IBM® Tivoli® Federated Identity Manager
Version 6.2.2

# *Installation Guide*

GC27-2718-01

IBM® Tivoli® Federated Identity Manager
Version 6.2.2

# *Installation Guide*

GC27-2718-01

**Note**

Before using this information and the product it supports, read the information in “Notices” on page 99.

**Edition notice**

This edition applies to version 6, release 2, modification 2 of IBM Tivoli Federated Identity Manager (product number 5724-L73) and to all subsequent releases and modifications until otherwise indicated in new editions.

# Contents

# Figures

# Tables

# About this publication

IBM® Tivoli® Federated Identity Manager Version 6.2.2 implements solutions for federated single sign-on, Web services security management, and provisioning that are based on open standards. IBM Tivoli Federated Identity Manager extends the authentication and authorization solutions provided by IBM Tivoli Access Manager to simplify the integration of multiple existing Web solutions.

This guide describes how to install IBM Tivoli Federated Identity Manager.

## Intended audience

The target audience for this book includes network security architects, system administrators, network administrators, and system integrators. Readers of this book should have working knowledge of networking security issues, encryption technology, keys, and certificates. Readers should also be familiar with the implementation of authentication and authorization policies in a distributed environment.

This book describes an implementation of a Web services solution that supports multiple Web services standards. Readers should have knowledge of specific Web services standards, as obtained from the documentation produced by the standards body for each respective standard.

Readers should be familiar with the development and deployment of applications for use in a Web services environment. This includes experience with deploying applications into an IBM WebSphere® Application Server environment.

## Publications

Read the descriptions of the IBM Tivoli Federated Identity Manager library, the prerequisite publications, and the related publications to determine which publications you might find helpful. The section also describes how to access Tivoli publications online and how to order Tivoli publications.

### IBM Tivoli Federated Identity Manager library

The publications in the IBM Tivoli Federated Identity Manager library are:

- *IBM Tivoli Federated Identity Manager Quick Start Guide*

  Provides instructions for getting started with IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager Installation Guide*

  Provides instructions for installing IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager Configuration Guide*

  Provides instructions for configuring IBM Tivoli Federated Identity Manager.
- *IBM Tivoli Federated Identity Manager Administration Guide*

  Provides instructions for completing administration tasks that are required for all deployments.
- *IBM Tivoli Federated Identity Manager Web Services Security Management Guide*

  Provides instructions for completing configuration tasks for Web services security management.

- *IBM Tivoli Federated Identity Manager Auditing Guide*

  Provides instructions for auditing IBM Tivoli Federated Identity Manager events.
- *IBM Tivoli Federated Identity Manager Error Message Reference*

  Provides explanations of the IBM Tivoli Federated Identity Manager error messages.
- *IBM Tivoli Federated Identity Manager Troubleshooting Guide*

  Provides troubleshooting information and instructions for problem solving.

You can obtain the publications from the IBM Tivoli Federated Identity Manager Information Center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html

## Prerequisite publications

To use the information in this book effectively, you should have some knowledge about related software products, which you can obtain from the following sources:

- Tivoli Access Manager Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml
- IBM WebSphere Application Server Version 8.0 Information Center:

  http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp

  You can obtain PDF versions of the IBM WebSphere Application Server documentation at:

  http://www.ibm.com/software/webservers/appserv/was/library/

## Related publications

You can obtain related publications from the IBM Web sites:

- *Enterprise Security Architecture Using IBM Tivoli Security Solutions*. This book is available in PDF (Portable Document Format) at http://www.redbooks.ibm.com/redbooks/pdfs/sg246014.pdf or in HTML (Hypertext Markup Language) at http://www.redbooks.ibm.com/redbooks/SG246014/
- *Federated Identity Management and Web Services Security with IBM Tivoli Security Solutions* (SG24-6394-01). This book is available in PDF at http://www.redbooks.ibm.com/redbooks/pdfs/sg246394.pdf or in HTML at http://www.redbooks.ibm.com/redbooks/SG246394/
- The Tivoli Software Library provides a variety of Tivoli publications such as white papers, datasheets, demonstrations, redbooks, and announcement letters. The Tivoli Software Library is available on the Web at: http://publib.boulder.ibm.com/tividd/td/tdprodlist.html
- The *Tivoli Software Glossary* includes definitions for many of the technical terms related to Tivoli software. The *Tivoli Software Glossary* is available at http://publib.boulder.ibm.com/tividd/td/tdprodlist.html

## Accessing terminology online

The IBM Terminology Web site consolidates the terminology from IBM product libraries in one convenient location. You can access the Terminology Web site at http://www.ibm.com/software/globalization/terminology

## Accessing publications online

IBM posts publications for this and all other Tivoli products, as they become available and whenever they are updated, to the Tivoli Information Center Web site at http://publib.boulder.ibm.com/infocenter/tivihelp/v3r1/index.jsp.

**Note:** If you print PDF documents on other than letter-sized paper, set the option in the **File → Print** window that allows Adobe Reader to print letter-sized pages on your local paper.

## Ordering publications

You can order hard copies of some publications.

**Many countries provide an online ordering service.**

Follow these steps to access this service:

1. Go to http://www-947.ibm.com/support/entry/portal/Documentation
2. Select **IBM Publications Center** from **Getting Started**.
3. Select your country from **Select a country/region/language to begin** and click the arrow icon.
4. Follow the instructions for how to order hard copy publications on Welcome to the IBM Publications Center.

**If your country does not provide an online ordering service, contact your software account representative to order publications.**

Follow these steps to find your local contact:

1. Go to http://www.ibm.com/planetwide/
2. Click your country name to display a list of contacts.

# 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 information center at http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html.

# Tivoli technical training

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

# Support information

If you have a problem with your IBM software, you want to resolve it quickly. IBM provides the following ways for you to obtain the support you need:

**Online**

Go to the IBM Software Support site at http://www.ibm.com/software/support/probsub.html and follow the instructions.

**IBM Support Assistant**

The IBM Support Assistant (ISA) is a free local software serviceability workbench that helps you resolve questions and problems with IBM software products. The ISA provides quick access to support-related information and serviceability tools for problem determination. To install the ISA software, see the *IBM Tivoli Federated Identity Manager Installation Guide*. Also see: http://www.ibm.com/software/support/isa.

**Troubleshooting Guide**
For more information about resolving problems, see the *IBM Tivoli Federated Identity Manager Troubleshooting Guide*.

## Conventions used in this book

This reference uses several conventions for special terms and actions and for operating system-dependent commands and paths.

### Typeface conventions

This publication 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: titles of publications, 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

### Operating system-dependent variables and paths

This publication uses the UNIX convention for specifying environment variables and for directory notation.

When using the Windows command line, replace $*variable* with % *variable*% for environment variables and replace each forward slash (/) with a backslash (\) in directory paths. The names of environment variables are not always the same in the Windows and UNIX environments. For example, %TEMP% in Windows environments is equivalent to $TMPDIR in UNIX environments.

**Note:** If you are using the bash shell on a Windows system, you can use the UNIX conventions.

# Chapter 1. Getting started

This topic summarize how to use each of the sections in this book. You will learn how to plan the installation, complete the installation, plan the configuration, and complete the configuration.

## Overview of deployment scenarios

Tivoli Federated Identity Manager federates user identities across multiple security infrastructures. It supports the creation and management of federated single sign-on environments. Tivoli Federated Identity Manager also extends the power of authorization decision software with web services standards.

Tivoli Federated Identity Manager supports the several deployment scenarios. Each deployment addresses a scenario that requires the secure handling of user identities in a distributed networking environment. You can install, configure, and administer each of the following scenarios independently.

**Federated single sign-on environments**

Tivoli Federated Identity Manager supports creating and managing federated single sign-on environments.

This scenario requires installing and configuring the software into an environment that is populated by additional servers and applications.

**Web services security management**

This scenario does not require deploying a federated single sign-on environment. IBM Tivoli Access Manager evaluates user requests for access to resources across companies and secure domains. User requests are in messages that adhere to web services standards.

Tivoli Federated Identity Manager processes the messages to provide authorization decisions. It can decide for other applications that deliver resources to the user, such as a WebSphere Application Server application.

**Note:** This scenario also provides federation capabilities by accepting identities from different domains.

**Tivoli Federated Identity Manager provisioning**

This scenario extends existing provisioning solutions across the Internet through web services standards. The scenario is separate from federated single sign-on, but it supports managing user identities in single sign-on environments.

**Identity token exchange**

The identity token exchange scenario supports transferring user credential information between different types of identity tokens. Tokens store authentication and authorization properties for users. There are several types of tokens. Each token uses a unique format and structure.

Many scenarios require transferring the information in one token to a token of another format. Doing so makes the authentication and authorization processes used by a specific deployment scenario accessible.

Tivoli Federated Identity Manager provides a security token service (STS) that supports a wide range of token types. The STS can exchange token types and perform modifications to token contents (for example, identity mapping) as needed.

**User Self Care**

This scenario provides a method for provisioning users into business-to-consumer environments. It provisions by supplying a set of operations for users to create and administer their own accounts. The operations include:

- Creating an account
- Creating and updating attributes associated with the account
- Changing passwords
- Recovering forgotten user IDs and passwords
- Deleting accounts

## Resources for planning a deployment

IBM supplies numerous resources to help your company develop a network deployment architecture that is appropriate for your business requirements.

Before installing and configuring Tivoli Federated Identity Manager, obtain the requirements and design for your environment. Typically, your security architect can provide this information.

Developing the requirements and designs involves making several business policy and technology decisions. This guide does not describe how to develop business policies, plan network architecture, or choose a web single sign-on protocol. Your architect must complete that process before you install and deploy Tivoli Federated Identity Manager.

Here are some resources for additional information:

- The IBM Redbook *Federated Identity Management with IBM Tivoli Security Solutions*.

  Use this document during the planning process. You can obtain it and other useful whitepapers from the IBM website.
- The IBM WebSphere Application Server Information Center on the IBM website.

  This site contains many publications and topics that describe strategies for the development and deployment of distributed applications.
- The IBM Tivoli Access Manager for e-business Information Center.

  This site contains publications that focus on how to securely manage user authentication and authorization in distributed network environments. You can access both product documentation and Redbooks®. These documents describe how Tivoli Access Manager defines and secures protected objects and user identities.
- Web services standards.

  Tivoli Federated Identity Manager, and the web services security management component in particular, support several open web services standards, such as WS-Security. For additional information about web services standards, see

  http://www.ibm.com/developerworks/webservices/standards/
- Services-oriented architecture.

  For information about service-oriented architecture from IBM, see http://www.ibm.com/soa

## Overview of installation and configuration

Installation and configuration tasks are specific to the product scenarios that you deploy.

You can view installation and configuration as separate tasks. Installing Tivoli Federated Identity Manager is separate from configuring files to support one or more features. This structure facilitates deployment across multiple computers in a distributed environment.

This guide describes how to:
- Install all of the scenarios.
- Configure federated single sign-on and token exchange.
- Deploy Tivoli Federated Identity Manager to support web services security management.

You are directed to other documentation for:
- The remainder of the Web services security management deployment instructions.
- Configuration instructions for federated identity provisioning.

The following topics provide an overview of the installation and configuration of each scenarios:
- "Overview of installation and configuration of federated single sign-on"
- "Overview of installation and configuration of web service security management" on page 4
- "Overview of installation and configuration of federated identity provisioning" on page 4
- "Overview of installation and configuration of token exchange scenarios" on page 5
- "Overview of installation and configuration of user self care scenarios" on page 5

### Overview of installation and configuration of federated single sign-on

This topic discusses tasks to install and configure federated single sign-on.

Follow this process to install and configure federated single sign-on:
1. Plan the installation. Read the following instructions:
   - Chapter 1, "Getting started," on page 1
   - Chapter 2, "Planning the installation," on page 7
2. Install the Tivoli Federated Identity Manager files. Use the instructions in Chapter 3, "Installing federated single sign-on or token exchange," on page 15.
3. Configure your federated single sign-on environment. The planning and configuration steps are located in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

   The instructions provide topics on how to plan your configuration. The planning steps involve some tasks that are common to all federation deployments. It also includes some tasks that are specific to each type of single sign-on federation.

Read the planning topics that apply to your environment before you begin any configuration. The planning topics describe the data and properties that you must supply to complete the configuration. You must know the values for all the required properties.

The management console provides wizards that guide you through the main tasks of creating a federation and adding a partner. There are additional tasks that require the exchange of configuration information between you and your IBM Business Partner. These tasks must be accomplished manually.

## Overview of installation and configuration of web service security management

Tivoli Federated Identity Manager can be deployed to provide web service security management, through installation and configuration of the web service security management feature.

Follow this process to install and configure web service security management:

1. Plan the installation. Read the following instructions:
   - Chapter 1, "Getting started," on page 1
   - Chapter 2, "Planning the installation," on page 7
2. Install Tivoli Federated Identity Manager.
   a. Follow the instructions in Chapter 4, "Installing Web services security management," on page 33.
   b. Choose one of the installation methods. See "Installation modes" on page 11.
3. Configure the web services security management environment.

   Establishing a Tivoli Federated Identity Manager domain is the first step.

   **Note:** Additional configuration steps vary depending on the deployment architecture. The steps can include:
   - Configuring WebSphere Application Server security.
   - Deploying the web service security management application into a Tivoli Access Manager environment.
   - Creating a Tivoli Federated Identity Manager trust service module chain.

   a. Establish a Tivoli Federated Identity Manager domain. See *IBM Tivoli Federated Identity Manager Configuration Guide*.
   b. Complete the configuration of a web services security management environment. See *IBM Tivoli Federated Identity Manager Web Services Security Management Guide*.

## Overview of installation and configuration of federated identity provisioning

This topic discusses tasks to install and configure the WS-Provisioning runtime feature.

Follow this process to install and configure federated identity provisioning:

1. Plan the installation. Read the following instructions:
   - Chapter 1, "Getting started," on page 1
   - Chapter 2, "Planning the installation," on page 7
2. Install Tivoli Federated Identity Manager files. See Chapter 5, "Installing federated provisioning," on page 39.

3. Configure your federated identity provisioning environment.

   Deploying a federated identity provisioning environment is often done after creating a federated single sign-on environment.

   After you deploy a single sign-on federation, no additional topics in this guide are required. To configure a federated identity provisioning environment, see *IBM Tivoli Federated Identity Manager Administration Guide*.

## Overview of installation and configuration of token exchange scenarios

Tivoli Federated Identity Manager can provide token exchange services when you install and configure the security token service.

The security token service is part of the Tivoli Federated Identity Manager management service and runtime component. This component provides core features, many of which are used in multiple deployment scenarios.

Installing components for token exchange scenarios is identical to the installation for federated single sign-on scenarios. Configuring those components are specific to the scenario type.

Follow this process to install and configure token exchange scenarios:

1. Plan the installation. Read the following instructions:
   - Chapter 1, “Getting started,” on page 1
   - Chapter 2, “Planning the installation,” on page 7
2. Install the Tivoli Federated Identity Manager files. See Chapter 3, “Installing federated single sign-on or token exchange,” on page 15.
3. Configure your token exchange scenario.

   Configuration instructions for a token exchange scenario are specific to:
   - The type of tokens to be exchanged.
   - The deployment environment, including the integration of Tivoli Federated Identity Manager with other products.

   All deployments require establishing a Tivoli Federated Identity Manager domain (management service). They also require deploying the Tivoli Federated Identity Manager runtime. The configuration instructions for token exchange guide you through these configuration tasks.

   The configuration instructions describe how to deploy the security token service modules that support Kerberos constrained delegation. This deployment includes Tivoli Access Manager WebSEAL Kerberos junctions. The junctions secures access to web servers.

   The deployment is specific to an environment that includes Microsoft integrated authentication (SPNEGO) for Kerberos tokens. IBM WebSphere Application Server is also deployed. You must configure it to support Tivoli Federated Identity Manager and to interact with the Microsoft environment.

   See the configuration steps in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

## Overview of installation and configuration of user self care scenarios

You can install User Self Care as part of a Tivoli Federated Identity Manager installation.

User Self Care is part of the Tivoli Federated Identity Manager management service and runtime component. This component provides core features, many of which are used in multiple deployment scenarios.

Installing components for user self care scenarios is identical to the installation for federated single sign-on scenarios. Configuring those components are specific to the scenario type.

Follow this process to install and configure user self care scenarios:

1. Plan the installation. Read the following instructions:
   - Chapter 1, “Getting started,” on page 1
   - Chapter 2, “Planning the installation,” on page 7
2. Install the Tivoli Federated Identity Manager files. See Chapter 3, “Installing federated single sign-on or token exchange,” on page 15. These instructions apply to User Self Care.

# Chapter 2. Planning the installation

Before installing Tivoli Federated Identity Manager, plan your environment and understand the product requirements.

Complete the following planning tasks:

1. Review the list of software that is distributed with Tivoli Federated Identity Manager. The distribution also includes prerequisites products.

   See "Software packaging."
2. Check with your procurement group to determine which of the following product licenses your company purchased:
   - IBM Tivoli Federated Identity Manager

     Includes the Tivoli Federated Identity Manager and Tivoli Access Manager software. Users can create a federation for multiple partner connections using this license.
   - IBM Tivoli Federated Identity Manager Business Gateway

     Includes only the Tivoli Federated Identity Manager software. Users can create a federation for multiple partner connections using this license. This license is also useful for organizations that already have Tivoli Access Manager in their computing environment.

     The Tivoli Federated Identity Manager Business Gateway documentation is a subset of the Tivoli Federated Identity Manager 6.2.2 documentation.
   - IBM Tivoli Federated Identity Manager Business Gateway for Single Partner

     Includes only the Tivoli Federated Identity Manager software which can create a federation for a single partner connection. This license is also useful for organizations that already have Tivoli Access Manager in their computing environment.

     The Tivoli Federated Identity Manager Business Gateway for Single Partner documentation is a subset of the Tivoli Federated Identity Manager 6.2.2 documentation.
3. Review the installation components and learn how they deploy individual features.

   See "Installation components" on page 8.
4. Decide which installation mode you want to employ.

   See "Installation modes" on page 11.
5. Make sure that you have the required access privileges.

   See "Required access privileges" on page 12.

## Software packaging

Tivoli Federated Identity Manager is distributed as a group of CDs or downloadable ISO images.

The software package includes the following software:

- Tivoli Federated Identity Manager
- IBM WebSphere Application Server Network Deployment
- IBM Tivoli Access Manager for e-business
- IBM Tivoli Directory Integrator

For a list of the ISO images in the product distribution, see the product page on the IBM Passport Advantage® website: http://www-01.ibm.com/support/docview.wss?uid=swg24031050.

The Hardware and Software requirements topic in the product information center provides a list of the supported versions for the prerequisite software. See http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html.

**Attention:** There might be issues when installing the product into a Windows operating system set to Turkish. To avoid problems, set the operating system to a language other than Turkish. After installing the product, you can change the language of the operating system back to Turkish.

## Installation components

Tivoli Federated Identity Manager has several components that you can install separately.

The installation components are:

- Management service and runtime
- Management console
- Federated provisioning
- Web services security management
- IBM Support Assistant

You can install all the components on one computer, or you can install them on multiple computers. Installations on one computer are typical for prototype or test environments. Installations across multiple computers are typical in production environments.

The software prerequisites vary for each component. Some software prerequisites must be on the same host (server). Other software prerequisites can be distributed across the network.

**Management service and runtime**

This component serves two functions:

- Provides the basic management service and runtime. Federated single sign-on, web services security management, and federated provisioning use it.
- Contains the federated single sign-on feature.

All installations require the management service and runtime. They are always installed together.

**Management console**

Administers all components. The console is often installed on the same computer as the management service and runtime. You can install the console on a different computer.

The WebSphere Application Server is a prerequisite. It is a plug-in to the Integrated Solutions Console, which is the management console that is built into the WebSphere Application Server. Before installing the Tivoli Federated Identity Manager management console, install WebSphere Application Server on the same computer.

The management console is not required to be on the same computer as the web services security management component or the federated provisioning component.

The typical deployment scenarios for the console are:

- *On the same system as the management service and runtime.*

  The WebSphere Application Server system that hosts the Tivoli Federated Identity Manager management service also hosts other WebSphere applications.
- *On a different system from the management service and runtime.*

  All management console plug-ins run from a computer that is dedicated to administering all WebSphere applications. Tivoli Federated Identity Manager is one of these applications.

  The administrator installs only the Tivoli Federated Identity Manager management console on the computer. The Tivoli Federated Identity Manager management service and runtime are on another computer.

**Federated provisioning**

Deployment of federated provisioning depends on deployment of the management service and runtime. The management service and runtime are not required to be on the same computer as the provisioning component.

The management console is on the same computer.

**Web services security management**

Deployment of web services security management depends on the management service and runtime deployment. The management service and runtime are not required to be on the same computer as the web services security management component.

The management console is not required to be on the same computer.

**IBM Support Assistant**

A software serviceability workbench that helps you resolve questions and problems with IBM software products. It has no dependencies on any Tivoli Federated Identity Manager components.

## Using the components to deploy product features

Deploying each feature requires installing more than one component. You can either:

- Install all the required components on one computer, or
- Distribute the components across the multiple computers.

These common scenarios for deploying the components are based on the product features:

**Federated single sign-on**

Required components for a single computer deployment:

- Management service and runtime
- Management console

Required components for distributed deployment:

- Management service and runtime on one computer
- Management console on another computer

The web services security management component is not used with federated single sign-on. The federated provisioning component is not required for deploying federated single sign-on.

**Web services security management**

Required components for a single computer deployment:

- Management service and runtime
- Management console
- Web services security management

Options for distributed deployment:

- Management service, runtime, and web services security manager on one computer. Management console on a separate computer.

  Use this option to separate administration activities (console) from runtime activity.
- Management service, runtime, and management console on one computer. Web services security manager on a separate computer.
- Each component on a separate computer:
  - Management service and runtime (computer 1)
  - Management console (computer 2)
  - Web services security manager (computer 3)

**Federated provisioning**

Required components for a single computer deployment:

- Management service and runtime
- Management console
- Federated provisioning

Options for distributed deployment:

- Management service, runtime, and federated provisioning on one computer. Management console on a separate computer.

  Use this option to separate administration activities (console) from runtime activity.

**Identity token exchange**

Required components for a single computer deployment:

- Management service and runtime
- Management console

Required components for distributed deployment:

- Management service and runtime on one computer
- Management console on another computer

The web services security management component and the federated provisioning component are not required.

**User self care**

Required components for a single computer deployment:

- Management service and runtime
- Management console

Requirements for distributed deployment:

- Management service and runtime on one computer
- Management console on another computer

The web services security management component is not used. The federated provisioning component is not required.

When planning the component deployment, keep in mind:

- You must deploy the management console into the environment (either locally or remotely) when deploying any components.
- Each Tivoli Federated Identity Manager component has different software prerequisites. Assemble the required software prerequisites as needed for each computer.

  The software prerequisites are described in topics specific to the installation of each component.

# Installation modes

Before beginning the installation, become familiar with how the features can be installed and choose an installation mode.

The Tivoli Federated Identity Manager installation supports two interactive modes and one silent mode. The interactive modes consist of a graphical mode and a console (text-based) mode.

## Graphical mode

In this mode, each installation presents a series of panels that prompt for the required information. Each panel has online help. Commands to start the installation are platform-specific.

*Table 1. Commands to start the installation program in graphical mode*

| **Platform** | **Command to start the installation program** |
|---|---|
| AIX® | `install_aix_ppc.bin` |
| Linux on Power Systems™ | `install_linux_ppc.bin` |
| Linux on System x® | `install_linux_x86.bin` |
| Linux on System z® | `install_linux_s390.bin` |
| Solaris | `install_sol_sparc.bin` |
| Windows | `install_win32.exe` |

## Console mode

Use the *console mode* to install the product in a non-graphical environment, such as a server system without a video card. Console mode installation accomplishes the same tasks and requires the same user input as the graphical mode.

Commands to start the installation are platform-specific. Choose console mode by adding `-console` as a command-line option.

*Table 2. Commands to start the installation program in console mode*

| **Platform** | **Command to start the installation program** |
|---|---|
| AIX | `install_aix_ppc.bin -console` |
| Linux on Power Systems | `install_linux_ppc.bin -console` |

Table 2. Commands to start the installation program in console mode (continued)

| Platform | Command to start the installation program |
|---|---|
| Linux on System x | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe -console` |

### Silent mode

The *silent mode* installation reads input values from a script file with a common set of options. To use silent mode, you must first create a file that contains the input values. This file is called a *response file*.

Silent mode is typically not used for the initial product installation. Use one of the interactive modes (graphical or console) for initial installation and create the response file from the results. See Chapter 8, "Using silent mode installation," on page 55.

## Required access privileges

To install Tivoli Federated Identity Manager, you must have read/write permission for the installation location.

Security features on the system where you want to install the product might require you to log in with a user name and password.

If you are installing Tivoli Federated Identity Manager on an existing version of WebSphere Application Server with security enabled, you must provide the following information:

- Administrator user name
- Administrator password
- Truststore file location
- Truststore password
- Keystore file location (optional)
- Keystore password (optional)

You must also be able to write to the `/lib` and `/plugins` subdirectories in WebSphere Application Server.

For example:

**AIX**

```
/usr/IBM/WebSphere/AppServer/lib
/usr/IBM/WebSphere/AppServer/plugins
```

**Linux, or Solaris**

```
/opt/IBM/WebSphere/AppServer/lib
/opt/IBM/WebSphere/AppServer/plugins
```

**Windows**

```
C:\Program Files\IBM\WebSphere\AppServer\lib
C:\Program Files\IBM\WebSphere\AppServer\plugins
```

**Attention:** Installing the product as a user other than the root or Administrator user might require additional steps. See Appendix G, “Installing as a user other than root or administrator,” on page 87.

# Chapter 3. Installing federated single sign-on or token exchange

You must complete several tasks to install federated single sign-on or token exchange. The tasks in this section apply to both scenarios.

In the token exchange scenario, Tivoli Federated Identity Manager uses the security token service to exchange user credentials between different token formats. An example of this scenario is deploying the Kerberos constrained delegation trust modules in an environment with WebSEAL junctions.

**Note:** Tivoli Federated Identity Manager supports OAuth 1.0 and OAuth 2.0 protocols. Installing the federated single sign-on also installs the OAuth 1.0 and 2.0 features.

Complete the following tasks:

1. “Planning the installation of the federated single sign-on feature”
2. “Installing prerequisites for federated single sign-on” on page 17
3. “Runtime and management service installation worksheet” on page 25
4. “Installing the federated single sign-on feature” on page 29

## Planning the installation of the federated single sign-on feature

Federated single sign-on requires you to install the management console and the management service and runtime components.

**Management service and runtime**
Provides basic Tivoli Federated Identity Manager functions, such as management of domains and keys. This component also provides the implementation of federated single sign-on.

**Management console**
Provides a management or administration interface for Tivoli Federated Identity Manager domains. This component is a plug-in to the WebSphere Application Server administration console.

**Note:** Federated single sign-on does not require the Tivoli Federated Identity Manager web services security management or federated provisioning components.

Each component has software prerequisites.

### Software prerequisites for the runtime and management service component

The runtime and management service component requires WebSphere Application Server. In some deployment scenarios, Tivoli Access Manager for e-business is also required.

The runtime and management service deploys all Tivoli Federated Identity Manager features. The software prerequisites vary depending on which feature you deploy.

- WebSphere Application Server is required for all deployments of Tivoli Federated Identity Manager.

- Tivoli Access Manager for e-business is required for deployments that use WebSEAL as a point of contact server.

## WebSphere Application Server

**Note:** WebSphere Application Server Version 6.1 and later are supported.

Tivoli Federated Identity Manager is implemented as a WebSphere Application Server application. You must deploy WebSphere Application Server on the same computer before installing the management service and runtime components.

Tivoli Federated Identity Manager can use either the Embedded or Network Deployment version. Most deployments use Network Deployment.

**WebSphere Application Server Network Deployment**

Supports WebSphere applications and deploys WebSphere clusters. The product distribution includes a CD or ISO image of this product.

**Note:** Each major release is supplemented by Refresh and Fix Packs. Tivoli Federated Identity Manager requires the installation of specific Refresh or Fix Packs. To view the required Refresh and Fix Packs, see the topic Hardware and Software Requirements in the Tivoli Federated Identity Manager Information Center.

**Embedded WebSphere Application Server**

Contains an administration console that is a subset of the full WebSphere Application Server administration console. It supports the Tivoli Federated Identity Manager management console component when it is deployed on a separate computer that already has WebSphere Application Server. This version:

- Is not released as a separate product. It has embedded functions in other products.
- Is a lightweight and easily deployed.
- Is primarily intended to provide application support.
- Does not support true WebSphere clustering.

This product is intended for deployments that require minimal WebSphere Application Server administration.

This scenario can include simple deployments that implement only one WebSphere application or small deployments, such as prototypes, test systems, or proof of concept. It typically is not used in large-scale or production deployments because it does not support clusters.

## IBM Tivoli Access Manager for e-business

Tivoli Federated Identity Manager separates authenticating users and evaluating user authorities (permissions to access resources) from federating identities and authorities. This separation makes it possible to use other products for processing authentication and authorization of user requests (assertions).

Tivoli Federated Identity Manager provides authentication and authorization functions by working with IBM Tivoli Access Manager for e-business.

The management service interacts with the IBM Tivoli Access Manager for e-business policy and authorization servers. Through these servers, the management service resolves requests for user information that is stored in user registries. IBM Tivoli Access Manager for e-business manages these registries.

For federated single sign-on, the management service requires the IBM Tivoli Access Manager for e-business WebSEAL server when WebSEAL is the point of contact server. This reverse proxy server acts as the point of contact for routing requests and responses to and from Tivoli Federated Identity Manager.

**Note:** The management service is also used in scenarios where IBM Tivoli Access Manager for e-business is not required. These scenarios include federated single sign-on with WebSphere as the point of contact server and scenarios for web service security management.

Each major release of IBM Tivoli Access Manager for e-business is supplemented by Fix Packs. Tivoli Federated Identity Manager might require specific Fix Packs.

To view the required Fix Packs, see the topic Hardware and Software Requirements on the Tivoli Federated Identity Manager Information Center.

### Software prerequisites for the management console component

The management console component provides a management or administrative interface for managing Tivoli Federated Identity Manager domains. The console is a plug-in to the administrative console in WebSphere Application Server.

This component is in the same installation image (CD or ISO image) as the management service and runtime component. You can install the management console at the same time as management service and runtime.

You can install the management console on the same computer as the management service and runtime or on a separate computer. Some deployments prefer to separate administration activities from runtime activities. For these deployments, install the management console on a computer that hosts none of the other Tivoli Federated Identity Manager components.

The management console depends on the WebSphere Application Server administrative console. You can:

- Install Network Deployment on the same computer before you install the management console.
- Install the Embedded WebSphere Application Server on the same computer as the management console. This version is part of the Tivoli Federated Identity Manager installation. You can specify the embedded version with the graphical user installation for the management console and install it at the same time.

**Note:** For more information about the Embedded and Network Deployment, see “Software prerequisites for the runtime and management service component” on page 15.

## Installing prerequisites for federated single sign-on

Learn how to install the software prerequisites for the Tivoli Federated Identity Manager federated single sign-on feature.

## Installing WebSphere Application Server

Tivoli Federated Identity Manager is deployed as an application into a WebSphere environment. It runs as an application in either a stand-alone server environment or a Network Deployment cluster.

### About this task

In both deployment environments, you must install the prerequisite Refresh Pack and Fix Packs. In the cluster environment, you must install the Network Deployment and deploy the cluster before adding Tivoli Federated Identity Manager.

**Note:** If you have an existing Network Deployment, a new installation is not required. If you have an existing deployment, make sure to apply all the requiredWebSphere Application Server Fix Packs. See "Installing WebSphere Application Server Refresh Packs and Fix Packs" on page 20.

**Note:** When installing the product on separate WebSphere profiles (such as `AppSrv01` and `AppSrv02`), provide different server names for each profile. For example, if you name the server on the first profile `server1`, then name the server on the second profile `server2`.

**Note:** If you plan to run Tivoli Federated Identity Manager on servers managed by a deployment manager, you only need to install Tivoli Federated Identity Manager once for each deployment manager. In this case, you do not need to install Tivoli Federated Identity Manager on each node that is managed by a deployment manager. This applies for both single servers and clusters managed by a deployment manager.

You should only install Tivoli Federated Identity Manager into an application server profile for scenarios where that profile is not federated into a cell, for example, when it is a stand-alone server that has its own Administration console.

### Installing WebSphere Application Server for Network Deployment

IBM WebSphere Application Server Network Deployment is distributed with Tivoli Federated Identity Manager. The instructions in this topic apply to both stand alone server profile or cluster profile deployments.

### Procedure

1. Take one of the following actions:
   - Access the IBM WebSphere Application Server Network Deployment CD for your operating system.
   - Extract the image that you downloaded from Passport Advantage.
2. Run the WebSphere installation script.
   - AIX, Solaris, or Linux: `./launchpad.sh`
   - Windows `C:\launchpad.bat`

   Installation notes:
   - Remember the installation directory that you specify. You must supply it when you install Tivoli Federated Identity Manager management service and runtime.
   - The WebSphere **Core product files** are required. Additional WebSphere packages are optional.
3. Select **Launch the Profile creation wizard**.

4. Select **Create an Application Server profile**. The software creates a profile name, profile directory, node name, and host name.
5. Specify the SOAP connector port. The default port is 8880. If you change it, remember the new port number. The Tivoli Federated Identity Manager runtime installation prompts you to confirm this value.
6. Optional: Take the following actions:
   a. Select the **Launch the First steps console**.
   b. Click **Finish**.
   c. Select **Installation Verification**. The system returns information similar to the following line:

   ```
   ADMU3000I: Server server1 open for e-business; process id is 1991
   ```

   d. You can access the `SystemOut.log` file to monitor WebSphere Application Server startup and execution. Example locations:

| Operating system | Example location |
|---|---|
| AIX | `# /usr/IBM/WebSphere/AppServer/profiles/default/logs/server1/SystemOut.log` |
| Solaris or Linux | `# /opt/IBM/WebSphere/AppServer/profiles/default/logs/server1/SystemOut.log` |
| Windows | `C:\Program Files\IBM\WebSphere\AppServer\profiles\default\logs\server1\SystemOut.log` |

7. Verify that you can use the administrative console.
   a. Use a browser to access the console URL. For example, if the host name is `idp.example.com`:

   `http://idp.example.com:9060/admin`

   b. The software prompts you to log on to the administration application. If you do not see the prompt, the application server is not running correctly. Leave **User ID** blank and click **Login** to access the administrative console Welcome page.
8. Record your values for the installation properties in the following table.

| Property | Default value | Your value |
|---|---|---|
| Installation directory | • AIX<br>`/usr/IBM/WebSphere/AppServer`<br>• Solaris or Linux<br>`/opt/IBM/WebSphere/AppServer`<br>• Windows<br>`C:\Program Files\IBM\WebSphere\AppServer` | |
| SOAP port | 8879 | |

### What to do next

Go to "Installing WebSphere Application Server Refresh Packs and Fix Packs."

## Installing WebSphere Application Server Refresh Packs and Fix Packs

If WebSphere Application Server is already installed, apply the required Fix packs and Refresh packs.

### Before you begin

Check the lists of required Fix and Refresh packs. See the Hardware and Software Requirements link in the Tivoli Federated Identity Manager Information Center. http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html.

### About this task

You can download the Refresh Pack and Fix Packs from the IBM Support website.

### Procedure

1. Access the WebSphere Application Server support site:

   `http://www.ibm.com/software/webservers/appserv/was/support/`
2. Select **Fixes by version** in the Download section to see a comprehensive list of fixes.
3. Select the link for your version.
4. Select **Download information** for instructions on how to download and install the fixes.

### What to do next

Take one of the following actions:

- For a stand-alone server (application server profile), go to "Installing Tivoli Access Manager" on page 22.
- For a cluster environment, go to "Installing a WebSphere Application Server cluster."

## Installing a WebSphere Application Server cluster

You must install the WebSphere Application Server cluster before you can install Tivoli Federated Identity Manager.

### Before you begin

You must install the WebSphere Application Server. If you have not done so, see the following topics:

- "Installing WebSphere Application Server for Network Deployment" on page 18
- "Installing WebSphere Application Server Refresh Packs and Fix Packs"

### About this task

Tivoli Federated Identity Manager is an application in a WebSphere cluster.

You can configure WebSphere clusters several ways, depending on many factors including the deployment topology. This section provides the process for a simple cluster with one node (one application server). Consult the WebSphere Application Server documentation for instructions that apply to your environment.

You can access online topics about WebSphere Application Server at the information center: http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp.

You can access information in book form at the WebSphere Application Server library: http://www.ibm.com/software/webservers/appserv/was/library/.

## Procedure

1. Use the **Profile Creation** wizard to create a deployment manager profile.
2. Use the **First Steps** console to start the deployment manager.
3. Use the **Profile Creation** wizard to create an Application Server profile.
4. Use either the **First Steps** console or the **startServer** command to start the application server.
5. Click **System Administration** > **Nodes** to add the application server node. The node goes in the cell on administrative console of the deployment manager.
6. Install the IBM HTTP Server.
   a. Install the WebSphere Application Server web server plug-ins.
   b. Configure the web server with the **Plug-ins installation** wizard. The wizard creates a script named `configure`*`your_Web_server_name`* in the *`plugins_install_root`*`/bin` directory.
   c. Run the script to create a web server definition in the administrative console. You can then use the administration console to manage the web server.
7. Open a browser and log on to the WebSphere console:

   `http://`*`your_WebSphere_Deployment_Manager_host_name`*`:9060/ibm/console`
8. Select **Servers** > **Clusters**.
9. Click **New** in the Server Cluster page.
10. Enter the information requested by the Create New Cluster wizard.
    a. Specify a cluster name. For example, `fimCluster`.
    b. Select the **Create a replication domain** check box.
    c. Select **Select an existing server to add**. Ensure that the server you created, such as `server1`, is shown in the menu.
    d. Click **Next**.
11. (Optional) Create additional cluster members, if necessary, by specifying a name and mode for each member.
12. Click **Next**.
13. Click **Finish** to create the cluster.
14. Click **Save**.
15. Select **Synchronize changes with Nodes** on the Server Cluster page.
16. Click **Save**.

### Results

This process completes the WebSphere cluster configuration that is required to install Tivoli Federated Identity Manager.

### What to do next

After you install Tivoli Federated Identity Manager:

- Create a Tivoli Federated Identity Manager domain.
- Deploy the runtime application. There are additional configuration instructions for deploying the runtime into the WebSphere cluster.

## Installing Tivoli Access Manager

Some Tivoli Federated Identity Manager federated single sign-on deployments require Tivoli Access Manager for e-business components. These components are used by the runtime and management services component. They are not needed for the management console.

The information in this section applies to Tivoli Federated Identity Manager package users.

Tivoli Access Manager for e-business components:

- Are required for a single sign-on federation with WebSEAL as a point of contact server.
- Are not required for a single sign-on federation with WebSphere as a point of contact server.
- Are not required for a Tivoli Federated Identity Manager single sign-on federation with WebSphere as a point of contact server

Tivoli Federated Identity Manager supports Tivoli Access Manager for e-business Versions 6.1, 6.0, and 5.1.

The Hardware and Software requirements link on the Tivoli Federated Identity Manager information center lists required Tivoli Access Manager for e-business fix packs.

For IBM Tivoli Access Manager for e-business documentation, see:

http://www.ibm.com/software/tivoli/products/access-mgr-e-bus/

### Installing a user registry

Tivoli Access Manager requires access to a user registry.

The information in this section applies to Tivoli Federated Identity Manager package users.

Tivoli Access Manager supports several user registries. The user registries that Tivoli Federated Identity Manager can use are listed in its Information Center. See the Hardware and Software requirements link: http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html

**Note:** When you deploy federated single sign-on, some of the supported protocols require an alias service when interacting with the user registry. Tivoli Federated Identity Manager supplies a default alias service for LDAP user registries.

For other registry types such as Microsoft Active Directory, Lotus® Domino®, and Novell eDirectory, you must develop a custom alias service.

## Installing a policy server and authorization server

Install and configure a policy server and an authorization server for each Tivoli Access Manager secure management domain.

The information in this section applies to Tivoli Federated Identity Manager package users.

The Tivoli Federated Identity Manager domain configuration uses several options that you specify when installing the policy and authorization servers. Table 3 lists those settings.

*Table 3. Policy server and authorization server settings that are used during Tivoli Federated Identity Manager configuration*

| **Tivoli Access Manager setting** | **Description** |
|---|---|
| Administrator ID | The identifier for the administrator account of the management domain.<br>The default administrator ID is **`sec_master`**. |
| Administrator password | The password for the administrator account of the management domain |
| Policy Server Hostname | The host name or IP address of the policy server.<br>For example:<br>`ammgr.example.com` |
| Policy Server SSL Port | The port number on which the policy server listens for SSL requests.<br>The default port number is **7135**. |
| Authorization Server Hostname | The host name or IP address of the authorization server.<br>For example:<br>`amacld.example.com` |
| Authorization Server Port | The port number on which the authorization server listens for authorization requests.<br>The default port number is **7136**. |
| Domain | The name of the management domain.<br>The domain enforces security policies for authentication, authorization, and access control. The default domain name is **Default**. |

## Installing a WebSEAL server

A Tivoli Federated Identity Manager domain for federated single sign-on might require a Tivoli Access Manager WebSEAL server as a point of contact server.

The information in this section applies to Tivoli Federated Identity Manager package users.

A single sign-on federation uses several settings from the WebSEAL server installation. Table 4 lists these settings.

*Table 4. WebSEAL settings used when creating a Tivoli Federated Identity Manager single sign-on federation*

| **WebSEAL setting** | **Description** |
|---|---|
| Enable HTTPS access | Specifies whether to enable or disable HTTPS access.<br>The Tivoli Federated Identity Manager configuration prompts you to configure a Point of Contact Server. You can specify either HTTPS or HTTP for the server URL. You can choose HTTPS only if you enabled HTTPS access during WebSEAL configuration. |
| Enable HTTP access | Specifies whether to enable or disable HTTP access.<br>The Tivoli Federated Identity Manager configuration prompts you to configure a Point of Contact Server. You must specify either HTTPS or HTTP for the server URL. You can choose HTTP only if you enabled HTTP access during WebSEAL configuration.<br>**Note:** HTTPS is typically used in Tivoli Federated Identity Manager deployments. |
| Local Host name | The host name of the IBM Tivoli Access Manager for e-business WebSEAL server.<br>For example:<br>`webseal1.example.com`<br>The Tivoli Federated Identity Manager configuration prompts you to configure a Point of Contact Server. **Local host name** must correspond to the Tivoli Federated Identity Manager option **Point of Contact**. |

## Installing Tivoli Access Manager Fix Packs

Tivoli Access Manager is periodically updated with Fix Packs. You must install any Fix Packs that are prerequisites for Tivoli Federated Identity Manager.

The information in this section applies to Tivoli Federated Identity Manager package users.

The current list of Fix Packs is on the Tivoli Information Center. Follow these steps to determine if you must install a Fix Pack:

1. Access the Welcome page for Tivoli Federated Identity Manager:

   http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.2/toc.xml
2. Select **Hardware and Software Requirements**.

**Note:** This release of Tivoli Federated Identity Manager is compatible with older releases of IBM Tivoli Access Manager for e-business. Compatibility depends on the application of specific Fix Packs for each older release. The compatibility requirements are listed in the Hardware and Software Requirements topic.

You can obtain the IBM Tivoli Access Manager for e-business Fix Packs from the product support site.

## Runtime and management service installation worksheet

Installing the runtime and management service component requires you to supply values for certain properties. Use this worksheet to record those values.

### Installation on existing version of WebSphere Application Server

If you install the component on an *existing* version of WebSphere Application Server, you must know if administration security is enabled. An *existing* version is either

- The version supplied by Tivoli Federated Identity Manager that is already installed.
- A compatible version of WebSphere Application Server that is already installed.

**Note:** You cannot change default values from the console after the installation.

*Table 5. Properties for runtime component installation on existing version of WebSphere Application Server*

| Property | Default value | Your value |
|---|---|---|
| **Directory name** | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |
| **When WebSphere Application Server administration security is *not* enabled:** | | |
| **WebSphere Application Server installation directory** | **AIX**<br>`/usr/IBM/WebSphere/AppServer`<br>**Linux or Solaris**<br>`/opt/IBM/WebSphere/AppServer`<br>**Windows**<br>`C:\Program Files\IBM\WebSphere\AppServer` | |
| **WebSphere Application Server SOAP connector port**<br>Specifies the port number on which WebSphere Application Server handles SOAP communication. | `8879` | |

*Table 5. Properties for runtime component installation on existing version of WebSphere Application Server (continued)*

| Property | Default value | Your value |
|---|---|---|
| **Artifact resolution port**<br>Specifies the port for exchanging SOAP messages between partners. For example, this port is used during the retrieval of SAML assertions when the Browser Artifact profile is used.<br>**Attention:** This port *must* be available even if your federation does not use SOAP messages. | `9444` | |
| **Note:** If you previously installed the embedded version, the installation does *not* prompt for the installation directory. | | |
| **When WebSphere Application Server administration security is enabled:** | | |
| **WebSphere Application Server administrator user name** | | |
| **WebSphere Application Server administrator password** | | |
| **SSL Trusted Java™ keystore file**<br>Specifies the truststore file for WebSphere Application Server. | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM/ewas/profiles/itfimProfile/etc/trust.p12`<br>**Windows**<br>`C:\Program Files\IBM\FIM\ewas\profiles\itfimProfile\etc\trust.p12` | |
| **SSL Trusted Java keystore password**<br>Specifies the password for accessing the WebSphere truststore. | `WebAS` | |
| **SSL Java keystore file**<br>Specifies the keystore file for WebSphere Application Server. | | |
| **SSL Java keystore password**<br>Specifies the password for accessing the WebSphere keystore. | | |
| **Note:** If you previously installed the embedded version, the installation prompts for the SSL Java keystore. It does not show the password. | | |

## Installation on embedded version of WebSphere Application Server

**Note:** You cannot change default values from the console after the installation.

*Table 6. Properties for runtime component installation on embedded version of WebSphere Application Server*

| Property | Default value | Your value |
|---|---|---|
| **Directory name** | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |
| **WebSphere Application Server administrator user name** | `fimadmin` | |
| **WebSphere Application Server administrator password** | | |
| **Application server port**<br>Specifies the port number that WebSphere Application Server uses to communicate over HTTP. | `9080` | |
| **Secure application server port**<br>Specifies the port number that WebSphere Application Server uses to communicate over HTTPS. | `9443` | |
| **Administration port**<br>Specifies the port number that the WebSphere Application Server administrative console uses for HTTP. | `9060` | |
| **Secure administration port**<br>Specifies the port number that the WebSphere Application Server administrative console uses for HTTPS. | `9043` | |
| **SOAP port**<br>Specifies the port number on which WebSphere Application Server handles SOAP communication. | `8879` | |

*Table 6. Properties for runtime component installation on embedded version of WebSphere Application Server (continued)*

| Property | Default value | Your value |
|---|---|---|
| **Artifact resolution port**<br>Specifies the port for exchanging SOAP messages between partners. For example, this port is used during the retrieval of SAML assertions when the Browser Artifact profile is used.<br>**Attention:** This port *must* be available even if your federation does not have SOAP messages. | `9444` | |

When you install Tivoli Federated Identity Manager with the embedded version of WebSphere Application Server, the installation program determines if the standard ports are available. The determination is made by examining what ports are currently in use. If default ports are in use, it increments each port value by 1 until all the necessary port values are free. The ports are detected during the initial installation of the embedded version.

If you install additional components at a later time with the embedded version, the installation cannot automatically detect available ports.

If you previously installed the embedded version and want to install an additional component at a later time, select **No** when prompted whether you want to use an existing version of WebSphere Application Server.

## IIS Web plug-in installation worksheet

Use this worksheet to record the values you must supply during the IIS Web plug-in component installation.

*Table 7. Properties for IIS plug-in component installation*

| Property | Default value | Your value |
|---|---|---|
| Directory name | `C:\Program Files\IBM\FIM` | |
| IIS virtual host to configure (Select one or more hosts to configure from a list.) | | |

## Apache or IBM HTTP Server Web plug-in installation worksheet

Use this worksheet to record the values you must supply during the Apache or IHS Web plug-in component installation.

*Table 8. Properties for Apache or IHS plug-in component installation*

| Property | Default value | Your value |
|---|---|---|
| Directory name | `/opt/IBM/FIM` | |

*Table 8. Properties for Apache or IHS plug-in component installation (continued)*

| Property | Default value | Your value |
|---|---|---|
| Server configuration file location | The location of the server configuration file. For example:<br>**IBM HTTP Server**<br>`/opt/IBM/HTTPServer/conf/httpd.conf`<br>**Apache HTTP Server**<br>`/etc/httpd/conf/httpd.conf` | |

# Installing the federated single sign-on feature

You can install the federated single sign-on feature in either graphical or console mode.

## Before you begin

The federated single sign-on feature requires two Tivoli Federated Identity Manager components:

- Runtime and management services
- Management console

This topic describes how to install both components. It also describes how to install only the runtime and management service; some deployments require the management console to be installed on a different computer.

If you must install the management console on a different computer, follow the instructions in this topic and continue with Chapter 6, “Installing the management console,” on page 47.

The installation supports following scenarios for WebSphere Application Server:

**An environment with an existing WebSphere Application Server**

The existing WebSphere Application Server can be

- One that you installed as a prerequisite.
- An existing installation that meets the version and fix pack requirements.

Follow the instructions in “Installing federated single sign-on on an existing WebSphere Application Server” on page 30.

**An environment without WebSphere Application Server**

Install the embedded version of WebSphere Application Server. This version is provided with Tivoli Federated Identity Manager. Follow the instructions in “Installing federated single sign-on with an embedded WebSphere Application Server” on page 31.

**Note:** The embedded installation is typically used only in limited small-scale scenarios, such as prototyping or test environments. For production environments, and scenarios that include Tivoli Access Manager and large user registries, use full (non-embedded) IBM WebSphere Application Server Network Deployment.

## Installing federated single sign-on on an existing WebSphere Application Server

You can install federated single sign-on in an existing WebSphere environment. You can use either the graphical or console mode.

### Before you begin

**Note:** Do **not** use these instructions *if* you installed the embedded version of WebSphere as part of a previous installation of Tivoli Federated Identity Manager and want to modify its settings. Use "Installing federated single sign-on with an embedded WebSphere Application Server" on page 31.

Ensure that the computer on which you are installing meets the hardware and operating system requirements. To review the requirements:

1. Access http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html.
2. Select **Hardware and Software Requirements**.

### Procedure

1. Insert the CD into or download the image onto the computer on which you want to install the feature.
2. Start the installation:

*Table 9. Commands to start the installation program in graphical or console mode*

| **Platform** | **Command to start the installation program in graphical mode** | **Command to start the installation program in console mode** |
|---|---|---|
| **Note:** The installation assumes that WebSphere Application Server is listening on `localhost`. If it is not listening on `localhost`, specify the host name by adding a parameter. For example, on Linux:<br>`./install_linux_x86.bin -W websphereProperties.adminClientConnectHost=<hostname>` | | |
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on Power Systems | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

3. Select a language.
4. Click **OK**.
5. Accept the license agreement.
6. Click **Next**.
7. Click **Next** on the Welcome screen.
8. Specify an installation directory at **Directory name**. Take one of the following actions:
   - Accept the default directory.
   - Click **Browse** to select a directory on the file system.

9. Select the features you want to install. Do not select any other features except the following ones.
   - **Runtime and Management Services**
   - **Management console** *if* you are installing the management console on the same computer
10. Click **Next**.
11. Select **Yes** to use an existing installation of WebSphere Application Server.
12. Click **Next**.
13. Select whether the existing WebSphere Application Server has administration security enabled.
   - If you selected **Yes**, enter the administration security settings for the existing installation.
   - If you selected **No**, enter the directory and port information.

     **Note:** If you installed the embedded version as part of a previous installation of Tivoli Federated Identity Manager, the installation prompts only for port information.
14. Click **Next**.
15. Click **Next**.
16. Verify that adequate free space is available.
17. Click **Next**.
18. Verify that the information is correct.
19. Click **Next**. It might take a few minutes to install the files. A status bar shows the installation progress. A summary panel indicates that the installation is complete.
20. Click **Finish**.

## Installing federated single sign-on with an embedded WebSphere Application Server

You can install the embedded WebSphere Application Server when you install federated single sign-on.

### Before you begin

Ensure that the computer on which you are installing meets the hardware and operating system requirements. To review the requirements:

1. Access http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.tivoli.fim.doc_6.2.2/ic/ic-homepage.html.
2. Select **Hardware and Software Requirements**.

### About this task

The embedded WebSphere server is typically used only in limited small-scale scenarios such as prototyping or test environments. Production environments and scenarios that include Tivoli Access Manager and large user registries, typically use the full (non-embedded) IBM WebSphere Application Server Network Deployment.

### Procedure

1. Insert the CD into or download the image onto the computer on which you want to install the feature.

2. Start the installation:

*Table 10. Commands to start the installation program in graphical or console mode*

| Platform | Command to start the installation program in graphical mode | Command to start the installation program in console mode |
|---|---|---|
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on Power Systems | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

3. Select a language.
4. Click **OK**.
5. Accept the license agreement.
6. Click **Next**.
7. Click **Next**.
8. Specify an installation directory at **Directory name**. Take one of the following actions:
   - Accept the default directory.
   - Click **Browse** to select a directory on the file system.
9. Select the features you want to install. Do not select any other features except the following ones.
   - **Runtime and Management Services**.
   - **Management console** *if* you are installing the management console on the same computer
10. Click **Next**.
11. Select **No** to install the embedded WebSphere Application Server.

    **Note:** If you installed the embedded version in a previous Tivoli Federated Identity Manager installation, select **No**.
12. Click **Next**.
13. Enter the requested information:
    a. Enter the administrative user name, the password, and a confirmation of the password.
    b. Enter the port information.
    c. Click **Next**.
14. Verify that adequate free space is available.
15. Click **Next**.
16. Verify that the information is correct.
17. Click **Next**. It might take a few minutes to install the files. A status bar shows the installation progress. A summary panel indicates that the installation is complete.
18. Click **Finish**.

# Chapter 4. Installing Web services security management

You must complete several tasks to install Web services security management.

Follow this process to install Web Services security management:
1. "Planning the installation of Web services security management"
2. "Installing software prerequisites for Web services security management" on page 35
3. "Completing the Web services security management installation worksheet" on page 36
4. "Installing the Web services security management feature" on page 36

## Planning the installation of Web services security management

You can deploy Web services security management into different scenarios. The properties of each deployment scenario determine what software to install.

Tivoli Federated Identity Manager deployment scenarios typically span multiple computers. You must understand the network topology of your security infrastructure before you install Web services security management.

You install and configure Web services security management into a IBM Tivoli Federated Identity Manager deployment. Each deployment must have two other IBM Tivoli Federated Identity Manager components installed and configured. The other components are runtime and management services and the management console.

The deployment environment typically includes IBM WebSphere Application Server as a middleware server. It also includes IBM Tivoli Access Manager for e-business as an authorization solution. These two products are prerequisites for runtime and management services.

### Prerequisites for each deployment scenario

Web services security management is deployed into one of the following scenarios. Each scenario has specific prerequisites.

**Authentication and authorization**

Authenticates users and provides authorization decisions in response to requests for access to protected resources or services.

It requires access to a user registry, such as the one provided by Tivoli Access Manager. Runtime and management services manages access to the user registry. This component is a prerequisite for all Web services security management deployments. Installing Tivoli Access Manager meets the requirement.

The prerequisites are:
- WebSphere Application Server
- Tivoli Access Manager
- Tivoli Federated Identity Manager runtime and management service component
- Tivoli Federated Identity Manager management console component

**Conversion of token types**

Converts an incoming token type to a different token type for WebSphere Application Server.

It requires WebSphere Application Server for hosting the component. This scenario does not require any other prerequisites.

**Note:** After completing the installation, you can configure this component to communicate with a WebSphere server other than the local one. This configuration requirement does not affect the installation process.

The prerequisites are:

- WebSphere Application Server
- Tivoli Federated Identity Manager runtime and management service component
- Tivoli Federated Identity Manager management console component

## Software prerequisites in a distributed environment

You can deploy Web services security management into different distributed environments. These environments can include all Tivoli Federated Identity Manager components on one computer. Typically, however, deployments distribute components across multiple computers.

The software installation sequence depends on your topology. It also depends on if you previously installed prerequisites while installing other components.

The following environments are typical deployment scenarios:

**Web services security management on a *separate* computer from the runtime and management services component**

You must first install the other Tivoli Federated Identity Manager components on other computers. The components are runtime and management services and the management console.

The only required prerequisite on the host computer for Web services security management is WebSphere Application Server.

If you did not previously install any Tivoli Federated Identity Manager components, the installation sequence is:

1. On one computer, install the runtime and management services component and the management console component. The installation sequence is:
   a. Install WebSphere Application Server.
   b. Install Tivoli Access Manager.
   c. Install Tivoli Federated Identity Manager runtime and management service component.
   d. Install Tivoli Federated Identity Manager management console.

   **Note:** You can install the management console on its own computer, separate from the runtime and management service component.
2. On the computer on which you want to install Web services security management:
   a. Install WebSphere Application Server.
   b. Install Web services security management.

**Web services security management on the *same* computer as runtime and management services.**

You must first install the runtime and management services component. The prerequisites are WebSphere Application Server and Tivoli Access Manager.

**Note:** Installing runtime and management services satisfies the prerequisite for WebSphere Application Server. This sequence also satisfies the Web services security management scenarios that require access to a Tivoli Access Manager user registry for authorization decisions.

The installation sequence is:

1. WebSphere Application Server
2. Tivoli Access Manager
3. Tivoli Federated Identity Manager runtime and management service component
4. Tivoli Federated Identity Manager management console
5. Web services security management component

## Installing software prerequisites for Web services security management

For most installation scenarios, you must install prerequisites while installing Web services security management.

The prerequisites depend on the deployment scenario and on the current state of the security infrastructure. The prerequisites also depend on your installation plan. You can either:

- Complete an initial installation of Tivoli Federated Identity Manager *and* Web services security management.
- Add Web services security management to an existing deployment.

### Installing Tivoli Federated Identity Manager and Web services security management

There are several supported scenarios for deploying Web services security management. If you have not already done so, review the supported scenarios in "Planning the installation of Web services security management" on page 33.

For a new deployment, you must install prerequisite software.

The minimum prerequisite for Web services security management is WebSphere Application Server. Deploying Web services security management also depends on both management services and the management console.

To install all the necessary software, complete the following steps:

1. Install the runtime and management service. This component requires you to install
   - WebSphere Application Server
   - Tivoli Access Manager

   See Chapter 3, "Installing federated single sign-on or token exchange," on page 15. The installation steps apply.
2. Install the management console.

This component requires WebSphere Application Server. When you install the management console on the same computer as the runtime and management services, the WebSphere runtime prerequisite satisfies the management console requirement.

When you install the management console on a separate computer, you must install:

- WebSphere Application Server
- The management console

See Chapter 6, "Installing the management console," on page 47.

### Adding Web services security management to an existing Tivoli Federated Identity Manager deployment

You can add Web services security management to an existing deployment under the following scenarios:

- Installing it on a computer that already has a Tivoli Federated Identity Manager component. Components include runtime and management services or the management console.

  For this scenario, there are no prerequisites.
- Installing it on a computer with *no* Tivoli Federated Identity Manager components installed.

  WebSphere Application Server is a prerequisite.

  See "Installing WebSphere Application Server" on page 18.

## Completing the Web services security management installation worksheet

You can view, print, and fill out the properties worksheet for installing Web services security management.

*Table 11. Properties for Web services security management feature installation*

| Property | Default value | Your value |
|---|---|---|
| Tivoli Federated Identity Manager installation directory | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |

When installing Web services security management on the same computer as either runtime and management services or the management console, put it in the same directory as the other components.

## Installing the Web services security management feature

You can install Web services security management in either graphical or console mode.

### Before you begin

Verify that you installed the prerequisite software for your deployment scenario.

## Procedure

1. Insert the CD into or download the image onto the computer on which you want to install the software.
2. Access the command line.
3. Use one of the following commands to start the installation.

*Table 12. Commands to start the installation program in graphical or console mode*

| Platform | Command to start the installation program in graphical mode | Command to start the installation program in console mode |
|---|---|---|
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on Power Systems | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

**Note:** The installation is designed for the WebSphere Application Server deployment to listen on`localhost`. If it does not listen on `localhost`, specify the host name by adding a parameter to the installation command. For example, on Linux:

```
./install_linux_x86.bin -W
websphereProperties.adminClientConnectHost=<hostname>
```

4. Select a language.
5. Click **OK**.
6. Click **Next** to agree to the license terms.
7. Click **Next** in the Welcome screen.
8. Take one of the following actions:
   - Specify an installation directory at **Directory name**.
   - Accept the default directory.
   - Click **Browse** to select a directory on the file system.
9. Select **Web Services Security Management**.
10. Clear the check boxes for the other features.
11. Click **Next**.
12. Verify that adequate free space is available.
13. Click **Next**.
14. Verify that the information about the installation summary is correct.
15. Click **Next**. Installing the files might take a few minutes. A status bar indicates progress. When the installation finishes, the software shows a summary of the installation.
16. Click **Finish**.

# Chapter 5. Installing federated provisioning

Installing federated provisioning requires deploying prerequisite software. After installing the prerequisites, you can install the WS-Provisioning runtime component.

Follow this process:

1. “Planning federated provisioning”
2. “Installing software prerequisites for federation provisioning” on page 40
3. “Completing the WS-Provisioning runtime installation worksheet” on page 44
4. “Installing WS-Provisioning runtime” on page 44

## Planning federated provisioning

Install and configure WS-Provisioning runtime into a Tivoli Federated Identity Manager deployment. Each deployment must have two other components installed and configured. The other components are runtime and management services and the management console.

The deployment environment typically includes WebSphere Application Server as a middleware server. It includes IBM Tivoli Access Manager for e-business as an authorization solution. These products are prerequisites for runtime and management services.

Before you install provisioning, you must install and configure a distributed application environment. This environment is the same as the environment required by runtime and management services. You must also include IBM Tivoli Directory Integrator.

For a federated provisioning deployment in a prototype or test environment, you can install all software for client and server on one computer. In a production environment, the software is typically distributed across multiple computers.

WS-Provisioning runtime can communicate with any other provisioning service that supports the WS-Provisioning standard. The Tivoli Federated Identity Manager provisioning service:

- Has no requirements on an environment that hosts and supports provisioning services from an independent vendor. Such an environment must supply its own methods for building and authenticating WS-Provisioning messages.
- Does not require this environment use the prerequisites. Prerequisites include WebSphere Application Server, Tivoli Access Manager, or IBM Tivoli Directory Integrator.
- Requires additional prerequisites beyond the ones required for deploying the runtime and management services feature. Tivoli Federated Identity Manager provisioning requires installing and deploying runtime and management services.

After installing the prerequisites for the runtime and management services, you must install additional prerequisites to support WS-Provisioning runtime.

You must install some prerequisites on the computer that hosts the federated provisioning. You can install other prerequisites on other computers and access them through network connections.

**Install the following prerequisites on the *same* computer as Tivoli Federated Identity Manager provisioning:**

- WebSphere Application Server.
- Tivoli Access Manager Java runtime environment.

  **Note:** The Java runtime environment is required only when you deploy the provisioning demonstration scenario. The demonstration scenario is an optional It is not required for WS-Provisioning support.

**Install the following prerequisites on a *different* computer than Tivoli Federated Identity Manager provisioning:**

- Tivoli Federated Identity Manager runtime and management service component.

  This component requires WebSphere Application Server and Tivoli Access Manager.
- Tivoli Federated Identity Manager management console.

  This component requires WebSphere Application Server.

## Installing software prerequisites for federation provisioning

The federated provisioning feature requires installing and configuring some prerequisites.

The prerequisites and the installation sequence depend on your security infrastructure deployment. The installation tasks differ, depending on if you are doing an initial deployment or adding federated provisioning to an existing deployment.

### Initial installation of Tivoli Federated Identity Manager

If you have not installed any Tivoli Federated Identity Manager components or prerequisites, complete an installation of federated single sign-on.

The software is not required to be on the same computer as federated provisioning. Follow this process:

1. Install runtime and management service.

   **Note:** If you intend to deploy the management console on the same computer as the runtime and management service, you can install it at the same time.

   See Chapter 3, “Installing federated single sign-on or token exchange,” on page 15.
2. Install the management console.

   If you did not install the management console when you installed the runtime and management services component, you must install it before installing federated identity provisioning.

   See Chapter 6, “Installing the management console,” on page 47.
3. Install IBM Tivoli Directory Integrator.

   This product is required by federated provisioning.

   See “Installing IBM Tivoli Directory Integrator” on page 41.

4. Install the IBM Tivoli Access Manager for e-business Java runtime environment.

   Federated provisioning includes a demonstration scenario. The demonstration requires the Java runtime environment. Installing the demonstration is optional. If you do not want to install the demonstration, do not install this prerequisite.

   See "Installing Tivoli Access Manager Java runtime environment" on page 43.
5. Install WebSphere Application Server on the *same* computer as federated provisioning.
   - If you installed either Tivoli Federated Identity Manager or IBM Tivoli Directory Integrator on the computer that hosts federated provisioning, you have met this prerequisite. Go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.
   - If you must install WebSphere Application Server, see the product documentation or the installation summary, "Installing WebSphere Application Server" on page 18.

### Adding federated provisioning to a Tivoli Federated Identity Manager deployment

If you already established a Tivoli Federated Identity Manager single sign-on federation, follow this process:

1. Install IBM Tivoli Directory Integrator.

   See "Installing IBM Tivoli Directory Integrator."
2. Install the IBM Tivoli Access Manager for e-business Java runtime environment.

   The federated provisioning feature includes a demonstration scenario. The demonstration requires the Java runtime environment. Installing the demonstration is optional. If you do not want to install the demonstration, do not install this prerequisite.

   See "Installing Tivoli Access Manager Java runtime environment" on page 43.
3. If you install the WS-Provisioning runtime on a *different* computer than single sign-on federation or IBM Tivoli Directory Integrator, you must install WebSphere Application Server.

   See the WebSphere Application Server documentation. You can also check the installation summary, "Installing WebSphere Application Server" on page 18.
4. After you install all the prerequisites, go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.

## Installing IBM Tivoli Directory Integrator

Federated provisioning requires the installation of IBM Tivoli Directory Integrator.

### About this task

WS-Provisioning runtime requires you to install IBM Tivoli Directory Integrator. You must also make it accessible in a distributed application environment. WS-Provisioning runtime does *not* require you to install Tivoli Federated Identity Manager and IBM Tivoli Directory Integrator on the same host.

The following procedure summarizes an example installation on Linux. For complete installation instructions for your platform, see the *IBM Tivoli Directory Integrator Administration Guide* on:

`http://publib.boulder.ibm.com/infocenter/tiv2help/index.jsp`

### Procedure

1. Run the setup file:

   ```
   ./setupIntelLinux.bin
   ```

2. Click **Next** on the Welcome panel.
3. Accept the software license agreement.
4. Click **Next**.
5. Accept the default installation directory or specify a different location.

   For example, the default installation directory on Linux is:

   ```
   /opt/IBM/IBMDirectoryIntegrator
   ```

6. Click **Next**.
7. Select one of the solutions locations. You can accept the default **Use a tdi subdirectory under my home directory**.

   A summary panel shows the installation directory and size of the installation.

8. Click **Next**.
9. Click **Next** to begin the installation.

   A panel confirms the successful completion of the installation.

10. Click **Finish**.
11. Choose one of the following options:
    - For IBM Tivoli Directory Integrator Version 6.1, go to What to do next.
    - For IBM Tivoli Directory Integrator Version 6.0, install a Fix Pack. Go to "Installing IBM Tivoli Directory Integrator Version 6.0 Fix Pack 1."

### What to do next

You next action depends on whether you want to install the provisioning demonstration scenario.

- To skip the installation, go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.
- To install it on the client, go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.
- To install it on the server, go to "Installing Tivoli Access Manager Java runtime environment" on page 43.

## Installing IBM Tivoli Directory Integrator Version 6.0 Fix Pack 1

Using Tivoli Federated Identity Manager EAR files with IBM Tivoli Directory Integrator requires Fix Pack 1. You can obtain the fix pack from the IBM Support website.

### About this task

**Note:** This task applies only to IBM Tivoli Directory Integrator Version 6.0. Tivoli Federated Identity Manager Version 6.1 includes IBM Tivoli Directory Integrator Version 6.1. It does not require the Fix Pack.

### Procedure

1. Access the support website.

   ```
   http://www.ibm.com/software/sysmgmt/products/
     support/IBMDirectoryIntegrator.html
   ```

2. Enter **`6.0.0-TIV-ITDI-FP0001`** in the Search window:

3. Select **IBM Tivoli Directory Integrator Ver 6.0 Fixpack 1(6.0.0-TIV-ITDI-FP0001**.

   From the fix pack page, do the following steps:
4. Download the fix pack for your platform.
5. Download **6.0.0-TIV-ITDI-FP0001.README**

   **Note:** If you have difficulty locating the fix pack with the preceding instructions, access the following URL:

   ```
   http://www-1.ibm.com/support/docview.wss?rs=697&context=SSCQGF&dc=D400&q1=
    6.0.0-TIV-ITDI-FP0001&uid=swg24009208&loc=en_US&cs=utf-8&lang=en
   ```
6. Install the fix pack by running the setup program. For example, on Linux:

   ```
   ./setupFPLinux.bin -is:javahome "/opt/IBM/IBMDirectoryIntegrator/_jvm"
   ```
7. Click **Next** on the Welcome panel.
8. Accept the software license agreement.
9. Click **Next**.
10. Accept the default installation directory or specify another location.

    For example the fault installation directory on Linux is:

    ```
    /opt/IBM/IBMDirectoryIntegrator
    ```

    A summary panel shows the installation directory and size of the installation.
11. Click **Next**.
12. Click **Next**.

    A panel indicates the successful completion of the installation.
13. Click **Finish**.

### What to do next

Your next task depends on if you want to use the provisioning demonstration scenario.

- If you do not want to use it, go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.
- If you want to use it on the client, go to "Completing the WS-Provisioning runtime installation worksheet" on page 44.
- If you want to use it on the server, go to"Installing Tivoli Access Manager Java runtime environment."

## Installing Tivoli Access Manager Java runtime environment

You must install the Tivoli Access Manager Java runtime environment if you intend to use the demonstration scenario for federated provisioning.

### Before you begin

The information in this section applies to Tivoli Federated Identity Manager package users. It also applies to organizations that already have IBM Tivoli Access Manager for e-business in their computing environment.

Install IBM JRE 1.4.2 before running this installation. See *Installing prerequisite products* in the *IBM Tivoli Access Manager for e-business Base System Installation Guide*.

### About this task

**Attention:** This component is required only on the provisioning server. The demonstration scenario does not create users on the client. When installing provisioning on the client, skip this topic; see “Installing WS-Provisioning runtime.”

The Tivoli Federated Identity Manager provisioning demonstration scenario provides example customer code. The demonstration includes the Tivoli Access Manager Java Administration API. This API creates Tivoli Access Manager users. You can enable or disable their accounts.

The Java Administration API requires installing the Tivoli Access Manager Java runtime environment. Install it on the host where the demonstration scenario runs the provisioning service in the *server* role.

You can install from either an installation wizard or utilities. For complete instructions, see *Setting up an Access Manager Runtime for Java system* in the *IBM IBM Tivoli Access Manager for e-business Base System Installation Guide*. You can access this document from the Tivoli Access Manager information center: `http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/topic/com.ibm.itame.doc/welcome.htm`

## Completing the WS-Provisioning runtime installation worksheet

You can view, print, and fill out the properties worksheet for installing WS-Provisioning runtime.

Install WS-Provisioning runtime in the same directory on the same computer as the runtime and management service.

*Table 13. Properties for WS-Provisioning runtime feature installation*

| Property | Default value | Your value |
|---|---|---|
| Tivoli Federated Identity Manager installation directory | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |

## Installing WS-Provisioning runtime

This topic describes how to install the WS-Provisioning runtime feature by using either the graphical or console mode.

### Before you begin

Verify that you installed the prerequisites that are required for your deployment scenario. See “Installing software prerequisites for federation provisioning” on page 40.

### Procedure

1. Insert the CD into or download the image onto the computer on which you want to perform the installation.

2. Access the command line.
3. Use one of the following commands to start the installation.

Table 14. Commands to start the installation program in graphical or console mode

| Platform | Command to start the installation program in graphical mode | Command to start the installation program in console mode |
|---|---|---|
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on System p® | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

**Note:** The installation is designed for the WebSphere Application Server deployment to listen on `localhost`. If it does not listen on `localhost`, specify the host name by adding a parameter to the installation command. For example, on Linux:

```
./install_linux_x86.bin -W
websphereProperties.adminClientConnectHost=<hostname>
```

4. Select a language.
5. Click **OK**.
6. Click **Next** to agree to the license terms.
7. Click **Next** on the **Welcome** panel.
8. Take one of the following actions:
   - Specify an installation directory at **Directory name**.
   - Accept the default directory.
   - Click **Browse** to select a directory on the file system.
9. Select **WS-Provisioning Runtime**.
10. Clear the check boxes for the other features.
11. Click **Next**.
12. Verify that adequate free space is available.
13. Click **Next**.
14. Verify that the information is correct on the installation summary.
15. Click **Next** Installing the files might take a few minutes. A status bar indicates progress. When the installation finishes, the software shows a summary of the installation
16. Click **Finish**.

## What to do next

The next task depends on yourTivoli Federated Identity Manager installation scenario. See the *IBM Tivoli Federated Identity Manager Administration Guide* for details about these tasks.

- If you are performing an initial installation, do the following tasks if you have not already done so:
  1. Create the domain.

2. Configure a single sign-on federation.
3. Deploy and configure federated provisioning.

- If you *already* deployed and configured a domain and a single sign-on federation, deploy and configure federated provisioning.

# Chapter 6. Installing the management console

The management console is often installed on the same computer as the management service and runtime. You can also install the console on a separate computer.

To install the management console, complete the following tasks:

1. "Planning the installation of the management console"
2. "Console installation worksheet" on page 48
3. "Installing the management console" on page 51

## Planning the installation of the management console

To separate administration functions from runtime functions, you can install the management console on a separate computer from other Tivoli Federated Identity Manager components.

The management console is a plug-in to the WebSphere Application Server administration console. In some deployment scenarios, you might want to use the management console on the same computer as the administration console.

The management console is packaged with Tivoli Federated Identity Manager runtime and management services and the federated provisioning. During the installation, you can select it as one of the components to install. In many scenarios, the administrator installs the management console at the same time as another component.

If your scenario requires installing the management console separately, you must installWebSphere Application Server.

You can satisfy this prerequisite in one the following ways:

- Install a supported version of WebSphere Application Server.
- Install the embedded WebSphere Application Server. The embedded version is distributed with Tivoli Federated Identity Manager.

  The embedded version

  - Is a lightweight version of the server and administration console.
  - Provides all the support required by the Tivoli Federated Identity Manager management console.
  - Supports environments that run a limited number of applications.
  - Supports environments that do not require the full WebSphere administration support.

  The management console installation prompts to specify if you want to install the embedded version. If you select it, a separate installation is not required. it is installed during the Tivoli Federated Identity Manager component installation.

Follow this process:

1. Decide which version of WebSphere Application Server you want to use.
2. Take one of the following actions:
   - To use the embedded WebSphere Application Server, go to step 3 on page 48.

- To install a separate WebSphere Application Server server:
  a. Access the Tivoli Federated Identity Manager information center.
  b. Review the list of supported versions.
  c. Install the server. See the instructions on the WebSphere Application Server information center.

3. Complete “Console installation worksheet.”

# Console installation worksheet

You can view, print, and fill out the properties worksheet for installing the management console component.

**Note:**

- If you install the console on the same server as the runtime component, some of the properties are the same. Use the values from the “Runtime and management service installation worksheet” on page 25.
- You cannot change default property values on the console after installation.

## Installation on an existing version of WebSphere Application Server

An *existing* version is either:

- The separately installable version provided with Tivoli Federated Identity Manager. It must already be installed.
- A compatible version of WebSphere Application Server that is already installed.

If you are installing the management console on an existing version of WebSphere, you must know whether administration security is enabled.

*Table 15. Properties for console component installation on existing version of WebSphere Application Server*

| Property | Default value | Your value |
|---|---|---|
| **Directory name** | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |
| **When WebSphere Application Server administration security is *not* enabled:** | | |
| **WebSphere Application Server installation directory** | **AIX**<br>`/usr/IBM/WebSphere/AppServer`<br>**Linux or Solaris**<br>`/opt/IBM/WebSphere/AppServer`<br>**Windows**<br>`C:\Program Files\IBM\WebSphere\AppServer` | |

*Table 15. Properties for console component installation on existing version of WebSphere Application Server (continued)*

| Property | Default value | Your value |
|---|---|---|
| **WebSphere Application Server SOAP connector port**<br>Specifies the port number for SOAP communication. | `8879` | |
| **Note:** If you previously installed the embedded version, the installation does *not* prompt for the installation directory. | | |
| **When WebSphere Application Server administration security is enabled:** | | |
| **WebSphere Application Server administrator user name** | | |
| **WebSphere Application Server administrator password** | | |
| **SSL Trusted Java keystore file**<br>Specifies the truststore file. | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM/ewas/profiles/itfimProfile/etc/trust.p12`<br>**Windows**<br>`C:\Program Files\IBM\FIM\ewas\profiles\itfimProfile\etc\trust.p12` | |
| **SSL Trusted Java keystore password**<br>Specifies the password for accessing the WebSphere truststore. | `WebAS` | |
| **SSL Java keystore file**<br>Specifies the keystore file used by WebSphere Application Server. | | |
| **SSL Java keystore password**<br>Specifies the password for accessing the keystore. | | |
| **Note:** If you previously installed the embedded version, the installation does *not* prompt for the SSL Java keystore and password. | | |

## Installation on embedded version of WebSphere Application Server

*Table 16. Properties for console component installation on embedded version of WebSphere Application Server*

| Property | Default value | Your value |
|---|---|---|
| Directory name | **AIX, Linux, or Solaris**<br>`/opt/IBM/FIM`<br>**Windows**<br>`C:\Program Files\IBM\FIM` | |
| **WebSphere Application Server administrator user name** | `fimadmin` | |
| **WebSphere Application Server administrator password** | | |
| **Application server port**<br>Specifies the port number for communicating over HTTP. | `9080` | |
| **Secure application server port**<br>Specifies the port number for communicating over HTTPS. | `9443` | |
| **Administration port**<br>Specifies the port number that the administrative console uses for HTTP. | `9060` | |
| **Secure administration port**<br>Specifies the port number that the WebSphere Application Server administrative console uses for HTTPS. | `9043` | |
| **SOAP port**<br>Specifies the port number for SOAP communication. | `8879` | |

**Note:**

- When you use the embedded version, the installation program determines if the standard ports are available by examining what ports are currently in use. If the default ports are in use, it increments each port value by 1 until all the necessary port values are free.

  The ports are detected during the initial installation of the embedded version. If you install additional components later on the embedded version, the available ports are not detected automatically.
- If you want to install an additional component at a later time on the embedded version, select **No** when you are prompted about whether you want to use an existing version.

# Installing the management console

You can install the management console in either graphical or console mode.

## Before you begin

- Make sure the computer on which you are installing meets the requirements.
- Decide which WebSphere Application Server deployment you want. Your choices are:
  - The embedded version that is included with Tivoli Federated Identity Manager.
  - An existing WebSphere installation. It must already be installed and configured on the server.

  You can install the management console individually.

## Procedure

1. Insert the CD into or download the image onto the computer on which you want to install the software.
2. Access the command line.
3. Use one of the following commands to start the installation.

*Table 17. Commands to start the installation program in graphical or console mode*

| Platform | Command to start the installation program in graphical mode | Command to start the installation program in console mode |
|---|---|---|
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on System p | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

   **Note:** The installation is designed for the WebSphere Application Server deployment to listen on `localhost`. If it does not listen on `localhost`, specify the host name by adding a parameter to the installation command. For example, on Linux:

   ```
   ./install_linux_x86.bin -W
   websphereProperties.adminClientConnectHost=<hostname>
   ```

4. Select a language.
5. Click **OK**.
6. Click **Next** to agree to the license terms.
7. Click **Next** on the Welcome screen.
8. Take one of the following actions:
   - Specify an installation directory at **Directory name**.
   - Accept the default directory.

- Click **Browse** to select a directory on the file system.

9. Select **Management Console**.
10. Clear the check boxes for the other features.
11. Click **Next**.
12. Take one of the following actions.
    - Select **Yes** if you want to use an existing installation of WebSphere Application Server.
    - Select **No** if you installed the embedded version as part of a previous installation.
13. Click **Next**.
14. Take one of the following actions:
    - If you *are* using an existing WebSphere installation, go to step 15.
    - If you are *not* using an existing WebSphere installation:
      a. Enter the WebSphere administrative user name, the password, and a confirmation of the password for this installation.
      b. Enter the WebSphere port information for this installation.
      c. Click **Next**.
      d. Go step 16.
15. Take one of the following actions:
    - If you *are not* using an existing WebSphere installation and completed step 14, go to step 16.
    - If you *are* using an existing WebSphere installation:
      a. Select whether the existing WebSphere Application Server has administration security enabled.
      b. Click **Next**.
      c. Take one of the following actions,:
         - If you selected **Yes**, enter the administration security settings for the existing WebSphere installation.
         - If you selected **No**, enter the directory and port information for the existing WebSphere installation.
      d. Click **Next**.

    **Note:** If you installed the embedded version during a previous Tivoli Federated Identity Manager installation, you are prompted only for port information.
16. Verify that adequate free space is available.
17. Click **Next**.
18. Verify that the installation summary is correct.
19. Click **Next**. Installing the files might take a few minutes. A status bar indicates progress. When the installation finishes, the software shows a summary of the installation.
20. Click **Finish**.

# Chapter 7. Installing the IBM Support Assistant

IBM Support Assistant Lite is embedded in Tivoli Federated Identity Manager. You can install it to provide access to support-related information and to serviceability tools for problem determination.

## About this task

You can install IBM Support Assistant Lite in either graphical or silent mode.

## Procedure

1. Insert the CD into or download the image onto the computer on which you want to install the software.
2. Access the command line.
3. Use one of the following commands to start the installation.

*Table 18. Commands to start the installation program in graphical or console mode*

| Platform | Command to start the installation program in graphical mode | Command to start the installation program in console mode |
|---|---|---|
| AIX | `install_aix_ppc.bin` | `install_aix_ppc.bin -console` |
| Linux on System p | `install_linux_ppc.bin` | `install_linux_ppc.bin -console` |
| Linux on System x | `install_linux_x86.bin` | `install_linux_x86.bin -console` |
| Linux on System z | `install_linux_s390.bin` | `install_linux_s390.bin -console` |
| Solaris | `install_sol_sparc.bin` | `install_sol_sparc.bin -console` |
| Windows | `install_win32.exe` | `install_win32.exe -console` |

**Note:** The installation is designed for the WebSphere Application Server deployment to listen on `localhost`. If it does not listen on `localhost`, specify the host name by adding a parameter to the installation command. For example, on Linux:

```
./install_linux_x86.bin -W
webspherePropertİes.adminClientConnectHost=<hostname>
```

4. Select a language.
5. Click **OK**.
6. Click **Next** to agree to the license terms.
7. Click **Next** in the Welcome screen.
8. Take one of the following actions:
   - Specify an installation directory at **Directory name**.
   - Accept the default directory.
   - Click **Browse** to select a directory on the file system.
9. Select **IBM Support Assistant plugin for Federated Identity Manager**.
10. Clear the check boxes for the other features.
11. Click **Next**.
12. Verify that adequate free space is available.

13. Click **Next**.
14. Verify that the installation summary is correct.
15. Click **Next**. Installing the files might take a few minutes. A status bar indicates progress. When the installation finishes, the software shows a summary of the installation.
16. Click **Finish**.
17. Uncompress the `TFIMISALite.zip` archive.

    The archive contains the data collection tool for Tivoli Federated Identity Manager.

    The installation copies the archive file to the `tools/isa` subdirectory in the Tivoli Federated Identity Manager installation directory. For example, `/opt/IBM/FIM/tools/isa`.

## What to do next

For information about IBM Support Assistant Lite, see the *IBM Tivoli Federated Identity Manager Problem Determination Guide*.

# Chapter 8. Using silent mode installation

Tivoli Federated Identity Manager can be installed on a silent mode using a response file. You can install several features at the same time on the same server or individual features on separate servers by using a response file. This topic provides procedures for the silent installation mode.

**Note:** The Tivoli Federated Identity Manager provides sample response files that are located under the `/rsp` directory in the Tivoli Federated Identity Manager CD or ISO image. You can use the sample silent installer response file and update its values according to your requirements.

Review the feature requirements and decided if you want to install the features together or separately.

Decide between the following environment configurations:

- An existing supported version of WebSphere Application Server.
- The embedded version of WebSphere Application Server. It is included with Tivoli Federated Identity Manager.

## Creating a response file

A response file records the actions you want the installation wizard to perform.

### Procedure

1. Start the installation wizard for the appropriate operating system and specify the file name to record the options.

   **AIX** **`./install_ppc_aix.bin`** `-options-record` *response_file_name*

   **Solaris**
   **`./install_sol_sparc.bin`** `-options-record` *response_file_name*

   **Linux on System x**
   **`./install_linux_x86.bin`** `-options-record` *response_file_name*

   **Linux on System z**
   **`./install_linux_s390.bin`** `-options-record` *response_file_name*

   **Windows**
   **`install_win32.exe`** `-options-record` *response_file_name*
2. In each of the panels, specify values for the various options.
3. Click **Finish** to create the response file.
4. Open the new response file in a text editor.
   a. Delete the two extra instances of `-G licenseAccepted=false`. Ensure that there is only *one* **`licenseAccepted`** parameter left, and that it is set to `true`. For example, `-G licenseAccepted=true`.
   b. Review the other values. Some response files might contain macros instead of data.
5. Make the response file available to the people or processes who must install the component.

## Using a response file

After creating a response file, use it with the installation wizard to install the component in a predetermined manner.

### Before you begin

If you generated an installation response file, you must edit it with a text editor and delete the two extra instances of `-G licenseAccepted=false`. Ensure that there is only *one* **`licenseAccepted`** parameter left, and that it is set to true. For example: `-G licenseAccepted=true`.

### Procedure

1. Open a command prompt.
2. Start the installation or uninstallation wizard for the appropriate operating system and specify the file name of the response file.

   **AIX** **`./install_ppc_aix.bin`** `-silent -options` *response_file_name*

   **Solaris**
   **`./install_sol_sparc.bin`** `-silent -options` *response_file_name*

   **Linux on System x**
   **`./install_linux_x86.bin`** `-silent -options` *response_file_name*

   **Linux on System z**
   **`./install_linux_s390.bin`** `-silent -options` *response_file_name*

   **Windows**
   **`install_win32.exe`** `-silent -options` *response_file_name*

   The wizard runs and performs the necessary installation steps. Errors are written to the standard error device (STDERR) and to the log file.

   You can also start the wizard from a script or batch file that is part of an automated process.

# Appendix A. Upgrading to version 6.2.2

The process for upgrading from a previous version of Tivoli Federated Identity Manager can vary. It depends on whether your existing environment had an existing or an embedded version of WebSphere Application Server.

Use the appropriate upgrade procedures for your environment:

- "Upgrading on an existing WebSphere Application Server installation"
- "Upgrading on an embedded WebSphere Application Server installation" on page 59
- "Upgrading on a new WebSphere Application Server installation" on page 61
- "Making Java calls made from XSLT files work properly after upgrading" on page 64
- "Upgrading LDAP" on page 64
- "Migrating SAML 2.0 alias service entries" on page 65
- "Migration information for cluster environment" on page 68

## Upgrading on an existing WebSphere Application Server installation

Use these instructions to upgrade from a previous version that was installed on an existing version of WebSphere Application Server to version 6.2.2. This process installs version 6.2.2 on the existing WebSphere Application Server.

### Before you begin

Before continuing with this upgrade procedure:

- Ensure that your Tivoli Federated Identity Manager installation is at level 6.1.1 or later. To check your installation level:
  1. Log on to the WebSphere Application Server administrative console.
  2. Check the version number on the Welcome page.
- If your Tivoli Federated Identity Manager installation is not at the required level, download the appropriate fix pack.
  1. Go to the Download section of the Tivoli Federated Identity Manager Support site at: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html.
  2. Follow the fix pack installation instructions.
  3. Return to these upgrade instructions.
- Ensure that your existing WebSphere Application Server installation has the appropriate fix pack.
  - If you are using WebSphere Application Server version 6.1, you must install fix pack 15.
  - If you are using WebSphere Application Server version 7.0, you must install fix pack 17.
  - If you are using WebSphere Application Server version 8.0, you must install fix pack 1.

## About this task

This upgrade procedure requires that you install version 6.2.2 on an existing version of WebSphere Application Server where the previous version is installed.

## Procedure

1. Make a note of your existing domain properties.
   a. On the existing system, log on to the WebSphere Application Server administrative console.
   b. Select **Tivoli Federated Identity Manager** > **Domains**.
   c. Select a domain.
   d. Click **Properties**.

   **Note:** You need this information to recreate the connection between the administration console and the management service with the domain wizard.
2. Back up the configuration of your existing environment.
   a. Select **Tivoli Federated Identity Manager** > **Domain Management** to export the existing configuration.
   b. Click **Import and Export Configuration**.
   c. Select the appropriate domain.
   d. Click **Export Configuration**.
   e. When prompted, specify the location where the exported configuration `JAR` file is to be saved.
   f. Click **OK** to save configuration. If the upgrade fails, you can import the saved configuration.
3. Uninstall the previous version of Tivoli Federated Identity Manager. See the procedures in Appendix I, "Uninstalling Tivoli Federated Identity Manager," on page 91.

   **Note:** You must delete the domain from the *console only* so that the configuration information about the WebSphere Application Server or WebSphere cluster is *not* removed.
4. Install Tivoli Federated Identity Manager version 6.2.2. The procedure depends on the product scenario that you deploy, see "Overview of installation and configuration" on page 3 for more information.

   **Attention:**
   - You must install version 6.2.2 on the same computer where the previous version is installed.
   - During the installation, when you are given the option to use an existing version of WebSphere Application Server, select **Yes**.
5. When the installation is successful, you must restart the WebSphere Application Server where the runtime and management service component is installed.
6. When the server restarts, activate and deploy the domain.
   a. Log on to the WebSphere Application Server administrative console.
   b. Select **Tivoli Federated Identity Manager** > **Domains**.
   c. Click **Create** to create a domain. The Domain creation wizard prompts you for domain information.

      For instructions on creating a domain, see the *IBM Tivoli Federated Identity Manager Configuration Guide*.

d. In the Create Domain Complete panel, select the **Make this domain the active management domain** check box to make the domain active.

e. When your deployment uses Tivoli Access Manager as a point of contact, verify that the Tivoli Access Manager properties are set for the new domain.

   1) Select **Tivoli Federated Identity Manager** > **Domains**.

   2) Select your domain. Verify that it is the active domain.

   3) Select **Properties**.

      **Note:** In some upgrade scenarios, properties for Tivoli Access Manager are not automatically migrated. For these scenarios, you must manually enter the properties.

      If the properties for Tivoli Access Manager are missing, you must first unconfigure the runtime before updating the properties:

      a) Select **Tivoli Federated Identity Manager** > **Domain Management** > **Runtime Node Management**.

      b) Select the runtime in the table.

      c) Click **Unconfigure**.

   4) Enter the Tivoli Access Manager properties.

   5) Click **OK**.

f. Select **Tivoli Federated Identity Manager** > **Domain Management** > **Runtime Node Management**.

   **Note:** If the following error shows, you can ignore it and continue with the next step:

   ```
   FBTCON166E: An error was encountered while retrieving environmental
   settings. Check the environmental settings
   and try again.
   ```

g. Click **Deploy Runtime**.

h. Select the runtime in the table.

i. Click **Configure**.

### What to do next

For some deployments, there are additional tasks required. Complete the following tasks if they apply to your environment:

- “Making Java calls made from XSLT files work properly after upgrading” on page 64
- “Migration information for cluster environment” on page 68

## Upgrading on an embedded WebSphere Application Server installation

You can upgrade Tivoli Federated Identity Manager from a previous version of the embedded WebSphere Application Server. The upgrade is installed on the embedded version.

### Before you begin

- Ensure that your installation is at level 6.1.1.1 or later. To check your installation level:
  1. Log on to the WebSphere Application Server administrative console.
  2. Check the version number on the Welcome page.

- If your installation is not at the required level, download the appropriate fix pack.
  1. Go the Download section of the Tivoli Federated Identity Manager Support site: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html.
  2. Follow the fix pack installation instructions.
  3. Return to these upgrade instructions.
- Ensure that you:
  – Have copies of the SSL certificates from your current environment.
  – Have these certificates available for your new environment.

## About this task

This procedure requires that you install version 6.2.2 on the embedded version of WebSphere Application Server.

## Procedure

1. Find out and make a note of your existing domain properties.

   **Note:** When the domain wizard recreates the connection between the administrative console and the management service, it requires this information.
   a. On the existing system, log on to the WebSphere Application Server administrative console.
   b. Click **Tivoli Federated Identity Manager** > **Domains**.
   c. Select a domain.
   d. Click **Properties**.
2. Back up the configuration of your existing environment.
   a. Select **Tivoli Federated Identity Manager** > **Domain Management** to export the existing configuration.
   b. Click **Import and Export Configuration**.
   c. Select the appropriate domain.
   d. Click **Export Configuration**.
   e. When prompted, specify the location where you want to save the exported JAR file. Use this file to import your configuration into the 6.2.2 version installation.
   f. Click **OK**.
3. Uninstall the previous version of Tivoli Federated Identity Manager. See Appendix I, “Uninstalling Tivoli Federated Identity Manager,” on page 91.
4. Install Tivoli Federated Identity Manager version 6.2.2. The procedure depends on the product scenario that you deploy. See “Overview of installation and configuration” on page 3 for more information.

   **Attention:** During the installation, when asked if you want to use an existing version of WebSphere Application Server, select **No**.
5. When the installation is successful, restart the WebSphere Application Server where the runtime and management services is installed.
6. Create and deploy a domain.
   a. Log on to the WebSphere Application Server administrative console.
   b. Select **Tivoli Federated Identity Manager** > **Domains**.

c. Click **Create** to create a domain. The Domain creation wizard prompts for domain information.

   For further instructions on creating a domain, see the *IBM Tivoli Federated Identity Manager Configuration Guide*.

d. Supply the information from step 1 on page 60.

e. Verify that the Tivoli Access Manager domain properties that you entered are correct.

f. In the Create Domain Complete panel, select the **Make this domain the active management domain** check box to make the domain active.

g. Select **Tivoli Federated Identity Manager** > **Domain Management** > **Runtime Node Management**.

h. Click **Deploy Runtime**.

i. Select the runtime in the table.

j. Click **Configure**.

7. Import the configuration that you exported in step 2 on page 60.

   a. From the WebSphere Application Server administrative console, select **Tivoli Federated Identity Manager** > **Domain Management** > **Import and Export Configuration** > **Import Configuration**.

   b. Select the domain into which you want to import the configuration archive.

   c. At **Configuration Archive**, take one of the following actions:

      - Enter the fully qualified path name to the exported `JAR` file. For example: `/tmp/fimconfig_20061011–114614–0500.jar`.
      - **Browse** to the file.

   d. Click **Import Configuration**.

8. Review your configuration to ensure that the importing process completed successfully.

9. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.

10. Replace the SSL certificates on the version 6.2.2 system with the SSL certificates and configuration that you intend to use. See the procedures in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

### What to do next

Go to “Making Java calls made from XSLT files work properly after upgrading” on page 64 if appropriate for your environment.

## Upgrading on a new WebSphere Application Server installation

Use these instructions to upgrade to Tivoli Federated Identity Manager version 6.2.2 on a new version of WebSphere Application Server.

### Before you begin

Before continuing with this upgrade procedure:

- Ensure that your Tivoli Federated Identity Manager installation is at level 6.1.1 or later. To check your installation level:
  1. Log on to the WebSphere Application Server administrative console.
  2. Check the version number on the Welcome page.

- If your Tivoli Federated Identity Manager installation is not at the required level, download the appropriate fix pack.
  1. Go to the Download section of the Tivoli Federated Identity Manager Support site at: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html.
  2. Follow the fix pack installation instructions.
  3. Return to these upgrade instructions.
- Ensure that you:
  - Have the appropriate fix pack for the new WebSphere Application Server installation.
    - If you use WebSphere Application Server version 6.1, you must install fix pack 15.
    - If you use WebSphere Application Server version 7.0, you must install fix pack 17.
    - If you use WebSphere Application Server version 8.0, you must install fix pack 1.
  - Have copies of the SSL certificates from your current environment.
  - Have these certificates available for your new environment.

## About this task

The following procedure describes the steps you must complete when you are upgrading to a new version of a WebSphere instance.

**Note:** You must install the new version of WebSphere Application Server and Tivoli Federated Identity Manager in the same machine as the previous versions were installed. Otherwise, this procedure fails.

## Procedure

1. Make a note of your existing domain properties.
   a. On the existing system, log on to the WebSphere Application Server administrative console.
   b. Select **Tivoli Federated Identity Manager** > **Domains**.
   c. Select a domain.
   d. Click **Properties**.
2. Back up the configuration of your existing environment.
   a. Select **Tivoli Federated Identity Manager** > **Domain Management** to export the existing configuration.
   b. Click **Import and Export Configuration**.
   c. Select the appropriate domain.
   d. Click **Export Configuration**.
   e. When prompted, specify the location where you want to save the exported configuration JAR file. Use this file to import your configuration into the 6.2.2 version installation.
   f. Click **OK**.
3. Uninstall the previous version of Tivoli Federated Identity Manager.

   See Appendix I, “Uninstalling Tivoli Federated Identity Manager,” on page 91 for details.
4. Uninstall the previous version the WebSphere Application Server.

See the topic on Uninstalling WebSphere Application Server in the WebSphere Application Server Information Center: http://publib.boulder.ibm.com/infocenter/wasinfo/v8r0/index.jsp.

5. Install WebSphere Application Server. See "Installing WebSphere Application Server" on page 18.
6. Install Tivoli Federated Identity Manager version 6.2.2.

   The procedure depends on the product scenario that you deploy. See "Overview of installation and configuration" on page 3 for more information.

   **Attention:**

   - You must install version 6.2.2 on the same computer where the previous version had been installed.
   - During the installation, when you are given the option to use an existing version of WebSphere Application Server, select **Yes**.
7. When the installation is successful, you must restart the WebSphere Application Server where the runtime and management service component is installed.
8. Create and deploy a domain.
   a. Log on to the WebSphere Application Server administrative console.
   b. Select **Tivoli Federated Identity Manager** > **Domains**.
   c. Click **Create** to create a domain. The Domain creation wizard prompts you for domain information.

      For instructions on creating a domain, see the *IBM Tivoli Federated Identity Manager Configuration Guide*.
   d. Supply the domain properties that you noted in step 1 on page 62.
   e. Verify that the Tivoli Access Manager domain properties that you entered are correct.
   f. In the Create Domain Complete panel, select the **Make this domain the active management domain** check box to make the domain active.
   g. Select **Tivoli Federated Identity Manager** > **Domain Management** > **Runtime Node Management**.

      **Note:** If the following error shows, you can ignore it and continue with the next step:

      ```
      FBTCON166E: An error was encountered while retrieving environmental
      settings. Check the environmental settings
      and try again.
      ```
   h. Click **Deploy Runtime**.
   i. Select the runtime in the table.
   j. Click **Configure**.
9. Import the configuration that you exported in step 2 on page 62.
   a. From the WebSphere Application Server administrative console, select **Tivoli Federated Identity Manager** > **Domain Management** > **Import and Export Configuration** > **Import Configuration** to import the configuration archive.
   b. Select the domain into which you want to import the configuration archive.
   c. At **Configuration Archive**, take one of the following actions:
      - Enter the fully qualified path name to the exported `JAR` file. For example: `/tmp/fimconfig_20061011–114614–0500.jar`.
      - Click **Browse** to search for the file.

d. Click **Import Configuration**.

10. Review your configuration to ensure that the importing process completed successfully.
11. Click **Load configuration changes to Tivoli Federated Identity Manager runtime**.
12. Replace the SSL certificates on the version 6.2.2 system with the SSL certificates and configuration that you intend to use. See the procedures in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

## Making Java calls made from XSLT files work properly after upgrading

Starting with WebSphere Application Server, version 7, you cannot make Java calls from XSLT files. If Java is required, implement and deploy a Java mapping module.

### About this task

You might have made Java calls from XSLT files in a previous version of Tivoli Federated Identity Manager. To keep these calls working properly after an upgrade, place the `.jar` file with the `XSLT` extension class in the `ext` subdirectory.

### Procedure

1. Go to the `/ext` directory.
2. Locate the `.jar` file contains the XSLT extension class.
3. Move the `.jar` file to the appropriate directory.

   **AIX** `/usr/IBM/WebSphere/AppServer/java/jre/lib/ext/`

   **Linux or Solaris**
   `/opt/IBM/WebSphere/AppServer/java/jre/lib/ext/`

   **Windows**
   `C:\Program Files\IBM\WebSphere\AppServer\java\jre\lib\ext\`
4. Restart WebSphere Application Server.

## Upgrading LDAP

Use the LDAP upgrade tool to preserve existing aliases from earlier versions of Tivoli Federated Identity Manager.

### About this task

In the earlier Tivoli Federated Identity Manager versions (before to 6.2.1), the LDAP alias service created aliases only for user accounts that existed in the LDAP server.

In versions 6.2.1 and 6.2.2, the LDAP alias service stores aliases for any user identifier. The LDAP attribute that stores the user identifier differs from earlier versions. You must run the tool to preserve any existing aliases from earlier versions.

The LDAP upgrade tool completes the migration process. It does the following tasks:

- Moves user aliases to Tivoli Federated Identity Manager Version 6.2.2.
- Performs a reverse migration to earlier versions.

- Migrates directly.
- Produces an `LDIF` file with the required changes. An `LDIF` file is manually reviewed and applied to the LDAP server.

The entry parameters for the LDAP upgrade tool resemble the parameters in the **`ldapsearch`** command. The parameters include

- `-reverse` for performing a reverse migration.
- `-deleteAbandonedEntries` for deleting any entries pointing to a DN that no longer exists. This process occurs before the migration step.
- `-Z` for enabling the SSL connection to the LDAP server.

### Procedure

1. Open the command prompt.
2. Run the following command:

   **Note:** The `.jar` file for the tool is at `FIM_install_directory/tools/ldap/itfim-ldap.jar`.

   ```
   java -classpath [itfim-ldap.jar] com.tivoli.am.fim.ldap.MigrateLDAP
      -h [LDAP server] -p [LDAP port, normally 389] -D [bind credential]
      -w [bind password] -ldif /tmp/fim622-migration.ldif
   ```

## Migrating SAML 2.0 alias service entries

Use the alias service migration tool to preserve existing aliases from earlier versions of Tivoli Federated Identity Manager.

### About this task

The alias service stores mappings between a user identity and one or more string aliases on a per *federation context* basis. In the actual alias service interfaces, this *federation context* is also called as the *partner ID*. The primary clients of the alias service are SAML 2.0 federations by using persistent name identifiers.

In the earlier versions of Tivoli Federated Identity Manager (before 6.2.2), the *federation context* is the ProviderID of the SAML partner. There is no difference between the federation context if two or more federations import the same partner metadata. This task might cause potential privacy and functional problems.

In this version, a unique identifier is introduced in the partner ID parameter of the UserIdDescriptor object that is passed to the alias service client. This approach includes the federation ID in the partner ID as part of alias service operations for SAML 2.0 federations. It also uses a per-partner federation property to toggle how a partner stores and retrieves aliases from the alias service.

Existing aliases and federations work without any migration. But if they are modified to use the new alias service format, you must use the alias service migration tool to migrate existing aliases.

Tivoli Federated Identity Manager provides an alias service delegate so that an authenticated user can manage their alias service entries. The delegate is accessed through the `/sps/alias` URI and uses a query string parameter called **`partner`** to determine which partner to obtain aliases for.

For SAML 2.0 federations that are using the new format of storing aliases, the query string parameter value must be in the format federationID|partnerID. For example:

**For old format aliases:**
    https://fim1.ibm.com:9443/sps/alias?partner=https://fim2.ibm.com:9443/sps/saml20sp/saml20

**For new format aliases:**
    https://fim1.ibm.com:9443/sps/alias?partner=https://fim1.ibm.com:9443/sps/saml20idp/saml20|https://fim2.ibm.com:9443/sps/saml20sp/saml20

## Procedure

1. On a computer that hosts the Tivoli Federated Identity Manager management service, access the command line.
2. Configure the CLASSPATH to include the following jar files:
   - itfim-alias-migration.jar (available from <*FIM_HOME*>/tools/aliasmigration/ directory)
   - The WebSphere Application Server web services thin client jar (available from <*WAS_HOME*>/runtimes/ and commonly called com.ibm.ws.webservices.thinclient_*X.Y.Z*.jar, where *X.Y.Z* depends on the WebSphere Application Server version being used)
   - com.ibm.ws.security.crypto.jar (available from <*WAS_HOME*>/plugins/)

   For example, enter the following command in a UNIX or Linux command line:
   ```
   CLASSPATH=.:/opt/IBM/WebSphere/AppServer/plugins/
   com.ibm.ws.security.crypto.jar:/opt/IBM/FIM/tools/aliasmigration/itfim-
   alias-migration.jar:/opt/IBM/WebSphere/AppServer/runtimes/
   com.ibm.ws.webservices.thinclient_7.0.0.jar
   ```
3. Perform one of the following steps:

   **UNIX** Load the setupCmdLine.sh script into the current shell (../setupCmdLine.sh).

   setupCmdLine.sh is located in <*WAS_HOME*>/profiles/<profile_name>/bin, where <*WAS_HOME*> is typically /opt/IBM/WebSphere/AppServer.

   **Windows**
   Run the setupCmdLine.bat file.

   setupCmdLine.bat is located in <*WAS_HOME*>/profiles/<profile_name>/bin, where <*WAS_HOME*> is typically C:\Program Files\WebSphere\AppServer.
4. Run the following command to start the alias service migration tool:
   ```
   java com.tivoli.am.fim.alias.migration.AliasMigration
   -type <ldap|db2|derby> -infoscvurl <http(s)://tfim-host:tfim-port/Info/
   InfoService> -partnerName <partner display name>
   -federationName <federation display name>
   ```

   The following table outlines the common JDBC or LDAP-specific options of the tool:

*Table 19. Alias service migration tool parameters*

| Parameter | Description | Other |
|---|---|---|
| **-type <type>** | The type of alias service that is being migrated. Can be either LDAP, DB2®, or Derby. | Required, All types |

*Table 19. Alias service migration tool parameters (continued)*

| Parameter | Description | Other |
|---|---|---|
| **-infosvcurl <url>** | The URL for the Tivoli Federated Identity Manager Infomation Service, which is typically `http://fim-host:fim-port/Info/InfoService`. | Required, All types |
| **-infosvcuser <username>** | The user name for authenticating with the Tivoli Federated Identity Manager Information Service, which is used in web service call BA header. | Optional, All types |
| **-infosvcpwd <password>** | The password for authenticating with the Tivoli Federated Identity Manager Information Service, which is used in web service call BA header. | Optional, All types |
| **-partnerName <display name>** | The display name of the partner whose aliases must be migrated. | Required, All types |
| **-federationName <display name>** | The display name of the federation whose aliases must be migrated. | Required, All types |
| **-reverse** | Perform a reverse migration as opposed to a forward migration. | Optional, All types |
| **-h <host>** | The host parameter of the LDAP server for the alias service. | Required, LDAP only |
| **-p <port>** | The port parameter of the LDAP server for the alias service. Default value is `389`. | Optional, LDAP only |
| **-D <bind dn>** | The LDAP bind credential. For example, `cn=root`. | Optional, LDAP only |
| **-w <password>** | The LDAP bind password. | Optional, LDAP only |
| **-file <filename>** | Outputs the alias changes to a file. For LDAP, this parameter is an LDIF file. For JDBC, this file contains a series of SQL statements. | Optional, All types |
| **-Z** | Enables the SSL connection to the LDAP server. | Optional, LDAP only |
| **-configRoot <suffix>** | Overrides the alias service config root. Default value is `cn=itfim`. | Optional, LDAP only |
| **-silent** | Performs migration without a confirmation prompt for LDAP access. | Optional, LDAP only |

**Notes:**

a. You must use the WebSphere Application Server Java to run this tool.

b. If the Tivoli Federated Identity Manager Information Service requires authentication though BA header, you can pass parameters to the tool. See Table 19 on page 66 for details.

   If the Information Service uses an SSL endpoint, you must configure the SSL client properties. One way to configure this is to specify `'com.ibm.SSL.ConfigURL'` as a Java system property and point it to the WebSphere Application Server `ssl.client.props` file. This file is typically available at `<WAS_HOME>/profiles/AppSrv01/properties/ssl.client.props`.

   To set this property as a Java system property, specify it on the command line:

   ```
   -Dcom.ibm.SSL.ConfigURL=file://<WAS_HOME>/profiles/AppSrv01/
      properties/ssl.client.props
   ```

   A sample command that configures the SSL client properties:

   ```
   java -Dcom.ibm.SSL.ConfigURL=file://<WAS_HOME>/profiles/AppSrv01/properties/
      ssl.client.props com.tivoli.am.fim.alias.migration.AliasMigration
      -type derby -infosvcurl https://fim.ibm.com:9443/Info/InfoService
      -federationName saml20idp -partnerName saml20sp -infosvcuser fimadmin
      -infosvcpwd password
   ```

   An example of SSL connection on LDAP is:

   ```
   java -Dcom.ibm.SSL.ConfigURL=file://<WAS_HOME>/profiles/AppSrv01/properties/
      ssl.client.props com.tivoli.am.fim.alias.migration.AliasMigration
      -type ldap -infosvcurl http://fim1.demo.com:9080/Info/InfoService
      -partnerName "saml20sp_CoName" -infosvcuser fimadmin -infosvcpwd password
      -h fim1.demo.com -D cn=root -w Passw0rd -federationName "saml20idp"
      -p 636 -Z -reverse -file ldif_sec.txt
   ```

   You can specify a Java system property to output logging information. To enable Java logging, specify `-DLogging.Level=<FINE|FINER|FINEST|ALL>` on the command line as part of tool invocation.

   Here is an example:

   ```
   java -DLogging.Level=ALL com.tivoli.am.fim.alias.migration.AliasMigration
      -type ldap -infosvcurl http://fim1.demo.com:9080/Info/InfoService
      -partnerName "saml20sp_CoName" -h fim1.demo.com -D cn=root -w Passw0rd
      -federationName saml20idp -reverse -silent -file ldif.txt
   ```

## Migration information for cluster environment

The name of the Tivoli Federated Identity Manager runtime changes when deployed into WebSphere clusters. This change might require you to manually update some application information for the runtime.

The 6.2.2 installation supports an automated migration feature that detects the presence of a previous version. You must reapply your own customization after migration when you deploy Tivoli Federated Identity Manager into a WebSphere cell that supports multiple clusters.

In version 6.1.1, the runtime was deployed to a cluster as an application named **ITFIMRuntime-*<clustername>***. There might be an **ITFIMRuntime-*<clustername>*** application deployed to each cluster in the cell.

In 6.2.2, the runtime is deployed to a cluster as application name **ITFIMRuntime**. For each cluster, the **ITFIMRuntime** module-to-server mappings are updated with the cluster location. In this situation, there is one **ITFIMRuntime** application for the cell. The module-to-server mappings specify where it is installed.

When you deploy the runtime for Version 6.2.2, the deployment checks for the existence of an **ITFIMRuntime-*<clustername>*** application. When it finds one, the deployment moves the application information to the newly deployed **ITFIMRuntime** application. The deployment then removes the **ITFIMRuntime-*<clustername>*** application.

If there is more than one **ITFIMRuntime-*<clustername>*** application, the deployment program moves only the one for the cluster into which the new **ITFIMRuntime** application has been deployed. It deletes the remaining older runtime applications.

When the other clusters in the cell are deployed, the **ITFIMRuntime** module-to-server mappings table is updated with the locations of the other clusters. This update installs **ITFIMRuntime** for each of the other clusters.

Some application information from an **ITFIMRuntime-*<clustername>*** deployment might require manual updating in the **ITFIMRuntime** application for Version 6.2.2. For example, update the *security role to user/group mappings* of the **ITFIMRuntime** application if there is more than one cluster in a cell.

# Appendix B. tfimcfg reference

Use the `tfimcfg` command to configure LDAP settings for the Integrated Solutions Console installation and to configure WebSEAL as a Point of Contact server.

## tfimcfg usage

```
TFIM Autoconfiguration Tool Version 6.2.2 [110529a]

Usage: java -jar tfimcfg.jar [-action <mode>] [options]
The tfimcfg tool has several modes of operation.  Each mode uses different
command line options.

Configuring and unconfiguring WebSEAL servers:
   -action tamconfig: configures a WebSEAL server.  This mode is the default.
   Options:
      -cfgfile <file>: WebSEAL configuration file.
         This option is required.
      -rspfile <file>: response file for non-interactive configuration.
         Default: interactive configuration
      -record: generate response file without making changes to WebSEAL configuration
      -sslfactory <ssl connection factory>: secure socket layer connection factory.
         If FIPS is enabled, this option must be set to TLS.
         Default: SSL

   -action tamunconfig: unconfigures a WebSEAL server.
   Options:
      -cfgfile <file>: WebSEAL configuration file.
         This option is required.
      -rspfile <file>: response file for non-interactive unconfiguration.
         Default: interactive configuration
      -sslfactory <ssl connection factory>: secure socket layer connection factory.
         If FIPS is enabled, this option must be set to TLS.
         Default: SSL

Configuring and unconfiguring LDAP servers:
   -action ldapconfig: configures an LDAP server.
      -rspfile <file>: response file to control the configuration. The
         response file should be based on the sample ldapconfig.properties
         file. This option is required.

   -action ldapunconfig: unconfigures an LDAP server.
      -rspfile <file>: response file to control the configuration. The
         response file should be based on the sample ldapconfig.properties
         file. This option is required.
```

When you run `tfimcfg`:

- To configure an LDAP server, it also creates several user accounts. The user accounts are required by the single sign-on demonstration application.
- To set up the LDAP accounts for the administration console user, you call `tfimcfg` with the following parameters:

  ```
  -action ldapconfig
  ```

  This action creates the demonstration user accounts.

## Configure Tivoli Access Manager using the tfimcfg.jar tool

You can configure Tivoli Access Manager WebSEAL as a contact point for a federation using the `tfimcfg.jar` tool.

Run the command (`java -jar tfimcfg.jar`) to view a list of options associated with the tool.

See Using tfimcfg to Configure WebSEAL for Federations.

## tfimcfg limitation with Sun Java 1.4.2.4

Certain versions of Sun Java are incompatible with `tfimcfg`.

The incompatibility causes the following error:

```
HPDAZ0602E Corrupted file: Insufficient information to contact Policy Server
```

The problem occurs because the Sun JRE cannot read the keystores generated by Tivoli Access Manager `PDJrteCfg`. When this error occurs, you must:

- Apply the latest JRE patches from Sun.
- If the problem persists after applying the patches from Sun, use an IBM JVM.

## tfimcfg LDAP properties reference

The `tfimcfg` utility reads a properties file to obtain the values for configuring an LDAP user registry. The properties file contains values that you can modify.

**`ldap.hostname`**
Specifies he LDAP server host name. Default: `localhost`

**`ldap.port`**
Specifies the LDAP port number. Default: `389`

The default value is for non-SSL communication. If you configure the LDAP server to communicate with SSL, the default port is 636.

**`ldap.suffix.add`**
Specifies whether `tfimcfg` adds suffixes to the LDAP server as needed. Supports only IBM Tivoli Directory Server Versions 6.1, 6.0, and 5.2.

Default: `ldap.suffix.add=true`

**`ldap.suffix.user.configuration`**
**`ldap.organization.configuration`**
Specifies whether `tfimcfg` creates LDAP containers to store Tivoli Federated Identity Manager users and groups. The users and groups are:

- Server users and groups
- Installation Verification Tool (IVT) users and groups

If you do not require them or already have LDAP containers for them, set these values to `false`.

When `ldap.organization.configuration` is `true`, `tfimcfg` creates the `dc=example,dc=com` LDAP objects.

Default:

```
ldap.suffix.user.configuration=true
ldap.organization.configuration=true
```

**`ldap.suffix.alias.configuration`**
Specifies whether `tfimcfg` creates an LDAP suffix to store single sign-on aliases. The default alias is `cn=itfim`.

```
ldap.suffix.alias.configuration=true
```

**`ldap.suffix.tam.configuration`**
Specifies whether `tfimcfg` creates the `secAuthority=Default` suffix for Tivoli Access Manager.

- If you have already configured Tivoli Access Manager, set this value to `false`.
- When Tivoli Access Manager is not using this LDAP server, set this value to `false`.

```
ldap.suffix.tam.configuration=true
```

**Note:** If the `secAuthority=Default` suffix already exists, `tfimcfg` ignores the value of the `ldap.suffix.tam.configuration` property.

**`ldap.fim.configuration`**
Specifies whether `tfimcfg` configures LDAP for the Tivoli Federated Identity Manager alias service.

Default value: `true`.

**`ldap.ivt.sp.configuration`**
Specifies whether `tfimcfg` creates users and groups for the service provider in the Installation Verification Tool (IVT) application.

Default value: `true`.

**`ldap.ivt.ip.configuration`**
Specifies whether `tfimcfg` creates users and groups for the identity provider in the Installation Verification Tool (IVT) application.

Default value: `true`.

**`ldap.modify.acls`**
Specifies whether `tfimcfg` attaches appropriate ACLs (access control lists) to the LDAP server. ACLs grant read and write access to the Tivoli Federated Identity Manager administrative users created by `tfimcfg`.

**Note:** `tfimcfg` attaches ACLs for IBM LDAP and Sun ONE servers. For other LDAP servers, you must attach the ACLs manually.

If you set the value to `false`, you must attach the ACLs manually.

Default value: `true`.

**`ldap.admin.dn`**
Specifies the DN used by the LDAP administrator to issue bind requests.

Default: `cn=root`

**`ldap.admin.password`**
Specifies the password for the LDAP administrator.

Default: `passw0rd`

**`ldap.security.enabled`**
Specifies whether communication with the LDAP server must use SSL.

Default: `false`.

**`ldap.security.trusted.jks.filename`**
Specifies the name of the Java keystore that contains the signer of the LDAP-presented SSL certificate that LDAP presents during trusted communications.

**`ldap.suffix.user.dn`**
**`ldap.suffix.user.name`**
**`ldap.suffix.user.attributes`**

**ldap.suffix.user.objectclasses**

When you want tfimcfg.jar to create LDAP containers for your users, set these values to control the Distinguished Names (DNs) that are used.

Defaults:

```
ldap.suffix.user.dn=dc=com
ldap.suffix.user.name=com
ldap.suffix.user.attributes=dc
ldap.suffix.user.objectclasses=domain
```

**ldap.suffix.alias.dn**

Specifies the Distinguished Name (DN) to use for storing single sign-on alias. This value of this property must begin with cn=. Modify this value when you do not want to use the default DN.

Default:

```
ldap.suffix.alias.dn=cn=itfim
```

**ldap.organization.dn**
**ldap.organization.name**
**ldap.organization.attributes**
**ldap.organization.objectclasses**

When you want tfimcfg.jar to create LDAP containers for your groups, you can set these values to control the Distinguished Names (DNs) that are used.

Defaults:

```
ldap.organization.dn=dc=example,dc=com
ldap.organization.name=example
ldap.organization.attributes=dc
ldap.organization.objectclasses=domain
```

**ldap.user.container.dn**
**ldap.group.container.dn**

Specifies the distinguished names to use for the containers for users and groups.

Defaults:

```
ldap.user.container.dn=cn=users,dc=example,dc=com
ldap.group.container.dn=cn=groups,dc=example,dc=com
```

**ldap.fim.server.bind.dn**
**ldap.fim.server.bind.shortname**
**ldap.fim.server.bind.password**

Specifies the distinguished name, short name, and password that the Tivoli Federated Identity Manager server (application) uses to bind to the LDAP server.

Default:

```
ldap.fim.server.bind.dn=uid=fimserver,cn=users,dc=example,dc=com
ldap.fim.server.bind.shortname=fimserver
ldap.fim.server.bind.password=passw0rd
```

**ldap.fim.admin.group.dn**
**ldap.fim.admin.group.shortname**

Specifies the distinguished name and short name for the Integrated Solutions Console administration group.

Default:

```
ldap.fim.admin.group.dn=cn=fimadmins,cn=groups,dc=example,dc=com
ldap.fim.admin.group.shortname=fimadmins
```

**ldap.user.objectclasses**
**ldap.group.objectclasses**
**ldap.user.shortname.attributes**

Specifies the values for LDAP containers for `user objectclass`, `group objectclass`, and `user shortname` attributes.

Default:

```
ldap.user.objectclasses=person,organizationalPerson,inetOrgPerson
ldap.group.objectclasses=groupOfUniqueNames
ldap.user.shortname.attributes=cn,sn,uid
```

## Default ldapconfig.properties file

The `ldapconfig.properties` file is distributed as part of the runtime and management service component. Many properties have default values.

```
ldap.hostname=localhost
ldap.port=389

# If true, new suffixes will be added to the LDAP server as needed.
# Only supported for IDS 5.2 and 6.0
ldap.suffix.add=true

# If true, data for the LDAP user suffix (dc=com, by default) will be
# created.
ldap.suffix.user.configuration=true

# If true, data for the SSO alias suffix (cn=itfim, by default) will be
# created.
ldap.suffix.alias.configuration=true

# If true, create the secAuthority=Default suffix for TAM
ldap.suffix.tam.configuration=true
ldap.fim.configuration=true
ldap.ivt.sp.configuration=true
ldap.ivt.ip.configuration=true
ldap.organization.configuration=true
ldap.modify.acls=true

ldap.admin.dn=cn=root
ldap.admin.password=passw0rd

ldap.security.enabled=false
ldap.security.trusted.jks.filename=

ldap.suffix.user.dn=dc=com
ldap.suffix.user.name=com
ldap.suffix.user.attributes=dc
ldap.suffix.user.objectclasses=domain

# DN to use for storing SSO aliases.  This must begin with cn=
ldap.suffix.alias.dn=cn=itfim

ldap.organization.dn=dc=example,dc=com
ldap.organization.name=example
ldap.organization.attributes=dc
ldap.organization.objectclasses=domain

ldap.user.container.dn=cn=users,dc=example,dc=com
ldap.group.container.dn=cn=groups,dc=example,dc=com

ldap.fim.server.bind.dn=uid=fimserver,cn=users,dc=example,dc=com
ldap.fim.server.bind.shortname=fimserver
ldap.fim.server.bind.password=passw0rd

ldap.fim.admin.group.dn=cn=fimadmins,cn=groups,dc=example,dc=com
ldap.fim.admin.group.shortname=fimadmins

ldap.user.objectclasses=person,organizationalPerson,inetOrgPerson
ldap.group.objectclasses=groupOfUniqueNames
ldap.user.shortname.attributes=cn,sn,uid
```

*Figure 1. Default values for `ldapconfig.properties`*

## Sample results from tfimcfg configuration of LDAP

This topic provides an example for running `tfimcfg` and the results.

The command for running `tfimcfg` to configure LDAP entries for the alias service and the demonstration application is

```
java -jar tfimcfg.jar -action ldapconfig -rspfile
   /tmp/ldapconfig.properties
```

The following content sample results from running the command on an identity provider. The example uses an `ldapconfig.properties` file that has the default values.

```
Configuring LDAP server.
LDAP server vendor: International Business Machines (IBM),
   version 6.0.
Adding LDAP suffix secAuthority=Default.
Reloading IBM Directory Server configuration.
Adding LDAP suffix dc=com.
Reloading IBM Directory Server configuration.
Creating LDAP object dc=com.
Adding LDAP suffix cn=itfim-cmd.
Reloading IBM Directory Server configuration.
Creating LDAP object cn=itfim-cmd.
Creating LDAP object dc=example,dc=com.
Creating LDAP object cn=users,dc=example,dc=com.
Creating LDAP object cn=groups,dc=example,dc=com.
Creating LDAP object uid=fimserver,cn=users,dc=example,dc=com.
Creating LDAP object cn=fimadmins,cn=groups,dc=example,dc=com.
Adding user uid=fimserver,cn=users,dc=example,dc=com to group
   cn=fimadmins,cn=groups,dc=example,dc=com.
Creating LDAP object o=identityprovider,dc=com.
Creating LDAP object cn=MEemployee,o=identityprovider,dc=com.
Creating LDAP object cn=MEmanager,o=identityprovider,dc=com.
Creating LDAP object cn=MEexecutive,o=identityprovider,dc=com.
Creating LDAP object cn=elain,o=identityprovider,dc=com.
Creating LDAP object cn=mary,o=identityprovider,dc=com.
Creating LDAP object cn=chris,o=identityprovider,dc=com.
Updating IBM LDAP ACLs for suffix CN=ITFIM-CMD.
Updating IBM LDAP ACLs for suffix SECAUTHORITY=DEFAULT.
Updating IBM LDAP ACLs for suffix DC=COM.
Done updating LDAP server configuration.
```

*Figure 2. Sample results from `tfimcfg.jar`*

## Modifying the Object Class of Users Created by tfimcfg Utility

The **`tfimcfg`** utility with the **`-action ldapConfig`** argument creates a set of demonstration users in LDAP.

### About this task

The object classes of the demonstration users are incompatible with the default WebSphere search parameters for user entries in IBM Tivoli Directory Server. The demonstration mapping rules assume that this set of demonstration users is available in LDAP.

The **`tfimcfg`** utility creates user entries in LDAP with these object classes: `person,organizationalPerson,inetOrgPerson`. The WebSphere search parameters for Tivoli Directory Server require that user entries contain `objectclass ePerson`. Due to this mismatch of object classes, WebSphere cannot locate the demonstration users in the user registry.

To work around this situation, modify the object classes of users created by the tfimcfg utility.

## Procedure

1. In a text editor, open the ldapconfig.properties file.
   ```
   /opt/IBM/FIM/tools/tamcfg/ldapconfig.properties
   ```
2. Locate the following line:
   ```
   ldap.user.objectclasses=person,organizationalPerson,
     inetOrgPerson
   ```
3. Modify the line.
   ```
   ldap.user.objectclasses=person,ePerson,organizationalPerson,
     inetOrgPerson
   ```
4. Run the tfimcfg -action ldapConfig utility.

## What to do next

To view a sample result of this change, use the following command:

```
# idsldapsearch -D cn=root -w passw0rd -b dc=com uid=mary
cn=mary,o=identityprovider,dc=com
displayName=Mary Manor
mail=mmanor@identityprovider.example.com
uid=Mary
userPassword=abcd1234
objectclass=top
objectclass=person
objectclass=ePerson
objectclass=organizationalPerson
objectclass=inetOrgPerson
employeenumber=987-65-4321
sn=Manor
cn=Mary
```

# Appendix C. Configuring user registry for embedded WebSphere

If you installed the embedded version of WebSphere Application Server, the federated repository was configured as your user registry. To use a different registry, you must modify the WebSphere Application Server settings.

## Procedure

1. Log on to the console.
2. Select **Security** > **Secure administration, applications, and infrastructure**.
3. Click **Security Configuration Wizard** to change the user registry.
4. Select **Enable application security** on **Specify extent of protection panel**.
5. Click **Next**.
6. Select the appropriate option for the user registry on **Secure the application serving environment**. Your choices are:
   - **Federated repositories**
   - **Standalone LDAP registry**
   - **Local operating system**
   - **Standalone custom registry**
7. Click **Next**.
8. Specify values for each of the registry configuration settings on **Configure user repository**. The online help provides descriptions of the fields.
9. Click **Next** and finish the wizard.
10. Save your configuration changes.
11. Stop the WebSphere Application Server.
12. Restart the WebSphere Application Server. You must use the same administrative name you used to log in.
13. From the console, select **Tivoli Federated Identity Manager** > **Manage Configuration** > **Domain properties**.
14. In the WebSphere Security section of the panel, update the following values:

    **`Administrative user name`**
    Replace the existing entry with the LDAP administrator account name that you entered in the previous step. For example, `ldapadmin`.

    **`Administrative user password`**
    Enter the password for LDAP administrator.
15. Save the changes.
16. Stop the WebSphere Application Server.
17. Restart the WebSphere Application Server.

# Appendix D. Reinstalling the runtime and management services feature with Tivoli Access Manager

You can uninstall runtime and management services. You can reinstall it later.

The information in this section applies to Tivoli Federated Identity Manager package users. It also applies to organizations that already have IBM Tivoli Access Manager for e-business in their computing environment.

When you install runtime and management services, you use the management console to deploy and configure it.

Configuration creates a Tivoli Access Manager identity for the system that hosts runtime and management services. This configuration completes the same configuration steps taken by administrators. These administrators use the **pdjrte** and **SvrSslCfg** commands to add applications to a Tivoli Access Manager domain.

When you want to remove runtime and management services, you must take the following actions for the existing runtime and management services:

- Remove the Tivoli Access Manager user identity.
- Remove the Tivoli Federated Identity Manager runtime from WebSphere Application Server applications.

Removing runtime and management services does not remove the **pdjrte** configuration. The **pdjrte** configuration contains the keys and certificates that are used when an application identity (such as runtime and management services) contacts the Tivoli Access Manager policy server.

**Note:** Tivoli Federated Identity Manager cannot remove the **pdjrte** configuration. The configuration might be used by another Tivoli Access Manager application.

If you reinstall runtime and management services, you must complete the deployment and configuration steps. When you configure runtime and management services, the configuration inherits the existing **pdjrte** settings. The settings are specific to keys and certificates used by the Tivoli Access Manager policy server. The settings were specified during **pdjrte** configuration.

- If the Tivoli Access Manager settings changed since the original **pdjrte** configuration, you must reconfigure **pdjrte** before the Tivoli Federated Identity Manager can operate successfully.
- To configure Tivoli Federated Identity Manager against a different policy server, you must configure **pdjrte** to work with it.

For more information about **pdjrte**, see the IBM Tivoli Access Manager for e-business documentation.

# Appendix E. Reconfiguring the runtime when Tivoli Access Manager changes

If you configure Tivoli Access Manager multiple times, your certificate does not match the certificate knowledge in the policy server. You must remove files to clear the certificate settings before you can successfully configure the runtime again.

The information in this section applies to Tivoli Federated Identity Manager package users. It also applies to organizations that already have IBM Tivoli Access Manager for e-business in their computing environment.

Configuration can fail when you configure Tivoli Access Manager more than one time.

When you configure Tivoli Access Manager, the following actions happen:

- Creates a key (certificate).
- Places knowledge of that key in the Tivoli Access Manager policy server.

Multiple configurations result in the certificate not matching the certificate knowledge in the policy server.

To clear the certificate settings, you must remove the following files :

```
/opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/PD.properties
/opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/PDCA.ks
```

# Appendix F. Reconfiguring the runtime to a different Tivoli Access Manager server

Reconfiguration of a node to use a different Tivoli Access Manager policy server or authorization server.

## Before you begin

The information in this section applies to Tivoli Federated Identity Manager package users. It also applies to organizations that already have IBM Tivoli Access Manager for e-business in their computing environment.

## Procedure

1. Unconfigure the node.
2. Remove the Tivoli Access Manager certificate files.

   ```
   /opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/PD.properties
   /opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/PDCA.ks
   ```
3. Modify your domain configuration to use revised settings for the new Tivoli Access Manager server.
4. Configure the node.

## What to do next

If the configuration fails, examine the error log file:

```
/opt/IBM/WebSphere/AppServer/java/jre/PolicyDirector/log/
   msg__amj_error1.log
```

# Appendix G. Installing as a user other than root or administrator

If you install Tivoli Federated Identity Manager as a user other than root or Administrator, clean the /tmp directory. When you install the Web plug-in components, you must manually modify some environment variables on the system where the plug-in is installed.

## About this task

When installing as non-root:

- Remove files and directories from the /tmp directory to avoid conflicts during the installation. For example, remove the itfim-wizard-install-optional.log file if it is in the /tmp directory.
- Modify the variables described in the following procedure. If you do not modify the environment variables, the plug-in cannot function properly after installation.

## Procedure

On the system where you want to install the plug-in, make the following changes:

**On Linux (for the Apache HTTP Server or IBM HTTP Server plug-in):**

1. Access a command prompt.
2. Type the following commands:

```
export ITFIMWEBPI=/opt/IBM/FIM/webpi
export PATH=$ITFIMWEBPI/bin:$PATH
```

**On Windows (for the IIS plug-in)**

1. Click **My Computer**.
2. Right-click in the folder, and click **Properties**.
3. Click the **Advanced** tab.
4. Click **Environment variables**.
5. Click **New**.
6. In the **Variable name** field, type a name.
7. In the **Variable value** field, type C:\Program Files\IBM\FIM\webpi.
8. Click **OK**.
9. Change the **PATH** variable to %ITFIMWEBPI%\bin;%PATH%

## Results

You can now continue with the Tivoli Federated Identity Manager installation instructions as applicable for your deployment.

# Appendix H. Running Tivoli Federated Identity Manager as a non-root user

Tivoli Federated Identity Manager can run as a non-root user. You must configure UNIX or Linux systems for this functionality to work. These configuration steps are not required for Windows systems.

## Before you begin

You must successfully install Tivoli Federated Identity Manager and its prerequisites as root.

## About this task

WebSphere Application Server and Integrated Solutions Console require a non-root user as an administrator.

**Note:** When installing as a non-root user, the user ID must match the WebSphere user ID.

These instructions use the following user and group:

- User: `wasadmin`
- Group: `wasgroup`

**Note:** When WebSphere Global Security is enabled, the registry for authenticating users must not be the local operating system registry. You must pick an LDAP registry or other registry. WebSphere uses the root user to access the Local operating system registry. Attempts to access the local operating system registry fail if WebSphere runs as a non-root user with security enabled.

## Procedure

1. As root, install the following software:
   - WebSphere Application Server, version 6.1
   - Integrated Solutions Console
   - Tivoli Federated Identity Manager management service and runtime
   - Tivoli Federated Identity Manager management console
2. Set the WebSphere Application Server version 6.1 environment to run as non-root.
   a. For information about the limitations of non-root installers, see: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.doc/info/aes/ae/cins_nonroot.html
   b. For information about creating profiles for non-root users, see: http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/topic/com.ibm.websphere.base.doc/info/aes/ae/tpro_manage_nonroot.html
   c. Stop all servers and the node agent. As part of the `chmod` commands described in the WebSphere documentation, run the following command for each node that you want to run as non-root:

      ```
      chgrp -R wasgroup /opt/IBM/WebSphere/AppServer/java/bin
      chmod -R g+rwx /opt/IBM/WebSphere/AppServer/java/bin
      ```

3. On the deployment manager computer, run the following commands to change permissions of Tivoli Federated Identity Manager files:

   ```
   chgrp -R wasgroup /opt/IBM/FIM
   chmod -R g+wr /opt/IBM/FIM
   ```

# Appendix I. Uninstalling Tivoli Federated Identity Manager

You must follow the process discussed in this topic to uninstall Tivoli Federated Identity Manager.

Follow this process to uninstall the product:

1. Decide which mode to use: interactive or silent uninstallation.
   - "Interactive uninstallation modes"
   - "Silent uninstallation mode" on page 92
2. Decide which components to remove.
3. Follow the instructions in the appropriate section.
   - "Uninstalling (interactive modes)" on page 93
   - "Uninstalling (silent mode)" on page 95

**Note:** Uninstalling the product does not require uninstalling or rolling back any fix packs.

## Interactive uninstallation modes

Tivoli Federated Identity Manager supports two interactive modes for uninstalling each component.

### Graphical mode

The graphical mode presents a series of panels that prompt for the required information.

*Table 20. Commands to start the uninstallation program*

| Platform | Commands to start the uninstallation program |
|---|---|
| AIX, Linux, or Solaris | **Runtime and management services**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin`<br>**Management console**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin`<br>**WS-Provisioning runtime**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin`<br>**Web services security management**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin` |
| Windows | **Runtime and management services**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`<br>**Management console**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`<br>**WS-Provisioning runtime**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`<br>**Web services security management**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe` |

### Console mode

Tivoli Federated Identity Manager provides the console mode for a non-graphical environment. An example of a non-graphical environment is a server system without a video card. Console mode accomplishes the same tasks and requires the same user input required by the graphical mode.

Choose console mode with the `-console` option.

*Table 21. Commands to start the uninstallation program*

| Platform | Commands to start the uninstallation program |
|---|---|
| AIX, Linux, or Solaris | **Runtime and management services**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin -console`<br>**Management console**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin -console`<br>**WS-Provisioning runtime**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin -console`<br>**Web services security management**<br>`/opt/IBM/FIM/_uninst/uninstaller.bin -console` |
| Windows | **Runtime and management services**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console`<br>**Management console**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console`<br>**WS-Provisioning runtime**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console`<br>**Web services security management**<br>`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console` |

## Silent uninstallation mode

Tivoli Federated Identity Manager supports a *silent mode* uninstallation.

This mode does not require you to provide any input. Input values are read from a file. The component is uninstalled with a common set of options from a script. To use silent mode, you must first create a *response file* that contains the input values.

For more information, see "Uninstalling (silent mode)" on page 95.

## Preparing to uninstall runtime and management services

You must perform certain tasks before you can uninstall the runtime and management services.

### About this task

Before removing the runtime and management services, you must:

- Unconfigure it.
- Undeploy it.
- Remove the Tivoli Federated Identity Manager domain.

This topic describes the process. See the *IBM Tivoli Federated Identity Manager Administration Guide* for complete directions.

### Procedure

1. Verify that the WebSphere Application Server is running.
2. Verify that the Tivoli Access Manager policy server is running.
3. Verify that the LDAP server is running.
4. Unconfigure runtime and management services. This action removes the configuration between the runtime and management services and the Tivoli Access Manager security domain.
5. Undeploy the runtime and management services. This action removes the runtime and management services from the WebSphere list of installed applications.
6. Delete the domain. See the topic on Deleting a domain in the *IBM Tivoli Federated Identity Manager Administration Guide*.

### What to do next

You can now run the uninstallation program in interactive or in silent mode:

- To run the program interactively, see "Uninstalling Tivoli Federated Identity Manager features."
- To run the program in silent mode, see "Uninstalling (silent mode)" on page 95.

# Uninstalling (interactive modes)

You use either graphical or console mode to uninstall the product. You can uninstall several features at the same time on the same server or individually on separate servers.

The following procedures describe the interactive uninstallation modes. For information about silent mode, see "Uninstalling (silent mode)" on page 95.

## Uninstalling Tivoli Federated Identity Manager features

You can uninstall the runtime and management services, management console, or WS-Provisioning runtime in either graphical or console mode.

### Procedure

1. Start the WebSphere Application Server, if it is not already started.
2. Start the uninstallation:

*Table 22. Commands to start the uninstallation program*

| Platform | Command for starting the uninstallation in graphical mode | Command for starting the uninstallation in console mode |
|---|---|---|
| AIX, Linux, or Solaris | `/opt/IBM/FIM/_uninst/uninstaller.bin` | `/opt/IBM/FIM/_uninst/uninstaller.bin -console` |
| Windows | `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe` | `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console` |

3. Select a language.
4. Click **OK**.
5. Click **Next** on the Welcome screen.
6. Select the check box for the features that you want to uninstall.

7. Click **Next**.
8. Specify whether the WebSphere Application Server has administration security enabled.
   - Click **Yes** if administration security is enabled.
   - Click **No** if administration security is not enabled.

   You specified this setting during the WebSphere Application Server installation.
9. Click **Next**.
10. Take one of the following actions.
    - If you did not enable WebSphere Application Server security, go to step 11.
    - If you enabled security:
      a. Enter the requested values.
      b. Click **Next**.
      c. Go to step 11.
11. Take the following actions:
    a. Specify the **WebSphere Application Server installation directory**. You can click **Browse** to select a directory on the file system.
    b. Specify the port number at **WebSphere Application Server SOAP connector port**.
    c. Click **Next**.
12. Verify that the installation summary information is correct.
13. Click **Next**. It might take a few minutes to remove the files. A status bar and a summary panel indicate the progress.
14. Click **Finish**.
15. Required: If you uninstalled the software from a Windows system, restart the system.
16. To completely remove Tivoli Federated Identity Manager, manually delete the application installation directory.

    **Attention:** Do not delete this directory unless you are removing **all** the components.
    - For AIX, Linux, or Solaris:

      ```
      /opt/IBM/FIM
      ```
    - For Windows:

      ```
      C:\Program Files\IBM\FIM
      ```

## Uninstalling Web services security management

You can uninstall Web services security management in either graphical or console mode.

### Procedure

1. Start the uninstallation.

*Table 23. Commands to start the uninstallation program*

| Platform | Starting in graphical mode | Starting in console mode |
|---|---|---|
| AIX, Linux, or Solaris | `/opt/IBM/FIM/_uninst/uninstaller.bin` | `/opt/IBM/FIM/_uninst/uninstaller.bin -console` |

*Table 23. Commands to start the uninstallation program (continued)*

| Platform | Starting in graphical mode | Starting in console mode |
|---|---|---|
| Windows | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe` | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe -console` |

2. Select a language.
3. Click **OK**.
4. Click **Next**.
5. Select Web services security management.
6. Click **Next**.
7. Verify that the WebSphere security information is correct.
8. Click **Next**. Removing files might take a few minutes. A status bar and summary panel indicate progress.
9. Click **Finish**.

   **Attention:** Do not delete the `_uninst_wssm` directory after uninstalling Web services security management. Removed the directory structure *only* after removing *all* Tivoli Federated Identity Manager components.

# Uninstalling (silent mode)

You can create and use a response file to uninstall Tivoli Federated Identity Manager. You can uninstall several features at the same time on the same server or individually on separate servers.

**Note:** Example response files are in the `/rsp` directory on the Tivoli Federated Identity Manager CD or ISO image.

The procedures for the silent uninstallation mode describe creating and employing response files.

## Creating a response file for uninstallation

You can create a response file to uninstall the product in silent mode.

### About this task

A response file records the actions to be performed by the uninstallation wizard.

**Note:** If you want to uninstall individual components, you must create a response file for each one.

### Procedure

1. Open a command prompt.
2. Start the wizard.

*Table 24. Commands for starting the wizard*

| Platform | For runtime and management services, management console, or WS-Provisioning runtime | For Web services security management |
|---|---|---|
| AIX, Linux, or Solaris | `/opt/IBM/FIM/_uninst/ uninstaller.bin -options-record` *`response_file_filename`*`.rsp` | `/opt/IBM/FIM/_uninst_wssm/ uninstaller.bin -options-record` *`response_file_filename`*`.rsp` |

Table 24. Commands for starting the wizard (continued)

| Platform | For runtime and management services, management console, or WS-Provisioning runtime | For Web services security management |
|---|---|---|
| Windows | `C:\Program Files\IBM\FIM\ _uninst\uninstaller.exe -options-record` *`response_file_filename`*`.rsp` | `C:\Program Files\IBM\FIM\ _uninst_wssm\uninstaller.exe -options-record` *`response_file_filename`*`.rsp` |

3. Specify the file name for recording the options.
4. Specify the values for the various options.
5. After completing the panels, click **Finish**.
6. Open the response file in a text editor.
7. Ensure that the features you want to uninstall are selected.
8. Locate the *`feature_name`*`.active=` statement for each feature. `True` indicates you want to remove that component. `False` indicates that you do not.
9. Review the rest of the response file to verify that the remaining values are correct. Some response files might contain macros rather than the specified data. In these cases, you must change these entries.
10. Make the response file available to the people or processes that perform the uninstall.

## Uninstalling with a response file

After creating a response file, you can use it with the wizard to uninstall components in a predetermined manner.

### Before you begin

Create a response file. See "Creating a response file for uninstallation" on page 95.

### About this task

The wizard runs and performs the necessary uninstallation steps. Errors are written to the standard error device (`STDERR`) and to the log file.

### Procedure

1. Open a command prompt.
2. Start the wizard.

   **Note:** You can also start the wizard from a script or batch file as part of an automated process.

Table 25. Commands for starting the wizard with a response file

| Component | Commands for AIX, Linux, or Solaris | Commands for Windows |
|---|---|---|
| Runtime and management services | `/opt/IBM/FIM/_uninst/ uninstaller.bin -silent -options` *`response_file_filename`*`.rsp` | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe -silent -options` *`response_file_filename`*`.rsp` |

*Table 25. Commands for starting the wizard with a response file (continued)*

| Component | Commands for AIX, Linux, or Solaris | Commands for Windows |
|---|---|---|
| Management console | `/opt/IBM/FIM/_uninst/ uninstaller.bin -silent -options` *`response_file_filename`*`.rsp` | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe -silent -options` *`response_file_filename`*`.rsp` |
| WS-Provisioning runtime | `/opt/IBM/FIM/_uninst/ uninstaller.bin -silent -options` *`response_file_filename`*`.rsp` | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe -silent -options` *`response_file_filename`*`.rsp` |
| Web services security management | `/opt/IBM/FIM/_uninst/ uninstaller.bin -silent -options` *`response_file_filename`*`.rsp` | `C:\Program Files\IBM\FIM\_uninst\ uninstaller.exe -silent -options` *`response_file_filename`*`.rsp` |

3. Specify the file name of the response file.

# 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 (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.
1623-14, Shimotsuruma, Yamato-shi
Kanagawa 242-8502 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.

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.

# Glossary

**access token**
In the context of OAuth, a string that represents authorization provided to the OAuth client. The string represents scopes and durations of access. It is granted by the resource owner and enforced by the OAuth or Authorization server.

**alias service**
The Tivoli Federated Identity Manager component that manages aliases, or name identifiers, that are passed between secure domains.

**artifact**
In the context of the SAML protocol, a structured data object that points to a SAML protocol message.

**artifact resolution service**
In the context of the SAML protocol, the endpoint in a federation where artifacts are exchanged for assertions.

**assertion**
In the context of the SAML protocol, data that contains authentication or attribute information or both types of information in a message.

**assertion consumer service**
In the context of the SAML protocol, the endpoint in a federation that receives assertions or artifacts as part of a single sign-on request or response.

**authorization code**
In the context of OAuth, a code that the Authorization server generates when the resource owner authorizes a request.

**authorization grant**
In the context of OAuth, a grant that represents the resource owner authorization to access its protected resources. OAuth clients use an authorization grant to obtain an access token. There are four authorization grant types: authorization code, implicit, resource owner password credentials, and client credentials.

**authorization server**
A server that processes authorization and authentications.

**binding**
In the context of SAML, the communication method used to transport the messages.

**browser artifact**
A profile (that is, a set of rules) in the SAML standard that specifies that an artifact is exchanged to establish and use a trusted session between two partners in a federation. Contrast with *browser POST*.

**browser POST**
A profile (that is, a set of rules) in the SAML standard that specifies the use of a self-posting form to establish and use a trusted session between two partners in a federation. Contrast with *browser artifact*.

**certificate**
In computer security, a digital document that binds a public key to the identity of the certificate owner. This digital document enables the certificate owner to be authenticated. A certificate is issued by a certificate authority and is digitally signed by that authority.

**client**
A software program or computer that requests services from a server.

**domain**
A deployment of the Tivoli Federated Identity Manager runtime component on WebSphere Application Server.

**endpoint**
The ultimate recipient of an operation.

**federation**
A relationship in which entities, such as differing businesses, agree to use the same technical standard (such as SAML or Liberty). This technical standard enables each partner in the relationship to access resources and data of the other. See also identity provider and service provider.

**identity mapping**
The process of modifying an identity that is valid in an input context to an identity that is valid in an output context.

**identity provider**
A partner in a federation that has responsibility for authenticating the identity of a user.

**intersite transfer service**
In the context of the SAML protocol, the endpoint in a federation to which a single sign-on request is sent.

**keystore**
In security, a file or a hardware cryptographic card where identities and private keys are stored, for authentication and encryption purposes. Some keystores also contain trusted, or public, keys.

**Metadata**
Data that describes a particular piece of information, such as settings for a configuration.

**OAuth client**
A third-party application that wants access to the private resources of the resource owner. The OAuth client can make protected resource requests on behalf of the resource owner once the resource owner grants it authorization.

**OAuth server**
Also known as the **Authorization server** in OAuth 2.0. The server that gives OAuth clients scoped access to a protected resource on behalf of the resource owner. An authorization server can also be the resource server.

**partner**
In data communications, the remote application program or the remote computer.

**point of contact server**
In the context of a federation, a proxy or application server that is the first entity to process a request for access to a resource.

**private key**
In secure communication, an algorithmic pattern used to encrypt messages that only the corresponding public key can decrypt. The private key is also used to decrypt messages that were encrypted by the corresponding public key. The private key is kept on the user system and is protected by a password.

**profile**
In the context of the SAML specification, a combination of protocols, assertions, and bindings that are used together to create a federation and enable federated single sign-on.

**protocol**
In the context of the SAML specification, a type of request message and response message that is used for obtaining authentication data and for managing identities.

**public key**
In secure communication, an algorithmic pattern used to decrypt messages that were encrypted by the corresponding private key. A public key is also used to encrypt messages that can be decrypted only by the corresponding private key. Users broadcast their public keys to everyone with whom they must exchange encrypted messages.

**refresh token**
In the context of OAuth, a string that is used to obtain a new access token when the current access token expires.

**resource owner**
In the context of OAuth, a type of user capable of authorizing access to a protected resource.

**resource server**
The server that hosts the protected resources. It can accept and respond to protected resource requests using access tokens. The resource server might be the same server as the authorization server.

**response file**
A file containing predefined values such as parameters and values used to control the actions of a component in a predetermined manner.

**request**
An item that initiates a workflow and the various activities of a workflow.

**SAML** See *security assertion markup language*.

**security assertion markup language**
A set of specifications written by the OASIS consortium to describe the secure handling of XML-based request and response messages that contain authorization or authentication information.

**service provider**
A partner in a federation that provides services to the user.

**Simple and Protected GSS API Negotiation Mechanism (SPNEGO)**
An authentication mechanism that provides single sign-on capability in Microsoft Windows environments.

**single sign-on**
An authentication process in which a user can access more than one system or application by entering a single user ID and password.

**SOAP** A lightweight, XML-based protocol for exchanging information in a decentralized, distributed environment. SOAP can be used to query and return information and start services across the Internet.

**SOAP back channel**
Communications that take place directly between two SOAP endpoints.

**SPNEGO**
Simple and Protected GSS API Negotiation Mechanism

**stanza** A group of lines in a file that together have a common function or define a part of the system. Stanzas are separated by blank lines or colons, and each stanza has a name.

**syntax** The rules for the construction of a command or statement.

**token** A particular message or bit pattern that signifies permission or temporary control to transmit over a network. In the context of SAML, token is used interchangeably with *assertion*.

**trust service**
The Tivoli Federated Identity Manager component that manages security tokens that are passed between security domains. The trust service is also referred to as the *Security Token Service*.

**Web service**
A self-contained, self-describing modular application that can be published, discovered, and invoked over a network using standard network protocols. Typically, XML is used to tag the data, and SOAP is used to transfer the data. A WSDL is used for describing the services available, and UDDI is used for listing what services are available.

**Web service security management**
The Tivoli Federated Identity Manager component that is used to establish and manage federation relationships for web service applications running on WebSphere Application Server that use WS-Security tokens.

# Index

Printed in USA

GC27-2718-01