

Security Access Manager
for Versions 6.1, 6.1.1, and 7.0

*Using Kerberos for Microsoft Windows
Authentication Foundation Guide*



Security Access Manager
for Versions 6.1, 6.1.1, and 7.0

*Using Kerberos for Microsoft Windows
Authentication Foundation Guide*



Note

Before using this information and the product it supports, read the information in “Notices” on page 29

This edition applies to Version 1.1 release i of the IBM Security Access Manager Integration with Kerberos for Windows Authentication and to all subsequent releases and modifications until otherwise indicated in new editions.

© **Copyright IBM Corporation 2004, 2013.**

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

Contents

Preface	v
About this publication	v
Access to publications and terminology	v
Publication Library	v
IBM Terminology website.	vi
Accessibility	vi
Technical training	vi
Support information	vi
Statement of Good Security Practices.	vii
Product name updates	vii
 Chapter 1. Introducing the integration	 1
Introduction	1
Integration product version information	2
Network connectivity considerations	3
 Chapter 2. Integration process	 5
Before you start	5
Time synchronization	5
User account ID synchronization or mapping	5
Configuration on the domain controller	6
IBM Tivoli Federated Identity Manager service account	6
Configuration on the IBM Tivoli Federated Identity Manager server	9
IBM Tivoli Federated Identity Manager service account user configuration.	9
Configure the WebSphere Application Server service	12
Create a trust chain.	15
Configuration on the IBM Security Access Manager server	22
 Chapter 3. Troubleshooting	 27
 Notices	 29
Trademarks	31

Preface

About this publication

This guide provides instructions on how to configure and manage your Active Directory, IBM Security Access Manager, (previously known as IBM Tivoli Access Manager), and Tivoli Federated Identity Manager installations to enable single sign-on using Kerberos tokens.

This document assumes that Active Directory is present and both IBM® Security Access Manager and IBM Tivoli® Federated Identity Manager are installed, configured and running on your network. It does not provide details on the installation and administration of these products, except where necessary to achieve integration.

This guide is for those responsible for the installation, deployment, and administration of IBM Security Access Manager, IBM Security Access Manager WebSEAL, and Kerberos.

Readers must be familiar with the following:

- Microsoft Windows and UNIX operating systems,
- Security management,
- Lightweight Directory Access Protocol (LDAP) and directory services,
- Supported user registries,
- Authentication and authorization.

Access to publications and terminology

The following publications complement the information contained in this document:

Publication Library

These publications complement the information that is contained in this publication:

Base Information

- *IBM Security Access Manager Base Installation Guide*
Explains how to install, configure, and upgrade Access Manager software, including the Web portal manager interface.
- *IBM Security Access Manager Base Administrator's Guide*
Describes the concepts and procedures for using Access Manager services. Provides instructions for managing tasks from the Web portal manager interface and by using the **pdadmin** command.

WebSEAL Information

- *IBM Security Access Manager WebSEAL Installation Guide*
Provides installation, configuration, and removal instructions for the WebSEAL server and the WebSEAL application development kit.
- *IBM Security Access Manager WebSEAL Administrator's Guide*

Provides background material, administrative procedures, and technical reference information for using WebSEAL to manage the resources of your secure Web domain.

- *IBM Security Access Manager WebSEAL Developer's Reference*

Provides administration and programming information for the Cross-domain Authentication Service (CDAS), the Cross-domain Mapping Framework (CDMF), and the Password Strength Module.

Web Gateway Appliance Information

- *IBM Security Access Manager Web Gateway Appliance Administration Guide*

Provides information about configuring and maintaining a Security Access Manager environment.

IBM Tivoli Federated Identity Manager information

- *IBM Tivoli Federated Identity Manager Installation Guide*

Explains how to install, configure, and upgrade IBM Tivoli Federated Identity Manager services.

- *IBM Tivoli Federated Identity Manager Administration Guide*

Describes the concepts and procedures for using IBM Tivoli Federated Identity Manager services.

- *Redbook: Federated Identity Manager and Web Services Security with IBM Tivoli Security Services*

This Federated Identity Redbook covers important aspects of using the IBM Tivoli integrated identity management architecture to build and deploy the IBM Tivoli Federated Identity Manager and Web Services Security components. See www.redbooks.ibm.com.

IBM Terminology website

The IBM Terminology website consolidates terminology for product libraries in one location. You can access the Terminology website at <http://www.ibm.com/software/globalization/terminology>.

Accessibility

Accessibility features help users with 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 can also use the keyboard instead of the mouse to operate all features of the graphical user interface.

Technical training

For technical training information, see the following IBM Education website at <http://www.ibm.com/software/tivoli/education>.

Support information

IBM Support provides assistance with code-related problems and routine, short duration installation or usage questions. You can directly access the IBM Software Support site at <http://www.ibm.com/software/support/probsub.html>.

Statement of Good Security Practices

IT system security involves protecting systems and information through prevention, detection and response to improper access from within and outside your enterprise. Improper access can result in information being altered, destroyed, misappropriated or misused or can result in damage to or misuse of your systems, including for use in attacks on others. No IT system or product should be considered completely secure and no single product, service or security measure can be completely effective in preventing improper use or access. IBM systems, products and services are designed to be part of a comprehensive security approach, which will necessarily involve additional operational procedures, and may require other systems, products or services to be most effective. IBM DOES NOT WARRANT THAT ANY SYSTEMS, PRODUCTS OR SERVICES ARE IMMUNE FROM, OR WILL MAKE YOUR ENTERPRISE IMMUNE FROM, THE MALICIOUS OR ILLEGAL CONDUCT OF ANY PARTY.

Product name updates

This publication was first established for IBM Tivoli Access Manager. IBM Tivoli Access Manager has since been superseded by IBM Security Access Manager.

Wherever in this guide, any figures and graphics that contain or refer to IBM Tivoli Access Manager, the use of IBM Security Access Manager is implied. There are no functionality discrepancies between IBM Tivoli Access Manager and IBM Security Access Manager.

Chapter 1. Introducing the integration

This chapter has the following sections:

- “Introduction”
- “Integration product version information” on page 2
- “Network connectivity considerations” on page 3

Introduction

IBM Tivoli Access Manager v6.1 introduced the concept of Kerberos junctions for WebSEAL. You can use a Kerberos junction to achieve single-sign-on to a web application that is enabled for Kerberos authentication. The Kerberos Security Token Service (STS) module that is introduced in IBM Tivoli Federated Identity Manager v6.2 manages the generation of the Kerberos token that is used to perform single-sign-on (SSO). You can use the established IBM Tivoli Access Manager user identity for the SSO operation.

IBM Tivoli Federated Identity Manager uses Microsoft extensions to Kerberos (Microsoft TechNet, 2004) to generate a valid Kerberos token. This token is based on a supplied user identity. Introduced in Windows Server 2003, the extensions come in two parts:

- Protocol transition: The protocol transition extension allows a Kerberos ticket to be issued based on a supplied user identity on behalf of a Kerberos principal.
- Constrained delegation: A service can use constrained delegation to obtain a Kerberos service ticket that can be consumed by a separate identity whose security context is to be delegated. Constrained delegation works only in the boundary of a domain.

You can use these two extensions together to create a Kerberos service ticket, on behalf of another user, which can access the target resource. IBM Tivoli Federated Identity Manager can use these extensions to create a Kerberos service ticket on behalf of the IBM Security Access Manager user accessing the web application.

Figure 1 on page 2 shows the typical sequence of steps that are involved in performing a Kerberos single sign-on (SSO) after the IBM Security Access Manager identity is established.

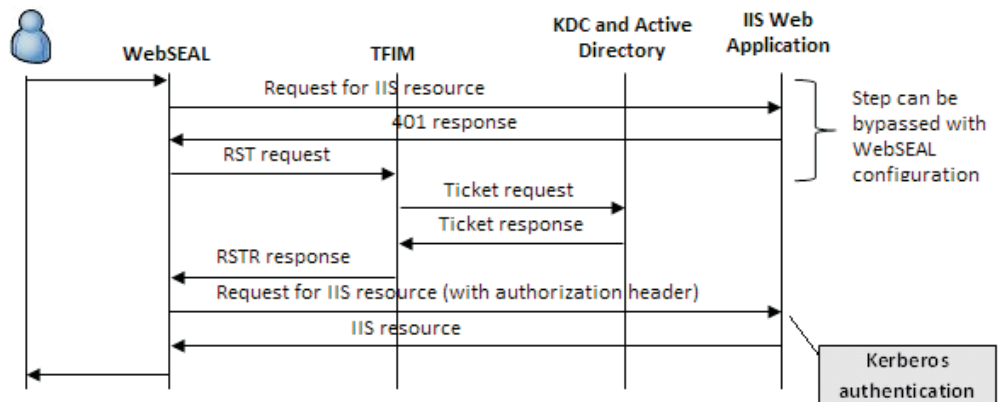


Figure 1. SSO sequence

This guide provides step-by-step instructions for the typical configuration in a Microsoft environment for Kerberos SSO. Typically, IBM Tivoli Federated Identity Manager is deployed in an IBM WebSphere® cluster. You can also use this guide in an environment where IBM Tivoli Federated Identity Manager is running as a stand-alone WebSphere Application Server. Figure 2 depicts the architecture of the environment. The host names that are included in the diagram are referenced throughout the remainder of this guide.

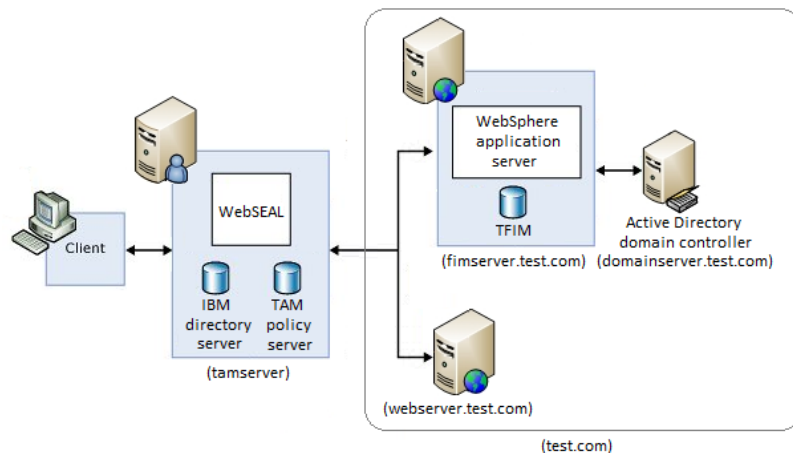


Figure 2. Environment overview

Note: This guide describes achieving web-based Single Sign-On (SSO) to Microsoft IIS by using the Windows Authentication option only. Individual applications that are hosted on Microsoft IIS cannot be inherently supported because of potential configuration that is required in the application and potential content filtering issues. See applicable Using Kerberos for Windows Authentication Guide for application-specific requirements and configuration.

Integration product version information

For information about the supported product versions, see the Release Notes.

Network connectivity considerations

IBM Tivoli Access Manager services typically run across multiple systems in the network. Some network paths must be open for the services to function correctly. All communication is over TCP/IP.

Chapter 2. Integration process

The following sections detail the steps required to achieve this integration.

- “Before you start”
- “Configuration on the domain controller” on page 6
- “Configuration on the IBM Tivoli Federated Identity Manager server” on page 9
- “Configuration on the IBM Security Access Manager server” on page 22

Before you start

This guide does not cover the configuration of the entire environment. In particular, the following product installations and configurations must already be complete:

Note: Consult the documentation outlined in “Access to publications and terminology” on page v for details on installing and configuring these products.

IBM Security Access Manager

- User registry configured with a supported registry.
- IBM Security Access Manager Policy Server installed.
- IBM Security Access Manager WebSEAL installed.

IBM Tivoli Federated Identity Manager

- Deployed to an WebSphere Application Service.
- An IBM Tivoli Federated Identity Manager domain is configured and the runtime is deployed to the domain.

See “Integration product version information” on page 2 for product details.

Time synchronization

Kerberos tickets rely on embedded time stamps to expire old tickets. For this reason, it is important to ensure that the clocks on all computers in the environment are synchronized.

User account ID synchronization or mapping

A Kerberos token can be acquired by the Kerberos Delegation module for accounts only that exist in the Microsoft Active Directory. When (the same) Microsoft Active Directory is configured as the IBM Security Access Manager user registry, the iv-cred that is passed to the IBM Security Federated Identity Manager Security Token Service (STS) already contains a valid Active Directory user account ID. If IBM Security Access Manager is configured against a different user directory either the user IDs must be synchronized or a mapping module is required to map the IBM Security Access Manager user ID to the target Microsoft Active Directory user ID for which the Kerberos token is acquired. In either case, the user account ID for which the Kerberos token is required must exist in the Microsoft Active Directory before the Kerberos Delegation module is invoked.

Configuration on the domain controller

Microsoft Windows Active Directory (AD) uses Kerberos authentication as its default security mechanism. There are two approaches:

1. Create an Active Directory (AD) user account and assign a Service Principal Name (SPN) to run as a Kerberos service and as the web application process. This is called *constrained delegation*.
2. Use the default NETWORKSERVICE account to perform Kerberos related authentication.

This guide uses the NETWORKSERVICE account to demonstrate Windows Authentication with Kerberos tokens.

IBM Tivoli Federated Identity Manager service account

Create and initialize an Active Directory user to run as a Kerberos service:

1. Select **Active Directory Users and Computers** from the **Administrative Tools** section of the Start menu.
2. Create a user whose password never expires.

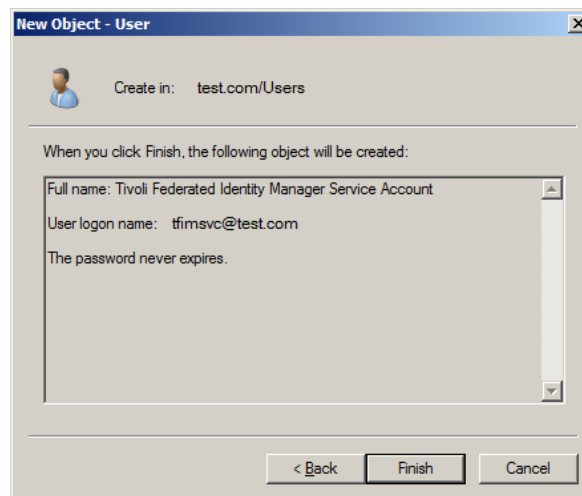


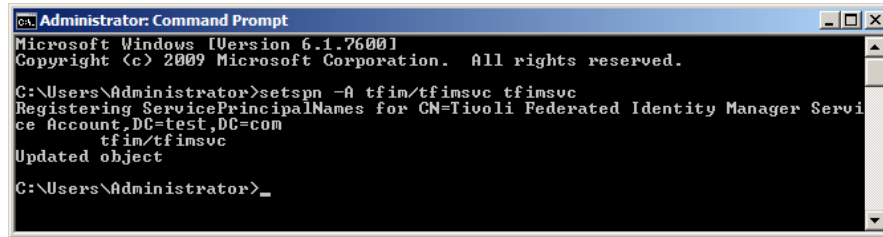
Figure 3. IBM Tivoli Federated Identity Manager service account user creation

3. Use the **setspn** command-line utility, which is provided as part of the Windows support tools, to set the SPN for the new Active Directory user. The syntax for **setspn** is shown in the following listing.

Listing 2. setspn command

```
setspn -A tfim/<TFIM User Name> <TFIM User Name>
```

Figure 4 on page 7 shows an example **setspn** command and its output.



```
Administrator: Command Prompt
Microsoft Windows [Version 6.1.7600]
Copyright (c) 2009 Microsoft Corporation. All rights reserved.

C:\Users\Administrator>setspn -A tfim/tfimsvc tfimsvc
Registering ServicePrincipalNames for CN=Tivoli Federated Identity Manager Service Account,DC=test,DC=com
tfim/tfimsvc
Updated object

C:\Users\Administrator>_
```

Figure 4. Setting the IBM Tivoli Federated Identity Manager user SPN

4. You must modify the IBM Tivoli Federated Identity Manager Active Directory user so that it is trusted to delegate for the HTTP service.
 - a. Select **Active Directory Users and Computers**, from the **Administrative Tools** section of the Start menu.
 - b. Open the properties for the IBM Tivoli Federated Identity Manager Active Directory user.
 - c. Select the **Delegation** tab.
 - d. Enable delegation to the IBM Tivoli Federated Identity Manager user by selecting the **Trust this user for delegation to specified services only** option.
 - e. Click **Add** select or specify the name of the target server machine, which is hosting the web application. This target server name can be the name of the machine hosting your custom ASP.NET application, your Microsoft SharePoint Server, your Microsoft Exchange Server OWA and such.
 - f. When asked to select the service type for the delegation, select the service appropriate for your environment.
 - g. Select the service type as "Http". When complete, click **OK**.

After completing the steps, the Delegation tab for the IBM Tivoli Federated Identity Manager user properties must look similar to the one shown in Figure 5 on page 8.

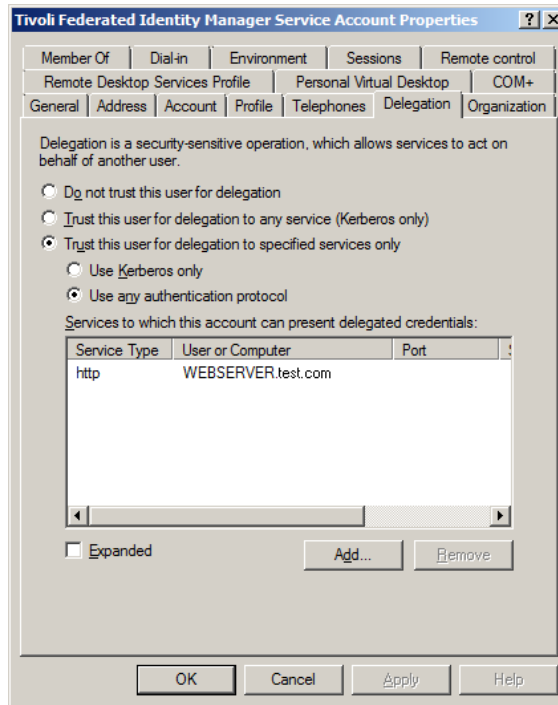


Figure 5. Enable permission to delegation to FIM Service Account

5. You must also add the IBM Tivoli Federated Identity Manager Active Directory user to the **Windows Authorization Access Groups** object.
 - a. Select **Active Directory Users and Computers**, from the **Administrative Tools** section of the Start menu.
 - b. Select the **Builtin** object.
 - c. Right-click **Windows Authorization Access Groups** object and select **Properties**.
 - d. Click **Add** to add the new IBM Tivoli Federated Identity Manager Active Directory user as a member of the group. See Figure 6 on page 9.

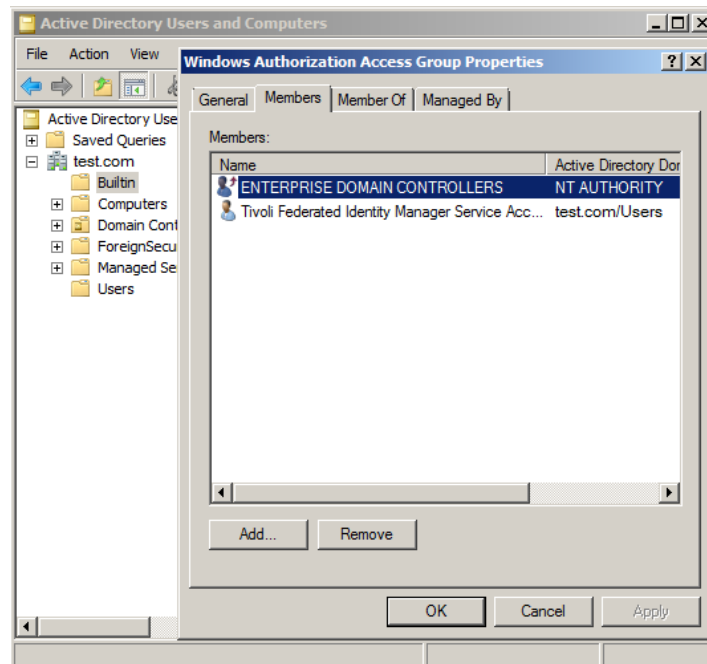


Figure 6. Windows authorization access groups

e. Click **OK**.

Configuration on the IBM Tivoli Federated Identity Manager server

There are several procedures to configure the IBM Tivoli Federated Identity Manager server.

- “IBM Tivoli Federated Identity Manager service account user configuration”
- “Configure the WebSphere Application Server service” on page 12
- “Create a trust chain” on page 15

IBM Tivoli Federated Identity Manager service account user configuration

1. The IBM Tivoli Federated Identity Manager Active Directory user that is created in Figure 3 on page 6 must be added as a member of the local **Administrators** group of the Federated Identity Manager server machine.

Note: In a clustered environment, you must repeat this step on all of the IBM Tivoli Federated Identity Manager servers.

- a. Select **Computer Management** from the **Administrative Tools** section of the Start menu.
- b. Locate the **Administrators** group under **Local Users and Groups -> Groups**.
- c. Add the IBM Tivoli Federated Identity Manager Active Directory user to the **Administrators** group as shown in Figure 7 on page 10.

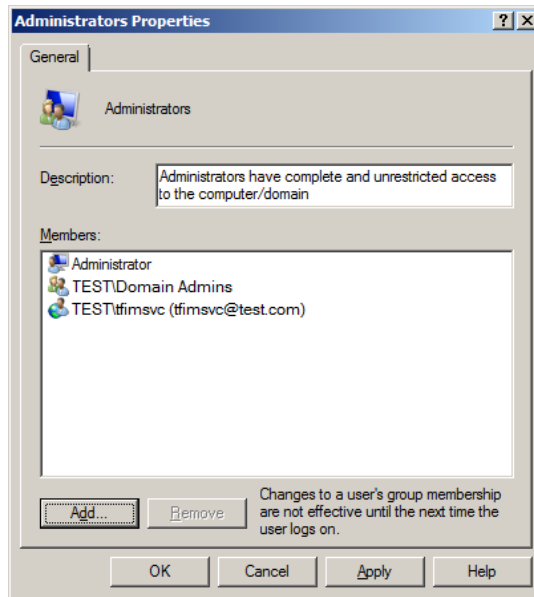


Figure 7. Using FIM service account user to local Administrators group

2. By default the security policy of the server does not allow an Active Directory user to run a local service.

Note: In a clustered environment, you must repeat this step on all of the IBM Tivoli Federated Identity Manager servers.

- a. Select **Local Security Policy** from the **Administrative Tools** section of the Start menu.
- b. Navigate to **Security Settings > Local Policies > User Rights Assignment**.
- c. Modify the "**Log on as a service**" local policy to include the new IBM Tivoli Federated Identity Manager Active Directory user so that the user can run WebSphere as a service. See Figure 8 on page 11.

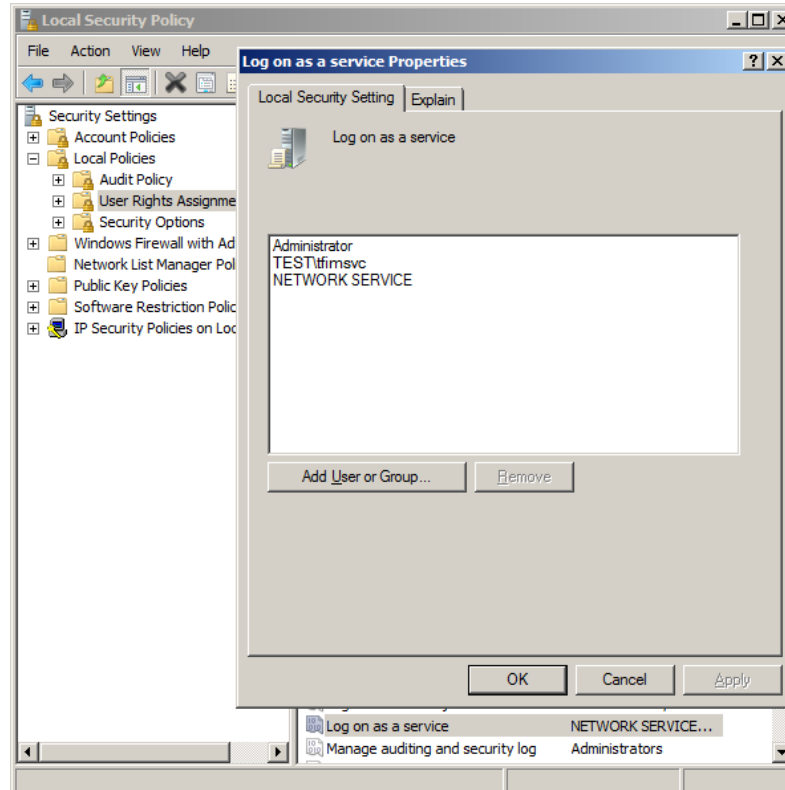


Figure 8. Log on as a service

3. Grant the IBM Tivoli Federated Identity Manager Active Directory user permission to act as part of the operating system on the WebSphere Application Server.

Note: In a clustered environment, you must repeat this step on all of the IBM Tivoli Federated Identity Manager servers.

- a. Select **Local Security Policy** from the **Administrative Tools** section of the Start menu.
- b. Navigate to **Security Settings > Local Policies > User Rights Assignment**.
- c. Modify the “**Act as a part of the operating system**” local policy to include the new IBM Tivoli Federated Identity Manager Active Directory user. See Figure 9 on page 12.

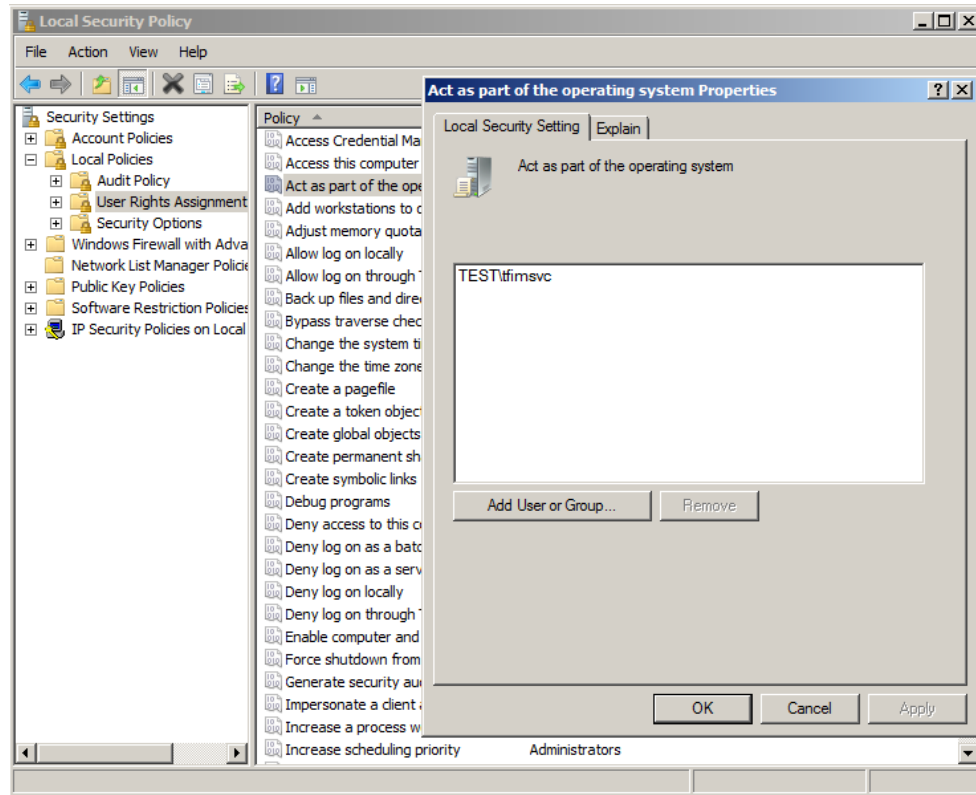


Figure 9. Enable FIM Service Account user to act as part of the operating system on WebSphere Server

Configure the WebSphere Application Server service

The WebSphere Application Server service that hosts the IBM Tivoli Federated Identity Manager runtime must run under the IBM Tivoli Federated Identity Manager Active Directory account. This configuration is required so that the service has permission to obtain Kerberos tickets for:

- Other users, and
 - A constrained set of target computers.
1. You must modify the WebSphere service to run as the IBM Tivoli Federated Identity Manager Active Directory user.
 - a. Open the **Services** control panel, which is available from the **Administrative Tools** section of the Start menu.
 - b. Modify the properties of the **IBM WebSphere Application Server** service.
 - c. Set the service logon user account to be the IBM Tivoli Federated Identity Manager Active Directory user. See Figure 10 on page 13.

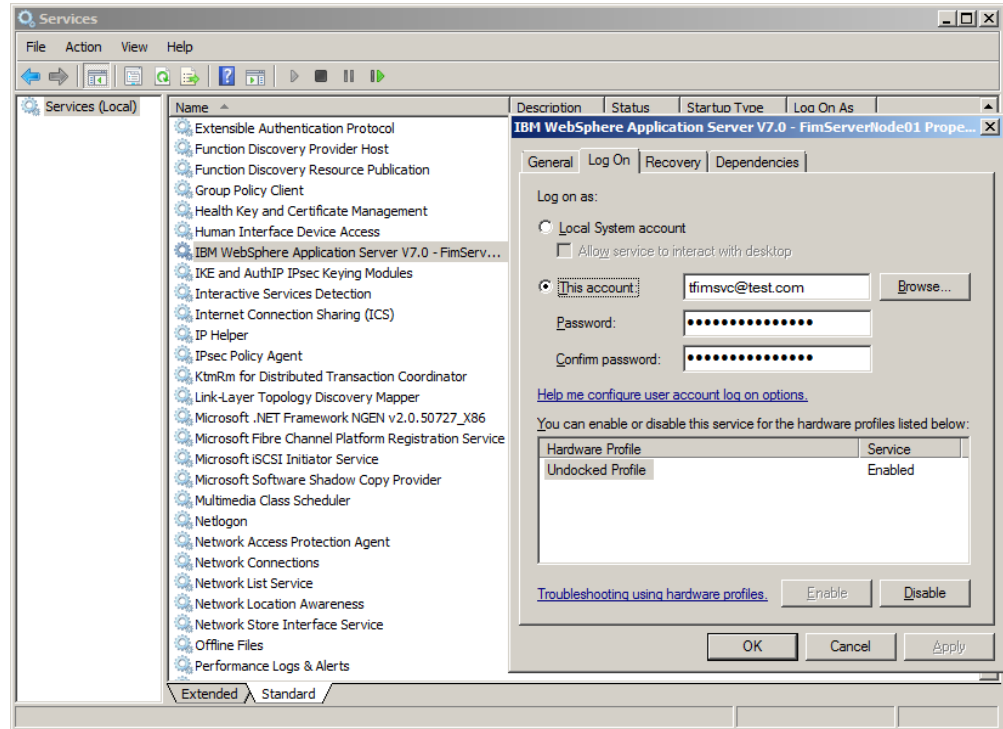


Figure 10. Set WebSphere service logon user account to be FIM Service Account

2. Restart WebSphere to reflect the changes to the Service properties.
 - a. If WebSphere is running, run the **Stop the server** command.
 - b. Run the **Start the server** command.

These commands are in the application menu. See Figure 11 on page 14.

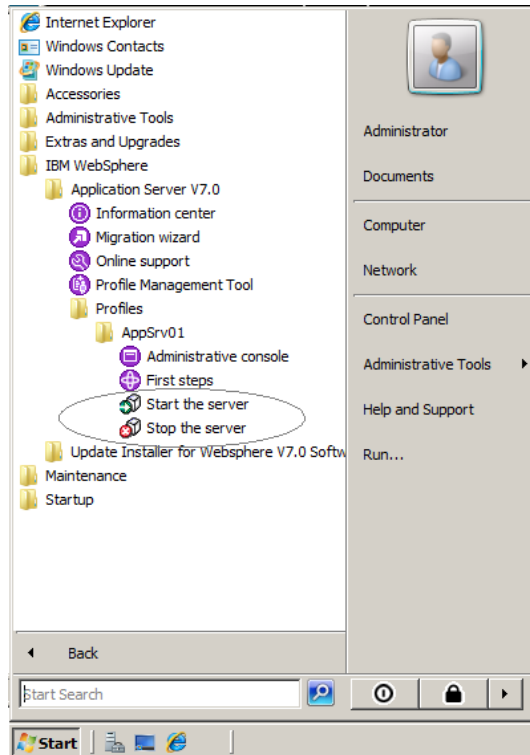


Figure 11. WebSphere Application Server restart

3. Ensure that the WebSphere Application Server service is running as the IBM Tivoli Federated Identity Manager Active Directory user.
 - a. Open Windows Task Manager.
 - b. Select the **Processes** tab.
 - c. Examine the process list to ensure that the following processes are run as the IBM Tivoli Federated Identity Manager Active Directory user:
 - java.exe
 - WasService.exe

See Figure 12 on page 15.

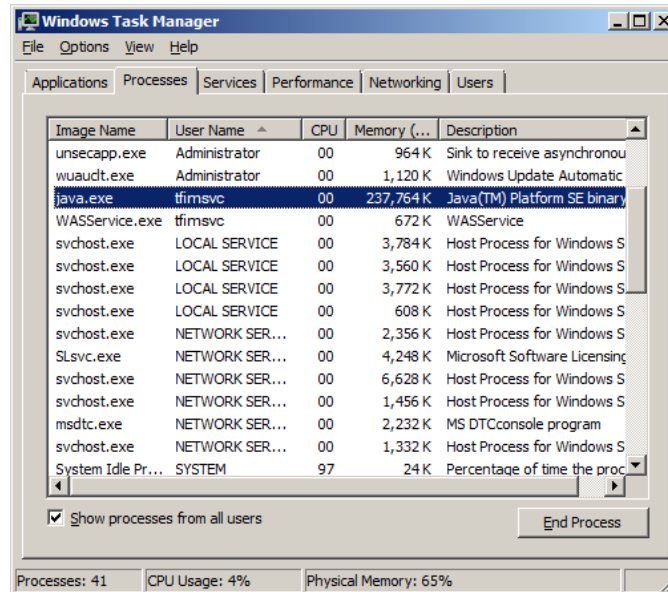


Figure 12. WebSphere Application Server runtime user validation

Create a trust chain

You must create an IBM Tivoli Federated Identity Manager trust chain that can create a Kerberos token from a supplied IVCred from IBM Security Access Manager WebSEAL. A trust chain comprises numerous IBM Tivoli Federated Identity Manager modules that are run in sequence.

The minimal trust chain that is required for a WebSEAL Kerberos junction consists of:

- An IVCred Token module, which extracts the user identity information from the IV Credential.
- A Kerberos Delegation module, which generates the Kerberos token.

You can use the default module instance for the IVCred Token module, but you must create a new Kerberos Delegation module instance to include in the trust chain. See “Create the Kerberos Delegation STS module instance” on page 16. When using the default module instance the user account ID contained within the IVCred must exactly match an existing user account ID in the Microsoft Active Directory. The use of IBM Security Access Manager that is configured against Microsoft Active Directory or synchronization of user account IDs between the IBM Security Access Manager directory and Microsoft Active Directory is not contained within this document.

Optionally, you can insert a mapping module between the IVCred Token module and the Kerberos Delegation module. You can use a mapping module to map the IBM Security Access Manager user ID with the Active Directory identity that is contained in the generated Kerberos token. The mapping module is used to match an IBM Security Access Manager user account ID to an existing user account ID in the Microsoft Active Directory when the IDs are different.

In either case, the user account ID for which the Kerberos token is required must exist in the Microsoft Active Directory before the Kerberos Delegation module being called.

For more information about creating the required trust chain, see “Create the Trust Chain” on page 18.

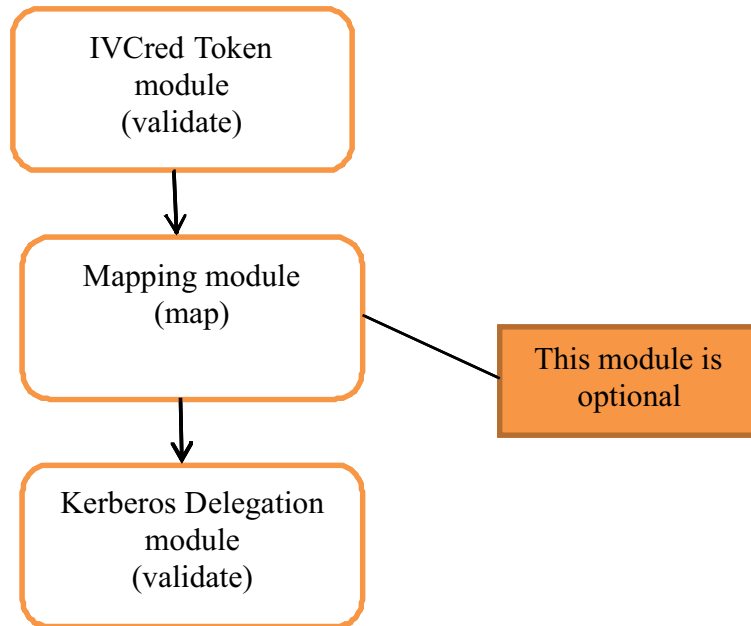


Figure 13. FIM trust chain for a WebSEAL Kerberos junction

Create the Kerberos Delegation STS module instance

1. From the WebSphere console, select **Tivoli Federated Identity Manager** to expand it.
2. Select **Configure Trust Service** to expand it.
3. Select **Module Instances**.
4. On the **Module Instances** page, click **Create**.
5. From the table presented, select the module type for the new Module instance to be **com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSModule**. This wizard gathers information to configure the new Kerberos Delegation STS module instance.
6. Click **Next**. See Figure 14 on page 17.

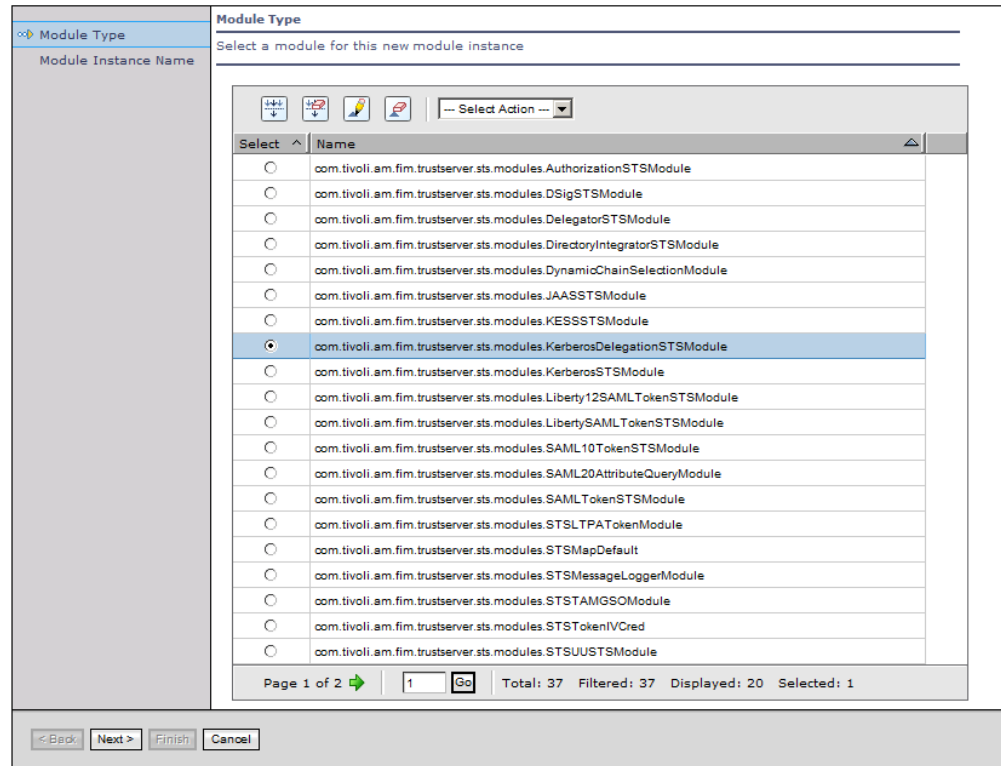


Figure 14. Kerberos Delegation STS module wizard – Step 1

7. On the second configuration page (Figure 15), enter a **Module Instance Name**, such as Kerberos Token. The wizard uses this module name in the construction of the trust chain.
8. Enter a value for **Module Instance Description**.
9. Click **Next** to proceed.

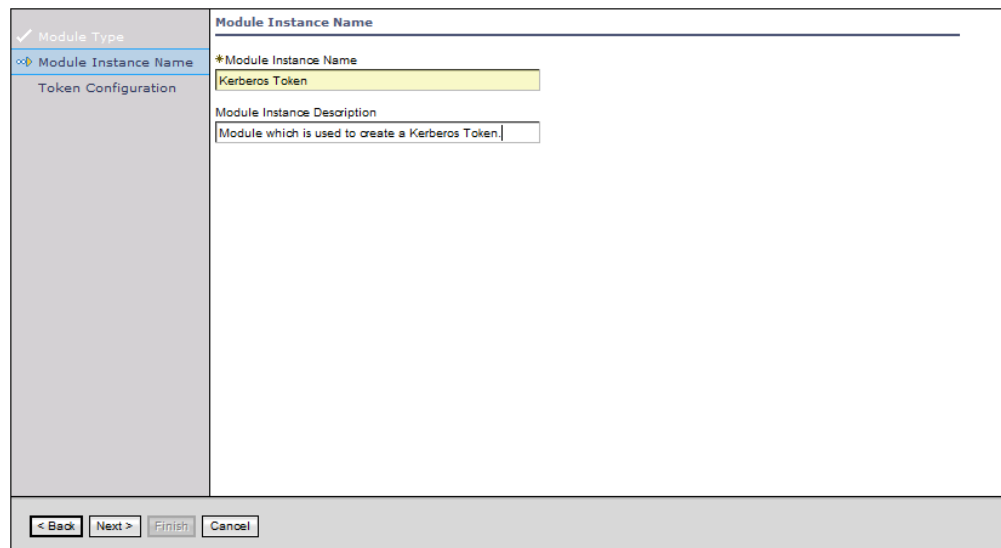


Figure 15. Kerberos Delegation STS module wizard -- Step 2

10. On the third configuration page (Figure 16 on page 18), specify the maximum size of the credential cache or accept the default.

Note: To enhance performance of successive ticket requests, IBM Tivoli Federated Identity Manager uses a least recently (LRU) collection of Kerberos Local Security Authority (LSA) logins.

The screenshot shows a configuration window titled "Kerberos Delegation Module Configuration". On the left, a sidebar lists three steps: "Module Type" (checked), "Module Instance Name" (checked), and "Token Configuration" (selected with a blue highlight). The main area on the right contains the text "Enter the required values to configure the Kerberos Delegation Module" and a single configuration item: "*Maximum size of the user credential cache" with a text input field containing the value "100". At the bottom of the window, there are four buttons: "< Back", "Next >", "Finish", and "Cancel".

Figure 16. Kerberos Delegation STS module wizard – Step 3

11. Click **Finish**. The Kerberos Delegation module is now configured.

Create the Trust Chain

1. From the WebSphere console, select **Tivoli Federated Identity Manager**.
2. Select **Configure Trust Service**.
3. Select **Trust Service Chains**.
4. On the displayed **Trust Service Chains** page, click **Create**.
5. Click **Next** after you read the introduction.
6. Figure 17 on page 19 shows the second page of the wizard. Enter a value for the **Chain Mapping Name** and **Description**.

Chain Mapping Identification	
Chain Mapping Name	WebSEAL Kerberos Junction
Description	Generate a token for a WebSEAL Kerberos junction.
<input type="checkbox"/> Create a dynamic chain	

< Back Next > Finish Cancel

Figure 17. Trust chain wizard - page 2

7. Click **Next**.
8. Complete the following fields on the next page of the wizard:
 - a. Select **Issue Oasis URI** as the **Request Type**. This value indicates that the request conforms to WS-Trust V1.3.
 - b. The **Address** field in the **AppliesTo** section corresponds to the WebSEAL **applies-to** configuration entry. This value is the domain name of the WebSEAL server. (Refer to Listing 3 under “Configuration on the IBM Security Access Manager server” on page 22). You can enter an exact value or you can use '*' as a wild card to represent multiple junctions to the same IBM Tivoli Federated Identity Manager machine. This value illustrates support for either http or https virtual junctions.
 - c. The **Service Name** in the **AppliesTo** section corresponds to the WebSEAL **service-name** configuration entry (refer to Listing 3 under “Configuration on the IBM Security Access Manager server” on page 22). The service name that WebSEAL sends in the Request Security Token (RST) is matched against the first field of the Service Name field after the colon, which is a port number for the service. In Figure 18 on page 20, the '*' character is used for both Service Name fields so that all requests with the same address are matched.
 - d. The **Address** value of the **Issuer** section must be amwebste-sts-client.
 - e. Select **Kerberos GSS V5** as the **Token Type** value. This value indicates the version of the Kerberos token to return.

<ul style="list-style-type: none"> ✓ Introduction ✓ Chain Mapping Identification ✚ Chain Mapping Lookup Chain Identification Chain Assembly Module Instance Settings Summary 	<h3>Chain Mapping Lookup</h3> <hr/> <p>Request Type</p> <p>Request Type: <input type="text" value="Issue Oasis URI"/> Request Type URI: <input type="text" value="http://docs.oasis-open.org/ws-sx/ws-trust/200512/Issue"/></p> <hr/> <p>Lookup Type</p> <p> <input checked="" type="radio"/> Use Traditional WS-Trust Elements (AppliesTo, Issuer, and TokenType) <input type="radio"/> Use XPath to Define Custom Lookup Rule </p> <hr/> <p>AppliesTo</p> <p>Address: <input type="text" value="REGEXP:(.*iamserver)"/></p> <p>Service Name: <input type="text" value="*"/> <input type="text" value="*"/></p> <p>Port Type: <input type="text" value=""/> <input type="text" value=""/></p> <hr/> <p>Issuer</p> <p>Address: <input type="text" value="amwebrie-sts-client"/></p> <p>Service Name: <input type="text" value=""/> <input type="text" value=""/></p> <p>Port Type: <input type="text" value=""/> <input type="text" value=""/></p> <hr/> <p>Token Type</p> <p>Token Type: <input type="text" value="Kerberos GSS V5"/> Token Type URI: <input type="text" value="http://docs.oasis-open.org/ws-sx/ws-kerberos-token-profile-1.1#GSS_Kerberosv5_AP_Rq"/></p>
	<p>< Back Next > Finish Cancel</p>

Figure 18. Trust chain wizard - page 3

- Enter a value for the **Chain Name** and **Description** on the fourth page of the wizard. See Figure 19.

<ul style="list-style-type: none"> ✓ Introduction ✓ Chain Mapping Identification ✓ Chain Mapping Lookup ✚ Chain Identification Chain Assembly Module Instance Settings Summary 	<h3>Chain Identification</h3> <hr/> <p>*Chain Name: <input type="text" value="WebSEAL Kerberos Junction"/></p> <p>Description: <input type="text" value="Generates a token for a WebSEAL Kerberos junction."/></p> <p><input type="checkbox"/> Initialize the chain upon startup of the Runtime</p>
	<p>< Back Next > Finish Cancel</p>

Figure 19. Trust chain wizard - page 4

- On the fifth page, you can assemble the two modules for the Trust Chain.
 - Add a **Default IVCred Token** module in **Validate** mode.
 - Add the **Kerberos Delegation** module that you created in “Create the Kerberos Delegation STS module instance” on page 16. Use **Issue** mode for this module.

Figure 20 on page 21 shows the result.

Introduction

Chain Mapping Identification

Chain Mapping Lookup

Chain Identification

Chain Assembly

Module Instance Settings

Summary

Chain Assembly

Construct a chain by selecting an instance and a mode and click Add to add the instance to the chain table. Continue until the chain table contains all required instances and then click Next.

Module Instance

Mode

Add selected module instance to chain

Trust Service Chain Modules

Select	Order	Module Instance Name	Module Instance Type	Mode
<input type="radio"/>	<input type="text" value="1"/>	Default IVcred Token	com.tivoli.am.fim.trustserver.sts.modules.STSTokenIVCred	validate
<input type="radio"/>	<input type="text" value="2"/>	Kerberos Token	com.tivoli.am.fim.trustserver.sts.modules.KerberosDelegationSTSTModule	issue

Total: 2 Selected: 0

Back

Next >

Finish

Cancel

- Click **Next**. You might be prompted with a warning that the module trust chain does not meet the Trust Service module chain structure. You can ignore the warning and click **Continue**.
- On the IVCred Module configuration page, no options are required. See Figure 21.

- Introduction
- Chain Mapping Identification
- Chain Mapping Lookup
- Chain Identification
- Chain Assembly
- Configure Module Chain Item 1**
- Configure Module Chain Item 2
- Summary

Access Manager Credential (IVCred) Module Configuration

Enter the required values to configure the Access Manager Credential Module.

Partner properties

☐ Enable signature validation

Select Validation Key

Keystore

Keystore Password

Select	Alias	Key Type	Days until ...	Subject DN
Total: 0 Filtered: 0 Displayed: 0 Selected: 0				

<ul style="list-style-type: none"> ✓ Introduction ✓ Chain Mapping Identification ✓ Chain Mapping Lookup ✓ Chain Identification ✓ Chain Assembly ✓ Configure Module Chain Item 1 Configure Module Chain Item 2 Summary 	Kerberos Delegation Module Configuration Enter the required values to configure the Kerberos Delegation Module
	Partner properties Default target Service Principal Name <input type="text"/>
	*Options for adding a suffix to the TAM username for Kerberos Authentication <input type="radio"/> Do not add a suffix to the username <input checked="" type="radio"/> Add the machine DNS domain as a suffix to the username <input type="radio"/> Add the configured suffix to the username
	The suffix to add if using a configured suffix <input type="text" value="@mydomain.com"/>
<input <="" <input="" td="" type="button" value=" Cancel "/>	

Figure 22. Trust chain wizard - page 7

- Click **Next**.
- Review the configuration on the final page. Click **Finish** to create the IBM Tivoli Federated Identity Manager Kerberos delegation trust chain.
- For the new trust chain to take effect, click **Load configuration changes to Tivoli Federated Identity Manager runtime**. If the changes are not applied, restart the WebSphere. See the restart operations in Figure 11 on page 14.

Configuration on the IBM Security Access Manager server

- You can configure the WebSEAL Kerberos junction in the WebSEAL configuration file. You must complete this configuration before you can create the virtual junction.

Modify the following two stanzas in the configuration file:

- [tfimssso:<jct-id>], which contains the general configuration details for the Kerberos junction, and
- [tfim-cluster:<cluster>], which contains the configuration details that are used to connect and communicate with IBM Tivoli Federated Identity Manager.

The following listing shows the configuration for the environment that is described in this guide. It includes only the configuration entries that differ from the default WebSEAL template configuration.

Listing 3. WebSEAL configuration file extract

```
#[tfimssso:<jct-id>]
[tfimssso:webapp]

#
# This stanza is used to hold the TFIM single sign-on configuration information
# for a single junction.
#
# For standard junctions the stanza name will be qualified with the name of the
# junction point (including the leading '/'). An example stanza name might be:
# [tfimssso:/junction_a]
#
# For virtual host junctions the stanza name will be qualified with the
# virtual host label. An example stanza name might be:
# [tfimssso:www.ibm.com]
#

# The type of token which will be requested from TFIM. This value should
# correspond to the 'Token Type URI' field for the corresponding trust chain
# within TFIM.
```

```

#token-type = http://docs.oasis-open.org/wss/oasis-wss-kerberos-token-profile-
1.1#GSS_Kerberosv5_AP_REQ
token-type = kerberos

# The 'applies-to' search criteria used when locating the appropriate STS
# module within TFIM. Generally this entry should be of the format:
# http://<webseal-server>/<junction> (similar to the URL which is used to
# access the junction).
#applies-to = http://<webseal-server>/<junction>
applies-to = http://tamserver.ibm.com

# The service-name configuration entry will be used:
# 1. By TFIM when searching for a matching trust chain. This configuration
# entry will be compared against the configured 'AppliesTo' service name
# value for each trust chain. The second field within the 'AppliesTo'
# service name configuration entry should be set to either '*' to match
# all service names, or it should be set to the value defined by this
# configuration item. Refer to the TFIM documentation for further
# details on configuring Trust Chains.
# 2. As the service principal name of the delegating user when creating a
# Kerberos token. The service principal name can be determined by
# executing the Microsoft utility 'setspn', i.e. setspn -L <user>,
# where <user> is the identity of the user which the junctioned Web server
# is running as.
#service-name = <spn>
service-name = HTTP/webserver.test.com

# The length of time, in seconds, by which the expiry time of a security token
# will be reduced. This entry is used to make allowances for differences in
# system times and transmission times for the security tokens.
renewal-window = 15

# This boolean value is used to indicate whether the security token which is
# produced by TFIM is only valid for a single transaction. An example of a
# one-time-token is a Kerberos token, which can only be used for a single
# authentication operation.
one-time-token = true

# This boolean value is used to control whether the requested
# BinarySecurityToken XML structure should be used in it's entirety, or whether
# only the encapsulated token should be used. This configuration entry should
# only be set to true if the junctioned Web server understands and expects the
# BinarySecurityToken XML structure.
preserve-xml-token = false

# The number of security tokens which should be retrieved from TFIM in a single
# request. This option is only valid for one-time-tokens where the
# corresponding TFIM module has also been coded to handle requests for multiple
# tokens via the 'Claims' construct. The resultant security tokens will be
# cached by WebSEAL and then used on subsequent requests. Tuning of this
# parameter will be important for performance of one-time-tokens. If the
# value is large there will be fewer requests to TFIM, but the responses to
# these requests will be larger.
token-collection-size = 10

# The type of mechanism which will be used to transmit the security token to
# the junctioned Web server. Possible values for this configuration entry
# are:
# header - The security token will be included in a header;
# cookie - The security token will be included in a cookie;
token-transmit-type = header

# The name given to the security token within the junctioned Web server
# request.
token-transmit-name = Authorization

# This boolean value is used to indicate whether a security token should be

```

```

# sent for every HTTP request, or whether WebSEAL should wait for a 401
# response from the back-end Web server before adding the security token. This
# configuration item is used to avoid the unnecessary overhead of generating
# and adding a security token to every request if the back-end Web server is
# capable of maintaining user sessions.
#always-send-tokens = false
always-send-tokens = true

# The name of the WAS cluster which houses this TFIM service. There should
# also be a corresponding [tfim-cluster:<cluster>] stanza which contains the
# definition of the cluster.
#tfim-cluster-name = my-cluster
tfim-cluster-name = FimServerNode01Cell

#[tfim-cluster:my-cluster]
[tfim-cluster:FimServerNode01Cell]

#
# This stanza contains definitions for a particular cluster of TFIM
# servers.
#

#
# A specification for the server which is used when communicating with a
# single TFIM server which is a member of this cluster. Values for this
# entry are defined as follows:
#
#      {[0-9],}<URL>
#
# Where the first digit (if present) represents the priority of the server
# within the cluster (9 being the highest, 0 being lowest). If the priority
# is not specified, a priority of 9 is assumed. The <URL> can be any
# well-formed HTTP or HTTPS URL.
#
# Multiple server entries can be specified for failover and load balancing
# purposes. The complete set of these server entries defines the
# membership of the cluster for failover and load balancing.
#
# server = 9,http://tfim.example.com/TrustServerWST13/services/RequestSecurityToken
server = 9,http://fimserver:9080/TrustServerWST13/services/RequestSecurityToken

```

Once the WebSEAL configuration file is updated with the junction configuration and the WebSEAL service is restarted, the actual virtual junction can now be created.

2. Use **pdadmin** to create the virtual junction for Kerberos as shown in the following listing:

Listing 4. Virtual junction create command

```
pdadmin sec_master> s t default-webseald-tamserver virtual create -t tcp
-h webserver.test.com -Y webapp
```

where:

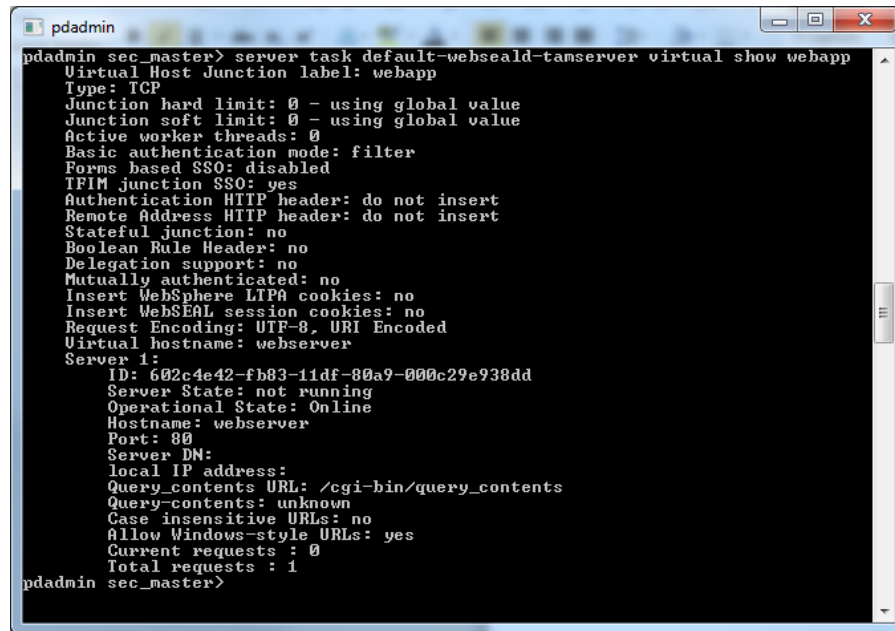
- t Specifies the type of virtual junction.
- h (hostname) Specifies the web server that is running IIS.
- Y Denotes the use of a Kerberos junction.

webapp

The configuration name that is used in the WebSEAL stanza, see Listing 3 in step 1 on page 22.

Additional information about creating virtual host junctions can be found in the *svrsslcfg* section of the *IBM Security Access Manager Command Reference*.

Figure 23 displays the attributes for the virtual host junction created from Listing 4.



```
pdadmin sec_master> server task default-webseald-tamserver virtual show webapp
Virtual Host Junction label: webapp
Type: TCP
Junction hard limit: 0 - using global value
Junction soft limit: 0 - using global value
Active worker threads: 0
Basic authentication mode: filter
Forms based SS0: disabled
TFIM junction SS0: yes
Authentication HTTP header: do not insert
Remote Address HTTP header: do not insert
Stateful junction: no
Boolean Rule Header: no
Delegation support: no
Mutually authenticated: no
Insert WebSphere LTPA cookies: no
Insert WebSEOL session cookies: no
Request Encoding: UTF-8, URI Encoded
Virtual hostname: webserver
Server 1:
  ID: 602c4e42-fb83-11df-80a9-000c29e938dd
  Server State: not running
  Operational State: Online
  Hostname: webserver
  Port: 80
  Server DN:
  local IP address:
  Query_contents URL: /cgi-bin/query_contents
  Query-contents: unknown
  Case insensitive URLs: no
  Allow Windows-style URLs: yes
  Current requests : 0
  Total requests : 1
pdadmin sec_master>
```

Figure 23. Virtual host junction attributes

3. You can now test the new Kerberos junction. Ensure that your IIS web server machine has a web application that uses Windows Authentication.

Chapter 3. Troubleshooting

If followed correctly, the environment configuration for Kerberos junctions demonstrated in this guide is not supposed to cause significant problems. However, if you encounter problems, see the following tips to help diagnose and resolve issues:

1. Kerberos tokens use time stamps to ensure that authentication does not take place using old or expired tokens. If WebSEAL tries to access a resource on a Kerberos junction and returns an error stating that no tokens were available, check the time stamp on all servers to ensure that they fall within a reasonable limit. Ideally, use a time synchronization server in the environment.
2. After restarting WebSphere Application Server and the IBM Tivoli Federated Identity Manager, it can take several minutes before the server is able to generate a token; even after the Windows Service states the service has started.
3. Examine the log file WebSphere Application Server **systemout.log** file and the WebSEAL log file to help determine the root cause of the problem.
4. Enable the IBM Tivoli Federated Identity Manager tracing for the Kerberos STS Module to provide more information about the generation of the Kerberos token. Tracing is managed through the standard WebSphere logging mechanism through the WebSphere Application Server console. The relevant logging component is **com.tivoli.am.fim.trustserver.sts**. See Figure 24.

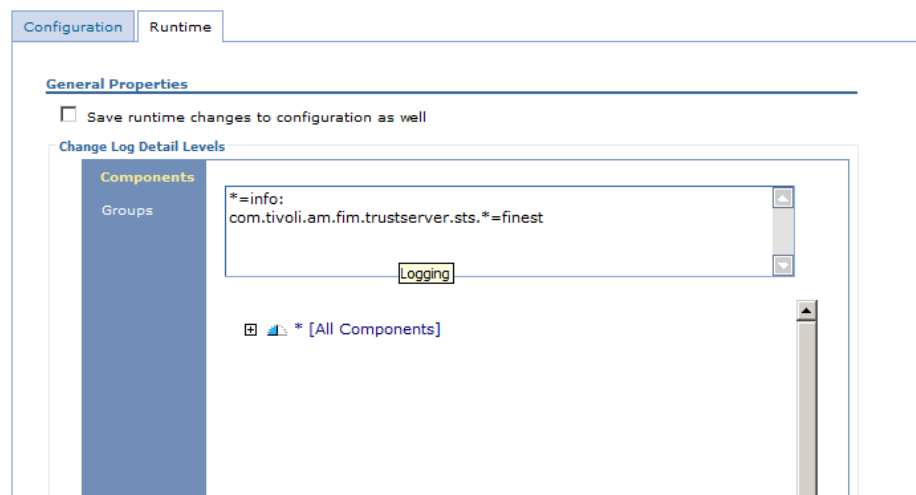


Figure 24. Troubleshooting IBM Tivoli Federated Identity Manager Kerberos Delegation

5. You can enable WebSEAL tracing for the IBM Tivoli Federated Identity Manager client to provide more information about attempts by WebSEAL to retrieve a Kerberos token from IBM Tivoli Federated Identity Manager. This tracing is managed through the IBM Security Access Manager tracing mechanism; controlled through **pdadmin server task <server-name> trace** commands. The relevant trace component is: **pdweb.sso.tfim**.
6. Ensure that the service you have configured in the **webseal-default.conf** file corresponds with the service that is listed when you run the **setspn -L** command (see Listing 5). Also ensure that you have configured IBM Tivoli Federated Identity Manager user with the correct delegation rights on the domain controller.

Listing 5. setspn -L

```
c:\users\Administrator>setspn -L webappsvc
```

Result:

```
Registered ServicePrincipalNames for CN=Web Application Service Account,  
CN=Users,DC=test,DC=com:HTTP/webserver.test.com
```

Notices

This information was developed for products and services offered in the U.S.A. IBM may 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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan, Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, 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 might 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 publication. IBM may make improvements and/or changes in the product(s) and/or the program(s) described in this publication 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
2Z4A/101
11400 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.

All statements regarding IBM's future direction or intent are subject to change or withdrawal without notice, and represent goals and objectives only.

All IBM prices shown are IBM's suggested retail prices, are current and are subject to change without notice. Dealer prices may vary.

This information is for planning purposes only. The information herein is subject to change before the products described become available.

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.

COPYRIGHT LICENSE:

This information contains sample application programs in source language, which illustrate programming techniques on various operating platforms. You may copy, modify, and distribute these sample programs in any form without payment to

IBM, for the purposes of developing, using, marketing or distributing application programs conforming to the application programming interface for the operating platform for which the sample programs are written. These examples have not been thoroughly tested under all conditions. IBM, therefore, cannot guarantee or imply reliability, serviceability, or function of these programs. You may copy, modify, and distribute these sample programs in any form without payment to IBM for the purposes of developing, using, marketing, or distributing application programs conforming to IBM's application programming interfaces.

Each copy or any portion of these sample programs or any derivative work, must include a copyright notice as follows:

© (your company name) (year). Portions of this code are derived from IBM Corp. Sample Programs. © Copyright IBM Corp. _enter the year or years_. All rights reserved.

If you are viewing this information in softcopy form, the photographs and color illustrations might not be displayed.

Trademarks

IBM, the IBM logo, and ibm.com[®] are trademarks or registered trademarks of International Business Machines Corp., registered in many jurisdictions worldwide. Other product and service names might be trademarks of IBM or other companies. A current list of IBM trademarks is available on the Web at Copyright and trademark information; at www.ibm.com/legal/copytrade.shtml.

Adobe, Acrobat, PostScript and all Adobe-based trademarks are either registered trademarks or trademarks of Adobe Systems Incorporated in the United States, other countries, or both.

IT Infrastructure Library is a registered trademark of the Central Computer and Telecommunications Agency which is now part of the Office of Government Commerce.

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.

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.

ITIL is a registered trademark, and a registered community trademark of the Office of Government Commerce, and is registered in the U.S. Patent and Trademark Office.

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



Java™ and all Java-based trademarks and logos are trademarks or registered trademarks of Oracle and/or its affiliates.

Cell Broadband Engine is a trademark of Sony Computer Entertainment, Inc. in the United States, other countries, or both and is used under license therefrom.

Linear Tape-Open, LTO, the LTO Logo, Ultrium, and the Ultrium logo are trademarks of HP, IBM Corp. and Quantum in the U.S. and other countries.

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



Printed in USA