



FORUM SENTRY™ VERSION 9

IBM TIVOLI® ACCESS MANAGER

WEBSEAL 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 IBM Tivoli® Access Manager Webseal Integration Guide, published May 2024.

D-OEM-SE-018156

Table of Contents

Contents

INTRODUCTION TO THE IBM WEBSEAL ACCESS MANAGER INTEGRATION GUIDE	2
<i>Audience for the IBM WEBSEAL ACCESS MANAGER Integration Guide</i>	<i>2</i>
<i>Conventions Used</i>	<i>2</i>
Assumptions	2
LOGON TO PRODUCT	3
<i>How To Log in to the Product</i>	<i>3</i>
<i>How To Logout of the Product</i>	<i>3</i>
IBM WEBSEAL ACCESS MANAGER INTEGRATION	4
WEBSEAL POLICIES	4
Use Case 1: Multi-domain Administration with Webseal Policies	4
Use Case 2: Authentication and Authorization with Webseal Policies	4
Webseal Policies with SSL Network Policies	5
Webseal Policies with SSL Policy Prerequisites	5
<i>Webseal Screen and Policy Terms</i>	<i>6</i>
<i>Protecting Your Virtual Resources</i>	<i>7</i>
<i>Sample Configurations for Webseal Policies</i>	<i>7</i>
Add a Run-time Webseal Policy	8
Run-time Access Control and Tivoli Group Privileges	10
Add a Design-time Webseal Policy	13
Design-time Access Control and Tivoli Group Privileges	14
Delete Webseal Policy	16
APPENDIX	17
<i>Appendix A - Constraints in Webseal Policies</i>	<i>17</i>
<i>Appendix B - Specifications in Webseal Policies</i>	<i>17</i>
INDEX	18

List of Figures

Figure 1: Login Screen	3
Figure 2: Logout Button	3
Figure 3: Webseal Policy Tiv_RunTime	4
Figure 4: User Policies Menu	8
Figure 5: Webseal Configuration	8
Figure 6: Run-time Access Control	10
Assign Run-time Privilege to Webseal Policies	11
Figure 7: ACL Management	11
Figure 8: ACL List	11
Figure 9: ACL Details	11
Figure 10: Design-time Access Control	14
Assign Design-time Privilege to Webseal Policies	15

INTRODUCTION TO THE IBM WEBSEAL ACCESS MANAGER INTEGRATION GUIDE

Audience for the IBM WEBSEAL ACCESS MANAGER Integration Guide

The *Forum Systems Sentry™ Version 9 IBM Tivoli® Access Manager Integration Guide* is for Security Managers who manage access and authorization controls through IBM WEBSEAL ACCESS MANAGER and the Forum Systems appliance. This person will design, manage and administer the system through the IBM WEBSEAL ACCESS MANAGER and create Access Manager WebSEAL policies, integrating them with the Forum Systems appliance.

Conventions Used

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 that 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.

Any specifications and constraints referenced in this volume appear in the Appendices of this volume.

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 WEBSEAL ACCESS MANAGER and Tivoli WebSEAL Version 5.1. It is assumed that WEBSEAL ACCESS MANAGER WebSEAL junctions protect a company's web services

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



Figure 1: Login Screen

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.



Figure 2: Logout Button

IBM WEBSEAL ACCESS MANAGER INTEGRATION


WEBSEAL ACCESS MANAGER (TAM) is an IBM product suite for identity management. The Forum Systems API Security Gateway leverages WEBSEAL ACCESS MANAGER's WebSEAL product to allow users of a Webseal Policy Server to authenticate and authorize users against Tivoli via policies that are built on the gateway. The Tivoli screen manages IBM TAM users and groups for use within the system. A Webseal Policy provides a dynamic means of authenticating and authorizing users against a Tivoli WebSEAL Server.

With TAM policies, no user information is stored on the appliance; instead, all information is dynamically exchanged directly with the Tivoli WebSEAL Server. You may create, edit and delete as many Webseal Policies on the appliance as you choose using the WebAdmin tool.

WEBSEAL POLICIES

In the following example, the Webseal Policy Tiv_RunTime defines the users stored on the Tivoli server and are treated as a group.

WEBSEAL ACCESS MANAGER

<input type="checkbox"/>	POLICY NAME	STATUS	WEBSEAL HOST ADDRESS
<input type="checkbox"/>	<u>Tiv_RunTime</u>		10.5.1.41:80

[Delete](#) [Enable](#) [Disable](#) [New](#)

Figure 3: Webseal Policy Tiv_RunTime

Use the following sequence of steps to manage Tivoli policies:

1. Administrator logs on to the appliance.
2. Administrator creates a Webseal Policy (Tiv_RunTime).
3. A group named Webseal-Tiv_RunTime is created (this group is not visible in the Groups screen).
4. The Administrator navigates to the ACLs screen, creates an ACL for Tivoli (Tiv_ACL) and assigns the Execute privilege to the Webseal-Tiv_Runtime group.

Note: Forum Sentry supports the use of Tivoli session cookies. The cookies that it supports are:

- PD-H-SESSSION-ID for http
- PD-S-SESSION-ID for https

The following configurations need to be made to WebSEAL to support cookies: 1) Enable Basic Auth for http and https, 2) and set ssl-id-sessions=no (found in the WebSEAL instance configuration file) to enable https connections to use cookies.

Use Case 1: Multi-domain Administration with Webseal Policies

- The Webseal user logs in to the appliance, and through the appropriate ACL, has access to Webseal- policies. The appliance authenticates the Webseal user through the Tivoli-Tiv_RunTime policy.

Use Case 2: Authentication and Authorization with Webseal Policies

- An Administrator creates a listener policy with Basic Auth enabled.

- During run-time, the Webseal user supplies credentials to the appliance. The appliance passes the credentials for the Tivoli-Tiv_RunTime policy, and sends them to the TAM for authentication. The TAM confirms that the Tivoli user is an authenticated user.

Note: It is assumed that a TCP type WebSEAL junction has already been created to protect the backend web services.

Webseal Policies with SSL Network Policies

Webseal Policies over SSL network policies use the HTTPS protocol for securing HTTP over SSL. Webseal Policies over SSL network policies allow users to add Tivoli over SSL when the product processes outbound documents. The status light changes from green to red as a network policy changes from enabled to disabled.

Webseal Policies with SSL Policy Prerequisites

Follow the listed sequence to create a Webseal Policy using SSL:

1. Create or import a key pair from the Keys screen.
2. Create an SSL policy from the SSL screen that refers to the key pair.
3. Create a Webseal Policy from the Tivoli screen with the Use Secure HTTP checkbox checked and an SSL policy selected from the SSL Initiation Policy drop down list.
4. Assign privileges for the Tivoli group to an ACL from the ACLs screen.

Webseal Screen and Policy Terms

When configuring your Webseal Policy Server from the Webseal screen, please consider the following:

TERM	DEFINITION
Policy Name	The name given to this Webseal Policy. Webseal Policies may be 5-32 alphanumeric characters.
WebSEAL Server	IP address on the network on which WebSEAL is hosted.
WebSEAL Port	The port for the Tivoli-WebSEAL server.
Use Secure HTTP	Used with an SSL Initiation Policy on the appliance, selecting Yes uses HTTPS for outgoing message. Selecting No means that outgoing messages are sent out via HTTP.
SSL Initiation Policy	A listing of SSL Initiation policies on the appliance to use for outgoing messages sent via HTTPS.
Administration Resource	The Resource Name used for Tivoli authorization of Forum Systems Sentry™ administrators.
Enable privileged access	Both options refer to design-time privileges: <ul style="list-style-type: none">• With Yes selected, the user has access to the WebAdmin as a super user.• With No selected, the user still have access to the WebAdmin with all Domain privileges set for the Group which this user is a member of.
Note: Forum Systems recommends always using the No option.	
Role Policy	The Role Policy used to restrict the Web Admin menu's for an administrator

Protecting Your Virtual Resources

Note: When IBM WEBSEAL ACCESS MANAGER 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 'WSDL POLICY SETTINGS' tab. At the top, there are navigation tabs: 'Services', 'Task Lists', 'Settings' (which is active), 'IDP Rules', 'Logging', and 'Documents'. Below the tabs, the 'Policy Name*' field contains 'QA Service'. The 'Policy Description' field is empty. The 'Labels' field is also empty. At the bottom, there is a checkbox labeled 'Protect virtual resource' which is currently unchecked.

- 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.

Sample Configurations for Webseal Policies

Sample configurations for Webseal Policies include:

- Add a Run-time Webseal Policy and Assign Privileges.
- Add a Design-time Webseal Policy and Assign Privileges.
- Edit / View a Webseal Policy.
- Delete a Webseal Policy.

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

Add a Run-time Webseal Policy

Users may create a run-time Webseal Policy with or without SSL. This instruction does not include SSL.

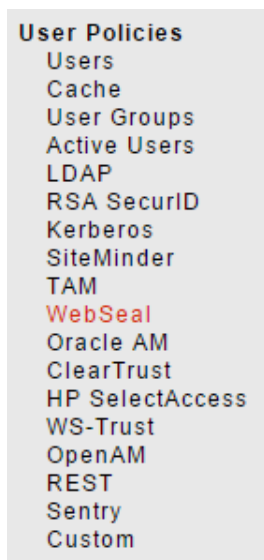


Figure 4: User Policies Menu

WEBSEAL ACCESS MANAGER > WEBSEAL ACCESS
MANAGER POLICY CONFIGURATION

WEBSEAL POLICY

Policy Name:	Tiv_RunTime
WebSEAL Server*:	<input type="text" value="10.5.1.41"/>
WebSEAL Port*:	<input type="text" value="80"/>
Use Secure HTTP:	<input type="checkbox"/>
SSL Initiation Policy:	<input type="text" value="IRS_PE_SSL_Initiation_Policy"/> Edit
Administration Resource*:	<input type="text" value="/"/>
Enable privileged access:	<input type="radio"/> Yes <input checked="" type="radio"/> No
Restrict Menus:	<input type="checkbox"/>
Role policy:	<input type="text" value="▼"/>

[Save](#)

Figure 5: Webseal Configuration

- From the ACCESS category of the Navigator, under User Policies, select **Webseal**.
- On the WEBSEAL ACCESS MANAGER screen, select **New**.
- On the WEBSEAL ACCESS MANAGER POLICY CONFIGURATION screen, in the Policy Name field, enter a **name** for this Webseal Policy.

Note: Webseal Policy names must be unique and may be from 5 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.

- In the WebSEAL Server field, enter the **IP address** on the network on which the Webseal Policy is hosted.
- In the WebSEAL Port field, enter the default **Port** on the network on which the Webseal Policy is hosted.
- Aligned with Use Security HTTP, select the **No** radio button; the SSL Initiation Policy drop down list is now disabled.
- Skip the SSL Initiation Policy option.
- In the Administration Resource field, enter the **name and path** of the authentication resource and its path that resides on the Webseal Policy server.
- Aligned with Enable privileged access, select the **No** radio button.
- Click **Save** and the WEBSEAL ACCESS MANAGER screen refreshes.

Run-time Access Control and Tivoli Group Privileges

Access privileges may be set for a Webseal Policy from the ACLs screen, which can be used to grant Read, Write or Execute privileges. The ACL DETAILS screen displays the privileges enabled for the Webseal Policies.

The Webseal Policy itself represents a population of users. The Webseal Policy will appear in the ACLs screen just as a standard group will appear, and Administrators can set Read, Write (for Administration) and Execute (for run-time processing) privileges to the Webseal Policy. The following graphic displays the relationship between IBM Webseal Policies and access control:

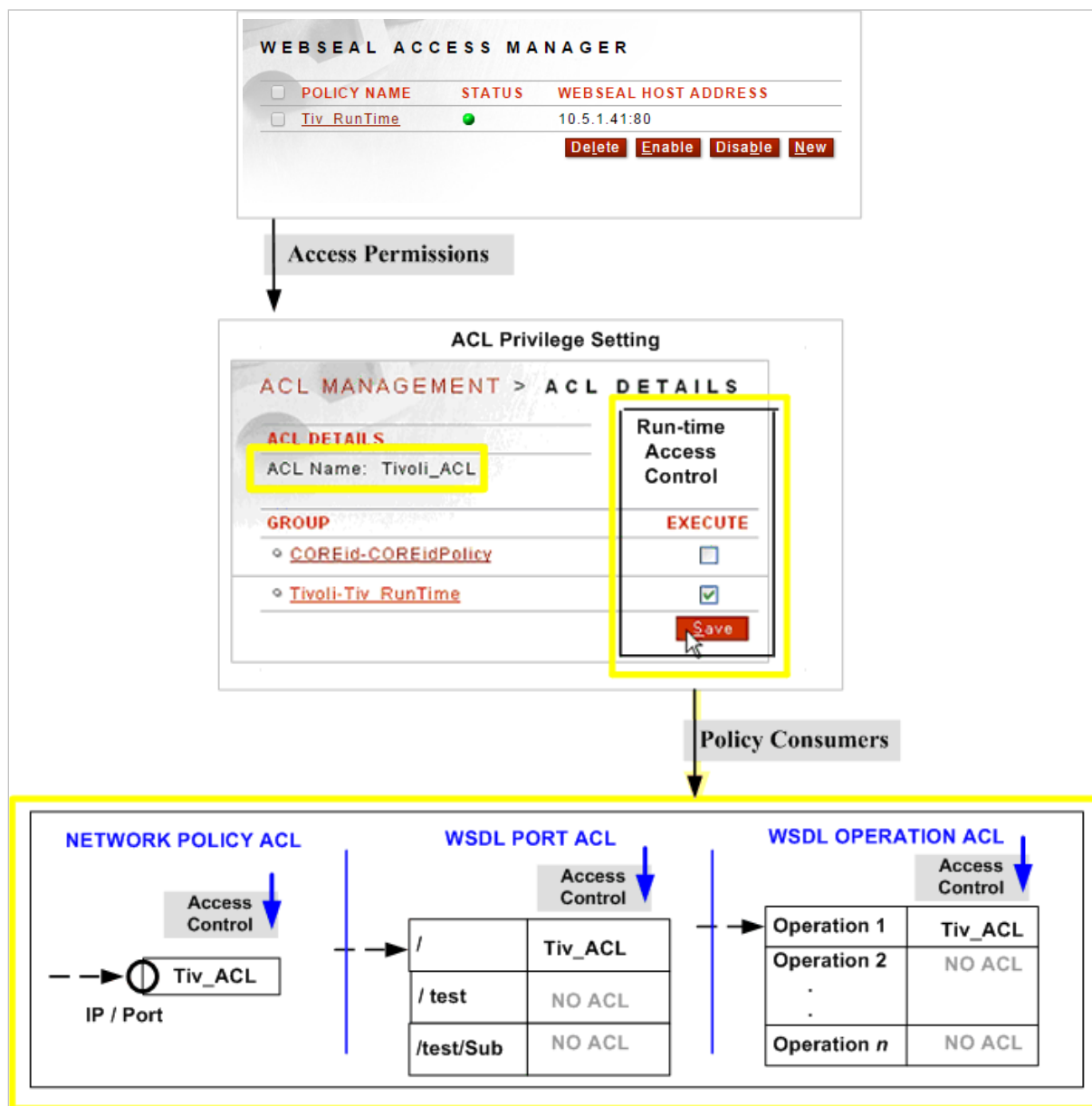


Figure 6: Run-time Access Control

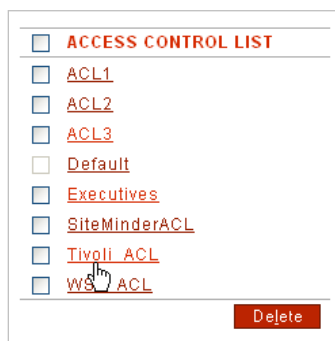
Assign Run-time Privilege to Webseal Policies

Follow these steps to assign the run-time privilege to Webseal Policies:



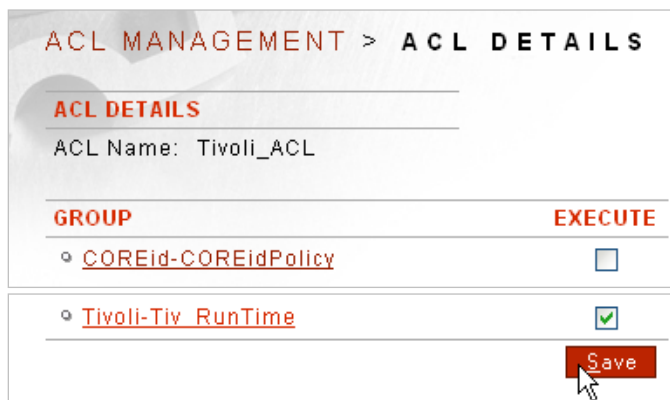
The screenshot shows the 'ACL MANAGEMENT' screen with a sub-header 'CREATE NEW ACCESS CONTROL LISTS'. Below this, it says 'Add one ACL name per line'. A text input field contains 'Tivoli_ACL'. At the bottom right, there is a red 'Create' button with a mouse cursor hovering over it.

Figure 7: ACL Management



The screenshot shows the 'ACCESS CONTROL LIST' screen. It lists several ACLs with checkboxes: ACL1, ACL2, ACL3, Default, Executives, SiteMinderACL, Tivoli_ACL, and WS_ACL. A red 'Delete' button is at the bottom right. A mouse cursor is hovering over the 'Tivoli_ACL' checkbox.

Figure 8: ACL List



The screenshot shows the 'ACL MANAGEMENT > ACL DETAILS' screen. It displays 'ACL Name: Tivoli_ACL'. Below is a table with two columns: 'GROUP' and 'EXECUTE'. The table has two rows: one for 'COREId-COREIdPolicy' with an unchecked checkbox, and one for 'Tivoli-Tiv_RunTime' with a checked checkbox. A red 'Save' button is at the bottom right with a mouse cursor hovering over it.

GROUP	EXECUTE
COREId-COREIdPolicy	<input type="checkbox"/>
Tivoli-Tiv_RunTime	<input checked="" type="checkbox"/>

Figure 9: ACL Details

- From the ACCESS category of the Navigator, navigate to **ACLs**.
- On the ACL MANAGEMENT screen, enter a new **ACL name** in the top text box.

Note: ACL policy names must be unique, are case sensitive and may be from 1 to 79 alphanumeric characters. The '@' character, underscores and dashes are allowed.

- Click **Create**, and the screen refreshes with the new ACL name added to the ACCESS CONTROL LIST listing.
- Select the ACL policy name, and the ACL DETAILS screen appears.

- Aligned with the Tivoli-Tiv_RunTime group name, check the **Execute** checkbox.
- Click **Save**.

Add a Design-time Webseal Policy

Design-time Webseal Policies may be created with or without SSL. This instruction assumes that an SSL policy has been previously created on the appliance to use. Users may create a design-time Webseal Policy with Tivoli server configuration settings. This action only saves the values entered on this screen. Tivoli groups and Tivoli users' data are retrieved during execution time.

- From the ACCESS category of the Navigator, under User Policies, select **Webseal**.
- On the WEBSEAL ACCESS MANAGER screen, select **New**.
- On the WEBSEAL ACCESS MANAGER POLICY CONFIGURATION screen, in the Policy Name field, enter a **name** for this Webseal Policy.

Note: Webseal Policy names must be unique and may be from 5 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.

- In the WebSEAL Server field, enter the **IP address** on the network on which the Webseal Policy is hosted.
- In the WebSEAL Port field, enter the default **Port** on the network on which the Webseal Policy is hosted.
- Aligned with Use Security HTTP, select the **Yes** radio button.
- From the SSL Initiation Policy drop down , select an **SSL Initiation policy** to associate with this policy.
- In the Administration Resource field, enter the **name and path** of the authentication resource and its path that resides on the Webseal Policy server.
- Aligned with Enable privileged access, select the **No** radio button.
- Click **Save** and the WEBSEAL ACCESS MANAGER screen refreshes.

Design-time Access Control and Tivoli Group Privileges

Access privileges may be set for a Webseal 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 Webseal Policies. The Webseal Policy itself represents a population of users allowed to access the resource saved in the policy. The Webseal Policy will appear in the DOMAINS screen just as a standard group will appear, and Administrators can set Read and Write (for Administration) privileges to the Webseal Policy. The following graphic displays the relationship between Webseal Policies and design-time access control:

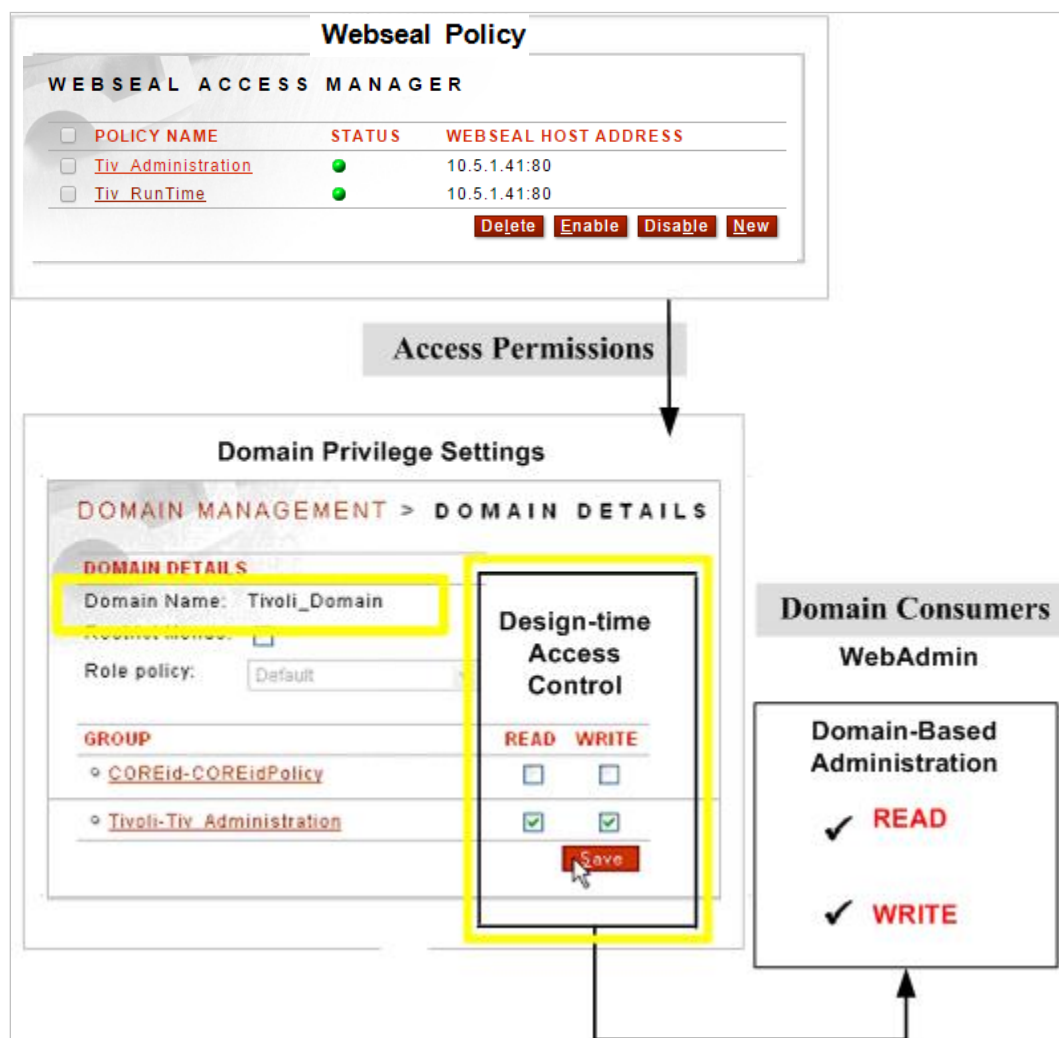


Figure 10: Design-time Access Control

Assign Design-time Privilege to Webseal Policies

Follow these steps to assign design-time privilege to Webseal Policies while creating them. To grant design-time access, either:

- Click the **Yes** radio button aligned with Enabled privileged access, or
- Click the **No** radio button aligned with Enabled privileged access. After creating the Webseal Policy, navigate to the **Domains** screen. Create a Domain and associate it with the Tivoli groups by checking **Read** and / or **Write** privileges on the Tivoli group.

With these settings, the Domain could then be configured on Network Policies, WSDL Policies, or XML Policies.

Edit or View Webseal Policy

Administrators may edit or view Tivoli group and Tivoli user information.

- Navigate to the **Tivoli** screen, and select a **Webseal Policy name** link.
- On the WEBSEAL ACCESS MANAGER POLICY CONFIGURATION screen, make desired changed.
- Click **Save**.

Delete Webseal Policy

Administrators may delete Webseal groups, users and settings at any time. A prompt appears, asking for confirmation of this deletion before the actual deletion action occurs. Clicking Delete all Webseal groups and Webseal users on the system and revert to the default settings on the Tivoli screen.

- Navigate to the **Webseal** screen, and the WEBSEAL ACCESS MANAGER screen appears.
- Check the **checkbox** aligned with a Webseal Policy name and select **Delete**.
- The “Are you sure you want to delete the selected Webseal Policies?” message appears. Click **OK**. The WEBSEAL ACCESS MANAGER screen refreshes.

APPENDIX

Appendix A - Constraints in Webseal Policies

ELEMENT SUPPORTED	CONSTRAINT	CHAR COUNT
Webseal Policy Name	Unique and case sensitive, may be from 5 to 32 alphanumeric characters, may include underscores, dashes and periods. However, no trailing or leading periods are allowed.	5-32

Appendix B - Specifications in Webseal Policies

ELEMENT SUPPORTED	SPECIFICATIONS
Webseal Policies	Unlimited *

* Limited only by disk space.

INDEX

ACL

- assign run-time privilege to Tivoli policies, 11
- add a run-time Tivoli policy, 8
- add design-time Tivoli policy, 13
- assign design-time privilege to Tivoli policies, 15
- assign run-time privilege to Tivoli policies, 11
- conventions used, iv
- delete Tivoli groups, users and configuration settings, 16
- delete Tivoli policy, 16
- Domain
 - assign design-time privilege to Tivoli policies, 15
- edit Tivoli groups, users and configuration settings, 16
- edit Tivoli policy, 16
- enable privileged access, 6
- log in to product, 3
- logout of product, 3
- sample configurations for Tivoli policies, 7
- sequence of steps to manage Tivoli policies, 4
- terms
 - in Tivoli policies, 6
 - in Tivoli screen, 6
- Tivoli
 - assigning design-time privilege to Tivoli policies, 15

Tivoli

- adding design-time Tivoli policy, 13
- adding run-time Tivoli policy, 8
- Administration Resource, 6
- assigning privileges to run-time Tivoli policies, 11
- deleting policy, 16
- deleting Tivoli groups, users and configuration settings, 16
- editing policy, 16
- editing Tivoli groups, users and configuration settings, 16
- Policy Name, 6
- SSL Initiation Policy, 6
- Use Secure HTTP, 6
- WebSEAL Port, 6
- WebSEAL Server, 6
- Tivoli policies
 - prerequisites for policies with SSL, 5
 - sample configurations for, 7
 - with SSL, 5
- Tivoli policy terms, 6
- Tivoli screen terms, 6
- Tivoli session cookies
 - supported by appliance, 4