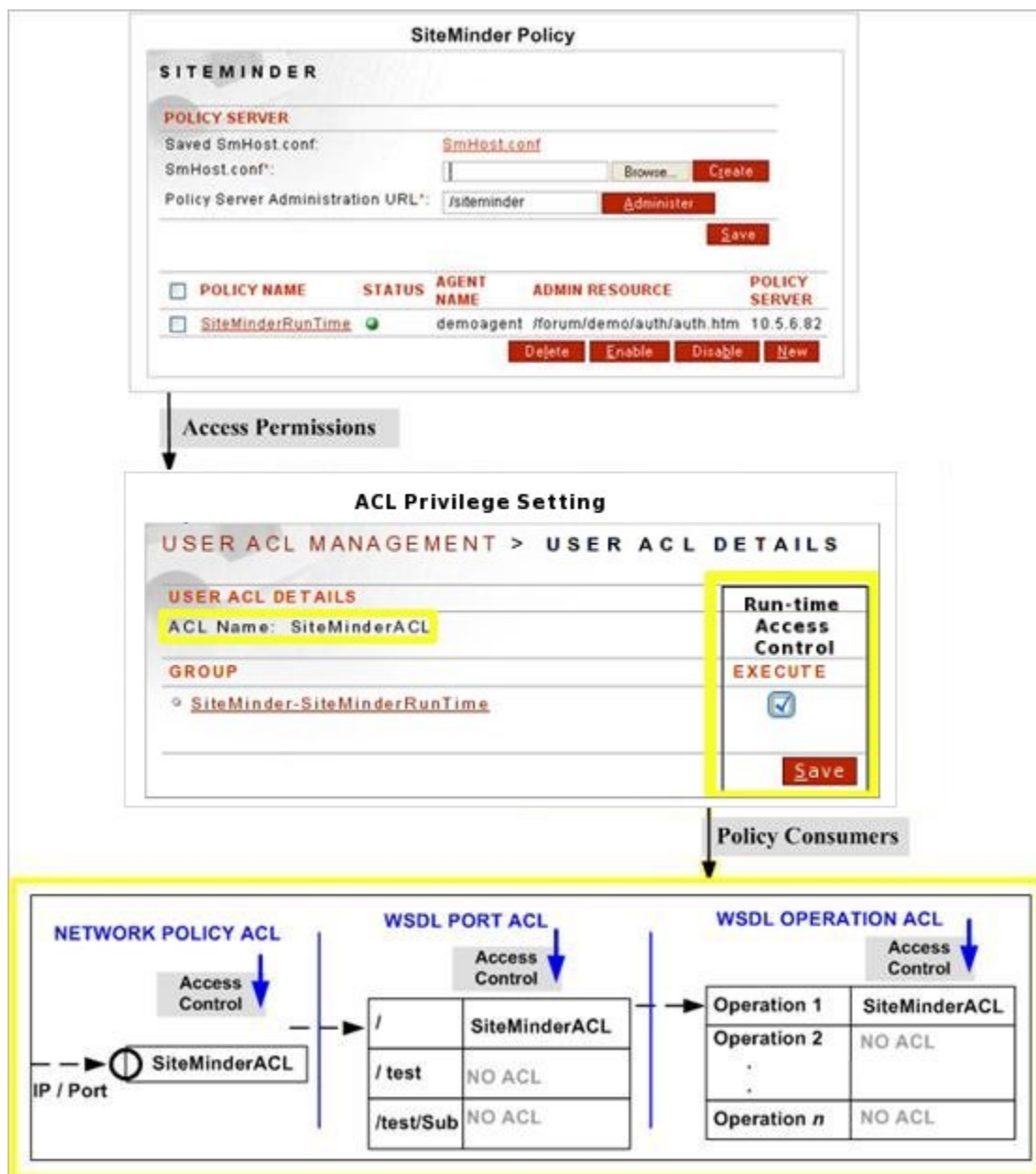


Figure 3: Run-time Access Control Defined in SiteMinder Policies by the Privilege Set in an User ACL.

Assign Run-time Privilege to SiteMinder Policies

The following example setting shows how to configure Execute privileges for the SiteMinderRunTime policy. With this setting, the User ACL could then be configured on Network Policies, WSDL Policies, or XML Policies to restrict incoming traffic based on the user's authentication and authorization of the protected resource defined by the SiteMinder policy.

USER ACL MANAGEMENT

CREATE NEW ACCESS CONTROL LISTS

Add one ACL name per line

SiteMinderACL

Create

ACCESS CONTROL LIST

☐ ACL1

☐ ACL2

☐ ACL3

☐ Default

☐ Executives

☐ SiteMinderACL

☐ WSTACL

Delete

USER ACL MANAGEMENT > USER ACL DETAILS

USER ACL DETAILS

ACL Name: SiteMinderACL

GROUP	EXECUTE
<input checked="" type="radio"/> SiteMinder-SiteMinderRunTime	<input checked="" type="checkbox"/>

Save

- From the ACCESS section of the Navigator, navigate to the **User ACLs** screen.
- On the USER ACL MANAGEMENT screen, enter an User **ACL policy** name in the top text box.
- In the ACCESS CONTROL LIST listing, select the new **User ACL policy name**.
- On the USER ACL DETAILS screen, aligned with the SiteMinder-SiteMinderRunTime group name, check the **Execute** checkbox.
- Click **Save**.

Note: For more information on User ACLs, refer to the ACL Policies section of the *Forum Systems Sentry™ Version 9 Access Control Guide*.

Add a Design-time SiteMinder Policy

Follow these steps to add a SiteMinder policy for design-time.

SITEMINDER

POLICY SERVER

Saved SmHost.conf: [SmHost.conf](#)

SmHost.conf*: Browse... Create

Policy Server Administration URL*: /siteminder Administer

Save

<input type="checkbox"/>	POLICY NAME	STATUS	AGENT NAME	ADMIN RESOURCE	POLICY SERVER	
<input type="checkbox"/>	SiteMinderRunTime	●	demoagent	/forum/demo/auth/auth.htm	10.5.6.82	Delete Enable Disable New

SITEMINDER > SITEMINDER POLICY CONFIGURATION

SITEMINDER POLICY

Policy Name*: SiteMinderAdministration

Enable privileged access: ☐ Yes ☒ No

Restrict Menus: ☐

Role policy:

Administration Resource*: /forum/demo1/auth.htm

Response Variable Identifier*: 224

Agent Name*: demoagent1

ADVANCED PASSWORD SERVICES

OnAccept Text Filter: *will expire.*

Response Text Mapping

<input type="checkbox"/>	FILTER EXPRESSION	REPLACE EXPRESSION
<input type="checkbox"/>	<input type="text"/>	<input type="text"/>

Apply Save

SITEMINDER

SiteMinder policy configuration saved

POLICY SERVER

Saved SmHost.conf: [SmHost.conf](#)

SmHost.conf*:

Policy Server Administration URL*:

<input type="checkbox"/>	POLICY NAME	STATUS	AGENT NAME	ADMIN RESOURCE	POLICY SERVER
<input type="checkbox"/>	SiteMinderAdministration	●	demoagent1	/forum/demo1/auth.auth	10.5.6.82
<input type="checkbox"/>	SiteMinderRunTime	●	demoagent	/forum/demo/auth/auth.htm	10.5.6.82

- From the ACCESS User Policies category of the Navigator, select **SiteMinder**.
- On the SITEMINDER screen, select **New**.
- On the SITEMINDER POLICY CONFIGURATION screen, in the Policy Name field, enter a **name** for this SiteMinder policy.

Note: SiteMinder policy names must be unique and may be from 1 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.

- Click **No** for Enable privileged access radio button.
- In the Administration Resource field, add the **Resource Name** used for SiteMinder authorization of Sentry administrators.
- In the Response Variable Identifier field, retain the default value of 224.
- In the Agent Name field, enter the **name** of the Web Agent that is requesting services from the SiteMinder Policy Server.
- If you desire to cache responses from SiteMinder then change the default value of the **Cache timeout** to the desired time in minutes.
- Select **Save** and the SITEMINDER screen refreshes with the message "SiteMinder policy configuration saved" visible at the top of the screen.

Design-time Access Control and SiteMinder Group Privileges

Access privileges may be set for a SiteMinder policy from the DOMAINS screen, which can be used to grant Read and Write privileges. The DOMAIN DETAILS screen displays the privileges enabled for the Forum SiteMinder policies. The Forum SiteMinder policy itself represents a population of users allowed to access the resources protected by SiteMinder. The Forum SiteMinder policy will appear in the DOMAINS screen just as a standard group will appear, and Administrators can set Read and Write (for Administration) privileges for the SiteMinder policy. The following graphic displays the relationship between SiteMinder policies and design-time access control:

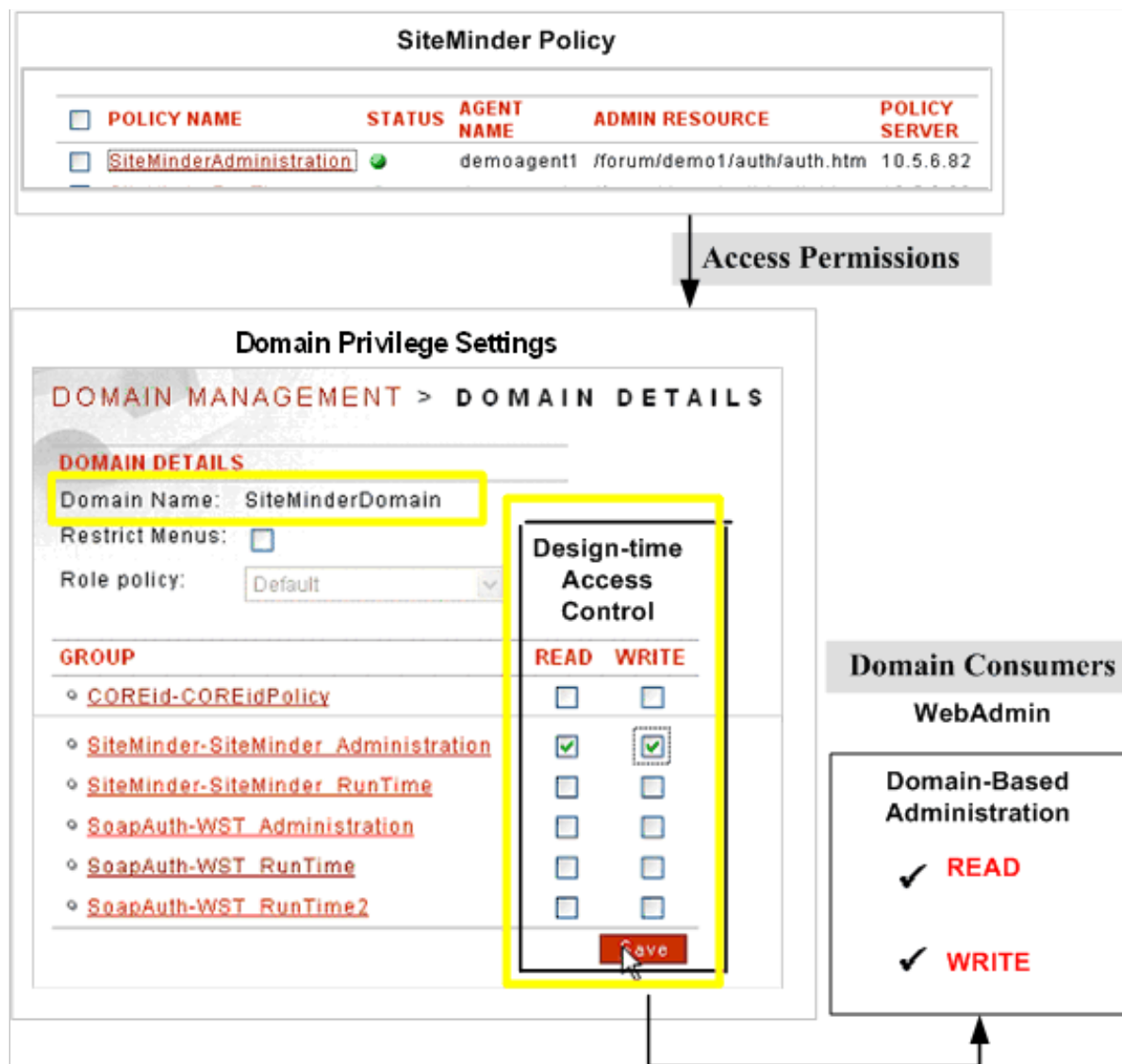


Figure 4: Design-time Access Control Defined in SiteMinder Policies by the Privilege Set in a Domain.

Configure a SiteMinder Policy for Advanced Password Services

Follow these steps to configure a SiteMinder policy for Advanced Password Services using a policy which was created from the above provided steps.

Adding a Filter Expression for SiteMinder Advanced Password Services

Filter expressions are used to customize messages provided by APS enabled Policy Server responses. These messages are by default configured to appear in error responses to the client and can optionally be configured to appear in successful responses to the client.

Follow these steps to add a filter expression used for SiteMinder Advanced Password Services:

SITEMINDER > SITEMINDER POLICY CONFIGURATION

SITEMINDER POLICY

Policy Name: SiteMinderRunTime

Enable privileged access: ☐ Yes ☒ No

Restrict Menus: ☐

Role policy:

Administration Resource*: /forum

Response Variable Identifier*: 224

Agent Name*: demoagent

ADVANCED PASSWORD SERVICES

OnAccept Text Filter: *.will expire.*

Response Text Mapping

<input type="checkbox"/> FILTER EXPRESSION	<input type="checkbox"/> REPLACE EXPRESSION
<input type="checkbox"/> PWD_EXPIRED\((.*)\)	<input type="text" value="Password has expired"/>

ADVANCED PASSWORD SERVICES

OnAccept Text Filter: *.will expire.*

Response Text Mapping

<input type="checkbox"/> FILTER EXPRESSION	<input type="checkbox"/> REPLACE EXPRESSION
<input type="checkbox"/> PWD_EXPIRED\((.*)\)	<input type="text" value="Password has already"/>
<input type="checkbox"/>	<input type="text"/>

ADVANCED PASSWORD SERVICES

OnAccept Text Filter: *.will expire.*

Response Text Mapping

<input type="checkbox"/> FILTER EXPRESSION	<input type="checkbox"/> REPLACE EXPRESSION
<input type="checkbox"/> PWD_EXPIRED\((.*)\)	<input type="text" value="Password has already"/>
<input type="checkbox"/> PWD_WARNING\((.*)\)	<input type="text" value="Password will expire"/>

- From the SiteMinder screen, select a SiteMinder policy.
- On the SITEMINDER POLICY CONFIGURATION screen, in the OnAccept Text Filter field, leave `.*will expire.*` to accept this default.
- In the Response Text Mapping area, under FILTER EXPRESSION, enter **PWD_EXPIRED\((.*)\)**.
- In the Response Text Mapping area, under REPLACE EXPRESSION, enter **Password has already expired.**
- Select **Apply** and the SITEMINDER POLICY CONFIGURATION screen refreshes and adds new text fields under the Response Text Mapping area under ADVANCED PASSWORD SERVICES for adding more filter expressions and replacement expressions.
- In the Response Text Mapping area, under FILTER EXPRESSION, enter **PWD_WARNING\((.*)\)**.
- In the Response Text Mapping area, under REPLACE EXPRESSION, enter **Password will expire.**
- Select **Apply** and the SITEMINDER POLICY CONFIGURATION screen refreshes.

Continue with the next topic.

Testing the SiteMinder Policy for Advanced Passwords

- Select **Test**.
- The SiteMinder screen refreshes and the message “Successfully authenticated with SiteMinder server.” is visible at the top of the screen.

Removing a Filter Expression for SiteMinder Advanced Password Services

Follow these steps to remove a filter expression used for SiteMinder Advanced Password Services:

- Check the **checkbox** under Response Text Mapping, and then select **Remove**.

Administer the Policy Server

Follow these steps to administer the Policy Server:

The screenshot shows the 'SITE MINDER' configuration interface. Under the 'POLICY SERVER' section, there are fields for 'SmHost.conf' (set to 'SmHost.conf') and 'Policy Server Administration URL' (set to '/siteminder'). Buttons for 'Browse...', 'Create', 'Administer', and 'Save' are present. Below this is a table with columns: POLICY NAME, STATUS, AGENT NAME, ADMIN RESOURCE, and POLICY SERVER. A single entry 'SiteMinderRunTime' is shown with a green status icon, agent name 'demoagent', and admin resource '/forum/demo/auth/auth.htm'. The policy server version is '10.5.6.82'. Action buttons 'Delete', 'Enable', 'Disable', and 'New' are at the bottom of the table.

POLICY NAME	STATUS	AGENT NAME	ADMIN RESOURCE	POLICY SERVER
SiteMinderRunTime	●	demoagent	/forum/demo/auth/auth.htm	10.5.6.82



1. From the ACCESS User Policies category of the Navigator, select **SiteMinder**.
2. On the SITE MINDER screen, select **Administer** and the Netegrity Policy Server screen appears, launching the SiteMinder UI.
3. Select **Administer Policy Server**.

Note: Please Refer to your SiteMinder documentation for information regarding SiteMinder Policy server administration.

SiteMinder Advanced Password Services with Tasks

SiteMinder allows users to implement and enforce password policies across multiple directories using the SiteMinder Advanced Password Services (APS) feature.

Use Case with SiteMinder APS: Map Attributes To XML Task

The Map Attributes to XML task allows you to set or insert attributes coming from LDAP, SiteMinder, or another identity source, and maps these attributes into XML document elements. The Map Attribute to XML task is a flexible way of configuring such a mapping by selecting the XML element and specifying the attribute to insert. You may map as many attributes per task as you want, but only one attribute per XML element. On a SiteMinder policy, use SM_ACCEPT_TEXT, a special attribute that is set from a SiteMinder WebAgent-OnAccept-Text attribute received during Advanced Password Services authentication.

Add the Map Attributes to XML Task for SiteMinder Policy

Follow these steps to map attributes to XML for a SiteMinder policy:

<input type="checkbox"/> #	TASK	STATUS
<input type="checkbox"/> 1	Identify Document	●
<div>Run Credentials Enable Disable Delete New</div>		

TASK TYPE

Conditional Identification <ul style="list-style-type: none"><input type="radio"/> Identify Document	User Identity and Access Control <ul style="list-style-type: none"><input type="radio"/> User Identity & Access Control<input type="radio"/> Logout	Credential Generation <ul style="list-style-type: none"><input type="radio"/> SAML Assertion<input type="radio"/> WS-Security Header
Mediation and Transformation <ul style="list-style-type: none"><input type="radio"/> AS2<input type="radio"/> Add XML Node<input type="radio"/> Convert CSV<input type="radio"/> Convert JSON<input type="radio"/> Convert SOAP<input type="radio"/> Convert Value<input type="radio"/> ebMS<input type="radio"/> Process Attachments<input type="radio"/> Enrich Message<input type="radio"/> Replace Document<input type="radio"/> Remove Transport Header<input type="radio"/> Remove WS-Security Header<input type="radio"/> Remove XML Node<input type="radio"/> Transform Document<input type="radio"/> ZIP Contents Processing	Flow Control <ul style="list-style-type: none"><input type="radio"/> Abort Processing<input type="radio"/> Cache Response<input type="radio"/> Delay Processing<input type="radio"/> Redirect<input type="radio"/> Remote Routing<input type="radio"/> WS-Addressing Validation and Conformance <ul style="list-style-type: none"><input type="radio"/> Validate Document Structure<input type="radio"/> Validate JSON<input type="radio"/> Validate X.509 Certificates Logging and Archiving <ul style="list-style-type: none"><input type="radio"/> Archive Document<input type="radio"/> Display WSDLs URIs<input type="radio"/> Log	Security Processing <ul style="list-style-type: none"><input type="radio"/> Decrypt Elements<input type="radio"/> Encrypt Elements<input type="radio"/> OpenPGP<input type="radio"/> Pattern Match<input type="radio"/> Receive Signature Confirmation<input type="radio"/> Send Signature Confirmation<input type="radio"/> Sign Document<input type="radio"/> Verify Document Signature<input type="radio"/> Virus Scan<input type="radio"/> WS-SecureConversation<input type="radio"/> XKMS Service
Attribute Mapping <ul style="list-style-type: none"><input checked="" type="radio"/> Map Attributes to XML<input type="radio"/> Map Attributes from XML<input type="radio"/> Map Attributes and Headers<input type="radio"/> Query Database<input type="radio"/> Query LDAP		

Next

MAP ATTRIBUTES TO XML

Task Type: Map Attributes to XML

Task Name*: Map Attributes to XML

Map From: User Attribute

On Error: ☒ Log & Halt Processing ☐ Log & Continue

SELECT TARGET ELEMENTS

☐ soap:Envelope

☐ soap:Header

☒ soap:Body

☐ ws:EchoResponse

☒ ws:EchoResult

☐ ws:Buf

Target Document Elements

ELEMENT	USER ATTRIBUTE
/soap:Envelope/soap:Body/ws:EchoResponse/ws:EchoResult	SM_ACCEPT_TEXT

Remove Apply Save

#	TASK	STATUS
1	Identify Document	●
2	Map Attributes to XML	●

Run Credentials Enable Disable Delete New

- From the TASK screen, select **New**.
- On the TASK TYPE screen, from the TASK TYPE screen, select the **Map Attribute to XML** radio button, and then click **Next**.
- On the MAP ATTRIBUTE to XML screen, aligned with On Error, keep the **Log & Halt Processing** option.
- From the SELECT ELEMENTS TO MAP section, check the **checkbox** prefacing the element whose attribute you want to map to the XML, and then select **Apply**. This will create the XPath expression used to identify this node during runtime.
- Under the ELEMENT column of the Document Element to Map section, the root/element selected populates the field.
- Under the ATTRIBUTE NAME column, overwrite the current USER ATTRIBUTE content and enter **SM_ACCEPT_TEXT**, the special attribute that is set from the SiteMinder WebAgent-OnAccept-Text attribute received during Advanced Password Services authentication.
- Select **Save**.

(For more information, refer to The Map Attributes to XML Task section of the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.)

Generate a cookie using a WS-Security Header Task

While adding this task, select a SAML token as the Security Token Type, select an X.509 DN as the SAML Identification Format, select both the Authentication and Attribute options as SAML Statement Types and select Cookie as a SAML Attribute value type.

Follow these steps to add a WS-Security Header task with SAML Assertion using the custom Attribute for Cookie to a message that did not previously have one.

- From the **TASK LIST** screen, select **New**.
- On the TASK TYPE screen, select the **WS-Security Header** radio button, and then click **Next**.
- On the TASK NAME screen, enter a **Task Name**, and then click **Next**.
- On the VERSION screen, select the **WSS 2004** radio button, and then click **Next**.
- On the MUST UNDERSTAND screen, check the **WS-Security processing by the recipient is mandatory** checkbox, and then click **Next**.
- On the SOAP ACTION screen, accept the default value or enter a **HTTP SOAP Action value**. Click **Next**.
- On the TIME TO LIVE screen, leave the Message expires checkbox unchecked for no expiration, or **check** and enter an **expiry period**.
- Click **Next**.

Note: For designing real-time processing tasks, the Time to LIVE should reflect the smallest window of opportunity which allows SAML requests to pass through the product, as well as maintain the highest level of security.

For testing purposes, the Time to LIVE value may be increased or disabled, allowing time to complete testing without having the SAML assertions expire.

- On the SECURITY TOKEN TYPE screen, select the **SAML** token radio button, and then click **Next**.
- On the SAML VERSION screen, select the **SAML 1.1** or **SAML 2.0** radio button, and then click **Next**.
- On the CONFIRMATION METHOD screen, select **Sender vouches**, and then click **Next**.
- On the SAM ISSUER screen, enter the value for the Issuer field, and then click **Next**.
- On the SAML AUDIENCE screen, accept the pre-populated SAML Audience, and then click **Next**.
- On the SAML TIME TO START screen, leave the checkbox checked to accept the default validity start time and click **Next**.
- On the SAML TIME TO EXPIRE screen, leave the Assertion expires checkbox unchecked for no expiration, or **check** and enter an **expiry period**.
- Click **Next**.
- On the DISALLOW SAML REUSE screen, leave the checkbox unchecked to allow caching of this assertion, and then click **Next**.
- On the USE SAML ADVICE screen, leave the **Use existing SAML assertions as advice** checkbox unchecked, and then click **Next**.
- On the SAML IDENTIFICATION FORMAT screen, check the X.509 **Distinguished Name** radio button, and then click **Next**.

- On the INCLUDE SAML FORMAT URI screen, leave the checkbox checked to **Include the identifier format URI**, and then click **Next**.
- On the SAML X.509 IDENTIFICATION screen, select the **Dynamic** option for retrieving the DN value. Click **Next**.

Note: Selecting the **Dynamic, based on protocol certificate** radio button applies the X.509 DN token of the user identified earlier during the User Identity and Access Control task.

Selecting the **Static, based on a specified user** radio button applies the selected X.509 DN token to this SAML Assertion.

SAML STATEMENT TYPE

☒ Authentication

☒ Attribute

☐ Authorization

Next

SAML AUTHENTICATION

☐ Include the client IP address

Next

ATTRIBUTE

Namespace*:

Name(s)*:

Value Type:

☐ Username

☐ Email

☐ DN

☐ Constant

☐ User attribute (e.g. LDAP)

☒ Cookie

Next

SIGN SAML ASSERTION

☐ Sign SAML assertion

Finish

- On the SAML STATEMENT TYPE screen, select the **Authentication** and **Attribute** checkboxes, and then click **Next**.
- On the SAML AUTHENTICATION screen, leave the checkbox unchecked to omit the client IP address. Click **Next**.
- On the SAML ATTRIBUTE screen, enter a **value** for the namespace.
- In the Name(s) field, enter **SMSESSION**.
- From the Value Type, select the **Cookie** radio button, and then click **Next**.
- On the SIGN SAML ASSERTION screen, choose whether to sign the assertion (requires that you have at least one XML Signature policy defined), and then click **Next**.
- On the INCLUDE CERTIFICATES screen, check the **Include certificates** checkbox, and then click **Next**.
- On the SIGN KEY INFO screen, check the **Sign key info** checkbox, and then click **Finish**.
- The TASK LIST screen refreshes.

TASK LISTS > TASK LIST

TASK LIST

Name*:

Description:

Sample Document: ▼

<input type="checkbox"/>	#	TASK	STATUS
<input type="checkbox"/>	1	↓ User Identity & Access Control	●
<input type="checkbox"/>	2	↑ WS-Security Header	●

- In the TASK LIST area, select **Save**.

Use Run Task List to View the SAML Cookie

The screenshot shows the 'TASK LIST' screen. At the top, there is a breadcrumb 'TASK LISTS > TASK LIST'. Below this is a form with the following fields: 'Name*' (containing 'EchoSoapIn-TaskList'), 'Description' (empty), and 'Sample Document' (a dropdown menu showing 'EchoSoapIn'). To the right of these fields are 'Apply' and 'Save' buttons. Below the form is a table with three columns: '#', 'TASK', and 'STATUS'. The table contains two rows: Row 1 has a checkbox, the number '1', a red downward arrow, the text 'User Identity & Access Control', and a green status dot. Row 2 has a checkbox, the number '2', a red upward arrow, the text 'WS-Security Header', and a green status dot. At the bottom of the table are several buttons: 'Run' (with a mouse cursor over it), 'Credentials', 'Enable', 'Disable', 'Delete', and 'New'.

#	TASK	STATUS
1	User Identity & Access Control	●
2	WS-Security Header	●

- From the TASK LIST screen, select **Run** to view the resulting document as processed by the Task List.

The screenshot shows the 'USER CREDENTIALS' screen. It has three input fields: 'User Name' (containing 'testuser'), 'Password' (containing masked characters '••••••••'), and 'Resource' (containing 'service/qaservice.asmx'). To the right of these fields is a 'Next' button with a mouse cursor over it.

- In the User Name field, enter a valid **SiteMinder username**.
- In the Password field, enter the valid **password** for the SiteMinder user.
- In the Resource field, enter a **URI** which represents the protected resource for this agent realm on the SiteMinder Policy server, and then click **Next**.

```

<?xml version="1.0" ?>
- <soap:Envelope xmlns:soap="http://schemas.xmlsoap.org/soap/envelope/">
- <soap:Header>
- <wsse:Security soap:mustUnderstand="1" xmlns:wsse="http://docs.oasis-open.org/wss/2004/01/oasis-200401-wss-wssecurity-secext-1.0.xsd">
- <saml:Assertion AssertionID="id-99367a0c92ae2c140af2103515c778e969c0dfb4" IssueInstant="2006-04-13T19:46:23.947Z" Issuer="http://www.forumsys.com/sentry" MajorVersion="1" MinorVersion="1" xmlns:saml="urn:oasis:names:tc:SAML:1.0:assertion">
<saml:Conditions NotBefore="2006-04-13T19:46:23.947Z" NotOnOrAfter="2006-04-13T20:46:22.947Z" />
- <saml:AuthenticationStatement AuthenticationInstant="2006-04-13T19:46:23.947Z" AuthenticationMethod="urn:oasis:names:tc:SAML:1.0:am:password">
- <saml:Subject>
<saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">UID=authorized,CN=AuthorizedUsers,O=Siteminder</saml:NameIdentifier>
- <saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
</saml:AuthenticationStatement>
- <saml:AttributeStatement>
- <saml:Subject>
<saml:NameIdentifier Format="urn:oasis:names:tc:SAML:1.1:nameid-format:X509SubjectName">UID=authorized,CN=AuthorizedUsers,O=Siteminder</saml:NameIdentifier>
- <saml:SubjectConfirmation>
<saml:ConfirmationMethod>urn:oasis:names:tc:SAML:1.0:cm:sender-vouches</saml:ConfirmationMethod>
</saml:SubjectConfirmation>
</saml:Subject>
- <saml:Attribute AttributeName="SMSESSION" AttributeNamespace="http://www.forumsys.com/sentry">
<saml:AttributeValue>SEOT2sHl52yHoeSLQ6CmaCDQ1knzUlGA1HEKvOMQgDwYvPJeya41z/fpHT70mJmcDnWl
</saml:AttributeValue>
</saml:Attribute>
</saml:AttributeStatement>
</saml:Assertion>
</wsse:Security>
</soap:Header>
+ <soap:Body>
</soap:Envelope>

```

INVALIDATE SESSION COOKIES

The Forum integration provides a means to invalidate an existing SiteMinder session cookie. This is provided by the Logout task in the task list.

Invalidating Session Cookies - The Logout Task

The Logout task is used for invalidating the session cookies. This task requires persistent session caching enabled on the SiteMinder policy server. For more information regarding persistent session caching, please refer to your SiteMinder documentation.

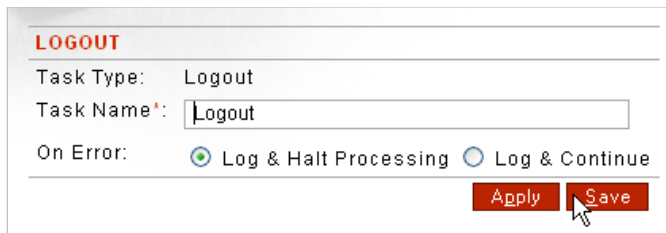
Adding the Logout Task

Follow these steps to add the Logout task:

<input type="checkbox"/> #	TASK	STATUS
<input type="checkbox"/> 1	Identify Document	
<div>Run Credentials Enable Disable Delete New</div>		

TASK TYPE		
Conditional Identification <ul style="list-style-type: none"><input type="radio"/> Identify Document	User Identity and Access Control <ul style="list-style-type: none"><input type="radio"/> User Identity & Access Control<input checked="" type="radio"/> Logout	Credential Generation <ul style="list-style-type: none"><input type="radio"/> SAML Assertion<input type="radio"/> WS-Security Header
Mediation and Transformation <ul style="list-style-type: none"><input type="radio"/> AS2<input type="radio"/> Add XML Node<input type="radio"/> Convert CSV<input type="radio"/> Convert JSON<input type="radio"/> Convert SOAP<input type="radio"/> Convert Value<input type="radio"/> ebMS<input type="radio"/> Process Attachments<input type="radio"/> Enrich Message<input type="radio"/> Replace Document<input type="radio"/> Remove Transport Header<input type="radio"/> Remove WS-Security Header<input type="radio"/> Remove XML Node<input type="radio"/> Transform Document<input type="radio"/> ZIP Contents Processing	Flow Control <ul style="list-style-type: none"><input type="radio"/> Abort Processing<input type="radio"/> Cache Response<input type="radio"/> Delay Processing<input type="radio"/> Redirect<input type="radio"/> Remote Routing<input type="radio"/> WS-Addressing Validation and Conformance <ul style="list-style-type: none"><input type="radio"/> Validate Document Structure<input type="radio"/> Validate JSON<input type="radio"/> Validate X.509 Certificates Logging and Archiving <ul style="list-style-type: none"><input type="radio"/> Archive Document<input type="radio"/> Display WSDLs URIs<input type="radio"/> Log	Security Processing <ul style="list-style-type: none"><input type="radio"/> Decrypt Elements<input type="radio"/> Encrypt Elements<input type="radio"/> OpenPGP<input type="radio"/> Pattern Match<input type="radio"/> Receive Signature Confirmation<input type="radio"/> Send Signature Confirmation<input type="radio"/> Sign Document<input type="radio"/> Verify Document Signature<input type="radio"/> Virus Scan<input type="radio"/> WS-SecureConversation<input type="radio"/> XKMS Service

Next



LOGOUT

Task Type: Logout

Task Name*: Logout

On Error: ☒ Log & Halt Processing ☐ Log & Continue

Apply Save

- From the TASK screen, select **New**.
- On the TASK TYPE screen, select the **Logout** radio button, and then click **Next**.
- On the LOGOUT screen, aligned with On Error, keep the **Log & Halt Processing** radio button setting.
- Click **Save**.

(For more information, refer to The Map Logout Task section of the *Forum Systems Sentry™ Version 9 Tasks Management Guide*.)

APPENDIX

Appendix A - Constraints for SiteMinder Policies

ELEMENT	CONSTRAINT	CHAR COUNT
SiteMinder Policy Name	Unique and case sensitive, may be from 1 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.	1-32
Response Variable Identifier	Response Variable Identifier valid values are from 0 to 255. The default is 224.	1-3

Appendix B - Specifications of SiteMinder Policies

ELEMENT SUPPORTED	CONSTRAINT
SiteMinder Policies	64

INDEX

add filter expression for SiteMinder APS	18	Response Text Mapping	8
add Logout task for SiteMinder policy server...	29	Response Variable Identifier.....	8
add Map attributes to XML task for SiteMinder policy	21	Saved SmHost.conf	6
add SiteMinder policy for design-time.....	15	Server	9
add SiteMinder policy for run-time	10	SiteMinder policies	
add WS-Security Header task.....	24	examples	9
administer SiteMinder policy server	20	SiteMinder policy	
Administration Resource	6, 8	adding filter expression for APS	18
Administrator password.....	9	adding for run-time	10
Administrator username	9	administering SiteMinder policy server.....	20
Agent Name	6, 8	configuring policy for APS	18
assign privileges for run-time access	14	Map attributes to XML task on SiteMinder	
configure SiteMinder policy for APS	18	policy	21
conventions used	1	removing filter expression for APS	19
Enable privileged access	8	testing for APS.....	19
examples for SiteMinder policies	9	SiteMinder Policy	
log in to product.....	2	adding policy for design-time.....	15
logout of product	2	assigning privileges for run-time access	14
Logout task		registering Forum product	12
adding for SiteMinder policy server	29	SmHost.conf	6
Name for host to be registered.....	9	Status	6
Name of host configuration object	9	terms	
OnAccept Text Filter	8	in SiteMinder Policy Configuration screen.....	8
Policy Name	6, 8	in SiteMinder screen.....	6
Policy Server Administration URL.....	6	in SiteMinder Trusted Host Registration	
Port.....	9	screen.....	9
register the product	12	test Advanced Password Services on SiteMinder	
registering trusted host with SiteMinder		policy.....	19
terms	9	WS-Security Header task	
remove filter expression for SiteMinder APS ...	19	adding	24