

IBM Tivoli Security Policy Manager



Tivoli Security Policy Manager Adapter for FileNet: Installation and User Guide

IBM Tivoli Security Policy Manager



Tivoli Security Policy Manager Adapter for FileNet: Installation and User Guide

Note

Before using this information and the product it supports, read the general information under “Notices,” on page 35.

This edition applies to version 1.0 of this adapter and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2010.**

US Government Users Restricted Rights – Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Contents

About this document	v
Intended audience	v
Accessibility	v
Tivoli technical training.	v
Conventions used in this document	v
Typeface conventions	v

Part 1. Tivoli Security Policy Manager Adapter for FileNet: Installation Guide. 1

Chapter 1. Introducing IBM Tivoli Security Policy Manager Adapter for FileNet	3
Overview	3
Supported platform	3
Prerequisite software	3
Hardware requirement	3
Installable components	4

Chapter 2. Installation and configuration 5	
Installation of Tivoli Security Policy Manager Plug-in 5	
Installation of TSPM Adapter for FileNet 6	

Part 2. Tivoli Security Policy Manager Adapter for FileNet: User Guide 9

Chapter 3. Working with Tivoli Security Policy Manager Adapter for FileNet . . . 11	
Building an application model using sample models 11	
Building an application model using RAD 11	
Creating a sample content in FileNet 19	
Impact of FileNet metadata size on transactions . . 20	
Enforcing policy 20	
Enforcing policy when switching between application 20	

Chapter 4. Configuring Tivoli Security Policy Manager for policy authoring . . 21	
Configuring security roles for accessing Tivoli Security Policy Manager Adapter for FileNet . . . 21	
Exporting security certificates from FileNet to Tivoli Security Policy Manager 21	
Creating a service registry 22	
Creating a policy distribution point 24	
Importing application model and metadata. 25	
Authoring a policy 26	
Authoring a sample policy 28	
Configuring a policy 30	
Distributing a policy 31	
Troubleshooting 32	

Appendix. Notices 35	
Trademarks 36	

About this document

IBM® Tivoli® Security Policy Manager enables you to continuously manage, monitor, and audit the security of your Web Services applications.

IBM Tivoli Security Policy Manager Adapter for FileNet®: Installation and User Guide describes how to install and configure Tivoli Security Policy Manager Adapter for FileNet and using it to author policies and enforce the policies on an Enterprise Content Management solution like FileNet.

Intended audience

This publication is designed for the system administrators and network administrators in an organization that uses IBM Tivoli Security Policy Manager to manage the security policies of its Web services applications.

Readers of this book should have working knowledge of the following topics:

- The implementation of IBM Tivoli Security Policy Manager in their environment
- Web services security concepts and practices
- Web applications
- IBM WebSphere® Application Server

Accessibility

Accessibility features help a user who has a physical disability, such as restricted mobility or limited vision, to use software products successfully. With this product, you can use assistive technologies to hear and navigate the interface. You also can use the keyboard instead of the mouse to operate all features of the graphical user interface.

For additional information, see the Accessibility topic in the Release Information section of the information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tspm.doc_70/welcome.htm.

Tivoli technical training

For Tivoli technical training information, refer to the IBM Tivoli Education Web site at <http://www.ibm.com/software/tivoli/education>.

Conventions used in this document

This document uses several conventions for special terms and actions, operating system-dependent commands and paths, and margin graphics.

Typeface conventions

This document uses the following typeface conventions:

Bold

- Lowercase commands and mixed case commands that are otherwise difficult to distinguish from surrounding text

- Interface controls (check boxes, push buttons, radio buttons, spin buttons, fields, folders, icons, list boxes, items inside list boxes, multicolumn lists, containers, menu choices, menu names, tabs, property sheets), labels (such as **Tip:**, and **Operating system considerations:**)
- Keywords and parameters in text

Italic

- Citations (examples: diskettes, and CDs)
- Words defined in text (example: a nonswitched line is called a *point-to-point line*)
- Emphasis of words and letters (words as words example: "Use the word *that* to introduce a restrictive clause."; letters as letters example: "The LUN address must start with the letter *L*.")
- New terms in text (except in a definition list): a *view* is a frame in a workspace that contains data.
- Variables and values you must provide: ... where *myname* represents....

Monospace

- Examples and code examples
- File names, programming keywords, and other elements that are difficult to distinguish from surrounding text
- Message text and prompts addressed to the user
- Text that the user must type
- Values for arguments or command options

Part 1. Tivoli Security Policy Manager Adapter for FileNet: Installation Guide

Chapter 1. Introducing IBM Tivoli Security Policy Manager Adapter for FileNet

This chapter introduces IBM Tivoli Security Policy Manager Adapter for FileNet and describes the components and procedures. This chapter contains the following sections:

- Overview
- Supported platform
- Prerequisite software
- Hardware requirement
- Installable components

Overview

IBM Tivoli Security Policy Manager Adapter for FileNet content entitlement solution uses Tivoli Security policy Manager to author policies and enforce the policies on the Enterprise Content Management solution like FileNet.

In this solution, the application content is hosted on FileNet, and the information model, metadata, and data of the application are imported into Tivoli Security Policy Manager to enable policy authoring in the application domain. This adapter helps author policies using the application semantics, instead of authoring policies in Tivoli Security Policy Manager semantics, such as resources, roles, and services. For example, in a health care application the policies can be authored using health care semantics, such as patients, doctors, and electronic health records.

Supported platform

Operating systems

- Microsoft® Windows® 2003 Server

Prerequisite software

The required software are as follows to implement the solution.

- The software required on the system with IBM Tivoli Security Policy Manager installed:
 - IBM Tivoli Security Policy Manager Version 7.1
 - IBM Installation Manager
 - IBM Tivoli Integrated Portal
- The software required on the system with IBM FileNet installed:
 - IBM FileNet P8 Version 4.5
 - Microsoft .NET Framework 3.5

Hardware requirement

Tivoli Security Policy Manager have its own set of hardware requirement that must be met. For documentation, see the IBM Tivoli Security Policy Manager Information Center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tspm.doc_70/welcome.htm.

FileNet have its own set of hardware requirement that must be met. For product documentation for FileNet P8 Platform, see at <http://www-01.ibm.com/support/docview.wss?rs=3247&uid=swg27010422>.

Installable components

Tivoli Security Policy Manager Adapter for FileNet is packaged as two separate components, and must be installed and configured as follows:

1. The Tivoli Security Policy Manger plug-in. This helps to author the policies, configure the policies, and export the policies.
2. Tivoli Security Policy Manger Adapter for FileNet. This helps to translate the policies to Access Control Lists (ACLs) of FileNet.

Chapter 2. Installation and configuration

Installing and configuring the Tivoli Security Policy Manager Adapter involves several steps that you must complete in an appropriate sequence. Review the prerequisite software before you begin the installation process.

Installation of Tivoli Security Policy Manager Plug-in

The Tivoli Security Policy Manager plug-in is packaged in the TSPM Adapter For FileNet Plugins.zip file. Download or copy the zip file on the system that has the prerequisite software installed for Tivoli Security Policy Manager. Unzip the zip file and extract the contents in the TSPM Adapter for FileNet Plugins folder on the system. After extracting, perform the following steps to install the Tivoli security Policy Manager plug-in:

1. Launch IBM Installation Manager. Do the following before you begin to install the software packages.
 - a. From the File menu, click Preferences.
 - b. On the left navigational pane of the Preferences window, select Repositories and then click Add Repository.
 - c. On the Add Repository window, enter repository.config along with its path name. You can click Browse to specify the repository.config file with path name.

Note: When the TSPM Adapter For FileNet Plugins.zip file is extracted, it contains a folder called output which is the Installation Manager repository. The repository.config file is present in the output folder.

- d. After adding the repository, click OK.

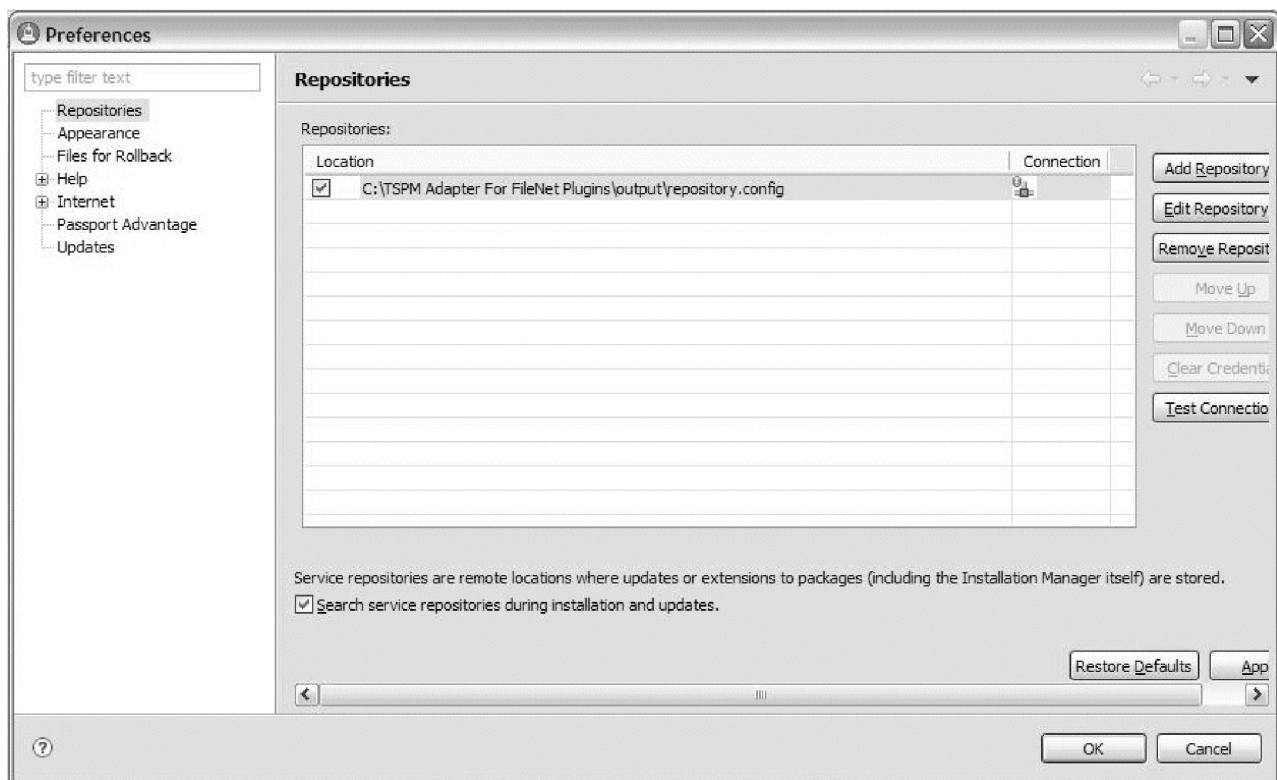


Figure 1. Adding a repository file

2. From the IBM Installation Manager window, click Install.
3. On the Install tab of the Install Packages wizard, select the TSPM Adapter for FileNet and click Next.
4. On the Location tab of the Install Packages wizard, do the following:
 - a. Ensure that Use the existing package group is selected.
 - b. From the Package Group Name section, select TSPM.
 - c. Click Next.
5. On the Features tab of the Install Packages wizard, select the TSPM Adapter for FileNet entry and click Next.
6. Review the information displayed on the Summary tab, and then click Install.
7. After the installation is complete, a confirmation message is displayed indicating that the package is installed. To display the log file, click the View Log File link.

The TSPM Adapter for FileNet package gets installed into the package group once the installation of the Tivoli Security Policy Manager plug-in is complete.

Installation of TSPM Adapter for FileNet

Before you begin with installation, ensure that the system on which you plan to install has all the prerequisite software. To install TSPM Adapter for FileNet, do the following:

1. Double-click TSPM Adapter for FileNet.exe.
2. On the TSPM Adapter for FileNet wizard, select English and then click OK.
3. Review the information displayed on the Introduction panel, and click Next to continue with installation.

4. On the Choose Install Folder panel, specify the folder where you wish to install and click Next.

Note: By default, the field is populated with the "C:\Program Files\IBM\TSPM Adapter For FileNet" folder.

5. Review the information displayed on the Pre-Installation Summary panel, and then click Next.
6. The installer installs the TSPM Adapter for FileNet components.
7. Next, the information about the installed IBM WebSphere must be provided to deploy TSPM Adapter for FileNet on the WebSphere. On the Enter the WebSphere details panel, enter the path where WebSphere is installed, node name, server name, and user credentials in the respective fields. The appserver profile provided must be same as that on which FileNet is installed. Click Next.



Figure 2. Details of WebSphere install location

8. Enter the FileNet P8 content engine details, and click Install.

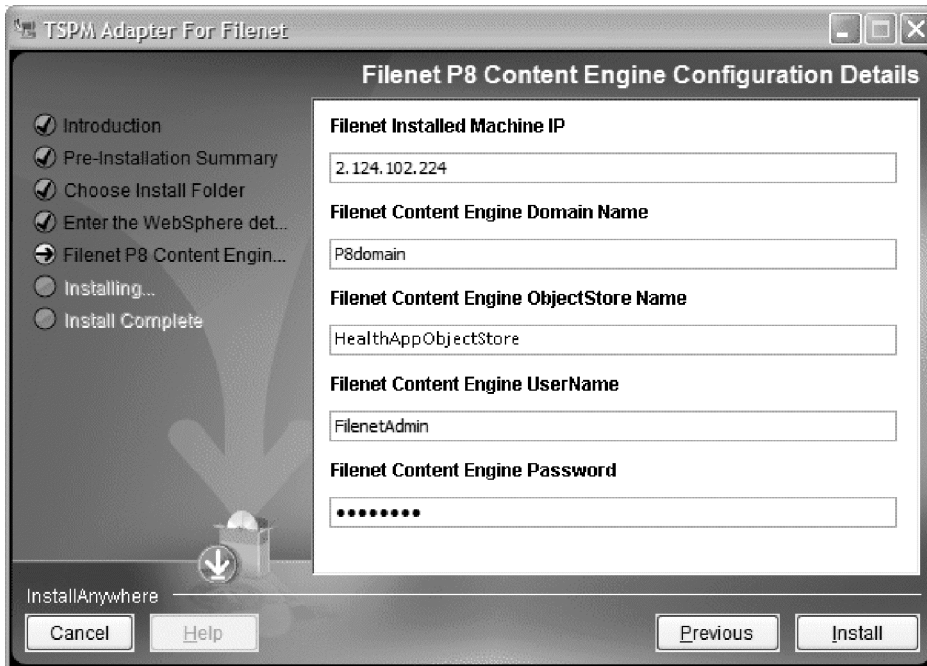


Figure 3. FileNet P8 content engine configuration details

9. On the Install Complete panel, the result of installation is displayed. To exit the installer, click Done.

After the installation, verify that the TSPM Adapter for FileNet is installed successfully by opening the URL in a browser window, for example `https://<hostname>:<port_number>/TSPMAdapterForFileNet/TSPMAdapterMetadataServlet?data=model&applctaion=HealthHighway`. At prompt, provide the FileNet administrator user ID and password.

Part 2. Tivoli Security Policy Manager Adapter for FileNet: User Guide

The Tivoli Security Policy Manager Adapter for FileNet enables user to author content protection policies using Tivoli Security Policy Manager. To author the policies, user must use the semantics of the applications that are hosted on FileNet. FileNet is the content repository that hosts various kinds of applications, whose data-models and metadata information can be used to author policies. The deployment architecture shows the various adapter components and their point of interactions.

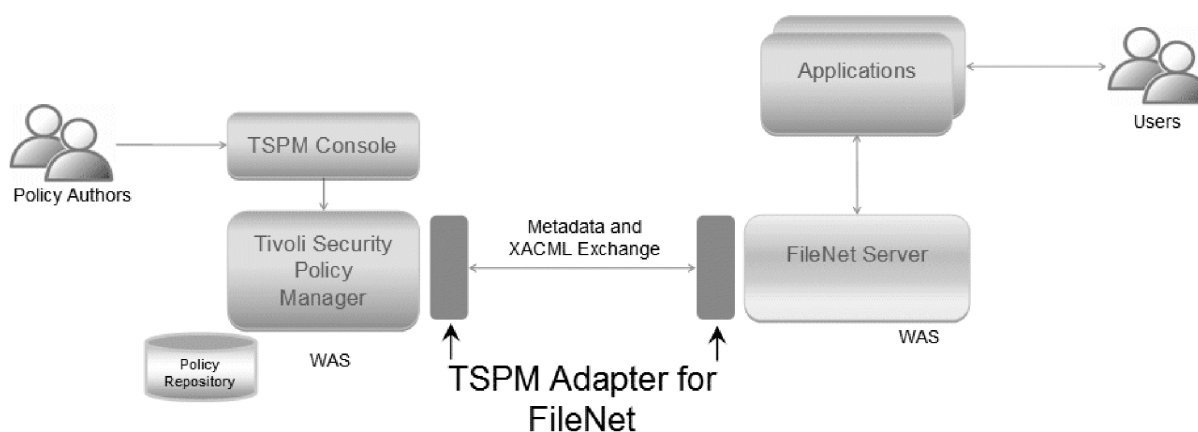


Figure 4. Deployment architecture

The first step towards authoring policies is to provide the adapter with the application models and metadata information.

Chapter 3. Working with Tivoli Security Policy Manager Adapter for FileNet

Policies can be authored for any applications that are hosted on FileNet. The semantics used for authoring are similar to the entities that are defined in the FileNet application. To enable this, the adapter needs to understand the semantics of the application. The basis of this understanding are the model files that are defined for each application hosted on FileNet. The applications on FileNet need to have a model file defined in an XSD file. There are several ways to build an XSD file.

- To write an application model using the sample model files provided as part of the adapter.
- To build a model file from scratch using the Rational® Application Developer (RAD) tool.

Building an application model using sample models

You can write an application model using the sample model files provided along with the adapter. The example application models provided are:

- Health care application model - HealthHighway.xsd
- Bank application model - TrustedBank.xsd

These model files are located in the following location:

```
WAS_HOME\profiles\AppSrv01\installedApps\<deployed cell>\
TSPMFileNetAdapter_war.ear\TSPMFileNetAdapterServlet.war\WEB-INF
```

Users can use these model files as a reference to write their own application models.

Building an application model using RAD

This example describes how to build an application model from scratch using the RAD tool. This application model uses the base FileNet model that is provided as part of the adapter. In this example, a sample bank application model is built that is latter represented in FileNet.

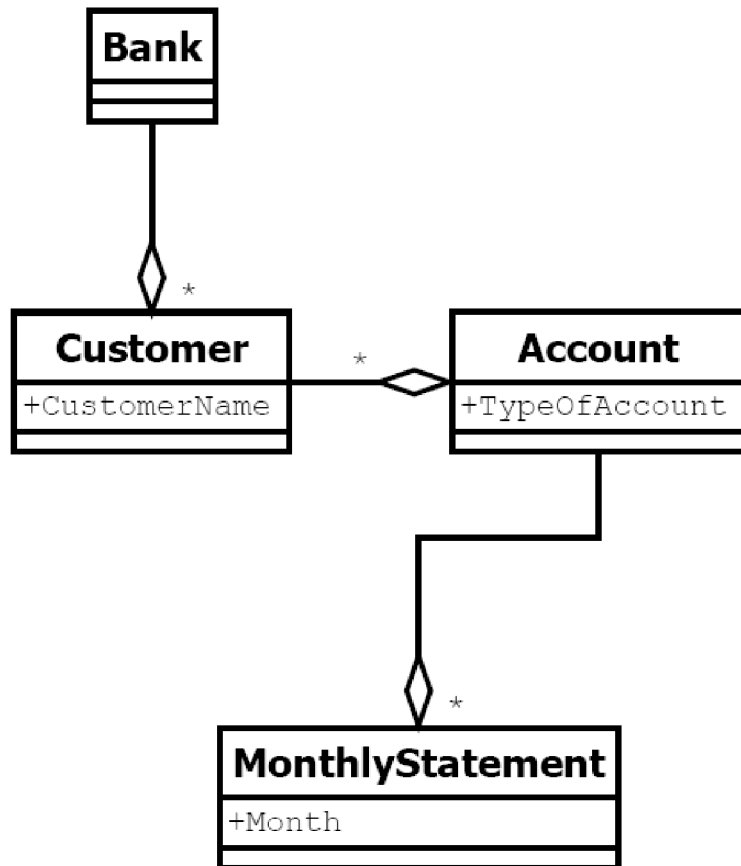


Figure 5. An example: Bank application model

The above figure shows that the Bank has a Customer class which has a property called CustomerName. The Account class has a property called TypeOfAccount, which is of enumeration type, and Account can have many MonthlyStatement class. The MonthlyStatement class has a property called Month. Now, if this application were to be modelled in FileNet the following will be its representation:

- Customer and Account will be classes that extend from Folder
- MonthlyStatement will be a class that extends from Document
- TypeOfAccount will be a choiceList

Using the RAD tool, the bank application model can be built using the following steps:

1. Launch the RAD tool.
2. From the File menu, click New and create a General project.
3. In the Project name field, enter a name. For example, TrustedBank. Click Next.
4. Create an xsd file, and enter a name, TrustedBankModel.xsd, for XML schema file in the File name field. Click Finish.
5. Import the FileNet.xsd file, which is provided along with the TSPM Adapter for FileNet. This file is located in the WAS_HOME\profiles\AppSrv01\installedApps\<deployed cell>\TSPMFileNetAdapter_war.ear\TSPMFileNetAdapterServlet.war\WEB-INF folder.

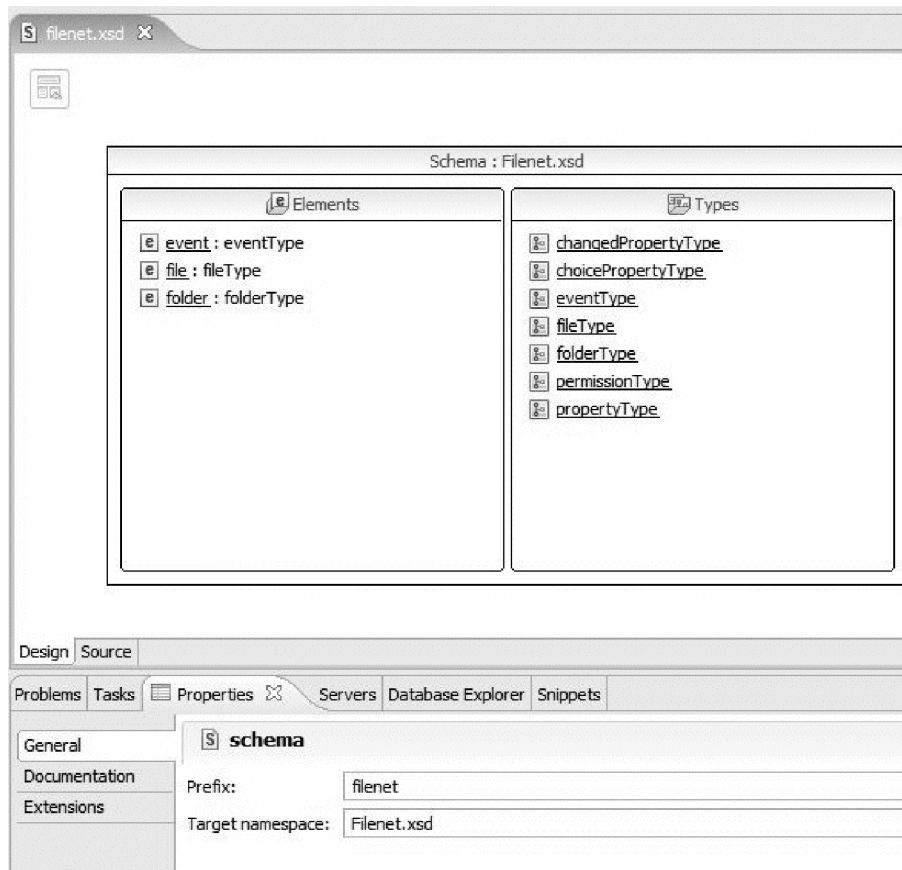


Figure 6. Importing FileNet.xsd file

6. Open the TrustedBankModel.xsd file in the design mode and set the namespace of the xsd to app.
7. To create and map the components of the bank application model, such as Customer, Account, and MonthlyStatement to their corresponding Types in FileNet, do the following:
 - a. Add a new complexType called CustomerType. Inherit this type through extension from filenet:foldertype. When you browse for classes, select the "Enclosing Project" option to include filenet.xsd.
 - b. Change the namespace of FileNet.xsd from the default prefix to "filenet".

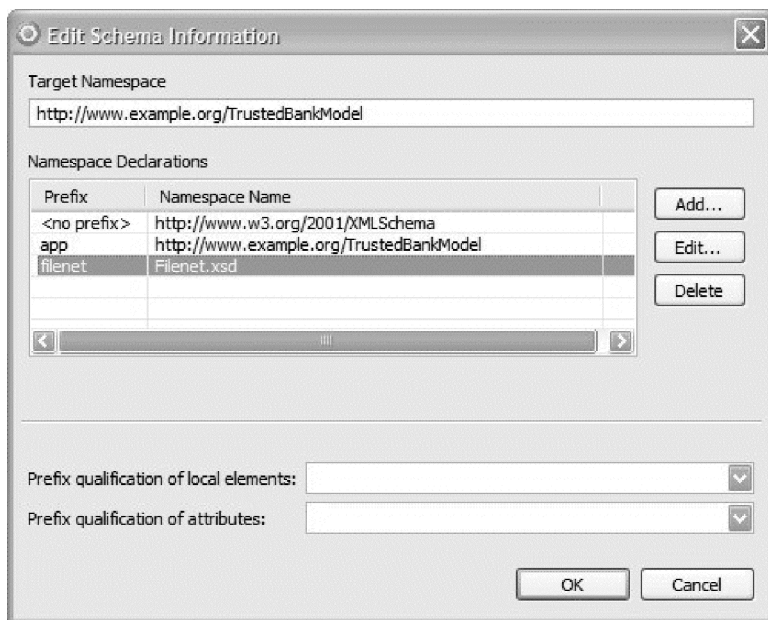


Figure 7. Setting namespace to filenet

- c. Create a new complexType called AccountType. Inherit this type through extension from filenet:foldertype.
- d. Create a new complexType called MonthlyStatementType and set the extension base to filenet:filetype.

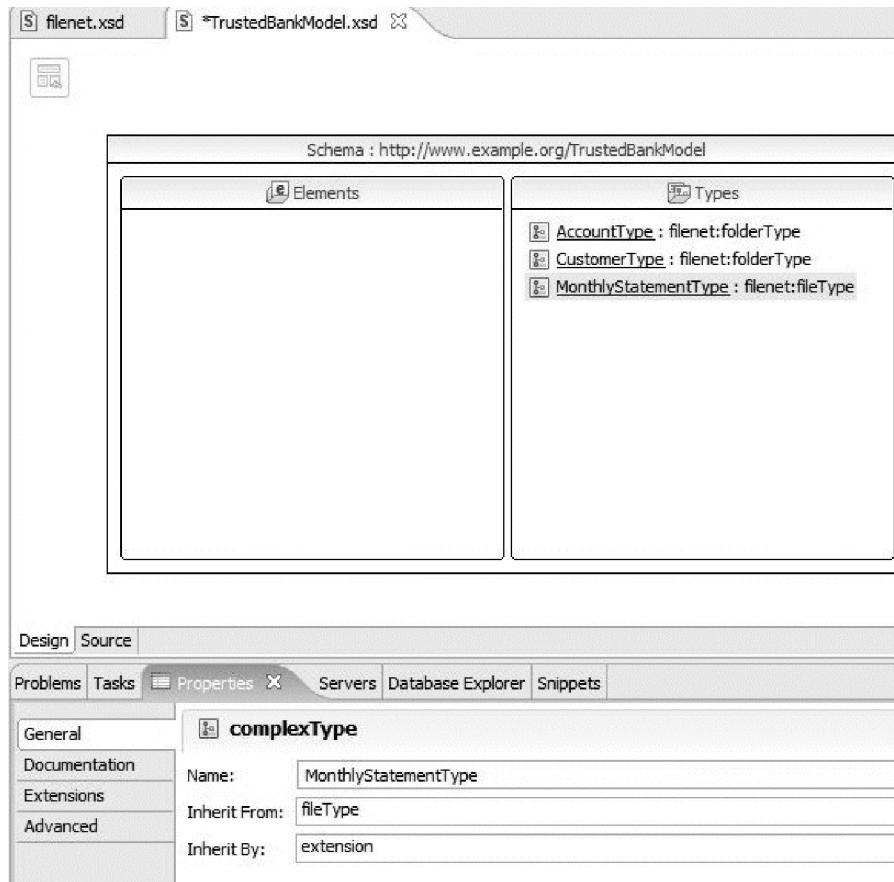


Figure 8. Defining the types for TrustedBankModel

8. Next, add elements for the Types defined.
 - a. Add an element to CustomerType called CustomerName and set the element's type to filenet:PropertyType.
 - b. Add an element to CustomerType called Accounts and set the element's type to app:AccountType. Set the maximum occurrence as "unbounded".
 - c. Add an element to AccountType called TypeOfAccount and set the element's type to filenet:choicePropertyType.
 - d. Add an element to AccountType called MonthlyStatement and set the element's type to app: MonthlyStatementType. Set the maximum occurrence as "unbounded".
 - e. Add an element to MonthlyStatementType called Month and set the element's type to filenet:choicePropertyType.

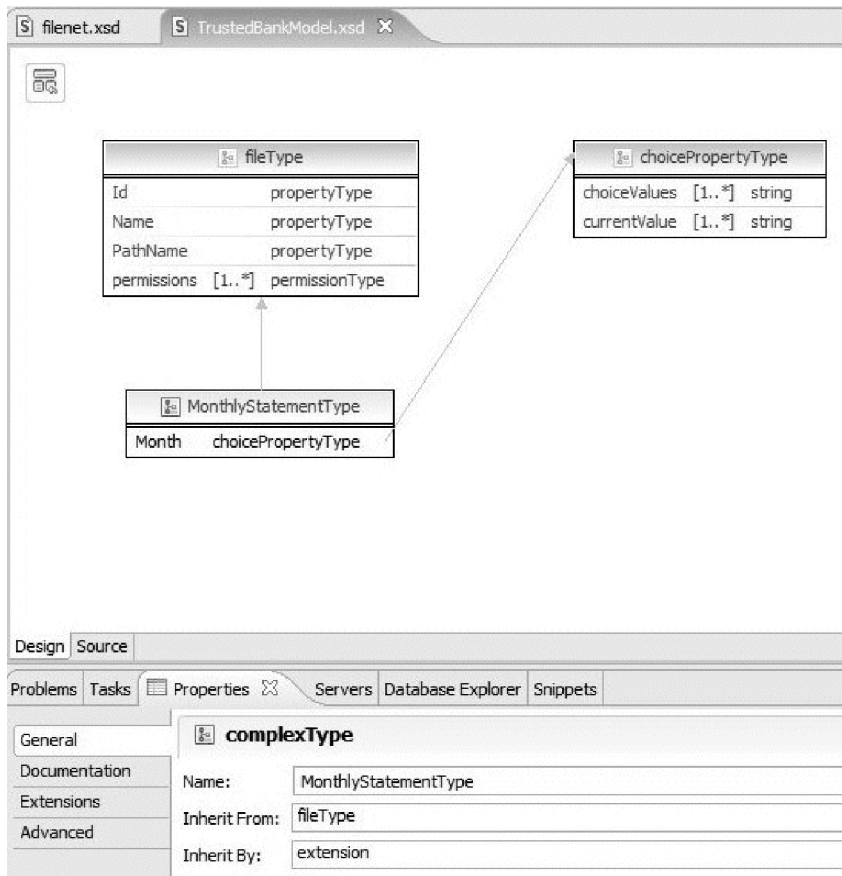


Figure 9. Adding an element to `MonthlyStatementType`

9. To create a bank application model and to represent it in FileNet, do the following:
 - a. Add a new complexType called `BankType`. Inherit this through extension from `filenet:foldertype`.
 - b. Add an element to `BankType` called `Customer` and set the element's type to `app:CustomerType`. Make the maximum occurrence as "unbounded".

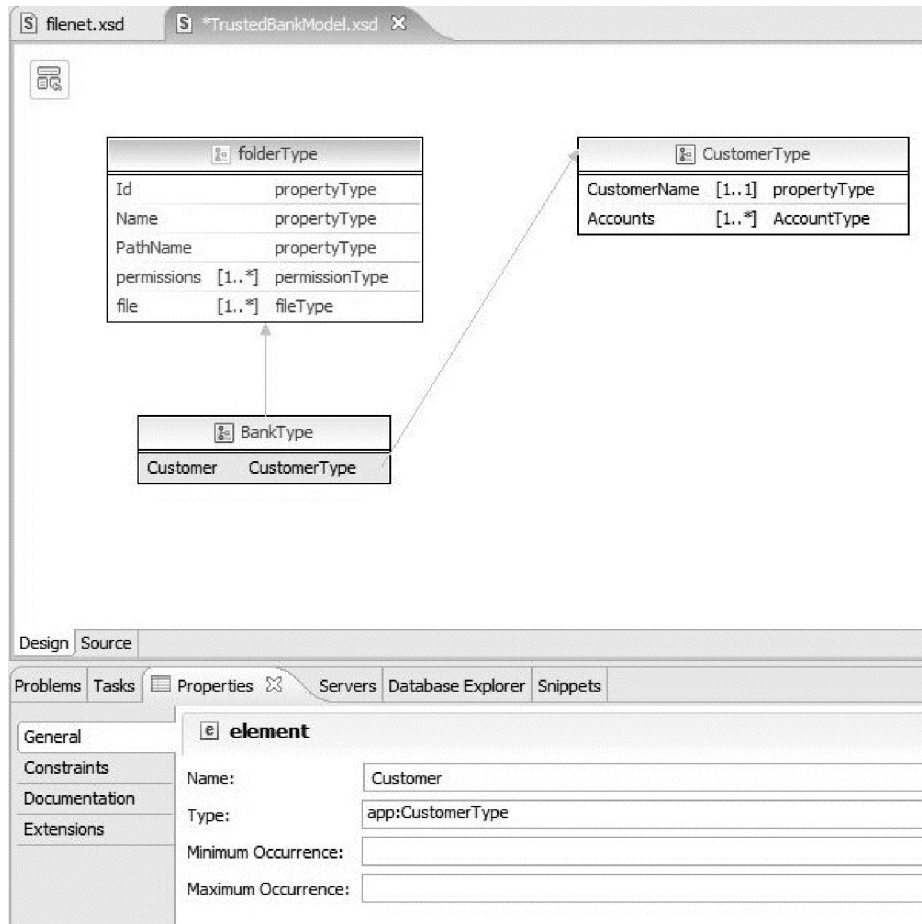


Figure 10. Adding an element to BankType

Bank is the top of the hierarchy class that defines the banking application model. The complex types are all defined.

10. Now, to add the elements to the model, do the following:
 - a. Add an element called Bank, and set its type to BankType.
 - b. Add an element called Account, and set its type to AccountType.
 - c. Add an element called Customer, and set its type to CustomerType.
 - d. Add an element called MonthlyStatement, and set its type to MonthlyStatementType.

This completes the bank application model.

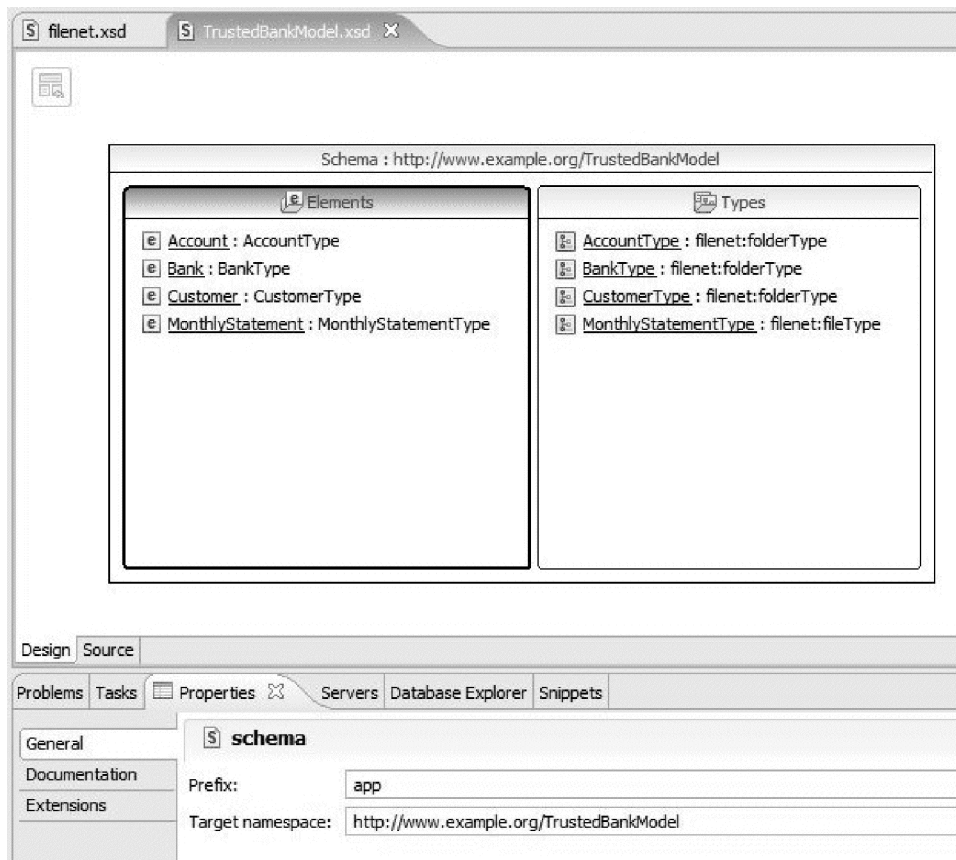


Figure 11. Representation of TrustedBankModel based on bank application model

Make the bank element the topmost element in the model file followed by other elements. The complexType definitions follow the element definitions. After building the models, update the configuration file with the top level Application class to include them in the adapter framework. The configuration file is located in WAS_HOME\profiles\AppSrv01\installedApps\<deployed cell>\TSPMFileNetAdapter_war.ear\TSPMFileNetAdapterServlet.war\WEB-INF\metadata.properties. A sample XML schema file of the TrustedBankModel.xsd is as follows:

```
<?xml version="1.0" encoding="UTF-8"?>
<schema targetNamespace="http://www.example.org/TrustedBankModel"
  xmlns="http://www.w3.org/2001/XMLSchema"
  xmlns:app="http://www.example.org/TrustedBankModel"
  xmlns:filenet="FileNet.xsd">
  <import schemaLocation="filenet.xsd" namespace="FileNet.xsd"></import>
  <element name="Bank" type="app:BankType"></element>
  <element name="Account" type="app:AccountType"></element>
  <element name="Customer" type="app:CustomerType"></element>
  <element name="MonthlyStatement" type="app:MonthlyStatementType"></element>
  <complexType name="CustomerType">
    <complexContent>
      <extension base="filenet:folderType">
        <sequence>
          <element name="CustomerName"
            type="filenet:propertyType" minOccurs="1">
          </element>
          <element name="Accounts" type="app:AccountType"
            maxOccurs="unbounded">
          </element>
        </sequence>
      </extension>
    </complexContent>
  </complexType>
</schema>
```

```

</complexContent>
</complexType>

<complexType name="AccountType">
  <complexContent>
    <extension base="filenet:folderType">
      <sequence>
        <element name="TypeOfAccount"
          type="filenet:choicePropertyType">
        </element>
        <element name="MonthlyStatements"
          type="app:MonthlyStatementType" maxOccurs="unbounded">
        </element>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<complexType name="MonthlyStatementType">
  <complexContent>
    <extension base="filenet:fileType">
      <sequence>
        <element name="Month"
          type="filenet:choicePropertyType">
        </element>
      </sequence>
    </extension>
  </complexContent>
</complexType>

<complexType name="BankType">
  <complexContent>
    <extension base="filenet:folderType">
      <sequence>
        <element name="Customer" type="app:CustomerType"></element>
      </sequence>
    </extension>
  </complexContent>
</complexType>

</schema>

```

Creating a sample content in FileNet

An example application, HealthHighwayApp sample content is provided as part of the installer. To load the sample content in FileNet, perform the following steps:

1. Edit the sample.property file provided in the samples subdirectory in the TSPM Adapter for FileNet directory. Modify the sample values for the following properties:

```

FILENET_USER#administrator
FILENET_PASSWORD#admin123
FILENET_SERVER#http://2.124.160.122:9080/wsi/FNCEWS40DIME/
OBJECTSTORE#HHStore
WASP_LOCATION#C:\\Program Files\\FileNet\\ContentEngine\\wsi

```

2. Edit the sample.bat file for the environment variables, WS_PLUGIN1 and WS_PLUGIN2, to specify your WebSphere installation folders. An example:

```

set WS_PLUGIN1="C:/Program Files/IBM/WebSphere/AppServer/plugins"
set WS_PLUGIN2="C:/Program Files/IBM/WebSphere/AppServer/deploytool/itp/plugins"

```

These folders contain the necessary jar files to load the samples. If the jar files in your installation are named with a different version number, then change the lines appropriately.

```

set CLASSPATH=%CLASSPATH%;%WS_PLUGIN1%/org.eclipse.emf.ecore_2.2.1.v200609210005.jar
set CLASSPATH=%CLASSPATH%;%WS_PLUGIN1%/org.eclipse.emf.common_2.2.1.v200609210005.jar
set CLASSPATH=%CLASSPATH%;%WS_PLUGIN2%/org.eclipse.xsd_2.2.2.v200702131851.jar

```

3. Run the sample.bat file to load FileNet with sample content.
4. Run the FileNet Enterprise Manager tool to create the values for the various Choice Lists that are created as part of the samples.
5. On the left navigational panel, click Choice Lists under Object Stores, and then double-click PatientState.

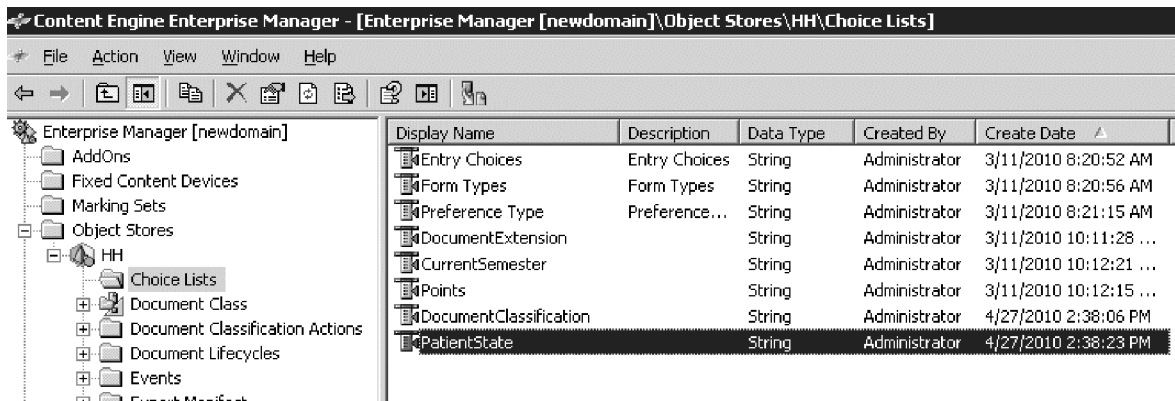


Figure 12. Objects under Choice Lists

6. Click the Choice Items tab, enter the various choice items for this choice list.

Impact of FileNet metadata size on transactions

The time taken to translate a policy based on a property change in the FileNet server is dependent on the content that is hosted in FileNet. The content size determines the size of the metadata file that is imported into the adapter to search for the set of folders and documents on which the policy is applied.

Enforcing policy

ACLs are created using the standard FileNet process of creating and updating ACLs. When a new set of policy is distributed from Tivoli Security Policy Manager, the FileNet ACLs corresponding to the earlier XACML are removed. A fresh set of ACLs are created using the batch mode update, and any ACLs that were manually created earlier are removed. The XACML obtained from Tivoli Security Policy Manager is the single source of reference for all ACLs that are present in FileNet. Additionally, the Adapter does not alter the ACL access precedence.

Enforcing policy when switching between application

To a enforce policy on application, when switching between applications run TSPM Adapter For FileNet.exe, and provide the new Objectstore name in the FileNet P8 Content Engine Configuration Details panel.

Chapter 4. Configuring Tivoli Security Policy Manager for policy authoring

Configuring security roles for accessing Tivoli Security Policy Manager Adapter for FileNet

The following steps must be followed to configure security roles from the WebSphere Application Server console on which the adapter is deployed.

1. Open the WebSphere Application Server console.
2. Navigate to Applications -> Enterprise Applications -> TSPMFileNetAdapter.
3. Select the Security role to user/group mapping.
4. Map the security roles based on the requirement, and then click OK. As an example, a sample window depicting the security role mapping is displayed.

Enterprise Applications > ConSecureConnectionServlet_war > Security role to user/group mapping

Security role to user/group mapping

Each role that is defined in the application or module must map to a user or group from the domain user registry.

Look up users Look up groups					
 					
Select	Role	Everyone?	All authenticated?	Mapped users	Mapped groups
☐	All Authenticated	☐	☒		

Figure 13. An example showing security role mapping

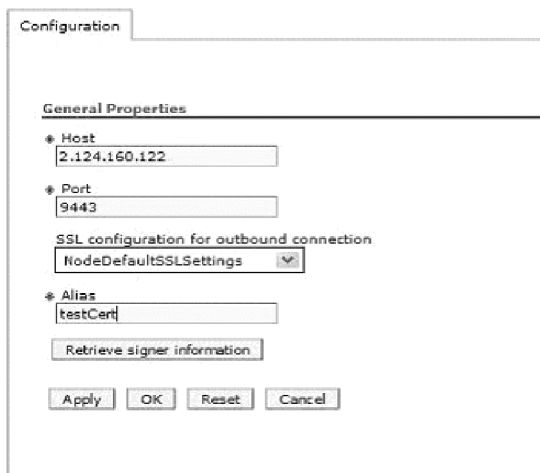
5. Save the changes made and restart WebSphere Application Server.

Exporting security certificates from FileNet to Tivoli Security Policy Manager

Tivoli Security Policy Manager Adapter for FileNet runs on a secure channel. Tivoli Security Policy Manager should first have the security certificate to access the adapter. The following steps must be followed to get the security certificate for Tivoli Security Policy Manager from the FileNet server.

1. From the WebSphere Application Server console navigate to Security -> SSL certificate and key management.
2. Select Manage endpoint security configurations.
3. Select the Node from the outbound section of the Local Topology.
4. Click Keystores and certificates. It will display all the available keystores and truststores.
5. Select the default node TrustStore.
6. Click signer certificates. This will display all the available certificates.
7. Click the Retrieve from port button.

8. In the Configuration general properties tab, enter the hostname and port number of the server from which to retrieve the signer certificate in the respective fields.
9. Select the NodeDefaultSSLSettings item from the SSL configuration for outbound connection list.
10. Enter an alias name in the Alias field.



Configuration

General Properties

* Host
2.124.160.122

* Port
9443

SSL configuration for outbound connection
NodeDefaultSSLSettings

* Alias
testCert

Retrieve signer information

Apply OK Reset Cancel

Figure 14. Obtaining SSL certificate

11. Click Retrieve signer information. This will retrieve the signer certificate from the specified host.
12. Save the signer certificate.
13. Repeat the steps to import the digital certificate into the TIP console.

Creating a service registry

A service registry must be created on Tivoli Security Policy Manager to connect to the adapter on the FileNet WebSphere instance. For this, do the following:

1. On the left navigational panel, click Service Registries.
2. Click Add.



Figure 15. Adding service registry

3. From the Registry type list, select IBM FileNet Service Registry.
4. On the Add Service Registry window, enter the following:
 - In the Name field, enter a name for the service registry.
 - In the Description field, enter an appropriate description for the service registry. This is optional.
 - In the FileNet P8 http URL field, enter the connection URL to the adapter running on the FileNet WebSphere instance.

Note: The adapter runs on a standard HTTPS protocol.

- Enter the user ID and password of the FileNet server administrator. Tivoli Security Policy Manager uses 64-bit encoding techniques to encode the username and password in the request object before sending it to the adapter.

Figure 16. Specifying service registry details

- To create service registry, click Finish.

Note: When the FileNet administrator user ID or password changes, this service registry must be edited and the new data entered must be saved.

Creating a policy distribution point

1. On the left navigational pane, click Policy Distribution Targets.
2. Click Add.
3. From the list, select IBM FileNet.
4. Enter a name in the Policy Distribution Target name field, and then click Next.

Figure 17. Selecting the type and providing target name

5. Enter URL to access the FileNet adapter, and then click Next. An example URL address: `https://<ipaddress>:9443/TSPMAdapterForFileNet/TSPMAdapterConnectorServlet`.
6. Click Finish

Importing application model and metadata

Tivoli Security Policy Manager import service provides the mechanism to discover the available applications on the FileNet server. This mechanism provides user with all the information about the available applications, so that the user can select the required application.

To import application model and metadata, do the following:

1. On the left navigational pane, select Services.
2. Click the Import services icon on the toolbar.

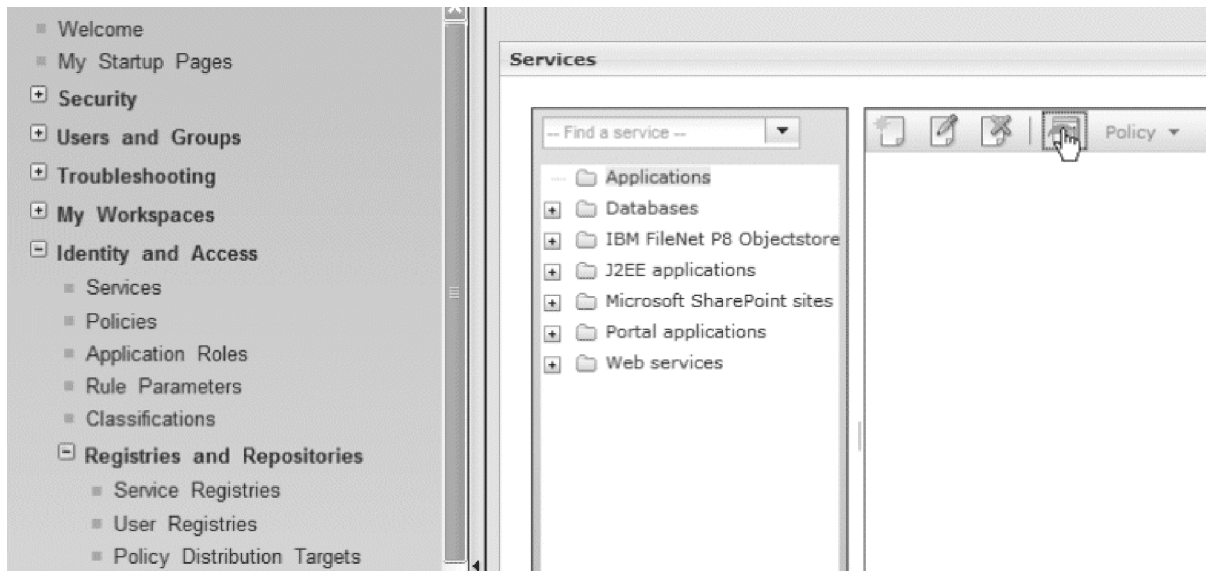


Figure 18. Importing application and services

3. Click Services from service registry as the service type.
4. Select Secure FileNet Registry as the service source.
5. If the user does not have any information about the available applications, do the following:
 - a. In the Enter the application name field, enter asterisks (*).
 - b. Click the Get Services button. All the available applications on FileNet gets discovered and gets populated in the Select the Application list.
 - c. From the Select the Application list, select the required service.

After selecting the required service, user can import the model and metadata into Tivoli Security Policy Manager. An example illustration of existing HealthHighwayApp application model on FileNet is displayed.

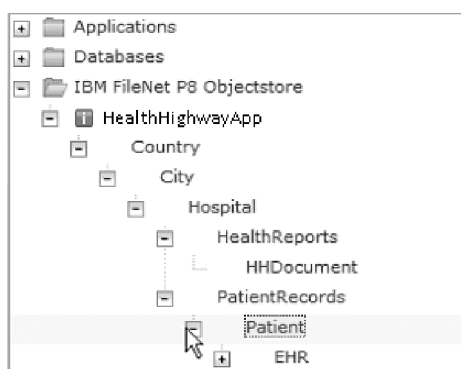


Figure 19. An example of existing application models and metadata

Authoring a policy

Authoring a policy using the application semantics involves the following:

- Identifying resources
- Creating user roles
- Creating conditions

Identifying resources

Resources are identified using the resource widgets that help in narrowing down the search to locate the required resources matching a given criteria. The Resource selection widget helps to narrow down the resource selection.

Resource :

Entity:	Property:	Relation:	Value:	+	-
City	Name	=	Bangalore		

[Select a resource](#)

Figure 20. Identifying the required resource

The Resource identification widget is available at both the policy level and rule level. When no resources are selected, user can use the link "Select a resource" in the Resource identification widget. To retrieve a required resource, do the following:

1. Click the Select a resource link.
2. In the widget window, do the following:
 - a. From the Entity list, select the required resource entity.
 - b. From the Property list, select a property associated with the entity.
 - c. From the Relation list, select the required relational operator.
 - d. From the Value list, specify the value of the property based on which the result is to be displayed.
 - e. To further narrow down the search result by adding more level of resource identification, click the + button.

Note: To remove the latest level of resource identification, click the - button.

Resource :

Entity:	Property:	Relation:	Value:		
City	Name	=	Bangalore		
Hospital	Name	=	Marthas Hos	+	-

[Select a resource](#)

Figure 21. Narrowing down the search for resource

Users can add multiple resources at policy level while only one resource at rule level. Before adding a new resource, user should select the parent service (topmost) and save the policy. This is because only the first combo box will get populated with the child elements of the service selected. Otherwise, the combo box will be empty if this is the first level in resource identification.

If a resource is selected as shown in the figure, the Xpath for the resource will be `//hh:HealthHighway//hh:City[Name/currentValue="Bangalore"]/hh:Hospital[Name/currentValue="Marthas Hospital"]`.

Creating user roles

Create user roles for a particular policy and assign them the required permissions. The users will be mapped to the users defined in the LDAP registry during the policy configuration stage.

Setting conditions

Additional conditions can be added to the policy, if required. These conditions can be:

- Restriction on resource
- Environment conditions (criteria such as specific date and time when the policy should be enforced, and so on)

Authoring a sample policy

In this section, authoring of a sample policy is described. The sample policy is defined in the following way: "Auditors will have access to the hospital billing records on the 3rd of every month". To author this policy, do the following:

1. On the Policies tab, click the Add new policy icon.

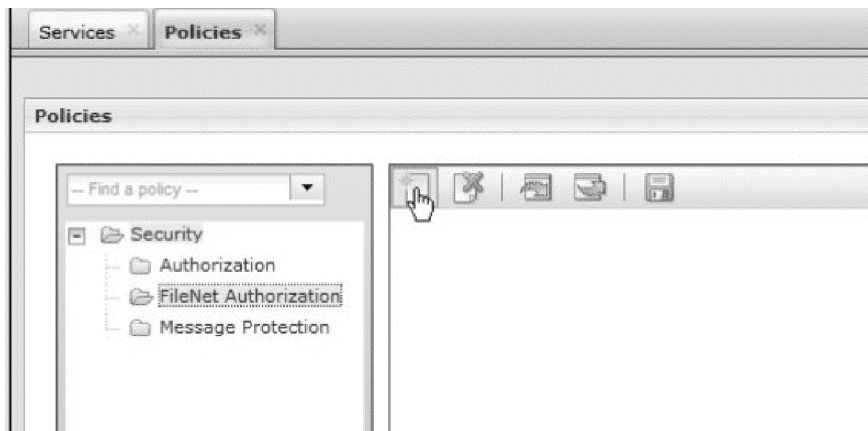


Figure 22. Adding a new policy

2. From the Select policy type window, select FileNet Authorization, and then click Next.
3. On the Policy Information panel, enter a name and description for the policy.
4. On the Application Roles tab, select Create a new role from the list and specify a role, Auditors, and click Create.
5. From the Select Services panel, click Add and then select HealthHighwayApp as the service.
6. Click OK to save the policy.
7. Click the Select a resource link.
8. From the Resource selection widget, select the resource based on your required criteria. For example:
 - From the Entity list, select BillingRecords.
 - From the Property list, select Name.
 - From the Relation list, select equal to (=).
 - From the Value list, select asterisks (*).

An example policy that will allow auditors to access all BillingRecords have been created.

9. Now, you need to add a rule, which gives the auditors access to the records on 3rd of every month.
Click the Add a rule link.

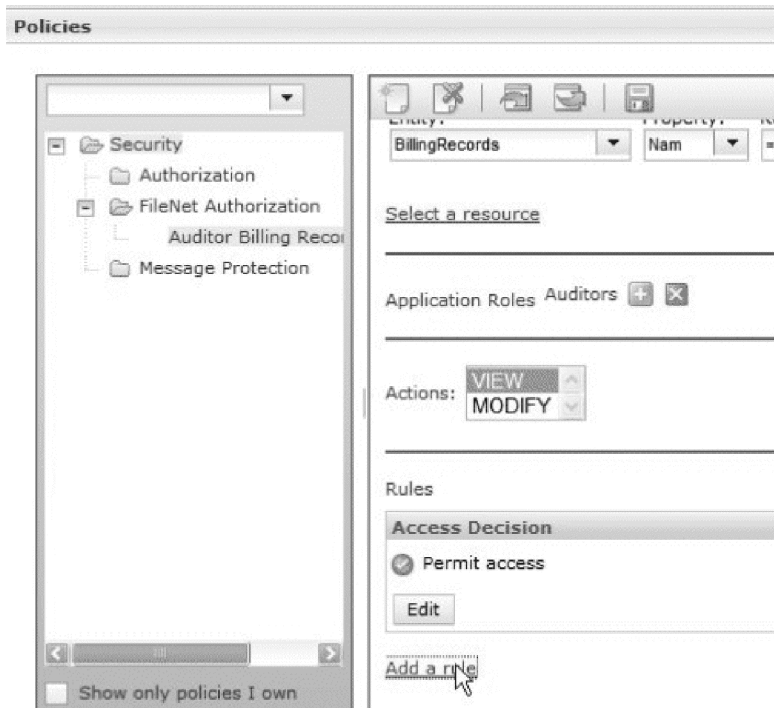


Figure 23. Creating and adding rule to provide auditors the required access

10. From the Time selection widget, specify the start date and time, occurrence, and end date and time. For example:
 - Specify the start time for the policy to be enforced along with the time zone.
 - Specify the start date and end date.
 - Specify the repetition interval.
 - Select Permit access from the list.

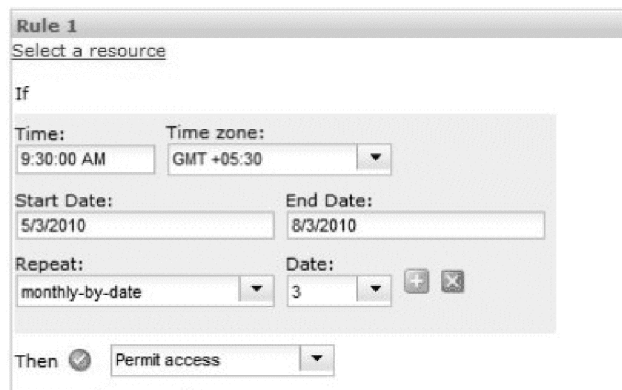


Figure 24. Granting access

The administrator can also create a policy to revoke access to auditors. This access is revoke by creating another rule. For example:

- Specify the start time for the policy to be revoked along with the time zone.
- Specify the start date and end date.
- Specify the repetition interval.
- Select Deny access from the list.

This means auditors will have access to the resource from the 3rd to 4th of every month.

Configuring a policy

After authoring a policy, the policy then needs to be configured. This involves mapping of the following:

- User roles
- Rule parameter

To configure a policy, do the following:

1. From the Policy menu on the Services tab, click Configure Policy.

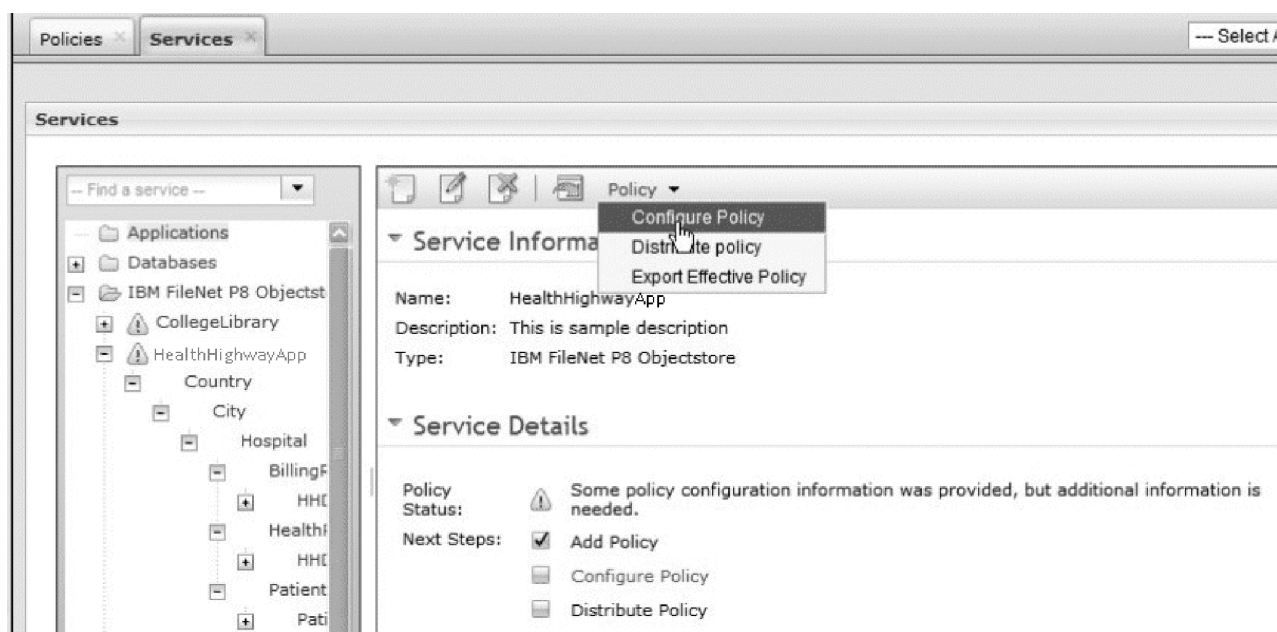


Figure 25. Configuring a policy

2. Select the required policy distribution target from the Available Policy Distribution Targets list and click Add.
3. Click Next.
4. On the Configure Policy window, select FileNet Authorization and then click Configure.
5. Now to create users in Active Directory, do the following:
 - a. Open the Active Directory console, and click Add group.
 - b. Enter the details for the group. For example, Auditors.
 - c. Click Add user.
 - d. Enter the details for the user and add the user as a member of the group, Auditors, that was previously created.
6. Now to map user roles, select Auditors in the Application Roles section and then click Update Mapping.

7. From the User registry list, select the required user registry and click OK.
8. In the appropriate fields, specify the Base DN, search query, and attribute to be displayed, and then click Search.

Configure Policy

Policy Configuration

To map an application role to a group, first select the user registry that contains the group "Search." Select the group that represents the application role from the search results list,

Application Role: Auditors

Group Search

User Registry:

FileNet Service Registry_dev

*Base DN

CN=Users,DC=p8demo1dom,DC=filenet,DC=local

*Search Query

objectClass=*

*Display Attribute

cn

Search

OK Cancel

Figure 26. Mapping an application role to a group

9. From the returned result, select the Auditors group from your LDAP, and click OK.
10. To map rule parameters, select date from the table under the Rule parameters section, and then click Update Mapping.
11. Select the Rule Parameter is contained in the request, in a standard location option, and then select the environment item from the list.
12. Repeat the steps for all the other rule parameters and click Done.

Distributing a policy

After configuring the policy, it needs to be distributed to the adapter running on the FileNet server. For this, do the following:

1. On the Services tab, click Policy and then click Distribute policy.
2. Select the Distribute the latest effective policy option, view the policy and then click OK.

Service name: HealthHighway

Policies:

 Auditor Billing Records Policy

 For any authorization policy conflicts that may occur, a policy's decision of "deny" will be us

Distribute the current or a previous effective policy version:

- ☒ Distribute the latest effective policy
☐ Distribute a previously distributed effective policy

 **View Policy**

Policy will be distributed to:

Policy will be distributed to:		
Policy Distribution Target ^	Operation ^	Policy Types Distributed ^
Secure FileNet PDT	Distribute policy	FileNet Authorization
Page 1 of 1	Total: 1	Filtered: 1 Displayed: 1

Figure 27. Distributing the policy

Troubleshooting

When configuring the policy and distributing it, you might come across some issues. Some of the issues that user might come across are:

ACLs not getting created or updated consistently

There could be various reasons for ACLs not getting created or updated. Some of the reasons that user can consider when troubleshooting are as follows:

- Ensure that the event generation feature in FileNet is not disabled.
- Ensure that the event-handlers are installed and configured.
- Ensure that the FileNet administrator user ID and password are correctly entered during the Tivoli Security Policy Manager Service Registry creation stage.

If the password has changed, run the Update to reflect the changes in Tivoli Security Policy Manager Service Registry.

In addition to above, check the log messages. If there are errors indicating that the event queue is full, then increase the size of the event queue by modifying the **EventQueue.size** property in the file called **TSPMFileNetAdapter.properties**. This file is located in `WAS_HOME\profiles\AppSrv01\TSPM_Adapter_for_FileNet`. Restart the WebSphere application server after making the change to effect the changes made.

Problem in accessing a resource as per a policy

Tivoli Security Policy Manager Adapter for FileNet does not resolve policy conflicts. It is possible that during batch mode enforcement, an object gets an ACL due to Policy A, and later the same ACL might be removed due to Policy B. If such changes occur, appropriate warning messages will be logged in the associated log file.

A time based policy that should get enforced at 9 AM every Wednesday and revoked at 9 PM on the same day have not got enforced, though the policy was distributed 10 AM

Time based policies are enforced and revoked based on time events. Since the policy was not distributed before 9 AM on Wednesday, this policy gets enforced when the criteria is met (on next occurrence of Wednesday 9 AM).

Problem with application getting listed in the Service Registry import screen

All available application need to be entered in the **metadata.properties** file located in WAS_HOME\profiles\AppSrv01\installedApps\<deployed cell>\TSPMFileNetAdapter_war.ear\TSPMFileNetAdapterServlet.war\WEB-INF. Ensure that at the top level within the object store, a folder with the same application name should exist.

Appendix. Notices

This information was developed for products and services offered in the U.S.A. IBM might not offer the products, services, or features discussed in this document in other countries. Consult your local IBM representative for information on the products and services currently available in your area. Any reference to an IBM product, program, or service is not intended to state or imply that only that IBM product, program, or service may be used. Any functionally equivalent product, program, or service that does not infringe any IBM intellectual property right may be used instead. However, it is the user's responsibility to evaluate and verify the operation of any non-IBM product, program, or service.

IBM may have patents or pending patent applications covering subject matter described in this document. The furnishing of this document does not give you any license to these patents. You can send license inquiries, in writing, to:

IBM Director of Licensing
IBM Corporation
North Castle Drive
Armonk, NY 10504-1785
U.S.A.

For license inquiries regarding double-byte (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

IBM World Trade Asia Corporation Licensing
2-31 Roppongi 3-chome, Minato-ku
Tokyo 106, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:

INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the information. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this information at any time without notice.

Any references in this information to non-IBM Web sites are provided for convenience only and do not in any manner serve as an endorsement of those Web sites. The materials at those Web sites are not part of the materials for this IBM product and use of those Web sites is at your own risk.

IBM may use or distribute any of the information you supply in any way it believes appropriate without incurring any obligation to you.

Licensees of this program who wish to have information about it for the purpose of enabling: (i) the exchange of information between independently created programs and other programs (including this one) and (ii) the mutual use of the information which has been exchanged, should contact:

IBM Corporation
Department MU5A46
11301 Burnet Road
Austin, TX 78758
U.S.A.

Such information may be available, subject to appropriate terms and conditions, including in some cases, payment of a fee.

The licensed program described in this document and all licensed material available for it are provided by IBM under terms of the IBM Customer Agreement, IBM International Program License Agreement, or any equivalent agreement between us.

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some measurement may have been estimated through extrapolation. Actual results may vary. Users of this document should verify the applicable data for their specific environment.

Information concerning non-IBM products was obtained from the suppliers of those products, their published announcements or other publicly available sources. IBM has not tested those products and cannot confirm the accuracy of performance, compatibility or any other claims related to non-IBM products. Questions on the capabilities of non-IBM products should be addressed to the suppliers of those products.

This information contains examples of data and reports used in daily business operations. To illustrate them as completely as possible, the examples include the names of individuals, companies, brands, and products. All of these names are fictitious and any similarity to the names and addresses used by an actual business enterprise is entirely coincidental.

If you are viewing this information softcopy, the photographs and color illustrations may not appear.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corporation in the United States, other countries, or both. If these and other IBM trademarked terms are marked on their first occurrence in this information with a trademark symbol ([®] or [™]), these symbols indicate U.S. registered or common law trademarks owned by IBM at the time this information was published. Such trademarks may also be registered or common law trademarks in other countries. A current list of IBM trademarks is available on the Web at "Copyright and trademark information" at www.ibm.com/legal/copytrade.shtml.

Adobe[®], the Adobe logo, PostScript[®], and the PostScript logo are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, and/or other countries.

Intel[®], Intel logo, Intel Inside[®], Intel Inside logo, Intel Centrino[®], Intel Centrino logo, Celeron[®], Intel Xeon[®], Intel SpeedStep[®], Itanium[®], and Pentium[®] are trademarks or registered trademarks of Intel Corporation or its subsidiaries in the United States and other countries.

Java[™] and all Java-based trademarks are trademarks of Sun Microsystems, Inc. in the United States, other countries, or both.

Linux[®] is a trademark of Linus Torvalds in the United States, other countries, or both.

Microsoft, Windows, Windows NT[®], and the Windows logo are trademarks of Microsoft Corporation in the United States, other countries, or both.

UNIX[®] is a registered trademark of The Open Group in the United States and other countries.

Other company, product, and service names may be trademarks or service marks of others.



Printed in USA