Layer 7 Tutorials
Getting Started

v5.0

Contents

1 Introduction

These tutorials are designed for external and internal consumption by Layer 7 customers and employees for product evaluation and training purposes. They assume that the appropriate Layer 7 supporting solutions have already been deployed, configured and licensed. They assume little to no familiarity with Layer 7's solutions otherwise, and they are very detail oriented to support even the least technical and experienced user.

It's recommended that you read this document before beginning any tutorials. All tutorials will reference this document and assume some of the knowledge contained in this document.

You should then complete ***Tutorial 1 - Deploy Tutorial Services***, and optionally ***Tutorial 2 - Test Tutorial SOAP Service*** and ***Tutorial 3 - Test Tutorial REST Service***–, because most other tutorials will use one and/or the other of these services.

Beyond that, you can do whatever tutorials interest you most. Some tutorials will have dependencies on other tutorials, and those will be identified in the prerequisites section of the dependent tutorial.

The tutorials are designed to present you with tutorial steps as quickly as possible. The steps are focused on guiding you through the tutorial as efficiently as possible. While the steps may contain additional helpful context, to avoid cluttering the steps, a section for more additional context can be found at the end of each tutorial. You're encouraged to read all additional context to get the full value of each tutorial.

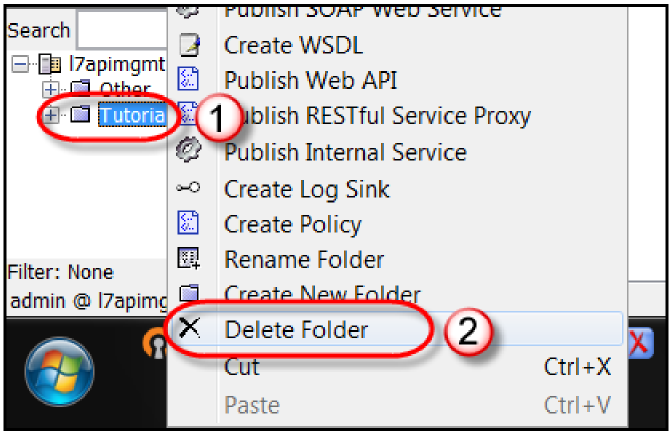
Note: The information provided here focuses on basic information needed for a basic understanding of Layer 7's solutions and successful completion of the other tutorials in this document. The information provided here should not be considered the only information available on the covered topics. There are many other sources of information that a user might find useful as they complete these tutorials or continue to use Layer 7 solutions in the future. Some of these sources of information include the online Policy Manager help mentioned below and Layer 7's official product documentation which can be download from Layer 7's customer portal.

2 General Information

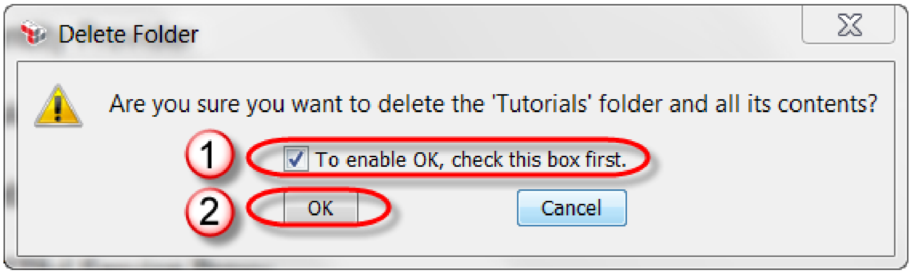
2.1 Cleaning Up

For the most part, if at any time after starting the ***Tutorial 1 - Deploy Tutorial Services*** you decide that you want to remove most of the tutorial work you've done on your gateway, you can simply remove the ***Tutorials*** folder and all of its contents.

You can remove the ***Tutorials*** folder by right clicking on the folder in the services and polices tree, and by selecting ***Delete Folder*** from the corresponding context menu.



In the Delete Folder dialog, check the option ***To enable OK...*** and click the ***OK*** button.



Are you sure you want to delete the 'Tutorials' folder and all its contents?

2.1.1 Clean Up Exceptions

Deleting services that have be set as portal managed will remove their corresponding APIs from the portal. However, depending on what else may have been done with those APIs in the portal, additional portal cleanup may be required.

If the internal debug trace policy is created for the first time and/or modified by any tutorials, the tutorials will not have instructed you to place it under the ***Tutorials*** folder, and so it will not be removed by removing the ***Tutorials*** folder.

Removing the ***Tutorials*** folder will also not undo any changes you've made to identity providers or any changes you've made via ***Tasks*** menu items.

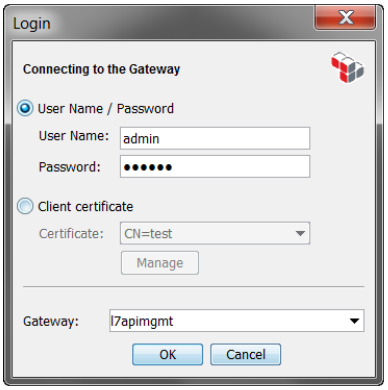
2.2 Using Policy Manager to Connect to a Gateway

Policy Manager is the primary user interface for connecting to and administrating Layer 7 gateways. It can either be installed as software (on either Windows or Linux; or Mac using the Linux distribution), or accessed via a browser via a URL hosted by each gateway. Many customers prefer the software version, because with it they can avoid potential browser related problems in their varied environments. However, both the software and browser versions are functionally equivalent.

Users must install the same version of Policy Manager software as the version of gateways they want to connect to using Policy Manager. For example, if a user has deployed a version 6.2 gateway, then they will need to install Policy Manager version 6.2 software. They will not be able to connect to that gateway using, for example, either Policy Manager version 6.0 or 7.0 software. You can have multiple versions of the Policy Manager software installed on the same workstation. You can also have multiple instances of the same or different versions of Policy Manager open and connected to the same or different gateways at one time on the same workstation.

After starting the software version of Policy Manager, you will be presented with the following dialog. If you're connecting to a brand new gateway, then you can login with the administrative user that you created during the initial configuration of the gateway. It is possible to configure gateways to allow role based access to LDAP (e.g. Microsoft Active Directory) users and groups. You can configure Policy Manager preferences to remember the user name you last logged in with.

Normally, in the Gateway field you specify just the host name or IP address of the gateway that you want to connect to. Policy Manager always tries to connect on port 8443 by default. If your gateway has been configured to accept Policy Manager connections on a different port, then you should specify that port using this syntax, ***<address>:<port>*** (e.g. l7apimgmt:9999).



Login

Connecting to the Gateway

● User Name / Password

User Name: admin

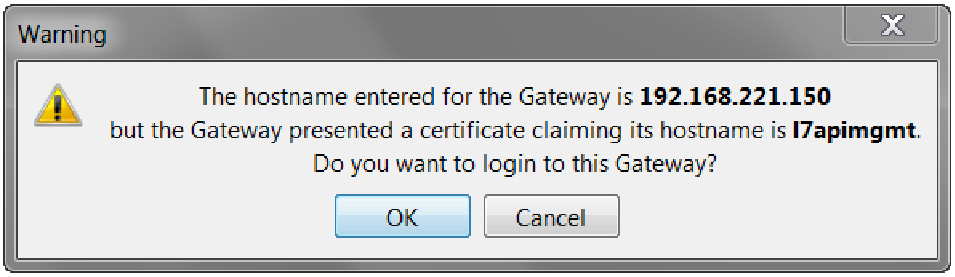
Password: ••••••

○ Client certificate

Certificate: CN=test

Gateway: l7apimgmt

If the gateway name or IP address that you entered does not match the host name of the SSL certificate presented by the gateway, you will receive the following warning. It's OK to ignore this warning by clicking the ***OK*** button.

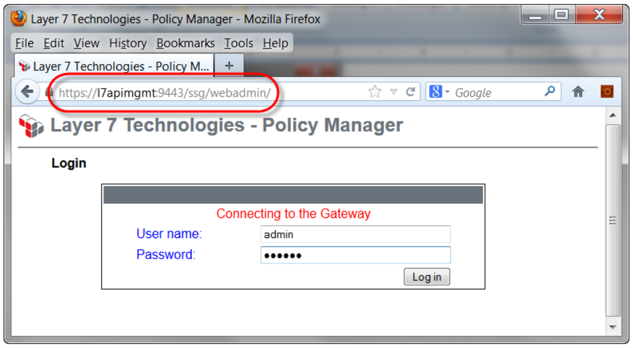


The hostname entered for the Gateway is **192.168.221.150**
but the Gateway presented a certificate claiming its hostname is **l7apimgmt**.
Do you want to login to this Gateway?

You can access the browser version of Policy Manager by browsing the following URL:

https://<gateway>:9443/ssg/webadmin/

Replace <gateway> with the host name or IP address of the gateway you're connecting to. Note the use of port ***9443***.



Layer 7 Technologies - Policy Manager - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Layer 7 Technologies - Policy M...
https://l7apimgmt:9443/ssg/webadmin/
Google
Log in

Layer 7 Technologies - Policy Manager

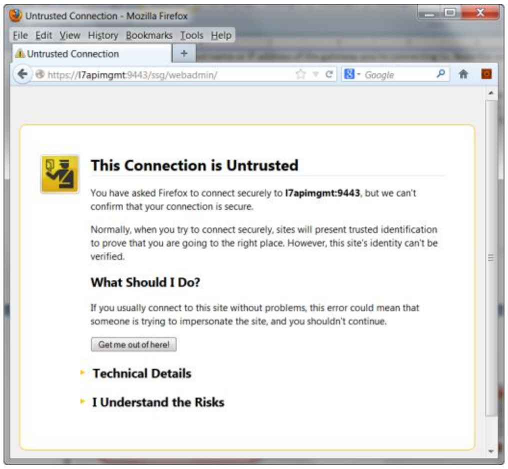
Login

Connecting to the Gateway

User name: admin

Password: ••••••

By default, new gateway's use a self-signed SSL certificate. If you're connecting to a new gateway, or a gateway that has not had its self-signed SSL certificate replaced by a signed certificate from a trusted certificate authority, then the browser will present you with a typical SSL certificate exception. It's OK to acknowledge the exception and continue.



Untrusted Connection - Mozilla Firefox
File Edit View History Bookmarks Tools Help
Untrusted Connection
https://l7apimgmt:9443/ssg/webadmin/
Google
Get me out of here!
Technical Details
I Understand the Risks

This Connection is Untrusted

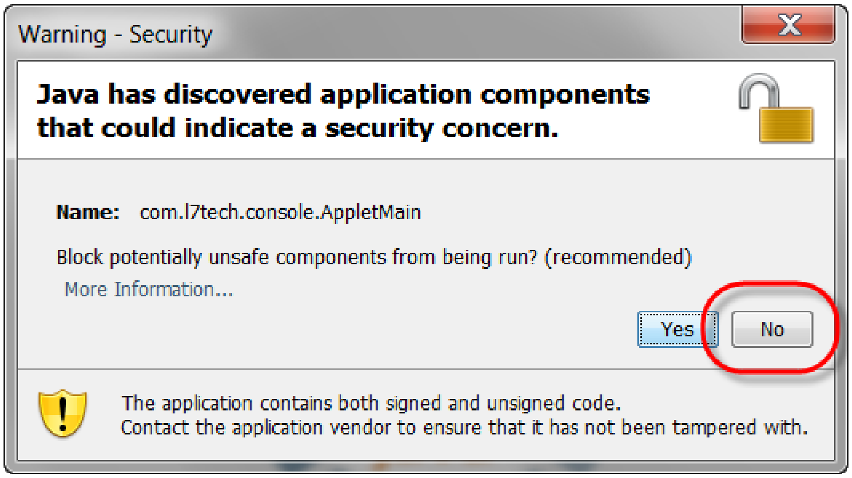
You have asked Firefox to connect securely to **l7apimgmt:9443**, but we can't confirm that your connection is secure.

Normally, when you try to connect securely, sites will present trusted identification to prove that you are going to the right place. However, this site's identity can't be verified.

What Should I Do?

If you usually connect to this site without problems, this error could mean that someone is trying to impersonate the site, and you shouldn't continue.

After providing your user name and password and clicking the ***Log in*** button, the browser will begin to load Policy Manager, and then you will be presented with the following dialog. ***It is important that you click on the No button for Policy Manager to work properly in your browser***.



Warning - Security

Java has discovered application components that could indicate a security concern.

Name: com.l7tech.console.AppletMain

Block potentially unsafe components from being run? (recommended)

More Information...

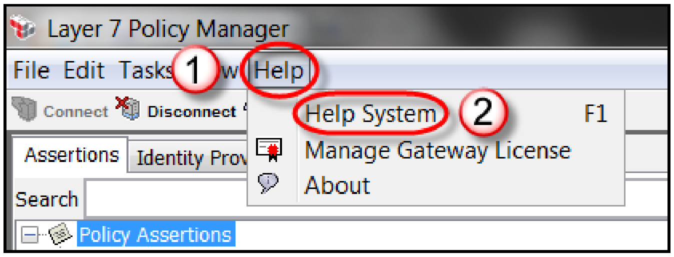
The application contains both signed and unsigned code.
Contact the application vendor to ensure that it has not been tampered with.

2.3 Policy Manager Help

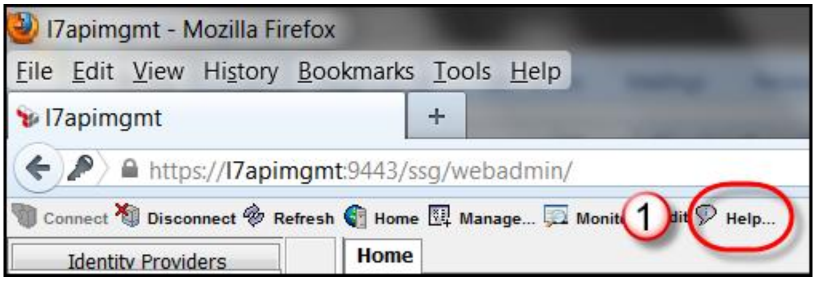
Policy Manager provides excellent online help. It's essentially a combination of Layer 7's Policy Manager User Manual and Policy Authoring User Manual PDFs, but in an easier to navigate and search format. It's an excellent resource regardless of your level of experience. You should take a moment to familiarize yourself with the Policy Manager online help before beginning other tutorials.

Whether you're using the Policy Manager software or browser-based version, you can quickly access online help by typing the ***F1*** key.

Or, in the Policy Manager software version, you can also access online help from the help menu:



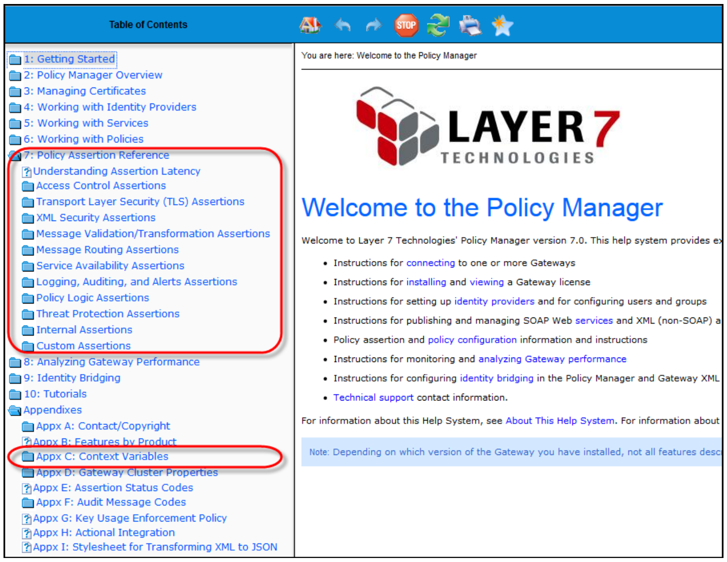
Or, in the Policy Manager browser-based version, you can also access online help on the toolbar:



l7apimgmt - Mozilla Firefox
File Edit View History Bookmarks Tools Help
l7apimgmt
+
https://l7apimgmt:9443/ssg/webadmin/
Connect
Disconnect
Refresh
Home
Manage...
Monit
1
dit
Help...
Identity Providers
Home

In either case, online help will open in your default browser (with either a file or HTTP URL). You can bookmark the online help URL and go directly to it in the future using your browser.

Particularly useful sections include ***7: Policy Assertion Reference*** and ***Appendixes/Appx C: Context Variables***. The tutorials found in ***10: Tutorials*** are older tutorials with dependencies the Layer 7 Sales Demo Environment. Those tutorials are not repeated in this document, but this document contains similar tutorials.



- 1: Getting Started
- 2: Policy Manager Overview
- 3: Managing Certificates
- 4: Working with Identity Providers
- 5: Working with Services
- 6: Working with Policies
- 7: Policy Assertion Reference
  - Understanding Assertion Latency
  - Access Control Assertions
  - Transport Layer Security (TLS) Assertions
  - XML Security Assertions
  - Message Validation/Transformation Assertions
  - Message Routing Assertions
  - Service Availability Assertions
  - Logging, Auditing, and Alerts Assertions
  - Policy Logic Assertions
  - Threat Protection Assertions
  - Internal Assertions
  - Custom Assertions
- 8: Analyzing Gateway Performance
- 9: Identity Bridging
- 10: Tutorials
- Appendixes
  - Appx A: Contact/Copyright
  - Appx B: Features by Product
  - Appx C: Context Variables
  - Appx D: Gateway Cluster Properties
  - Appx E: Assertion Status Codes
  - Appx F: Audit Message Codes
  - Appx G: Key Usage Enforcement Policy
  - Appx H: Actional Integration
  - Appx I: Stylesheet for Transforming XML to JSON

You are here: Welcome to the Policy Manager

Welcome to the Policy Manager

Welcome to Layer 7 Technologies' Policy Manager version 7.0. This help system provides ex

- Instructions for connecting to one or more Gateways
- Instructions for installing and viewing a Gateway license
- Instructions for setting up identity providers and for configuring users and groups
- Instructions for publishing and managing SOAP Web services and XML (non-SOAP) a
- Policy assertion and policy configuration information and instructions
- Instructions for monitoring and analyzing Gateway performance
- Instructions for configuring identity bridging in the Policy Manager and Gateway XML
- Technical support contact information.

For information about this Help System, see About This Help System. For information about

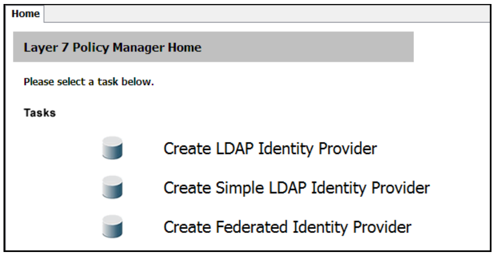
Note: Depending on which version of the Gateway you have installed, not all features desc

2.4 Policy Manager Overview

This section provides a quick orientation to Policy Manager, with some pointers that may be particularly useful to new users and/or users of these tutorials. It's not meant to be an exhaustive description of every Policy Manager feature.

2.4.1 Policy Manager Home

The Policy Manager Home is sort of the landing page of Policy Manager. It's the first thing you see after connecting to a gateway with Policy Manager, and it presents some links to some commonly performed tasks within Policy Manager. All of these tasks are accessible via the ***Tasks*** menu or context menus in other Policy Manager views.



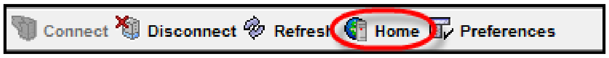
Layer 7 Policy Manager Home

Please select a task below.

Tasks

- Create LDAP Identity Provider
- Create Simple LDAP Identity Provider
- Create Federated Identity Provider

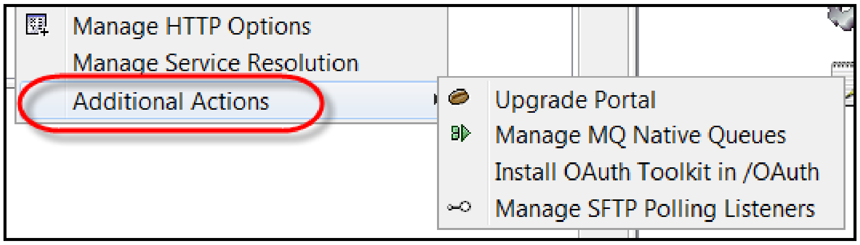
After users navigate away from the Policy Manager Home, they can return by clicking the ***Home*** button on the Policy Manager toolbar:



2.4.2 Menu Bar

In the Policy Manager menu bar, the ***Tasks, View and Help*** menus are of particular use.

The ***Tasks*** menu is used to configure many aspects of a gateway. Note that, depending on the version of your gateway and the possible Tactical assertions that you have installed, there may be any number of additional actions hidden at the bottom of the ***Tasks*** menu.

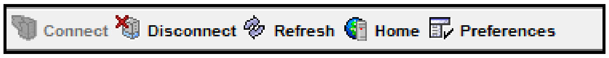

Manage HTTP Options
Manage Service Resolution
Additional Actions
Upgrade Portal
Manage MQ Native Queues
Install OAuth Toolkit in /OAuth
Manage SFTP Polling Listeners

The ***View*** menu is where you'll go to view the Policy Manager dashboard, audit records and log files.

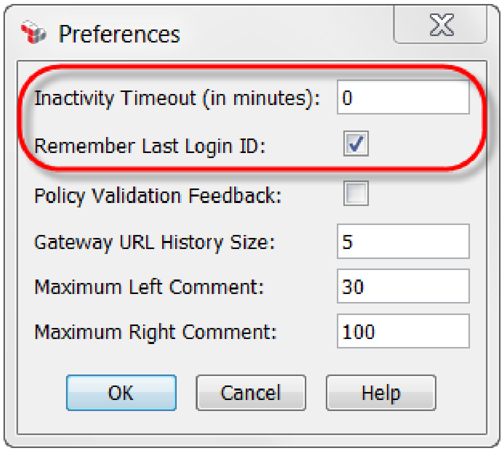
The ***Help*** menu is where you'll go to launch Policy Manager's online help.

2.4.3 Toolbar

The Policy Manager toolbar can be used to connect and disconnect Policy Manager from gateways, refresh different Policy Manager views (which is sometimes necessary to see folders, services and policies created by someone or something else outside of the current user's Policy Manager session), display the Policy Manager Home page, and set preferences.



Before beginning the tutorials, you may want to set your Inactivity Timeout to 0, and select to remember the last login ID.



Inactivity Timeout (in minutes): 0

Remember Last Login ID: ☑

Policy Validation Feedback: □

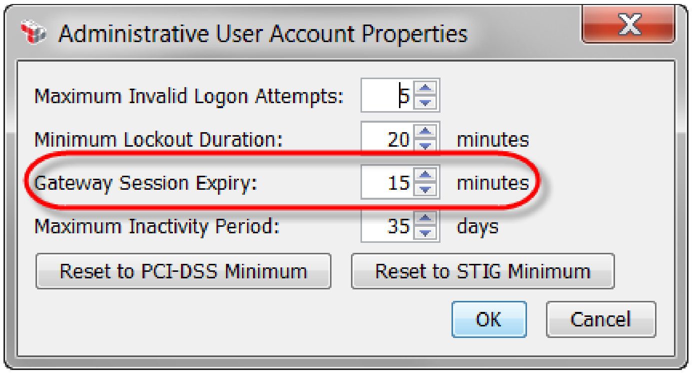
Gateway URL History Size: 5

Maximum Left Comment: 30

Maximum Right Comment: 100

Note: Administrative user session is also governed by the Gateway Session Expiry property of the administrative user account properties. This property can be set via the Tasks/Manage Account

Policies/Manage Administrative User Policy menu item. The maximum number of minutes that the property can be set to is 1440.



Administrative User Account Properties

Maximum Invalid Logon Attempts: 5

Minimum Lockout Duration: 20 minutes

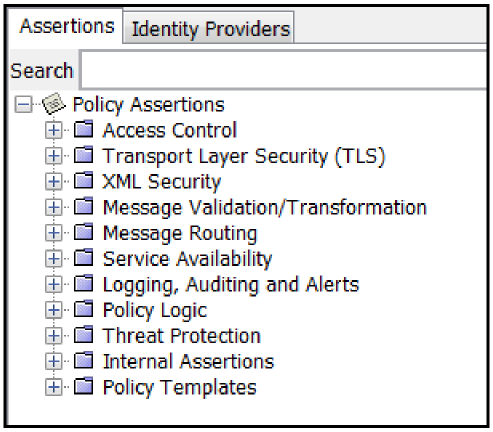
Gateway Session Expiry: 15 minutes

Maximum Inactivity Period: 35 days

2.4.4 Policy Assertions

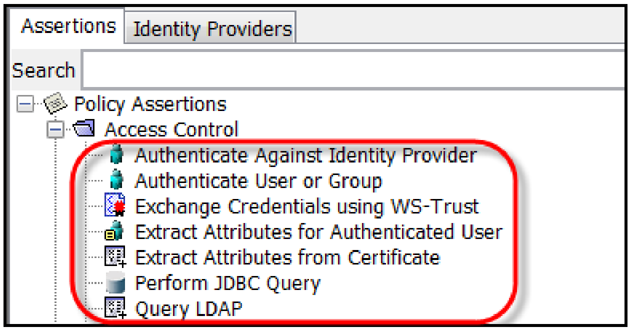
Messages sent to a Layer 7 gateway are resolved to services published on the gateway and are processed according to the policies of those services. Service policies (and policy fragments) are comprised of policy assertions.

The available policy assertions for a given gateway can be found in Policy Manager's policy assertion tree:



- Policy Assertions
  - Access Control
  - Transport Layer Security (TLS)
  - XML Security
  - Message Validation/Transformation
  - Message Routing
  - Service Availability
  - Logging, Auditing and Alerts
  - Policy Logic
  - Threat Protection
  - Internal Assertions
  - Policy Templates

All policy assertions are organized into one or more of ten categories (excluding Policy Templates which shows policies that have been exported to the current Policy Manager user's file system). Each of these categories expands to show many more specific policy assertions.



- Policy Assertions
  - Access Control
    - Authenticate Against Identity Provider
    - Authenticate User or Group
    - Exchange Credentials using WS-Trust
    - Extract Attributes for Authenticated User
    - Extract Attributes from Certificate
    - Perform JDBC Query
    - Query LDAP

At the time this section was written, the latest gateway version had approximately 150 out-of-the-box policy assertions. Additional policy assertions may exist depending on additional Layer 7 functionality that may have been optionally deployed, custom and/or encapsulated assertions that may have been created, and future feature releases that may have become available.

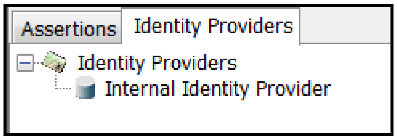
Policy assertions basically come in two flavors: policy assertions that accomplish something big through simple wizard driven configuration (e.g. the XML Security/Create SAML Token assertion), or policy assertions that act more as components of a language and which allow you to set variables, compare variables, perform conditional AND and OR logic, perform looping logic, etc.

Many of Layer 7's customers can get by with service policies that have just a few policy assertions to meet their more simple requirements. The vast majority of other customers can accomplish everything they want to do by creating sophisticated conditional policies that use policy assertions as components of a flexible policy language. Very rarely do customers want or need to create custom assertions using Layer 7's Custom Assertion SDK. However, custom assertions always remain an option for Layer 7 customers.

Note: The Search field can be used to easily fine assertions that contain a specified string in their name.

2.4.5 Identity Providers

There are four types of identity providers that can be created and/or managed on the Identity Providers tab (and via the ***Tasks*** menu): the Internal Identity Provider, standard LDAP identity providers, simple LDAP identity providers and federated identity providers.



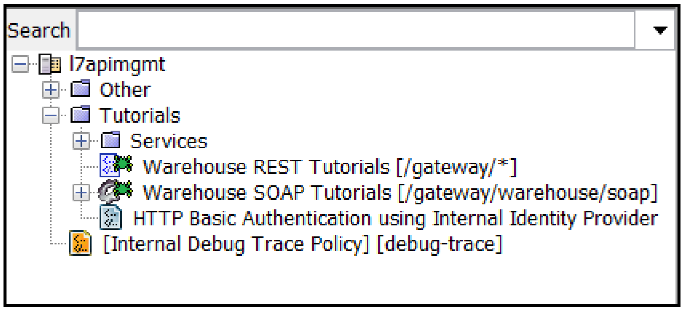
These identity providers are used for both role-based access control (RBAC) to the gateway's configuration (the Internal Identity Provider and standard LDAP identity providers only) and access control of traffic passing through the gateway (all identity providers). They can be used for user authentication, user and group authorization, and certificate validation.

The Internal Identity Provider contains the initial admin user of the gateway.

These identity providers should not be confused with industry standard identity providers (e.g. as defined by SAML, and other similar standards). Support for integrating with or acting as an industry standard identity provider is usually implemented in service policies on the Layer 7 gateway.

2.4.6 Folders, Services & Policies

Users can create and administrate a folder hierarchy of folders, services and policies on their gateways. This hierarchy ties in nicely with RBAC on the gateway such that users can groups can be assigned to automatically generated roles that let them see and work with specific paths within that hierarchy.



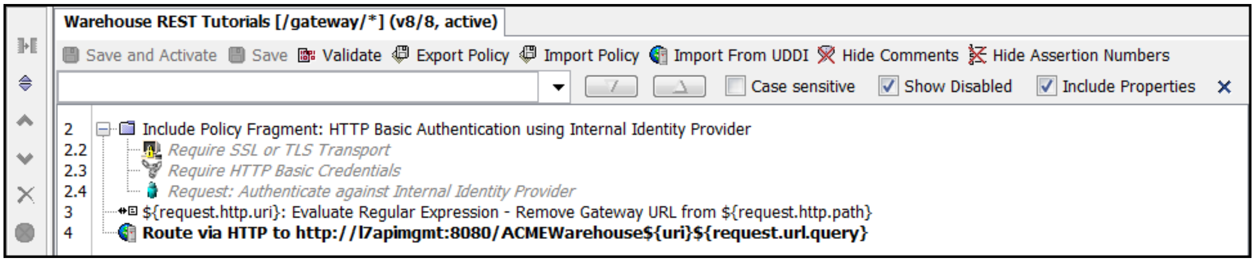
```
l7apimgmt
  Other
  Tutorials
    Services
    Warehouse REST Tutorials [/gateway/*]
    Warehouse SOAP Tutorials [/gateway/warehouse/soap]
    HTTP Basic Authentication using Internal Identity Provider
  [Internal Debug Trace Policy] [debug-trace]
```

Nodes within the tree have different right click context menus that give you direct access to menu commands for that specific node.

Note: The Search field can be used to easily fine services and policies that contain a specified string in their name.

2.4.7 Policy Editor

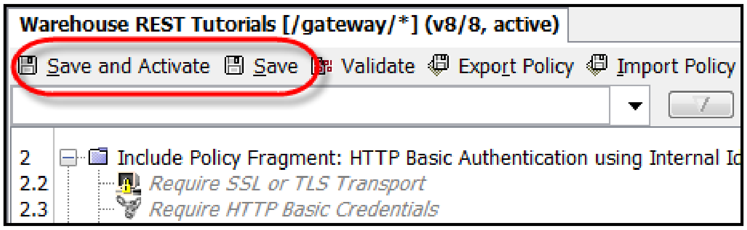
The policy editor is the primary interface for authoring service policies and policy fragments. Polices are authored by dragging and dropping policy assertions from the policy assertion tree to the policy editor (or for a select few policy assertions, by right clicking in the policy editor and selecting them from the context menu).



```
2    Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
2.2    Require SSL or TLS Transport
2.3    Require HTTP Basic Credentials
2.4    Request: Authenticate against Internal Identity Provider
3    ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
4    Route via HTTP to http://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}
```

2.4.7.1 Save & Activate versus Save

The policy editor toolbar has both ***Save and Activate*** and ***Save*** buttons. If a policy has changed since being opened in the policy editor, then these buttons will be enabled. The ***Save and Activate*** button will save the current changes to the policy as a new version of the policy, and it will make that new version of the policy the active policy version used by the gateway service when processing subsequent requests. The ***Save*** button will just save the current changes to the policy as a new version of the policy without making it the active policy version of the service.

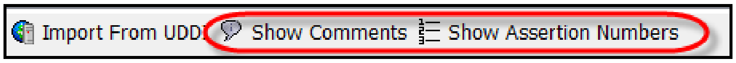


```
2    Include Policy Fragment: HTTP Basic Authentication using Internal Id
2.2    Require SSL or TLS Transport
2.3    Require HTTP Basic Credentials
```

In most cases, customers use the ***Save and Activate*** button. If you've made changes to your policy and you do not see those changes reflected in your tests, the first thing you should check to make sure of is that you've saved and activated those policy changes.

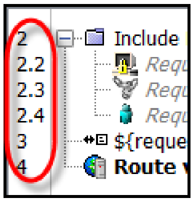
2.4.7.2 Show Comments and Assertion Numbers

For the tutorials, you should choose to show comments and assertion numbers:



Show Comments controls the visibility of left and right comments that can be attached to every assertion via the context menu displayed when right clicking that assertion (and not the visibility of the specific ***Policy Logic/Add Comment to Policy*** assertion).

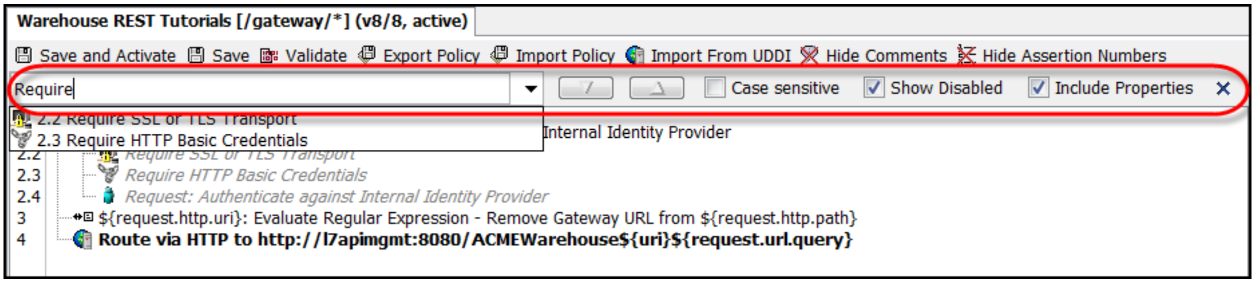
Show assertion numbers shows the ordinal number of the assertions in policy. Included policy fragments use a dot notation. The tutorials will often reference policy assertions in policy by their policy assertion number.



Policies always begin with assertion number 2, because all policies are actually wrapped by a ***Policy Logic/All assertions must evaluate to true*** assertion folder that's not displayed in the policy editor.

2.4.7.3 Searching for Assertions

You can search for policy assertions within a policy by clicking the ***Ctrl-F*** key combination on your keyboard while the policy editor has focus. This will display a set of search controls under the policy editor toolbar.



Require

□ Case sensitive ☑ Show Disabled ☑ Include Properties

2.2 Require SSL or TLS Transport
2.3 Require HTTP Basic Credentials

Internal Identity Provider

2.2 Require SSL or TLS Transport
2.3 Require HTTP Basic Credentials
2.4 Request: Authenticate against Internal Identity Provider
3 ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
4 **Route via HTTP to http://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}**

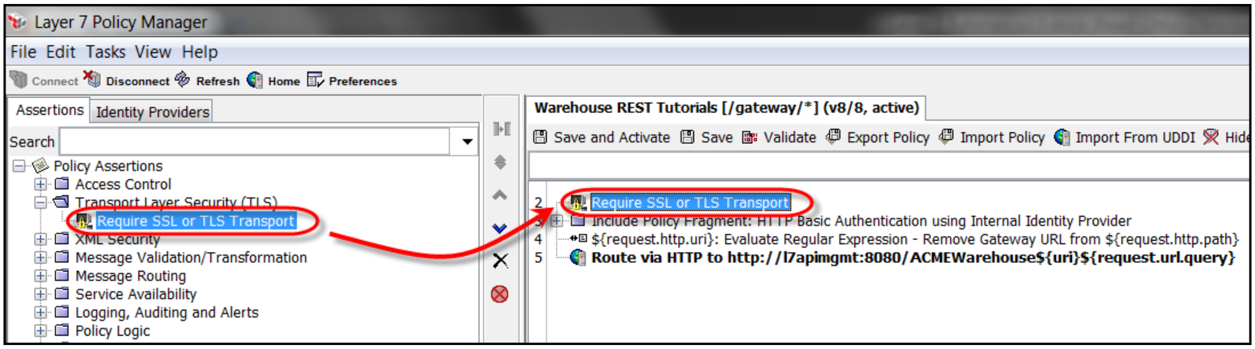
Begin searching by typing in the drop down text field.

2.5 Basic Policy Concepts

2.5.1 Policy Authoring

2.5.1.1 Drag & Drop

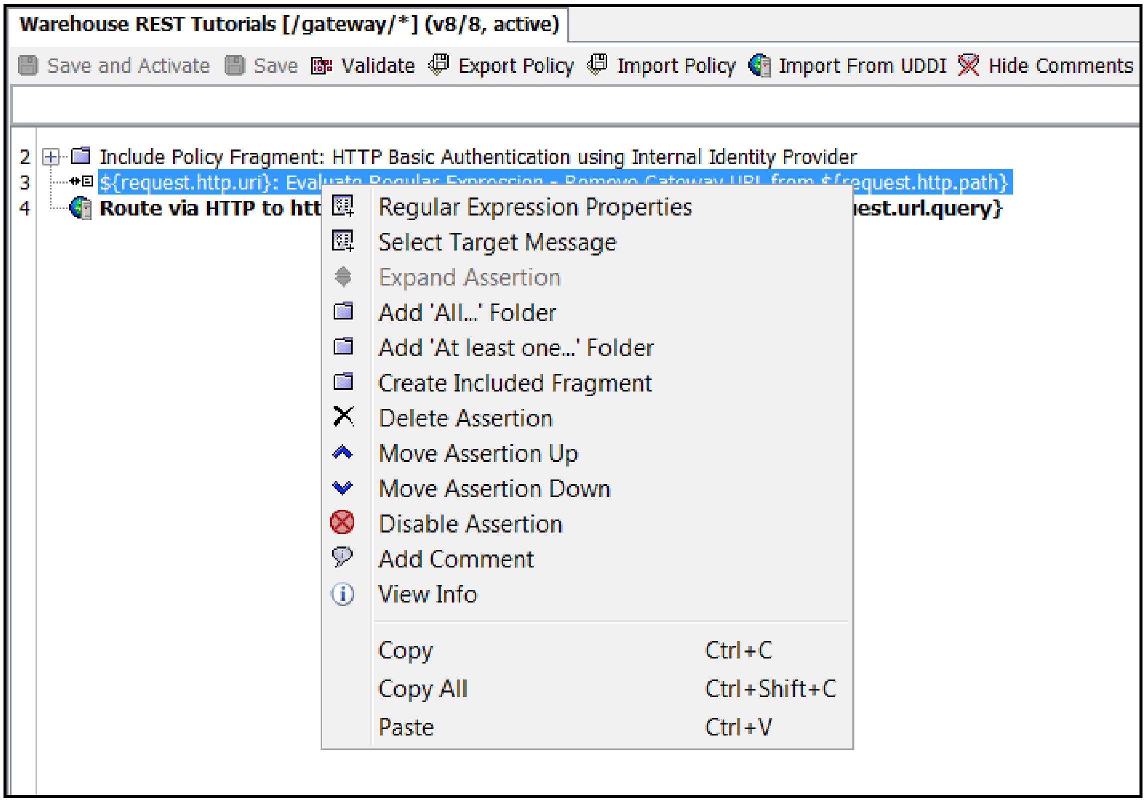
Polices are authored by dragging and dropping policy assertions from the policy assertion tree to the policy editor (or for a select few policy assertions, by right clicking in the policy editor and selecting them from the context menu).


Layer 7 Policy Manager
File Edit Tasks View Help
Connect Disconnect Refresh Home Preferences
Assertions Identity Providers
Search
Policy Assertions
Access Control
Transport Layer Security (TLS)
Require SSL or TLS Transport
XML Security
Message Validation/Transformation
Message Routing
Service Availability
Logging, Auditing and Alerts
Policy Logic
Warehouse REST Tutorials [/gateway/*] (v8/8, active)
Save and Activate Save Validate Export Policy Import Policy Import From UDDI Hide
2 Require SSL or TLS Transport
3 Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
4 ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
5 Route via HTTP to http://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}

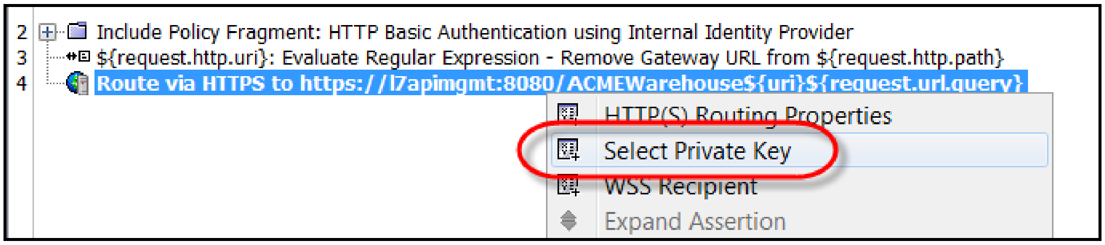
In general, assertions dropped on top of another assertion will be positioned after that assertion in policy. Assertions dropped at the very top of the policy editor will be positioned first in policy and assertions dropped at the very bottom of the policy editor will be positioned last in policy. Assertions dropped on a folder assertion will be positioned within the folder.

2.5.1.2 Context Menu

A context menu is displayed when you right click on an assertion in the policy editor. This context menu can be used to configure that assertion, add a select few additional assertions to the policy, and perform some additional edit actions.


Warehouse REST Tutorials [/gateway/*] (v8/8, active)
Save and Activate Save Validate Export Policy Import Policy Import From UDDI Hide Comments
2 Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3 ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
4 Route via HTTP to htt… …est.url.query}
Regular Expression Properties
Select Target Message
Expand Assertion
Add 'All...' Folder
Add 'At least one...' Folder
Create Included Fragment
Delete Assertion
Move Assertion Up
Move Assertion Down
Disable Assertion
Add Comment
View Info
Copy Ctrl+C
Copy All Ctrl+Shift+C
Paste Ctrl+V

Note: In some rare cases, the only way to configure certain aspects of certain assertions is via the context menu (e.g. if you need to specify a specific client key for mutual auth SSL from a HTTP route assertion to the backend service, you must do this through the context menu, otherwise the default gateway SSL key is used; there are other examples like this).



2 Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3 ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
4 Route via HTTPS to https://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}

2.5.1.3 Copy & Paste

Policy assertions can be copied from a policy in the policy editor, and pasted back to a different location in that same policy or pasted to another policy altogether.

To copy policy assertions you must first select them. You can select one policy assertion by left clicking on it. You can select multiple policy assertions by holding down either the Ctrl key or Shift key on your keyboard while left clicking on assertions.

Once you have selected the policy assertions that you want to copy, you can use Ctrl-C to copy them and Ctrl-V to paste them. You can also use the ***Edit*** menu or the right click context menu to copy and paste.

Layer 7 policy is actually represented as WS-Policy compliant XML. For example, when copying a simple ***Require SSL or TLS Transport*** assertion, the following XML is copied to the clipboard:

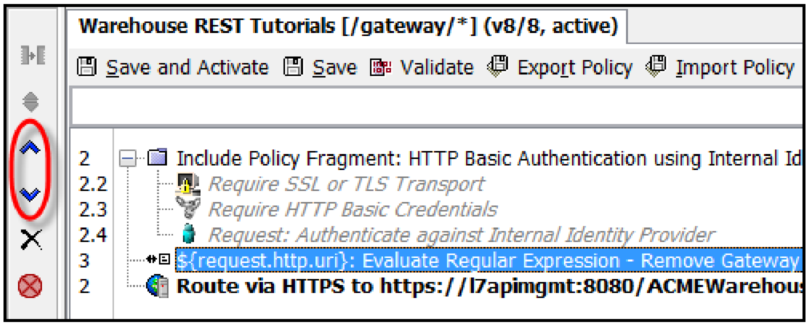
```
<?xml version="1.0" encoding="UTF-8"?>
<wsp:Policy xmlns:L7p="http://www.layer7tech.com/ws/policy"
xmlns:wsp="http://schemas.xmlsoap.org/ws/2002/12/policy">
    <wsp:All wsp:Usage="Required">
        <L7p:SslAssertion/>
    </wsp:All>
</wsp:Policy>
```

2.5.1.4 Configuration Dialogs

Most policy assertions have configuration dialogs that allow you to set many properties of those assertions. In some cases, these configuration dialogs are displayed automatically after dragging and dropping an assertion to the policy editor. In any case, these configuration dialogs can be displayed by double-clicking on the assertion in the policy editor, or by selecting the assertion properties menu item from the right click context menu of that assertion.

2.5.1.5 Moving Policy Assertions Up & Down

When dragging and dropping or copying and pasting policy assertions in the policy editor, they will not always be positioned where you want them to be. Policy assertions can be moved up or down in policy either individually or in groups of multiple assertions by using the ***Move Assertion Up*** and ***Move Assertion Down*** buttons on the toolbar to the left of the policy editor, or by selecting the corresponding menu items in the right click context menu.

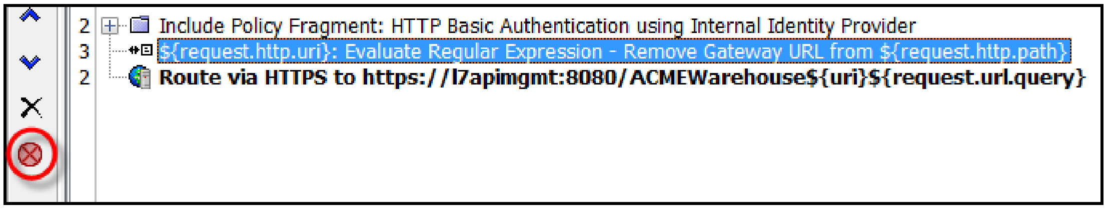


Warehouse REST Tutorials [/gateway/*] (v8/8, active)

```
2    Include Policy Fragment: HTTP Basic Authentication using Internal Id
2.2    Require SSL or TLS Transport
2.3    Require HTTP Basic Credentials
2.4    Request: Authenticate against Internal Identity Provider
3    ${request.http.uri}: Evaluate Regular Expression - Remove Gateway
2    Route via HTTPS to https://l7apimgmt:8080/ACMEWarehou
```

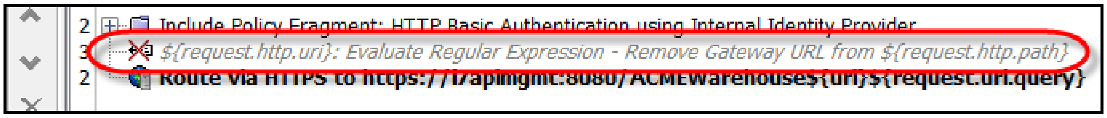
2.5.1.6 Disabling Policy Assertions

Policy assertions can be temporarily disabled without actually being removed from policy. You can disable one or more policy assertions by selecting them in the policy editor, and then by clicking on the Disable/Enable Assertion button on the toolbar to the left of the policy editor, or by selecting the corresponding menu items in the right click context menu.



```
2    Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3    ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
2    Route via HTTPS to https://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}
```

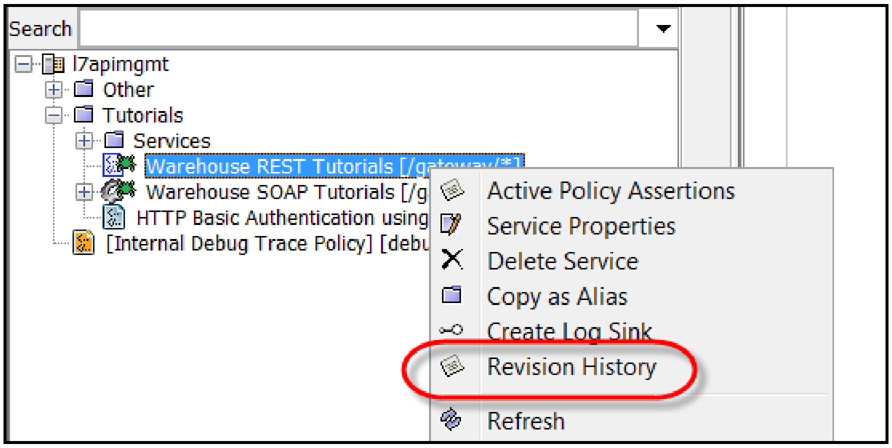
Disabled policy assertions have a red X through their icon, and are grayed out.

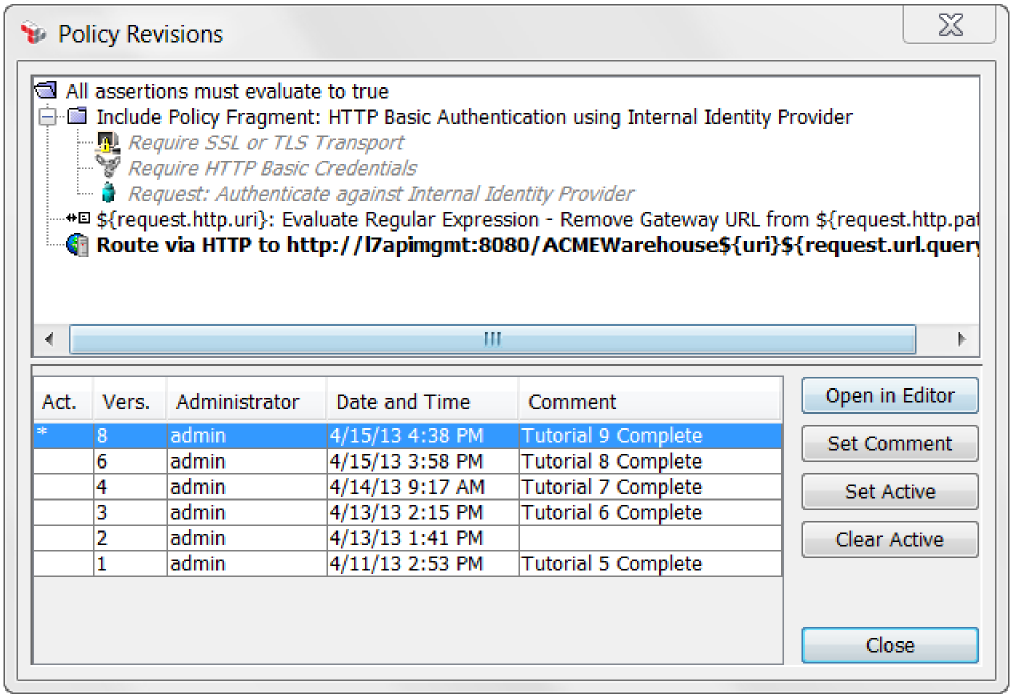


```
2    Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3    ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
2    Route via HTTPS to https://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}
```

2.5.1.7 Policy Revisions

Gateway services and policies maintain a history of policy revisions. The policy revision history for a specific service or policy is available from that item's right click context menu in the service and policy tree.





All assertions must evaluate to true
Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
Require SSL or TLS Transport
Require HTTP Basic Credentials
Request: Authenticate against Internal Identity Provider
${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.pat
Route via HTTP to http://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query

Act.	Vers.	Administrator	Date and Time	Comment
*	8	admin	4/15/13 4:38 PM	Tutorial 9 Complete
	6	admin	4/15/13 3:58 PM	Tutorial 8 Complete
	4	admin	4/14/13 9:17 AM	Tutorial 7 Complete
	3	admin	4/13/13 2:15 PM	Tutorial 6 Complete
	2	admin	4/13/13 1:41 PM	
	1	admin	4/11/13 2:53 PM	Tutorial 5 Complete

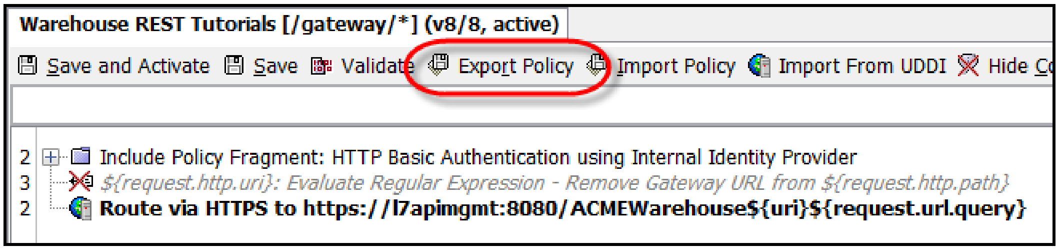
The gateway will maintain a configurable number (by default, 20) of uncommented policy revisions before it starts throwing away the oldest revisions. The gateway will never throw away revisions that have a comment.

Tutorials will use comments to mark policy revisions that represent a completed policy for a specific tutorial using a shared service. This will make it easy to reuse fewer service across more tutorials with known starting points, and to go back to policy revisions for tutorials that were completed at some point in the past.

To make a particular policy revision the active policy version of the service (which will be frequently required by tutorials to revert a service's policy to a known starting point for a particular tutorial), select that revision in the Policy Revisions dialog, and click the ***Set Active*** button.

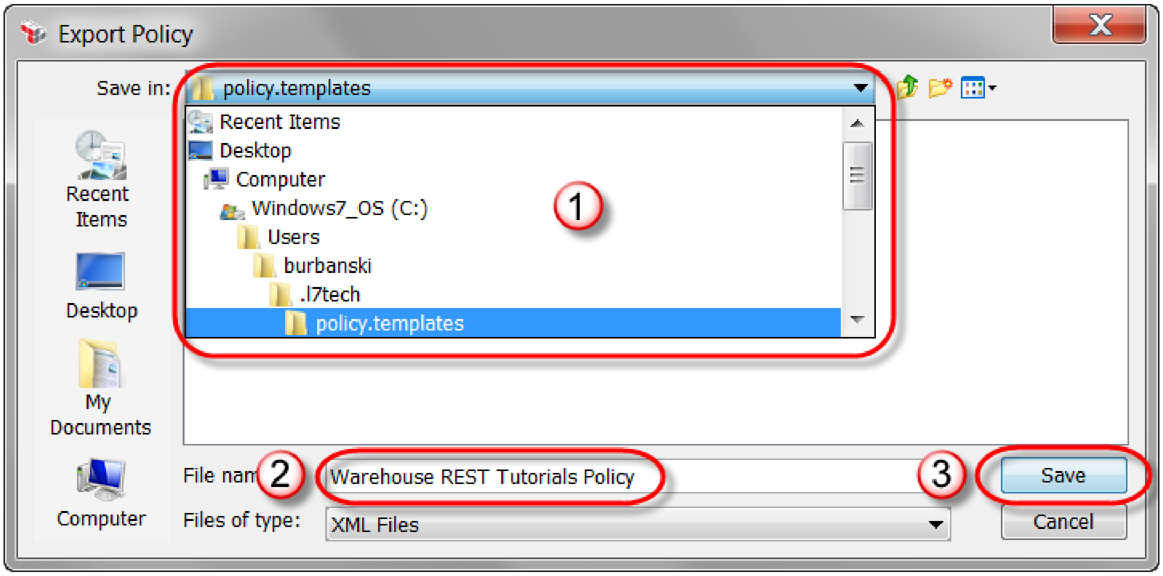
2.5.1.8 Exporting and Importing Policy

Using Policy Manager, policy can be exported from one gateway and imported to another. Policies can be exported by opening those policies in the policy editor, and by clicking the ***Export Policy*** button on the policy editor toolbar (or by select the ***File/Export Policy*** menu item).



2 Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3 *${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}*
2 **Route via HTTPS to https://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}**

By default, policies are exported to a user specific folder on the user's workstation (e.g. C:\Users\<username>\.l7tech\policy.templates), though you can select any available file system location to save your policy exports.

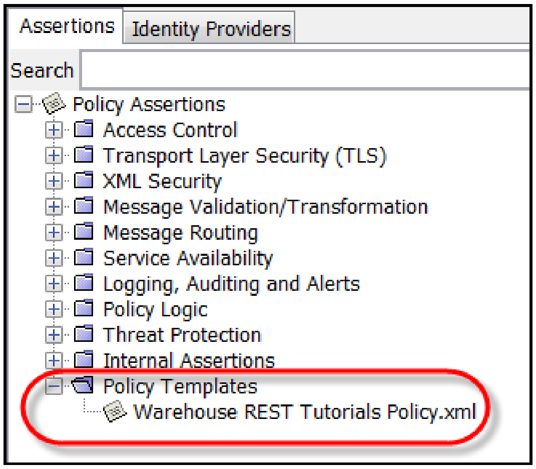


Save in: policy.templates

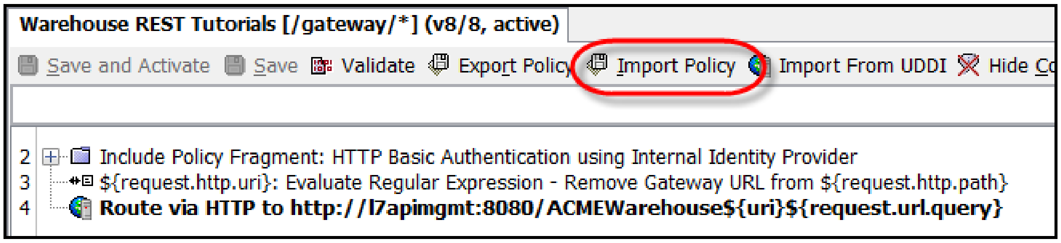
File nam: Warehouse REST Tutorials Policy

Files of type: XML Files

Policy exports saved to the default location are displayed as policy templates in the policy assertion tree:



In turn, policies can be imported by opening the current policy of the service or policy that you want to import to in the policy editor, and by clicking the ***Import Policy*** button on the policy editor toolbar (or by select the ***File/Import Policy*** menu item).



Warehouse REST Tutorials [/gateway/*] (v8/8, active)

```
2 Include Policy Fragment: HTTP Basic Authentication using Internal Identity Provider
3 ${request.http.uri}: Evaluate Regular Expression - Remove Gateway URL from ${request.http.path}
4 Route via HTTP to http://l7apimgmt:8080/ACMEWarehouse${uri}${request.url.query}
```

Policies can also be imported by dragging and dropping policy templates from the policy assertion tree to the policy editor.

In some cases, depending on what environmental dependencies might exist in an exported policy, a dialog might be displayed when importing that policy. The dialog will identify dependencies that must be resolved, and it will give you an opportunity to resolve those dependencies in several different ways.

2.5.2 Policy Execution

2.5.2.1 Execution Basics

Policy executes sequentially (unless using the ***Policy Logic/Run All Assertions Concurrently*** assertion) in order from the top of the policy to the bottom of the policy.

Each policy assertion is a constraint, and each policy assertion will succeed or fail at runtime depending on runtime conditions. Some policy assertions always succeed (e.g. the ***Policy Logic/Add Comment to Policy*** and ***Policy Logic/Continue Processing*** assertions), and one policy assertion always fails (namely the ***Policy Logic/Stop Processing*** assertion).

By default, when a policy assertion fails at runtime, then the policy fails and a descriptive but not revealing SOAP fault is returned to the consumer. However, this behavior is configurable in many ways as described in the next section.

Conditional AND and OR logic can be implemented in policy by using the ***Policy Logic/All assertions must evaluate to true*** and ***Policy Logic/At least one assertion must evaluate to true*** assertions respectively. These assertions are represented by folders that can contain other assertions, including other ***All assertions must evaluate to true*** and ***At least one assertion must evaluate to true*** assertions. The ***All assertions must evaluate to true*** assertion represents the AND condition, and succeeds if all immediate child assertions succeed. The ***At least one assertion must evaluate to true*** assertion represents the OR condition, and succeeds if at least one immediate child assertion succeeds. Processing exits the ***At least one assertion must evaluate to true*** assertion after the first child assertion succeeds. The remaining child assertions within the folder are not evaluated.

2.5.2.2 Error Handling

By default, when a policy assertion fails at runtime, then the policy fails and a descriptive but not revealing SOAP fault is returned to the consumer. However, this behavior is configurable in many ways.

There are policy assertions that themselves control what message will be returned to the consumer when a policy fails. They include the ***Logging, Auditing and Alerts/Customize SOAP Fault Response*** and ***Logging, Auditing and Alerts/Customize Error Response*** assertions. These assertions effect the gateway's error response behavior for errors the occur after these assertions in policy. You can have many of these assertions in your policy to change the error response behavior to be more specific throughout the policy. Review these assertions' features in the Policy Manager online help to better understand the options they offer. Any other assertion that effects that response to the consumer can also be used to control error response messages returned by the gateway (e.g. customers frequently use the ***Message Routing/Return Template Response to Requestor*** assertion for custom error messages).

Policy assertions can be wrapped with conditional logic to provide even greater control of error handling, and to allow additional policy to execute after an error has occurred (e.g. to add more detail to the audit trail and to generate alerts to administrators or administrative systems) before returning a custom error to the consumer. Or, using conditional logic, you can ignore errors altogether and continue processing messages through to the backend service.

3 Summary of Tutorials

This section summarizes the available tutorials in this package. The detailed tutorial documentation can be found for each of these tutorials in a folder of the same name within this package.

3.1 Tutorial 1 - Deploy Tutorial Services

This tutorial deploys sample SOAP and REST services for use by other tutorials.

3.2 Tutorial 2 - Test Tutorial SOAP Service

This tutorial guides you through testing the SOAP service deployed in ***Tutorial 1 - Deploy Tutorial Services***.

3.3 Tutorial 3 - Test Tutorial REST Service

This tutorial guides you through testing the REST service deployed in ***Tutorial 1 - Deploy Tutorial Services***.

3.4 Tutorial 4 - Publish SOAP Service

This tutorial shows you how to publish a gateway SOAP service (or proxy) for the tutorial Warehouse service deployed in ***Tutorial 1 - Deploy Tutorial Services*** which in practice would be hosted on an application server behind the gateway. This is one of the most common tasks performed by users of our gateway, and it is the starting point for enforcing additional policy on traffic sent through the gateway to a SOAP service as demonstrated in other tutorials.

3.5 Tutorial 5 - Publish REST Service

This tutorial shows you how to publish a gateway REST service (or proxy) for the tutorial Warehouse REST service deployed in ***Tutorial 1 - Deploy Tutorial Services*** which in practice would be hosted on an application server behind the gateway. This is one of the most common tasks performed by users of our gateway, and it is the starting point for enforcing additional policy on traffic sent through the gateway to a REST service or API as demonstrated in other tutorials.

3.6 Tutorial 6 - Basic Authentication

This tutorials shows you how to add some basic access control to your services using HTTP Basic credentials sent over SSL and authenticated against the gateway's internal identity provider.

3.7 Tutorial 7 - Basic Troubleshooting

This tutorial provides a basic recommended approach to troubleshooting runtime policy behavior on a gateway.

3.8 Tutorial 8 - Group Membership Authorization

This tutorials makes changes to the basic authentication added in ***Tutorial 6 - Basic Authentication*** to add group membership authorization. It also introduces you, in part, to conditional logic in policy.

3.9 Tutorial 9 - Policy Fragments

This tutorials demonstrates using a policy fragment to reuse centrally administered policy assertions in multiple service policies.

3.10 Tutorial 10 - Introduction to Context Variables

This tutorial provides an introduction to context variables. Context variables contain a wealth of information about the message processing context and associated meta-data and are an invaluable tool for building flexible, dynamic policies.

3.11 Tutorial 11 - Using Context Variables in XSL Transformations

This tutorial demonstrates the use of the XSLT assertion with the use of parameters. The XSLT tutorial will give you the basics of using XSLT to search for elements within a document and replace the values from inbound data from the request. The inbound request is an HTTP GET with URL parameters that are used to alter a set XML document. The tutorial utilizes the Loopback Service, HTTP Parameter passing, Context Variables, and XSLT.

3.12 Tutorial 12 - SSL Client Certificate Authentication

This tutorial demonstrates combining SSL client certificate authentication using a Layer 7 Federated Identity Provider with existing HTTP Basic authentication. The FIP acts as a sophisticated certificate trust store that can map users and groups to specific client certificates or virtual groups to signing certificates, and that can perform certificate validation based on a direct match or a trust chain of signing certificates to a trust anchor. Users can configure multiple FIPs for partitioning of different categories of certificates (e.g. partners, customers, etc.).

3.13 Tutorial 13 - Content-Based Routing

This tutorial demonstrates using the content of messages to make routing decisions about where to send service requests.

3.14 Tutorial 14 - Audit Sink and Audit Lookup Policies

This tutorial demonstrates using the audit sink policy to store and retrieve audit records to an external database using JDBC. For the purpose of this tutorial, we will create a new database instance on the gateway to act as an external gateway. If you have the ability to connect an actual remote DB, you may modify the steps for DB creation to apply for your database.

3.15 Tutorial 15 - Salesforce.com SSO

This tutorial will walk you through using the Gateway to support single sign-on to salesforce.com. It will demonstrate how you are able to login through your browser with one set of credentials and get automatically logged into salesforce.com using a SAML response that is constructed in a Gateway policy. There are two main configurations that will be needed for this tutorial. First, you will need to configure salesforce.com to support Single Sign-on and second a policy will be needed in the Gateway to support this use case.

3.16 Tutorial 16 - (Portal) Sign-in

This tutorial illustrates how an application developer signs onto the API Developer portal to discover APIs provided by the API management infrastructure.

3.17 Tutorial 17 - (Portal) Publish an API

This tutorial takes an API provider through the process of publishing an API already defined on the gateway to the API developer portal with application developers can discover and interact with the API.

3.18 Tutorial 18 - (Portal) Register Application and Use API Explorer

This tutorial takes an application developer through the steps of registering an application to consume an API, how an API provider enables the API to be consumed with an API key and OAuth and how the application developer calls the API through the API Explorer.

3.19 Tutorial 19 - Publish Loopback Service

This tutorial shows you how to publish a simple loopback service to a gateway. In other words, a service that will loopback (or echo back) any request sent to it. This sort of service is a useful starting point for doing many things on a gateway, including testing gateway functionality, stubbing out backend services while developing corresponding gateway services, and using the gateway to provide services directly.