Tivoli® Federated Identity Manager
Version 6.2.1

Installation Guide

IBM®

GC27-2718-00

Tivoli® Federated Identity Manager
Version 6.2.1

Installation Guide

IBM®

GC27-2718-00

Note
Before using this information and the product it supports, read the information in "Notices" on page 97.

This edition applies to version 6, release 2, modification 1 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 6.2.1 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 for z/OS Program Directory*

  Provides instructions for installing IBM Tivoli Federated Identity Manager on z/OS®.
- *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/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

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:

- IBM Tivoli Access Manager for e-business Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.itame.doc/toc.xml
- IBM WebSphere Application Server Version 6.1 Information Center:

  http://publib.boulder.ibm.com/infocenter/wasinfo/v6r1/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:

- The IBM Tivoli Federated Identity Manager Business Gateway Information Center at
- *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/glossary/tivoliglossarymst.htm

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 many Tivoli publications online at http://www.ibm.com/e-business/linkweb/publications/servlet/pbi.wss.

You can also order by telephone by calling one of these numbers:

- In the United States: 800-879-2755
- In Canada: 800-426-4968

In other countries, contact your software account representative to order Tivoli publications. To locate the telephone number of your local representative, perform the following steps:

1. Go to http://www.elink.ibmlink.ibm.com/publications/servlet/pbi.wss.
2. Select your country from the list and click **Go**.
3. Click **About this site** in the main panel to see an information page that includes the telephone number of your local representative.

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/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml.

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, and supports the creation and management of federated single sign-on environments. Tivoli Federated Identity Manager also extends the power of authorization decision software by leveraging Web services standards.

Tivoli Federated Identity Manager supports the following deployment scenarios:

- Federated single sign-on
- Provisioning
- Web services security management
- Identity token exchange
- User Self Care

Each deployment addresses a scenario that requires the secure handling of user identities in a distributed networking environment. Each of these scenarios can be installed, configured, and administered independently.

- Tivoli Federated Identity Manager enables the creation and management of federated single sign-on environments.

  Deployment of this scenario involves installation and configuration of Tivoli Federated Identity Manager into an environment that is also populated by additional servers and applications.
- The Web services security management scenario provides an authorization solution that can be used without deployment of a federated single sign-on environment.

  This scenario applies IBM Tivoli Access Manager authorization capabilities to the evaluation of user requests for access to resources across different companies and secure domains. When user requests are contained in messages that adhere to Web services standards, Tivoli Federated Identity Manager can process these messages to provide authorization decisions. The decisions are made on behalf of applications, such as WebSphere Application Server applications, that must deliver resources to the user. Note that this scenario also provides federation capabilities through its ability to accept identities from different domains.
- The Tivoli Federated Identity Manager provisioning scenario extends existing provisioning solutions across the Internet through the use of Web services standards.

  The provisioning scenario is separate from federated single sign-on, but can be used to support the management of user identities in single sign-on environments.
- The identity token exchange scenario supports the transfer of user credential information between different types of identity tokens. Tokens are used to store authentication and authorization properties for users. There are many different types of tokens, and each uses a unique format and structure. Many deployment scenarios require that the information contained in one token be transferred to a

token of another format, in order to be accessed by the authentication and authorization processes used by a specific deployment scenario.

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

- User Self Care provides a method by which users can be provisioned into business-to-consumer environments. User Self Care accomplishes this provisioning by supplying a set of operations that users can use 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

Before you can install and configure Tivoli Federated Identity Manager software, you must obtain from your security architect the requirements and design for your deployment environment. The process of developing the requirements and designs involves the making of a number of business policy decisions as well as technology decisions.

This administration guide does not describe the process for developing business policies, planning network architecture, and choosing a Web single sign-on protocol. Your architect should complete that process before you install and deploy Tivoli Federated Identity Manager. IBM supplies numerous resources to help your company develop a network deployment architecture that is appropriate for your business requirements.

Recommended resources:

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

  This redbook is a good resource for use during the planning process. You can obtain this Redbook and other useful whitepapers from the IBM Web site.
- The IBM WebSphere Application Server information center on the IBM Web site.

  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 is distributed network environments. You can access both product documentation and Redbooks® that describe the Tivoli Access Manager model for defining and securing both protected objects and user identities.
- Web services standards

  Tivoli Federated Identity Manager, and the Web services security management component in particular, support a number of 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 regarding service-oriented architecture from IBM, see:

http://www.ibm.com/soa

Overview of installation and configuration

The installation and configuration tasks for Tivoli Federated Identity Manager are specific to the product scenarios that you will deploy.

It is useful to view the two tasks–installation and configuration–as separate tasks. The installation of Tivoli Federated Identity Manager files is separate from the configuration of those files to support one or more features. This structure facilitates the deployment of Tivoli Federated Identity Manager across multiple computers in a distributed environment.

This guide describes how to *install* all of the scenarios. This guide describes how to *configure* federated single sign-on and token exchange, and also describes how to 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. For federated identity provisioning, you are also directed to other documentation for configuration instructions.

An overview of the installation and configuration of each scenario is discussed in the following topics.

- "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 6

Overview of installation and configuration of federated single sign-on

The documentation leads you through the tasks. Complete the instructions in the following order:

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.

   Note: Installation instructions for the z/OS platform are described in a separate book: *IBM Tivoli Federated Identity Manager for z/OS Program Directory*
3. Configure your federated single sign-on environment

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

You should read through the set of planning topics that apply to your environment before you being any configuration. The planning topics describe the data and properties that you will need to supply when completing the configuration tasks. You should determine that you 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 business partner. These tasks must be accomplished manually.

The planning and configuration steps are located in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

Overview of installation and configuration of Web service security management

The documentation leads you through the tasks. Complete the instructions in the following order:

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 following instructions:
   a. Chapter 4, "Installing Web services security management," on page 35
   b. Choose one of the installation methods. See "Installation modes" on page 11

   Note: Installation instructions for the z/OS platform are described in a separate book: *IBM Tivoli Federated Identity Manager for z/OS Program Directory*
3. Configure your Web services security management environment

   The establishment of a Tivoli Federated Identity Manager domain is the first step in configuring a Web services security management environment.

   Additional configuration steps vary depending on the deployment architecture. The steps can include configuration of WebSphere Application Server security, deployment of the Web service security management application into a Tivoli Access Manager environment, and creation of a Tivoli Federated Identity Manager trust service module chain.

   Configuration instructions:

   a. Use the instructions in the *IBM Tivoli Federated Identity Manager Configuration Guide* to establish a Tivoli Federated Identity Manager domain
   b. To complete the configuration of a Web services security management environment, see the *IBM Tivoli Federated Identity Manager Web Services Security Management Guide*.

Overview of installation and configuration of federated identity provisioning

Note: Federated identity provisioning is not supported on the z/OS platform.

The documentation leads you through the tasks. Complete the instructions in the following order:

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 5, "Installing federated provisioning," on page 41
3. Configure your federated identity provisioning environment

   The deployment of a federated identity provisioning environment is often done after the creation of a federated single sign-on environment.

   After you have deployed a single sign-on federation, you do not need to use any additional topics in this guide. Configuration of a federated identity provisioning environment is described in the *IBM Tivoli Federated Identity Manager Administration Guide*.

Overview of installation and configuration of token exchange scenarios

Tivoli Federated Identity Manager can be deployed to provide token exchange services, through installation and configuration of the security token service.

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

The *installation* of components for token exchange scenarios is identical to the installation for federated single sign-on scenarios. The *configuration* of those components are specific to the scenario type.

The documentation leads you through the tasks. Complete the instructions in the following order:

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.

   Note: Installation instructions for the z/OS platform are described in a separate book: *IBM Tivoli Federated Identity Manager for z/OS Program Directory*
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 integration of Tivoli Federated Identity Manager with other products.

   All deployments of Tivoli Federated Identity Manager require the establishment of a Tivoli Federated Identity Manager domain (management service) and the deployment of the Tivoli Federated Identity Manager runtime. The configuration instructions for token exchange guide you through these configuration tasks.

   The configuration instructions describe in detail the deployment of Tivoli Federated Identity Manager security token service modules for support of Kerberos constrained delegation. This deployment includes the use of Tivoli Access Manager WebSEAL Kerberos junctions, as a method of securing access to Web servers. The deployment is specific to an environment that includes Microsoft® integrated authentication (SPNEGO) using Kerberos tokens. IBM

WebSphere Application Server is also deployed, and must be configured 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 Tivoli Federated Identity Manager features, many of which are used in multiple deployment scenarios.

The *installation* of components for user self care scenarios is identical to the installation for federated single sign-on scenarios. The *configuration* of those components are specific to the scenario type.

The documentation leads you through the tasks. Complete the instructions in the following order:

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. These instructions apply to User Self Care.

   Note: Installation instructions for the z/OS platform are described in a separate book: *IBM Tivoli Federated Identity Manager for z/OS Program Directory*

Chapter 2. Planning the installation

Find information about Tivoli Federated Identity Manager installation requirements and prerequisites to consider as you plan your environment.

Before you can install the necessary software, you will need to plan your environment and understand the requirements of Tivoli Federated Identity Manager.

Complete the following planning tasks:

1. Review the list of software that is distributed with the Tivoli Federated Identity Manager product. The product distribution includes other products that are required as software prerequisites.

   See "Software packaging."
2. Learn about the Tivoli Federated Identity Manager installation components, and how they are combined to deploy each of the Tivoli Federated Identity Manager features.

   See "Installation components" on page 8
3. Understand the installation modes that you can choose.

   See "Installation modes" on page 11.
4. Understand the access privileges needed to install

   See "Required access privileges" on page 12.

Software packaging

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

The software packaging includes Tivoli Federated Identity Manager and its prerequisite 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 included in the product distribution, see the product page on the IBM Passport Advantage® Web site:

http://www.ibm.com/support/docview.wss?uid=swg24026572

For a list of the supported versions of each of the prerequisite software, see the Hardware and Software requirements topic on the Tivoli Federated Identity Manager information center:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

Attention: When planning your environment, be aware of possible product installation issues when installing into a Windows operating system set to Turkish. To avoid installation problems, set the operating system to a language other than Turkish. After installing the product, you can then change the language of the operating system back to Turkish.

Installation components

Tivoli Federated Identity Manager consists of a number of components that can be installed separately. The installation components are:

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

The components can all be installed on one computer, or can be installed across multiple computers. Installations on one computer are common for prototype or test environments. Installations across multiple computers are common in production environments.

The software prerequisites vary for each component. Some software prerequisites must be co-located on the same host (server) while other software prerequisites can be distributed across the network.

Management service and runtime

The management service and runtime is needed for all installations. This component serves two functions:

- It provides the basic management service and runtime for use by the federated single sign-on function, the Web services security management feature, and the federated provisioning feature.
- The runtime also contains the federated single sign-on feature.

The management service and runtime are always installed together.

Management console

The console is used to administer all components. The console is often installed on the same computer as the management service and runtime. The console can optionally be installed on a different computer.

The console has a software prerequisite on a WebSphere Application Server. The console is implemented as a plug-in to the Integrated Solutions Console. The Integrated Solutions Console is the management console that is built into WebSphere Application Server. This means that in order to install the Tivoli Federated Identity Manager management console, you must first install WebSphere Application Server on the same computer.

The management console does not have to be located 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

In this scenario, the WebSphere Application Server system that hosts the Tivoli Federated Identity Manager management service is also the system that hosts other WebSphere applications.

- On a different system from the management service and runtime

  In some scenarios, WebSphere administrators choose to run all management console plug-ins from a computer that is dedicated to administration of all WebSphere applications, including Tivoli Federated Identity Manager. In this case, the administrator chooses to install only the Tivoli Federated Identity Manager management console on the computer, and places the Tivoli Federated Identity Manager management service and runtime on another computer.

Federated provisioning

Deployment of federated provisioning is dependent on deployment of the management service and runtime. The management service and runtime do not have to be on the same computer as the provisioning component.

The management console does not have to be on the same computer.

Web services security management

Deployment of Web services security management is dependent on deployment of the management service and runtime. The management service and runtime do not have to be on the same computer as the Web services security management component.

The management console does not have to be on the same computer.

IBM Support Assistant

The IBM Support Assistant is 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

Deployment of each Tivoli Federated Identity Manager feature requires installation of more than one component. You can install all the required components on one computer, or you can distribute the components across the multiple computers.

This topic describes common scenarios for deploying the components. The supported common scenarios are based on the product features:

- Federated single sign-on
  - Required components for deployment on a single computer:
    - Management service and runtime
    - Management console
  - 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 deployment of federated single sign-on
- Web services security management
  - Required components for deployment on a single computer:
    - Management service and runtime

- Management console
- Web services security management

– Distributed deployment options

1. Management service and runtime, plus Web services security manager, on one computer. Management console on a separate computer.

   Useful when you want to separate administration activities (console) from runtime activity.

2. Management service and runtime, plus management console, on one computer. Web services security manager on a separate computer.
3. Each component can be 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 deployment on a single computer:
  - Management service and runtime
  - Management console
  - Federated provisioning

– Distributed deployment options
  - Management service and runtime, plus federated provisioning, on one computer. Management console on a separate computer.

    Useful when you want to separate administration activities (console) from runtime activity.

• Identity token exchange

– Required components for deployment on a single computer:
  - Management service and runtime
  - Management console

– 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 for deployment of identity token exchange.

• User self care

– Required components for deployment on a single computer:
  - Management service and runtime
  - Management console

– Distributed deployment:
  - Management service and runtime on one computer
  - Management console on another computer

The Web services security management component is not used with user self care.

The federated provisioning component is not required for deployment of user self care.

When planning the deployment of your components, keep in mind:

- The management console must be deployed into the environment (either locally or remotely) when deploying any of the Tivoli Federated Identity Manager components.
- Each of the Tivoli Federated Identity Manager components has different software prerequisites. This means that when you plan out your application deployment, you must assemble the required software prerequisites as needed for each computer.

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

Installation modes

Find information about different options for installing Tivoli Federated Identity Manager.

Before beginning the installation procedures, you will want to be familiar with how the features can be installed and then decide which installation mode you will use.

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

Graphical mode

Tivoli Federated Identity Manager provides a graphical user interface installation program. Each installation presents a series of panels that prompt for the information that is required to complete the task. Each panel has an online help panel that explains the contents of the installation panel.

The name of the installation binary is specific to each platform.

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

Platform	Command to start the installation program
AIX®	`install_aix_ppc.bin`
HP-UX on Itanium®	`install_hpux_ia64.bin`
Linux® on System p®	`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`

Note: For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

Console mode

Tivoli Federated Identity Manager supports an alternate installation mode, for use when installing in a non-graphical environment, such as on a server system that does not have a video card. This mode is called *console mode*.

Console mode installation accomplishes the same tasks and requires the same user input as required by the graphical installation.

You can choose console mode by adding the `-console` command line option when calling the installation launcher.

Table 2. Commands to start the installation program on console mode

Platform	Command to start the installation program
AIX	`install_aix_ppc.bin -console`
Linux on System p	`install_linux_ppc.bin -console`
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`

Note: For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

Silent mode

Tivoli Federated Identity Manager supports a *silent mode* installation. In this mode, the user is not required to provide any input. Instead, input values are read from a file. This permits the feature to be installed with a common set of options using a script. In order 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 initial installation of the product. Use one of the interactive modes (graphical or console) for initial installation, and use the output from it to create the response file.

For information about creating and using response files, see Chapter 8, "Using silent mode installation," on page 59.

Required access privileges

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

Depending on the security features that are configured on the system where you want to install the product, you might be required to log in with a username and password.

In addition, if you are installing Tivoli Federated Identity Manager on an existing version of WebSphere Application Server and security is enabled, you will be required to provide the following security-related information during the installation:

- administrator user name
- administrator password
- trust store file location
- trust store password
- keystore file location (optional)
- keystore password (optional)

In addition, 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
```

HP-UX, 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: If you are installing Tivoli Federated Identity Manager as a user other than the root or Administrator user, you might need to perform additional steps. For more information, see Appendix G, “Installing as a user other than root or administrator,” on page 85.

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

The topics in this section apply to deployment scenarios for federated single sign-on and for token exchange. The topics apply equally to both scenarios.

The token exchange scenario applies to deployments that limit their use of Tivoli Federated Identity Management to use of the security token service to exchange user credentials between different token formats. An example of this scenario is the deployment of Kerberos constrained delegation trust modules in an environment with WebSEAL junctions.

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 18
3. "Runtime and management service installation worksheet" on page 26
4. "Installing the federated single sign-on feature" on page 30

Planning the installation of the federated single sign-on feature

Installation and deployment of the federated single sign-on feature requires the installation of two Tivoli Federated Identity Manager components:

- Management service and runtime

  This component 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

  This component provides a management or administration interface for managing Tivoli Federated Identity Manager domains. This component is implemented as a plug-in to the administration console that is included in WebSphere Application Server

Note: To implement federated single sign-on, you do not need to install the Tivoli Federated Identity ManagerWeb services security management component or the Tivoli Federated Identity Manager federated provisioning component.

Each Tivoli Federated Identity Manager component has requirements on other software as software prerequisites.

Software prerequisites for the runtime and management service component

The runtime and management service component is dependent on prerequisite software.

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 is used for all deployment of allTivoli Federated Identity Manager features. The software prerequisites vary depending on which feature you are deploying.

- 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

Tivoli Federated Identity Manager is implemented as a WebSphere Application Server application. This means that a WebSphere Application Server server must be deployed on the same computer prior to the installation of the management service and runtime.

WebSphere Application Server is available in a number of product configurations. Tivoli Federated Identity Manager is intended to be used with:

- WebSphere Application Server Network Deployment

  This product supports WebSphere applications and is used to deploy WebSphere clusters. The Tivoli Federated Identity Manager product distribution includes a CD or ISO image of this product.

  Each major release of IBM WebSphere Application Server Network Deployment is supplemented by Refresh Packs and Fix Packs. Tivoli Federated Identity Manager requires the installation of specific Refresh Packs or Fix Packs.

  To view the current list of required Fix Packs, see the topic Hardware and Software Requirements on the Tivoli Federated Identity Manager Information Center on the IBM Web site.
- Embedded WebSphere Application Server

  This version of WebSphere Application Server is not released as a separate product, but is instead released as embedded functionality within other products. Embedded WebSphere Application Server is a lightweight, easily deployed, version of WebSphere Application Server. It is intended to primarily provide application support, and does not support true WebSphere clustering.

  Tivoli Federated Identity Manager includes embedded WebSphere Application Server. When you install the Tivoli Federated Identity Manager management service and runtime, you can optionally choose to install embedded WebSphere Application Server.

  Embedded WebSphere Application Server is appropriate for small deployments, such as prototypes, test systems, or proof of concept deployments. It typically is not used in large scale deployments and production deployments due to its lack of support for WebSphere clusters.

  Embedded WebSphere Application Server contains an administration console that is a subset of the full WebSphere Application Server administration console. This subset reflects the fact that the embedded WebSphere Application Server server is intended for deployments where minimal WebSphere Application Server administration is required. This scenario can include simple deployments that implement only one WebSphere application.

  In most deployments of the Tivoli Federated Identity Manager management service and runtime component, you will choose not to use embedded WebSphere Application Server but will instead use the full WebSphere Application Server Network Deployment product.

  Within Tivoli Federated Identity Manager deployments, embedded WebSphere Application Server can be useful to support the Tivoli Federated Identity

Manager management console component, when the management console is deployed on a separate computer that does already have WebSphere Application Server.

Note: WebSphere Application Server Version 6.1 and WebSphere Application Server Version 7.0 are supported.

Tivoli Access Manager

The Tivoli Federated Identity Manager model separates the authentication of users and the evaluation of user authorities (permissions to access resources) from the federation of the identities and authorities. This enables the use of other products in the processing of the authentication and authorization of user requests (assertions).

Tivoli Federated Identity Manager has been optimized to provide 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 server and authorization server. Through these servers, the management service resolves requests for user information that is stored in user registries managed by IBM Tivoli Access Manager for e-business

For federated single sign-on, the Tivoli Federated Identity Manager management service also requires installation of the IBM Tivoli Access Manager for e-business WebSEAL server, when you want to use WebSEAL as 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 requires the installation of specific Fix Packs.

To view the current list of required Fix Packs, see the topic Hardware and Software Requirements on the Tivoli Federated Identity Manager Information Center on the IBM Web site.

Software prerequisites for the management console component

The management console is dependent on WebSphere Application Server.

This console component provides a management or administration interface for managing Tivoli Federated Identity Manager domains. The console is implemented as a plug-in to the administration console that is included in WebSphere Application Server.

This component is contained within the same installation image (CD or ISO image) as the Tivoli Federated Identity Manager management service and runtime. The Tivoli Federated Identity Manager installation allows you to install it at the same time as the management service and runtime.

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

The management console is dependent on the deployment of WebSphere Application Server administration console. This can be accomplished in one of two ways:

- Installation of a separate WebSphere Application Server product such as WebSphere Application Server Network Deployment on the same computer, prior to installation of the management console
- Installation of the embedded WebSphere Application Server on the same computer as the management console. The embedded WebSphere Application Server is included in the Tivoli Federated Identity Manager installation binary. The graphical user installation for the management console allows you to specify to include the embedded WebSphere Application Server in the software to be installed at the same time as the management console.

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

Find information about installing WebSphere Application Server as a software prerequisite for Tivoli Federated Identity Manager.

About this task

Tivoli Federated Identity Manager is deployed as an application into a WebSphere environment. Tivoli Federated Identity Manager runs as an application in either a WebSphere Application Server standalone server environment or a WebSphere Application Server Network Deployment cluster.

In both deployment environments, you must install WebSphere Application Server Network Deployment and the prerequisite Refresh Pack and Fix Packs. In the cluster environment, you must also deploy the cluster before you add Tivoli Federated Identity Manager as an application.

Note: When you have an existing deployment of WebSphere Application Server Network Deployment, you do not need to install a new WebSphere Application Server. When you already have WebSphere Application Server deployed, you must ensure that you have applied the Fix Packs that Tivoli Federated Identity Manager requires. See “Installing WebSphere Application Server Refresh Packs and Fix Packs” on page 20.

Note: When installing Tivoli Federated Identity Manager on two separate WebSphere profiles (such as AppSrv01 and AppSrv02), provide different server names for the two profiles. For example, if you name the server on the first profile "server1," then name the server on the second profile "server2."

Installing WebSphere Application Server for Network Deployment

Find information about installing WebSphere Application Server Network Deployment as a software prerequisite for Tivoli Federated Identity Manager.

About this task

IBM WebSphere Application Server Network Deployment is distributed as part of the Tivoli Federated Identity Manager software distribution. The instructions in this topic apply to deployments of either a standalone server profile or a deployment manager (cluster) profile.

Procedure

1. Access the IBM WebSphere Application Server Network Deployment CD for your operating system, or unzip 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:
   - The installation directory that you specify will need to be supplied when you install the Tivoli Federated Identity Manager management service and runtime.
   - The WebSphere **Core product files** are required. The additional WebSphere packages are optional.
3. When the installation finishes, select **Launch the Profile creation wizard** and select **Create an Application Server profile**. The profile creation program creates a profile name, profile directory, node name, and host name.
4. Specify the SOAP connector port. The SOAP connector port defaults to port 8880. You will be asked to confirm this value during the Tivoli Federated Identity Manager runtime installation. If you change this value, remember the port number you selected.
5. When profile creation is complete, optionally select the **Launch the First steps console** check box. Click **Finish** and select **Installation Verification** You should see output similar to the following line:

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

   Note: You can access the SystemOut.log file to monitor WebSphere application server startup and execution. Example locations:
   - AIX

     ```
     # /usr/IBM/WebSphere/AppServer/profiles/default/logs/
     server1/SystemOut.log
     ```
   - Solaris, Linux, or HP-UX

     ```
     # /opt/IBM/WebSphere/AppServer/profiles/default/logs/
     server1/SystemOut.log
     ```
   - Windows

     ```
     C:\Program Files\IBM\WebSphere\AppServer\profiles\default\
        logs\server1\SystemOut.log
     ```
6. Verify that you can use the WebSphere administration console. Use a browser to access the console URL. For example, when the host name is `idp.example.com`:

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

You are prompted to log in to the administration application. If the prompt does not appear, the application server is not running correctly. You can leave the User ID field blank and click **Login**. The WebSphere Administration Console Welcome page is displayed.

7. Record your values for the installation properties in Table 3.

Table 3. WebSphere Application Server installation properties

Property	Default value	Your value

Installation directory	• AIX
	`/usr/IBM/WebSphere/AppServer`
	• Solaris, Linux, or HP-UX
	`/opt/IBM/WebSphere/AppServer`
	• Windows
	`C:\Program Files\IBM\WebSphere\AppServer`	

SOAP port	8879	

8. Continue with "Installing WebSphere Application Server Refresh Packs and Fix Packs."

Installing WebSphere Application Server Refresh Packs and Fix Packs

Find information about installing WebSphere Application Server Refresh Packs and Fix Packs as a software prerequisite for Tivoli Federated Identity Manager.

Before you begin

If you have an existing version of WebSphere Application Server already installed, ensure that you are using the required level of fix packs and refresh packs. Tivoli Federated Identity Manager requires one of the following additional software:

The current list of required fix packs and refresh packs is maintained on the Tivoli Information Center for Tivoli Federated Identity Manager.

- Obtain the list of Fix Packs from the Hardware and Software Requirements link on the Tivoli Information Center:

  http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

About this task

To download the WebSphere Application Server Refresh Pack and Fix Pack from the IBM Support Web site:

Procedure

1. Access the WebSphere Application Server support site:

   `http://www.ibm.com/software/webservers/appserv/was/support/`
2. Select the *Fixes by version* link in the Download section. A comprehensive list of recommended fixes for WebSphere Application Server is displayed.
3. Select the link for your version of WebSphere Application Server.
4. Select the *Download information* link for instructions on how to download and install the fixes.
5. Choose one of the following actions:

- When you are deploying a WebSphere Application Server as a standalone server (application server profile), you are finished with the WebSphere Application Server configuration. To continue configuring software prerequisites for Tivoli Federated Identity Manager, continue with "Installing Tivoli Access Manager" on page 22
- When you are deploying Tivoli Federated Identity Manager into a WebSphere Application Server cluster environment, continue with "Installing a WebSphere Application Server cluster."

Installing a WebSphere Application Server cluster

Find information about installing WebSphere Application Server cluster as a software prerequisite for Tivoli Federated Identity Manager.

Before you begin

Tivoli Federated Identity Manager is deployed as an application into a WebSphere cluster.

WebSphere clusters can be configured in many ways, depending on many factors including the deployment topology. This section provides a checklist for a simple cluster with one node (one application server). You should consult the WebSphere Application Server documentation for instructions that apply to your deployment environment.

You can access online topics about WebSphere Application Server at the information center:

http://publib.boulder.ibm.com/infocenter/wasinfo/v7r0/index.jsp

You can access information in book form at the WebSphere Application Server library:

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

About this task

The following steps summarize a deployment of a simple cluster.

Procedure

1. Verify that you have completed the WebSphere Application Server installation steps described in the following topics:
   - "Installing WebSphere Application Server for Network Deployment" on page 18
   - "Installing WebSphere Application Server Refresh Packs and Fix Packs" on page 20
2. Use the Profile Creation wizard to create a deployment manager profile.
3. Use the First Steps console to start the deployment manager.
4. Use the Profile Creation wizard to create an Application Server profile.
5. Use either the First Steps console or the **startServer** command to start the application server.
6. Add the application server node to the cell using the WebSphere Application Server administration console of the deployment manager. Click **System Administration → Nodes** to add the node.
7. Install the IBM HTTP Server.

a. Install the WebSphere Application Server Web server plug-ins. Configure the Web server using the Plug-ins installation wizard.
b. The Plug-ins installation wizard creates a script named `configure`*`your_Web_server_name`* in the *`plugins_install_root`*`/bin` directory. Run this script to create a Web server definition in the WebSphere Application Server administration console. You can then use the administration console to manage the Web server.

8. Open a browser and log in to the WebSphere console:
   `http://`*`your_WebSphere_Deployment_Manager_host_name`*`:9060/ibm/console`
9. Navigate to **Servers → Clusters**. The Server Cluster page is displayed. Click **New**.
10. The Create New Cluster wizard requests basic cluster information.
    a. Specify a cluster name. For example, `fimCluster`.
    b. Select the **Create a replication domain** check box.
    c. Select the **Select an existing server to add** radio button. Ensure that the server you have created, such as server1, is shown in the menu.
    d. Click **Next**.
11. Create additional cluster members if necessary, by specifying a name and mode for each member. Click **Next**.
12. Click **Finish** to create the cluster. A message is displayed, prompting you to save the changes.
13. Click **Save**. The Server Cluster page is displayed.
14. Select the **Synchronize changes with Nodes** check box. Click **Save**.

Results

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

After you install Tivoli Federated Identity Manager, you will create a Tivoli Federated Identity Manager domain and deploy the runtime application. At that time, there are additional configuration instructions for deploying the runtime into the WebSphere cluster.

Installing Tivoli Access Manager

Find information about installing Tivoli Access Manager as a software prerequisite for Tivoli Federated Identity Manager.

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

The Tivoli Access Manager for e-business components are used when the single sign-on federation uses WebSEAL as a point of contact server.

The Tivoli Access Manager for e-business components are not used when the single sign-on federation uses WebSphere as a point of contact server.

Note: If you plan to deploy a Tivoli Federated Identity Manager single sign-on federation that uses WebSphere as a point of contact server, you do not need to install any of the Tivoli Access Manager for e-business components.

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

See the Hardware and Software requirements on the Tivoli Federated Identity Manager information center for a list of fix packs required by Tivoli Federated Identity Manager for each version of Tivoli Access Manager for e-business.

You can access the IBM Tivoli Access Manager for e-business documentation for all versions from the Information Center link on product page on the Web at:

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

Installing a user registry

Find information about installing a user registry for Tivoli Access Manager as a software prerequisite for Tivoli Federated Identity Manager.

Tivoli Access Manager requires access to a user registry. Tivoli Access Manager supports a number of user registries. The user registries supported by Tivoli Access Manager that can be used for Tivoli Federated Identity Manager are listed on the Tivoli Information Center for Tivoli Federated Identity Manager.

See the link Hardware and Software requirements on the Information Center Welcome page:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

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

Find information about installing a policy server and an authorization server for Tivoli Access Manager as a software prerequisite for Tivoli Federated Identity Manager.

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

Several of the options that you specify when installing the policy server and authorization server are also used during configuration of a Tivoli Federated Identity Manager domain. Table 4 on page 24 lists the settings that you will be prompted for during Tivoli Federated Identity Manager configuration.

Table 4. Policy server and authorization server settings that are used during Tivoli Federated Identity Manager configuration

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

Installing a WebSEAL server

Find information about installing a WebSEAL server for Tivoli Access Manager as a software prerequisite for Tivoli Federated Identity Manager.

When a Tivoli Federated Identity Manager domain is created for federated single sign-on, the domain might require a Tivoli Access Manager WebSEAL server as a point of contact server.

Several settings that you specify when installing the WebSEAL server are also used when creating a single sign-on federation during Tivoli Federated Identity Manager configuration. Table 5 on page 25 lists the settings that you must supply when creating a single sign-on federation.

Table 5. 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 During Tivoli Federated Identity Manager configuration, you will be prompted to configure a Point of Contact Server. Your will specify either HTTPS or HTTP as part of the URL to the server. You can choose HTTPS only when you have enabled HTTPS access during WebSEAL configuration.
Enable HTTP access	Specifies whether to enable or disable HTTP access During Tivoli Federated Identity Manager configuration, you will be prompted to configure a Point of Contact Server. You will specify either HTTPS or HTTP as part of the URL to the server. You can choose HTTP only when you have enabled HTTP access during WebSEAL configuration. **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 For example: `webseal1.example.com` During Tivoli Federated Identity Manager configuration, you will be prompted to configure a Point of Contact Server. Your selection for **Local host name** will correspond to the Tivoli Federated Identity Manager option **Point of Contact**.

Installing IBM Tivoli Access Manager for e-business Fix Packs

Tivoli Access Manager is periodically updated with Fix Packs. You might need to install a Fix Pack as a software prerequisite for Tivoli Federated Identity Manager.

The current list of Fix Packs is kept on the Tivoli Information Center. To determine if you need to install a Fix Pack for your Tivoli Federated Identity Manager deployment:

1. Access the Welcome page for Tivoli Federated Identity Manager on the Tivoli Information Center.

   http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml
2. Select the Hardware and Software Requirements link.

Note: This release of Tivoli Federated Identity Manager is compatible with older releases of IBM Tivoli Access Manager for e-business. The compatibility is dependent 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 IBM Tivoli Access Manager for e-business support site.

Runtime and management service installation worksheet

This worksheet lists the properties for which you must supply a value during the installation of the runtime and management service component. You can prepare for the installation by noting the values you should use in the worksheet.

Installation on existing version of WebSphere Application Server

If you are installing the runtime and management service component on an *existing* version of WebSphere Application Server, you will need to know whether that installation has administration security enabled. An *existing* version is either the separately installable version that was provided with Tivoli Federated Identity Manager and that you have already installed or a compatible version of WebSphere Application Server that is already installed.

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

Property	Default value†	Your value

Directory name	**AIX, HP-UX, Linux, or Solaris**
	`/opt/IBM/FIM`
	Windows
	`C:\Program Files\IBM\FIM`	

When WebSphere Application Server administration security is *not* enabled:		

WebSphere Application Server installation directory	**AIX**
	`/usr/IBM/WebSphere/AppServer`
	HP-UX, Linux or Solaris
	`/opt/IBM/WebSphere/AppServer`
	Windows
	`C:\Program Files\IBM\WebSphere\AppServer`	

WebSphere Application Server SOAP connector port This is the port number on which the WebSphere Application Server handles SOAP communication.	`8879`	
Artifact resolution port This port is used for SOAP messages to be exchanged between partners. For example, this port is used during the retrieval of SAML assertions when the Browser Artifact profile is used. **Attention:** This port *must* be available even if your federation will not use SOAP messages.	`9444`	

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

Property	Default value†	Your value
Note: If you previously installed the embedded version of WebSphere Application Server, you will *not* be prompted 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™ key store file
 	
The truststore file used by WebSphere Application Server.
	AIX, HP-UX, Linux or Solaris
	`/opt/IBM/FIM/ewas/profiles/ itfimProfile/etc/ trust.p12`
	
	Windows
	`C:\Program Files\IBM\FIM\ ewas\profiles\ itfimProfile\etc\ trust.p12`	

SSL Trusted Java key store password The password needed to access the WebSphere truststore.	WebAS	
SSL Java key store file The keystore file used by WebSphere Application Server.		
SSL Java key store password The password needed to access the WebSphere keystore.		
Note: If you previously installed the embedded version of WebSphere Application Server, the prompts for the SSL Java key store and password will *not* be displayed.		

†Note:

- You cannot change these values using the console after installation.

Installation on embedded version of WebSphere Application Server

Table 7. Properties for runtime component installation on embedded version of WebSphere Application Server

Property	Default value†	Your value

Directory name	**AIX, HP-UX, Linux or Solaris**
	`/opt/IBM/FIM`
	Windows
	`C:\Program Files\IBM\FIM`	

WebSphere Application Server administrator user name	`fimadmin`	
WebSphere Application Server administrator password		
Application server port The port number that WebSphere Application Server uses to communicate over HTTP.	`9080`	
Secure application server port The port number that WebSphere Application Server uses to communicate over HTTPS.	`9443`	
Administration port The port number that the WebSphere Application Server administration console uses for HTTP.	`9060`	
Secure administration port The port number that the WebSphere Application Server administration console uses for HTTPS.	`9043`	
SOAP port The port number on which the WebSphere Application Server handles SOAP communication.	`8879`	

Table 7. Properties for runtime component installation on embedded version of WebSphere Application Server (continued)

Property	Default value†	Your value
Artifact resolution port This port is used for SOAP messages to be exchanged between partners. For example, this port is used during the retrieval of SAML assertions when the Browser Artifact profile is used. **Attention:** This port *must* be available even if your federation will not use SOAP messages.	9444	

†Notes®:

- You cannot change these values using the console after installation.
- When you install Tivoli Federated Identity Manager with the embedded version of WebSphere Application Server, the installation program determines whether the standard ports are available 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 of WebSphere Application Server. If you return to this installation at a later time to install additional components using the embedded version of WebSphere Application Server, the available ports will not be detected automatically.
- If you previously installed the embedded version of WebSphere Application Server, and want to install an additional component at a later time, select **No** when you are prompted as to whether you want to use an existing version of WebSphere Application Server.

IIS Web plug-in installation worksheet

This worksheet lists the properties for which you must supply a value during the IIS Web plug-in component installation. You can prepare for the installation by noting the values you should use in this worksheet.

Table 8. Properties for IIS plug-in component installation

Property	Default value	Your value
Directory name	C:\Program Files\IBM\FIM	
IIS virtual host to configure (You will select one or more hosts to configure from a list)		

Apache or IBM HTTP Server Web plug-in installation worksheet

This worksheet lists the properties for which you must supply a value during the Apache or IHS Web plug-in component installation. You can prepare for the installation by noting the values you should use in the worksheet.

Table 9. Properties for Apache or IHS plug-in component installation

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

Server configuration file location	The location of the server configuration file. For example:
	IBM HTTP Server
	`/opt/IBM/HTTPServer/conf/httpd.conf`
	Apache HTTP Server
	`/etc/httpd/conf/httpd.conf`	

Installing the federated single sign-on feature

Learn how to install the federated single sign-on feature using either the graphical mode 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 of these components. This topic also tells you how to install only the runtime and management service, since some deployments require the management console to be installed on a different computer. If you need to install the management console on a different computer, you can complete the instructions in this topic, and then see Chapter 6, "Installing the management console," on page 49.

The Tivoli Federated Identity Manager installation steps support two different scenarios for working with WebSphere Application Server:

- You can install onto an existing WebSphere Application Server.

  The existing WebSphere Application Server can be one that you just installed as a prerequisite, or can be an existing WebSphere Application Server that you have determined meets the requirements for version and fix packs.
- You can start with an environment that does not yet have WebSphere Application Server, and choose to install the embedded version of WebSphere Application Server that is included with the Tivoli Federated Identity Manager installation.

  This option 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, the full (non-embedded) IBM WebSphere Application Server Network Deployment product is used.

The installation steps to be taken depend on your choice for WebSphere Application Server.

Use the instructions in one of the following sections:

- "Installing federated single sign-on on an existing WebSphere Application Server"
- "Installing federated single sign-on with an embedded WebSphere Application Server" on page 33

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

Learn how to install the federated single sign-on feature using either the graphical mode or console mode.

Before you begin

Ensure that the machine on which you are installing meets the hardware and operating system requirements.

You can review the requirements by reading the Hardware and Software Requirements link on the Tivoli Information Center Welcome page for Tivoli Federated Identity Manager:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

Note: If you installed the embedded version of WebSphere Application Server as part of a previous installation of Tivoli Federated Identity Manager, and want to modify its settings, do not use these instructions. Use "Installing federated single sign-on with an embedded WebSphere Application Server" on page 33.

About this task

To install the federated single sign-on feature:

Procedure

1. Insert the CD into or download the image onto the machine on which you will install the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

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`
HP-UX on Itanium	`install_hpux_ia64.bin`	`install_hpux_ia64.bin -console`
Linux on System p	`install_linux_ppc.bin`	`install_linux_ppc.bin -console`

Table 10. Commands to start the installation program in graphical or console mode (continued)

Platform	Command to start the installation program in graphical mode	Command to start the installation program in console mode
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 Tivoli Federated Identity Manager installation assumes that the WebSphere Application Server to be deployed to is listening on `localhost`. When your WebSphere Application Server is not listening on `localhost`, you must specify the hostname. To do this add a parameter to your invocation of the installation binary. For example, on Linux:

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

- For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.
7. Select **Runtime and Management Services**. When you are installing the management console on the same computer, select **Management console** also. Do not select any other features. Click **Next**. The Existing WebSphere Application Server option panel is displayed.
8. Select **Yes** to indicate that you want to use an existing installation of WebSphere Application Server, and click **Next**.
9. Select whether the existing WebSphere Application Server has administration security enabled. Click **Next**.
   - If you selected **Yes**, enter the administration security settings for the existing installation of WebSphere Application Server you are using.
   - If you selected **No**, enter the directory and port information for the installation of WebSphere Application Server you are using.

     Note: If you installed the embedded version of WebSphere Application Server as part of a previous installation of Tivoli Federated Identity Manager, you will be prompted only for port information.
10. Click **Next** The Disk Space Summary panel is displayed.
11. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
12. Verify that the information is correct, and click **Next**. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.

13. Click **Finish**. The Tivoli Federated Identity Manager federated single sign-on feature installation is complete.

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

You can choose to install the embedded WebSphere Application Server when you are installing the installation components for federated single sign-on.

Before you begin

Note: Installation with the embedded WebSphere server 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, the full (non-embedded) IBM WebSphere Application Server Network Deployment product is recommended.

Ensure that the machine on which you are installing meets the hardware and operating system requirements.

You can review the requirements by reading the Hardware and Software Requirements link on the Tivoli Information Center Welcome page for Tivoli Federated Identity Manager:

http://publib.boulder.ibm.com/infocenter/tivihelp/v2r1/index.jsp?toc=/com.ibm.tivoli.fim.doc_6.2.1/toc.xml

About this task

To install the federated single sign-on feature:

Procedure

1. Insert the CD into or download the image onto the machine on which you will install the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

Table 11. 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`
HP-UX on Itanium	`install_hpux_ia64.bin`	`install_hpux_ia64.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: For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.
7. Select **Runtime and Management Services**. When you are installing the management console on the same computer, select **Management console** also. Do not select any other features. Click **Next**. The Existing WebSphere Application Server option panel is displayed.
8. Select **No** to indicated that you want to install the embedded WebSphere Application Server, and click **Next**.

   Note: If you installed the embedded version of WebSphere Application Server as part of a previous installation of Tivoli Federated Identity Manager, select **No**.
9. Enter the requested information:
   a. Enter the administrative user name, the password, and a confirmation of the password that will be used with this installation of WebSphere Application Server.
   b. Enter the port information that will be used with this installation of WebSphere Application Server. Then click **Next**. The Disk Summary panel is displayed.
10. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
11. Verify that the information is correct, and click **Next**. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.
12. Click **Finish**. The Tivoli Federated Identity Manager runtime and management services installation is complete.

Chapter 4. Installing Web services security management

Complete the following tasks in the specified order:

1. "Planning the installation of Web services security management"
2. "Installing software prerequisites for Web services security management" on page 37
3. "Completing the Web services security management installation worksheet" on page 39
4. "Installing the Web services security management feature" on page 39

Planning the installation of Web services security management

The Web services security management feature can be deployed into different scenarios. The software to be installed is determined by the properties of each deployment scenario.

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

The Web services security management feature is installed and configured into a IBM Tivoli Federated Identity Manager deployment, and each deployment must have two other IBM Tivoli Federated Identity Manager components installed and configured. The other components are the runtime and management services component and the management console component.

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

Software prerequisites for each deployment scenario

The Web services security management feature is deployed into one of two scenarios:

- Authentication and authorization

  Web services security management authenticates users and provides authorization decisions in response to requests for access to protected resources or services.
- Conversion of token types

  Web services security management converts an incoming token type to a different token type for use by WebSphere Application Server.

Each scenario has specific software prerequisites.

- Authentication and authorization

  In this scenario, Web services security management requires access to a user registry such as one provided by Tivoli Access Manager. Access to the Tivoli Access Manager user registry is managed by the Tivoli Federated Identity Manager runtime and management service component. Since the runtime and

management component is a prerequisite for all Web services security management deployments, the need for Tivoli Access Manager is met when that component is installed.

In summary, the software prerequisites for this scenario are:

– WebSphere Application Server
– Tivoli Access Manager
– Tivoli Federated Identity Manager runtime and management service component
– Tivoli Federated Identity Managermanagement console component

- Deployment of the Web services security management to provide token exchange services for WebSphere Application Server.

  In this scenario, Web services security management interacts with a WebSphere Application Server. Since WebSphere Application Server is a prerequisite for any system that hosts the Web services security management component, this scenario does not require installation of any other software prerequisites.

  Note that configuration of this scenario (after completion of the installation) can include configuration of Web services security management to communicate with a WebSphere Application Server server other than the local WebSphere Application Server. This configuration requirement does not affect the installation process.

  In summary, the software prerequisites for this scenario 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

The Web services security management component can be deployed into different distributed environments. These environments can include the deployment of all Tivoli Federated Identity Manager components on one computer, but more commonly include the distribution of those components across multiple computers.

The software installation sequence depends on your topology, and also depends on whether you have already installed some of the software prerequisites as part of the prior installation of other Tivoli Federated Identity Manager components.

Environments:

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

  In this environment, you must first install (on other computers) the other the Tivoli Federated Identity Manager components: the runtime and management services component and the management console component. The only required software prerequisite on the host computer for Web services security management is WebSphere Application Server.

  In this environment, when you have not previously installed any of the Tivoli Federated Identity Manager components, the software installation sequence is:

  1. On one computer, install the runtime and management services component and the management console component. The installation sequence for these components is:
     a. WebSphere Application Server

b. Tivoli Access Manager
c. Tivoli Federated Identity Manager runtime and management service component
d. Tivoli Federated Identity Manager management console.

Note that it is possible to install the management console on its own computer, separate from the runtime and management service component.

2. On the computer where you will use the Web services security management feature, install:
   a. WebSphere Application Server
   b. Tivoli Federated Identity Manager Web services security management component

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

  In this environment, you must first install the runtime and management services component. This software prerequisites for this component are WebSphere Application Server and Tivoli Access Manager.

  Note that by installing the runtime and management services component you will satisfy the Web services security management 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

  Note that it is possible to install the management console on its own computer, separate from the runtime and management service component.

Installing software prerequisites for Web services security management

In most installation scenarios, you must install software prerequisites as part of installing the Web services security management feature.

The list of software prerequisites to be installed varies depending on the deployment scenario and also on the current state of the security infrastructure. In particular, the software prerequisites depend on whether:

- You want to complete an initial installation of Tivoli Federated Identity Manager, including the Web services security management component.
- You want to add the Web services security management component to an existing Tivoli Federated Identity Manager deployment.

Initial installation of Tivoli Federated Identity Manager

When you want to install a new Tivoli Federated Identity Manager deployment, you must install prerequisite software.

The minimum software prerequisite for the Web services security management component is WebSphere Application Server. However, deployment of Web services security management is also dependent on both the Tivoli Federated Identity Manager management service and the Tivoli Federated Identity Manager management console.

When you want to install all the necessary Tivoli Federated Identity Manager software, you need to complete the following steps:

1. Install the Tivoli Federated Identity Manager runtime and management service component

   Installation of this component requires you to install these software prerequisites:

   a. WebSphere Application Server
   b. Tivoli Access Manager

   The installation of these software prerequisites is described in the documentation for federated single sign-on. The same installation steps apply here. See Chapter 3, "Installing federated single sign-on or token exchange," on page 15.
2. Install the Tivoli Federated Identity Manager management console component

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

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

   a. WebSphere Application Server
   b. Management console

   See Chapter 6, "Installing the management console," on page 49.

There are a number of supported scenarios for deploying Tivoli Federated Identity Manager 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 35.

Adding Web services security management to a Tivoli Federated Identity Manager deployment

When you want to add Web services security management to an existing Tivoli Federated Identity Manager deployment, there are two scenarios:

- Installing Web services security management on a computer that already has a Tivoli Federated Identity Manager component, such as the runtime and management services or the management console.

  For this scenario, the software prerequisites are:

  – None
- Installing Web services security management on a computer that does *not* have any Tivoli Federated Identity Manager components installed.

  For this scenario, the software prerequisites are:

  – WebSphere Application Server

  For installation instructions, see "Installing WebSphere Application Server" on page 18.

Completing the Web services security management installation worksheet

View and print the worksheet that lists the properties for which you must supply a value during the Web services security management feature installation. You can prepare for the installation by noting the values you should use in the worksheet.

Table 12. Properties for Web services security management feature installation

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

When you are adding the Web services security management component to a computer that has Tivoli Federated Identity Manager installed (either the runtime and management services or the management console), place the Web services security management component in the directory as the other Tivoli Federated Identity Manager components.

Installing the Web services security management feature

This topic describes how to install the Web services security management feature using either the graphical mode or console mode.

Before you begin

Before installing, verify that you have installed the software prerequisites that are required for your deployment scenario.

About this task

To install the Web services security management feature:

Procedure

1. Insert the CD into or download the image onto the machine on which you will install the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

Table 13. 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`
HP-UX on Itanium	`install_hpux_ia64.bin`	`install_hpux_ia64.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`

Table 13. Commands to start the installation program in graphical or console mode (continued)

Platform	Command to start the installation program in graphical mode	Command to start the installation program in console mode
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 Tivoli Federated Identity Manager installation assumes that the WebSphere Application Server to be deployed to is listening on `localhost`. When your WebSphere Application Server is not listening on `localhost`, you must specify the hostname. To do this add a parameter to your invocation of the installation binary. For example, on Linux:

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

- For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.
7. Select **Web Services Security Management**, clear the check boxes for the other features, and click **Next**. The Disk Space Summary panel is displayed.
8. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
9. Verify that the information is correct, and click **Next**. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.
10. Click **Finish**. The Tivoli Federated Identity Manager Web services security management installation is complete.

Chapter 5. Installing federated provisioning

Installation of the federated provisioning feature requires the deployment of some software prerequisites. When the prerequisites are installed, you can install the WS-Provisioning runtime component.

Complete the following instructions:

1. "Planning federated provisioning"
2. "Installing software prerequisites for federation provisioning" on page 42
3. "Completing the WS-Provisioning runtime installation worksheet" on page 47
4. "Installing the WS-Provisioning runtime component" on page 47

Planning federated provisioning

The WS-Provisioning runtime component is installed and configured into a IBM Tivoli Federated Identity Manager deployment, and each deployment must have two other IBM Tivoli Federated Identity Manager components installed and configured. The other components are the runtime and management services component and the management console.

Note: WS-Provisioning is not supported on IBM Tivoli Federated Identity Manager for z/OS platforms.

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

Before you install IBM Tivoli Federated Identity Manager provisioning, you must install and configure a distributed application environment. This environment is the same as the environment required for the IBM Tivoli Federated Identity Manager runtime and management services feature, with the addition of IBM Tivoli Directory Integrator.

In a prototype or test environment, all software for each side (client or server) of the federated provisioning deployment can be installed on one computer. In a production environment, the software is typically distributed across multiple computers.

The IBM Tivoli Federated Identity Manager WS-Provisioning runtime feature can communicate with any other provisioning service that supports the WS-Provisioning standard. The IBM Tivoli Federated Identity Manager provisioning service has no requirements on the environment that is hosting and supporting the other (third-party) provisioning service. The third-party environment must supply its own methods for building and authenticating WS-Provisioning messages. This means that IBM Tivoli Federated Identity Manager does not require that the third-party environment use the IBM Tivoli Federated Identity Manager prerequisites such as WebSphere Application Server, Tivoli Access Manager, or IBM Tivoli Directory Integrator.

IBM Tivoli Federated Identity Manager provisioning requires that the IBM Tivoli Federated Identity Manager runtime and management services feature be installed and deployed. The provisioning service adds additional software prerequisites beyond those prerequisites required for the deployment of the IBM Tivoli Federated Identity Manager runtime and management services feature.

After you have installed the prerequisites for the Tivoli Federated Identity Manager runtime and management services feature, you must install additional prerequisites to support the WS-Provisioning runtime feature.

Some of the prerequisites must be installed on the computer that hosts the federated provisioning. Other prerequisites can be installed on other computers and accessed through network connections.

- Software prerequisites that must be installed on the *same* computer as the IBM Tivoli Federated Identity Manager provisioning software
  - WebSphere Application Server
  - IBM Tivoli Directory Integrator
  - 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 part of theIBM Tivoli Federated Identity Manager provisioning software. It is not a required part of the WS-Provisioning support.
- Software prerequisites that can be installed on a *different* computer from the IBM Tivoli Federated Identity Manager provisioning software
  - 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 the installation and configuration of some software prerequisites.

The number of software prerequisites to install, and the sequence of their installation, depends on the state of your security infrastructure deployment. The installation tasks differ depending on whether you are about to being an initial deployment of Tivoli Federated Identity Manager domain, or if you are adding federated provisioning to an existing deployment.

Initial installation of Tivoli Federated Identity Manager

When you have not yet installed any of the Tivoli Federated Identity Manager components or their software prerequisites, you must first complete an installation of the federated single sign-on feature.

The software does not have to be on the same computer as the computer where you will install the federated provisioning feature.

1. Tivoli Federated Identity Manager runtime and management service component

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. Tivoli Federated Identity Manager 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 49.

3. IBM Tivoli Directory Integrator

   This product is required by the federated provisioning feature.

   See "Installing IBM Tivoli Directory Integrator" on page 44.

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

   The federated provisioning feature includes a demonstration scenario. The demonstration scenario has a software prerequisite on the IBM Tivoli Access Manager for e-business Java runtime environment. Installation of the demonstration scenario is optional. If you do not intend to install the demonstration scenario, you do not have to install this prerequisite.

   For installation instructions, see "Installing Tivoli Access ManagerJava runtime environment" on page 46.

5. Federated provisioning requires that WebSphere Application Server be installed on the *same* computer as the federated provisioning component.
   - If you have installed either Tivoli Federated Identity Manager or IBM Tivoli Directory Integrator on the computer that will host federated provisioning, you have met this prerequisite. Continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.
   - If you need to install WebSphere Application Server, see either the WebSphere Application Server documentation or see the installation summary in "Installing WebSphere Application Server" on page 18.

Adding federated provisioning to a Tivoli Federated Identity Manager deployment

When you have already established a Tivoli Federated Identity Manager single sign-on federation, the installation sequence for software prerequisites is:

1. IBM Tivoli Directory Integrator

   See "Installing IBM Tivoli Directory Integrator" on page 44.

2. IBM Tivoli Access Manager for e-business Java runtime environment

   The federated provisioning feature includes a demonstration scenario. The demonstration scenario has a software prerequisite on the IBM Tivoli Access Manager for e-business Java runtime environment. Installation of the demonstration scenario is optional. If you do not intend to install the demonstration scenario, you do not have to install this prerequisite.

   See"Installing Tivoli Access ManagerJava runtime environment" on page 46.

3. If you are installing the WS-Provisioning runtime on a *different* computer than one that hosts the single sign-on federation or the IBM Tivoli Directory Integrator product, you must install WebSphere Application Server.

   See either the WebSphere Application Server documentation or see the installation summary in "Installing WebSphere Application Server" on page 18.

4. When you have installed all of the software prerequisites, continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.

Installing IBM Tivoli Directory Integrator

The federated provisioning feature requires the installation of IBM Tivoli Directory Integrator.

About this task

The Tivoli Federated Identity Manager WS-Provisioning runtime feature requires that IBM Tivoli Directory Integrator be installed and accessible within a distributed application environment. The WS-Provisioning runtime feature does *not* require that Tivoli Federated Identity Manager and IBM Tivoli Directory Integrator be installed on the same host.

This topic summarizes an example installation on Linux. For complete installation instructions for your platform type, see the *IBM Tivoli Directory Integrator Administration Guide* on the Tivoli information center:

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

Summary of the installation on Linux:

Procedure

1. Execute the setup file:

   `./setupIntelLinux.bin`

   The InstallShield graphical installation starts. The Welcome panel is displayed.
2. Click **Next**.

   The software license is displayed.
3. Accept the software license agreement and click **Next**.

   The installation directory panel is displayed.
4. Accept the default installation directory or specify an alternative location. Click **Next**.

   Default installation directory on Linux:

   `/opt/IBM/IBMDirectoryIntegrator`

   You are prompted by the next panel to specify a location for your solutions.
5. Select one of the solutions location choices. You can accept the default selection of **Use a tdi subdirectory under my home directory**. Click **Next**.

   A summary panel states the installation directory and size of the installation.
6. Click **Next** to begin the installation.

   When the file extraction completes, a panel is displayed indicating the successful completion of the installation.
7. Click **Finish**.
8. Choose one:
   - When you are using IBM Tivoli Directory Integrator Version 6.1, continue with the next step.
   - When you are using IBM Tivoli Directory Integrator Version 6.0, you must install a Fix Pack. Continue with "Installing IBM Tivoli Directory Integrator Version 6.0 Fix Pack 1" on page 45.
9. Choose one:
   - If you do not plan to use the provisioning demonstration scenario, you have now finished installing prerequisites. Continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.

- If you plan to use the provisioning demonstration scenario, continue with the next step.

10. Complete this step only when you plan to use the provisioning demonstration scenario. Choose one:
    - When installing on the client side, you have now finished installing prerequisites. Continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.
    - When installing on the server side, you must install additional prerequisites. Continue with "Installing Tivoli Access ManagerJava runtime environment" on page 46.

Installing IBM Tivoli Directory Integrator Version 6.0 Fix Pack 1

About this task

Note: This topic applies only to installations of IBM Tivoli Directory Integrator Version 6.0. The Tivoli Federated Identity Manager Version 6.1 product includes IBM Tivoli Directory Integrator Version 6.1, which does not need the Fix Pack.

Fix Pack 1 is required in order to use the Tivoli Federated Identity Manager EAR files with IBM Tivoli Directory Integrator.

Obtain the fix pack from the IBM Support Web site by completing the following steps:

Procedure

1. Access the IBM Tivoli Directory Integrator Support Web site:
   ```
   http://www.ibm.com/software/sysmgmt/products/
     support/IBMDirectoryIntegrator.html
   ```
2. Enter the following text in the Search window:
   ```
   6.0.0-TIV-ITDI-FP0001
   ```
3. In the Search results, select the link:
   ```
   IBM Tivoli Directory Integrator Ver 6.0 Fixpack 1(6.0.0-TIV-ITDI-FP0001)
   ```
   The fix pack page is displayed.
4. Download the fix pack for your platform.
5. Download the README file:
   ```
   6.0.0-TIV-ITDI-FP0001.README
   ```

   Note: If you have difficulty locating the fix pack by using the instructions above, 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"
   ```
   The InstallShield graphical installation starts. The Welcome panel is displayed.
7. Click **Next**.
   The software license is displayed.
8. Accept the software license agreement and click **Next**.
   The installation directory panel is displayed.
9. Accept the default installation directory or specify an alternative location. Click **Next**.

Default installation directory on Linux:

`/opt/IBM/IBMDirectoryIntegrator`

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

10. Click **Next** to begin the installation.

    When the file extraction completes, a panel is displayed indicating the successful completion of the installation.

11. Click **Finish**.

12. Choose one:

    - If you do not plan to use the provisioning demonstration scenario, you have now finished installing prerequisites. Continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.
    - If you plan to use the provisioning demonstration scenario, continue with the next step.

13. Complete this step only when you plan to use the provisioning demonstration scenario. Choose one:

    - When installing on the client side, you have now finished installing prerequisites. Continue with "Completing the WS-Provisioning runtime installation worksheet" on page 47.
    - When installing on the server side, you must install additional prerequisites. Continue with "Installing Tivoli Access ManagerJava runtime environment."

Installing Tivoli Access ManagerJava runtime environment

About this task

Attention: This component is required only on the provisioning server side because the demonstration scenario does not create users on the client side. When installing provisioning on the client side, skip this topic and continue with "Installing the WS-Provisioning runtime component" on page 47.

The Tivoli Federated Identity Manager provisioning demonstration scenario provides example customer code that includes use of the Tivoli Access Manager Java Administration API. This API is used to create Tivoli Access Manager users and to enable or disable their accounts.

In order to use the Java Administration API, you must install the Tivoli Access Manager Java runtime environment on the host where the demonstration scenario will run the provisioning service in the *server* role.

Procedure

1. Ensure that IBM JRE 1.4.2 is installed before running the installation.

   See the topic "Installing prerequisite products" in the *IBM Tivoli Access Manager for e-business Base Installation Guide*

2. For complete installation instructions, see the *IBM Tivoli Access Manager Base Installation Guide* topic "Setting up a Java runtime environment system".

   You can access this document from the Tivoli Access Manager section of the Tivoli information center:

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

   Install using either an installation wizard or the native utilities.

Completing the WS-Provisioning runtime installation worksheet

View and print the worksheet that lists the properties for which you must supply a value during the WS-Provisioning runtime feature installation. You can prepare for the installation by noting the values you should use in the worksheet.

When you have already installed the Tivoli Federated Identity Manager runtime and management service on the computer where you plan to install the WS-Provisioning runtime component, install the WS-Provisioning runtime component in the same directory.

Table 14. Properties for WS-Provisioning runtime feature installation

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

Installing the WS-Provisioning runtime component

Before you begin

Before installing, verify that you have installed the software prerequisites that are required for your deployment scenario.

If you need to install software prerequisites, see "Installing software prerequisites for federation provisioning" on page 42

About this task

To install the WS-Provisioning runtime component:

Procedure

1. Insert the CD into or download the image onto the machine on which you will install the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

Table 15. 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`
HP-UX on Itanium	`install_hpux_ia64.bin`	`install_hpux_ia64.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`

Table 15. Commands to start the installation program in graphical or console mode (continued)

Platform	Command to start the installation program in graphical mode	Command to start the installation program in console mode
Solaris	`install_sol_sparc.bin`	`install_sol_sparc.bin -console`
Windows	`install_win32.exe`	`install_win32.exe -console`

Note:

- The Tivoli Federated Identity Manager installation assumes that the WebSphere Application Server to be deployed to is listening on `localhost`. When your WebSphere Application Server is not listening on `localhost`, you must specify the hostname. To do this add a parameter to your invocation of the installation binary. For example, on Linux:

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

- The WS-Provisioning component is not supported on Tivoli Federated Identity Manager for z/OS.

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.
7. Select **WS-Provisioning Runtime**, clear the check boxes for the other features, and click **Next**. The Disk Space Summary panel is displayed.
8. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
9. Verify that the information is correct, and click **Next**. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.
10. Click **Finish**. The Tivoli Federated Identity Manager WS-Provisioning runtime installation is complete.

What to do next

The next task to complete depends on your installation scenario.

- If you are doing an initial installation of Tivoli Federated Identity Manager, and have not yet created a domain and configured a single sign-on federation, you must do that now. When you finish configuring the single sign-on federation, you can deploy the provisioning files and configure the provisioning service.

  Steps:

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

     See *IBM Tivoli Federated Identity Manager Administration Guide*.

- If you have *already* deployed and configured a Tivoli Federated Identity Manager domain and a single sign-on federation, you can now deploy the provisioning files and configure the provisioning service.

  See *IBM Tivoli Federated Identity Manager Administration Guide*.

Chapter 6. Installing the management console

You can install the management 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 50
3. "Installing the management console feature" on page 53

Planning the installation of the management console

You can install the IBM Tivoli Federated Identity Manager management console on a computer that does not have any other IBM Tivoli Federated Identity Manager components.

When you want to separate administration functions from runtime functions, you can install the management console on a separate computer. The management console is a plug-in to the WebSphere Application Server administration console. In some deployment scenarios, you might want to use the IBM Tivoli Federated Identity Manager management console on the same computer as the WebSphere Application Server administration console.

The management console component is packaged in the same installation binary as the Tivoli Federated Identity Manager runtime and management services component and the federated provisioning component. During the installation, you have the opportunity to select it as one of the components to install. This means that in many Tivoli Federated Identity Manager scenarios, the administrator chooses to install the management console at the same time as one of the other components.

When your Tivoli Federated Identity Manager scenario requires that the management console be installed separately other Tivoli Federated Identity Manager components, there is one software prerequisite to install:

- WebSphere Application Server

You can satisfy this prerequisite in one of two ways:

- Install a supported version of WebSphere Application Server.
- Install the embedded WebSphere Application Server that is distributed as part of Tivoli Federated Identity Manager.

  The embedded WebSphere Application Server is a lightweight version of the server. It is intended to support environments that run a limited number of applications and do not require the full administration support provided by WebSphere Application Server. The embedded WebSphere Application Server provides a lightweight version of the WebSphere Application Server administration console, and provides all the support needed to run the Tivoli Federated Identity Manager management console.

  During the installation of the management console, you are prompted to specify whether you want to install embedded WebSphere Application Server. You can select it, and it is installed during the Tivoli Federated Identity Manager component installation.

This means that when you intend to use embedded WebSphere Application Server, you do not need to perform a separate installation of a software prerequisite.

Complete the following steps:

1. Decide which version of WebSphere Application Server you want to use.
   - To use the embedded WebSphere Application Server, skip this step.
   - When necessary, install a separate WebSphere Application Server server.
     a. Go to the Tivoli Federated Identity Manager information center to review the list of supported versions.
     b. Install the server by using the instructions in the documentation on the WebSphere Application Server information center.
2. Continue with "Console installation worksheet."

Console installation worksheet

This worksheet lists the properties for which you must supply a value during the management console component installation. You can prepare for the installation by noting the values you should use in the worksheet.

If you are installing the console on the same server where the runtime component is installed, some of the fields you are prompted for will be the same. Use the values from your "Runtime and management service installation worksheet" on page 26 for those fields.

Installation on existing version of WebSphere Application Server

If you are installing the management console component on an existing version of WebSphere Application Server, you will need to know whether that installation has administration security enabled. An *existing* version is either the separately installable version that was provided with Tivoli Federated Identity Manager and that you have already installed or a compatible version of WebSphere Application Server that is already installed.

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

Property	Default value†	Your value

Directory name	**AIX, HP-UX, Linux or Solaris**
	`/opt/IBM/FIM`
	Windows
	`C:\Program Files\IBM\FIM`	

When WebSphere Application Server administration security is *not* enabled:		

WebSphere Application Server installation directory	**AIX**
	`/usr/IBM/WebSphere/AppServer`
	HP-UX, Linux or Solaris
	`/opt/IBM/WebSphere/AppServer`
	Windows
	`C:\Program Files\IBM\WebSphere\AppServer`	

Table 16. Properties for console component installation on existing version of WebSphere Application Server (continued)

Property	Default value†	Your value
WebSphere Application Server SOAP connector port The port number on which the WebSphere Application Server handles SOAP communication.	8879	
Note: If you previously installed the embedded version of WebSphere Application Server, you will *not* be prompted 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 key store file
 	
The truststore file used by WebSphere Application Server.
	AIX, HP-UX, Linux or Solaris
	`/opt/IBM/FIM/ewas/profiles/ itfimProfile/etc/ trust.p12`
	
	Windows
	`C:\Program Files\IBM\FIM\ ewas\profiles\ itfimProfile\etc\ trust.p12`	

SSL Trusted Java key store password The password needed to access the WebSphere truststore.	WebAS	
SSL Java key store file The keystore file used by WebSphere Application Server.		
SSL Java key store password The password needed to access the keystore.		
Note: If you previously installed the embedded version of WebSphere Application Server, the prompts for the SSL Java key store and password will *not* be displayed.		

†Note:

- You cannot change these values using the console after installation.

Installation on embedded version of WebSphere Application Server

Table 17. Properties for console component installation on embedded version of WebSphere Application Server

Property	Default value†	Your value

Directory name	**AIX, HP-UX, Linux or Solaris**
	`/opt/IBM/FIM`
	Windows
	`C:\Program Files\IBM\FIM`	

WebSphere Application Server administrator user name	`fimadmin`	
WebSphere Application Server administrator password		
Application server port The port number that WebSphere Application Server uses to communicate over HTTP.	`9080`	
Secure application server port The port number that WebSphere Application Server uses to communicate over HTTPS.	`9443`	
Administration port The port number that the WebSphere Application Server administration console uses for HTTP.	`9060`	
Secure administration port The port number that the WebSphere Application Server administration console uses for HTTPS.	`9043`	
SOAP port The port number on which the WebSphere Application Server handles SOAP communication.	`8879`	

†Notes:

- You cannot change these values using the console after installation.
- When you install Tivoli Federated Identity Manager with the embedded version of WebSphere Application Server, the installation program determines whether

the standard ports are available 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 of WebSphere Application Server. If you return to this installation at a later time to install additional components using the embedded version of WebSphere Application Server, the available ports will not be detected automatically.

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

Installing the management console feature

Learn how to install the management console feature using either the graphical mode or console mode.

Before you begin

Be sure the machine on which you are installing meets the feature requirements.

Also, make sure you have decided whether you will use the embedded version of WebSphere Application Server that is included with the Tivoli Federated Identity Manager installation or an existing installation of WebSphere Application Server. If you plan to use an existing installation, make sure that you have the correct version installed and configured on the server before proceeding. You can install the management console feature individually.

About this task

To install the management console feature:

Procedure

1. Insert the CD into or download the image onto the machine on which you will install the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

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

Platform	Command to start the installation program
AIX	`install_aix_ppc.bin`
HP-UX on Itanium	`install_hpux_ia64.bin`
Linux on System p	`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`

Note:

- The Tivoli Federated Identity Manager installation assumes that the WebSphere Application Server to be deployed to is listening on `localhost`.

When your WebSphere Application Server is not listening on `localhost`, you must specify the hostname. To do this add a parameter to your invocation of the installation binary. For example, on Linux:

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

- For installation commands for the z/OS platform, see the *IBM Tivoli Federated Identity Manager for z/OS Program Directory*.

For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

Table 19. Commands to start the installation program on console mode

Platform	Command to start the installation program
AIX	`install_aix_ppc.bin -console`
HP-UX on Itanium	`install_hpux_ia64.bin -console`
Linux on System p	`install_linux_ppc.bin -console`
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`

Note: For installation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.
7. Select **Management Console**, clear the check boxes for the other features, and click **Next**. The Existing WebSphere Application Server option panel is displayed.
8. Select whether you want to use an existing installation of WebSphere Application Server, and click **Next**. If you installed the embedded version of WebSphere Application Server as part of a previous installation of Tivoli Federated Identity Manager, select **No**.
9. If you are *not* using an existing installation of WebSphere Application Server for the feature, continue with this step. Otherwise, continue with step 10.
   a. Enter the administrative user name, the password, and a confirmation of the password that will be used with this installation of WebSphere Application Server.
   b. Enter the port information that will be used with this installation of WebSphere Application Server. Then click **Next**. The Disk Summary panel is displayed. Continue with step 11 on page 55.
10. If you *are* using an existing installation of WebSphere Application Server for the feature, continue with this step. Otherwise, continue with step 11 on page 55.
    a. Select whether the existing WebSphere Application Server has administration security enabled.

b. Click **Next**.
   - If you selected **Yes**, enter the administration security settings for the existing installation of WebSphere Application Server you are using.
   - If you selected **No**, enter the directory and port information for the installation of WebSphere Application Server you are using.

     Note: If you installed the embedded version of WebSphere Application Server as part of a previous installation of Tivoli Federated Identity Manager, you will be prompted only for port information.

c. Click **Next** The Disk Space Summary panel is displayed and you will continue with step 11.

11. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
12. Verify that the information is correct, and click **Next**. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.
13. Click **Finish**. The Tivoli Federated Identity Manager management console installation is complete.

Chapter 7. Installing the IBM Support Assistant

The IBM Support Assistant Lite tool for Tivoli Federated Identity Manager 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 use either graphical mode or silent mode to install the IBM Support Assistant Lite tool.

Procedure

1. Insert the CD into or download the software image onto the machine on which you are installing the feature.
2. Use a command line to start the installation using either the graphical mode or console mode.

Table 20. 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`
HP-UX on Itanium	`install_hpux_ia64.bin`	`install_hpux_ia64.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 Tivoli Federated Identity Manager installation assumes that the WebSphere Application Server to be deployed to is listening on `localhost`. When your WebSphere Application Server is not listening on `localhost`, you must specify the hostname. To do this add a parameter to your invocation of the installation binary. For example, on Linux:

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

3. Select a language, and click **OK**. The software license agreement is displayed.
4. If you agree to the license terms, accept the license, and click **Next**. The Welcome screen is displayed.
5. Click **Next**. The installation directory panel is displayed.
6. Specify an installation directory in the **Directory name** field, or accept the default directory. Optionally, click **Browse** to select a directory on the file system.

7. Select **IBM Support Assistant plugin for Federated Identity Manager**, clear the check boxes for the other features, and click **Next**. The Disk Space Summary panel is displayed.
8. Verify that adequate free space is available, and click **Next**. The installation summary screen is displayed.
9. Verify that the information is correct, and click **Next**. The files are installed. When file installation completes, an installation summary panel is displayed.
10. Click **Finish**. The Tivoli Federated Identity Manager ISA Support Assistant installation is complete.
11. Uncompress the Tivoli Federated Identity Manager IBM Support Assistant Lite archive `TFIMISALite.zip`

    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`.

Results

For information on how to use the IBM Support Assistant Lite, see the *IBM Tivoli Federated Identity Manager Troubleshooting Guide*.

Chapter 8. Using silent mode installation

Learn how to create and use a response file to install the Tivoli Federated Identity Manager features at the same time on the same server, or individually on separate servers.

Prior to the installation, be sure that you have reviewed the feature requirements and decided if you will install the features together or separately on your servers.

You should also decide if you will use the following environment configurations:

- An existing supported version of WebSphere Application Server or the embedded version of WebSphere Application Server that is included with the Tivoli Federated Identity Manager software.

Note: Examples of response files are included in the /rsp directory on the Tivoli Federated Identity Manager CD.

The following procedures for the silent installation mode describe creating a response files and using the response files.

Creating a response file

A response file records the actions to be performed by the installation or uninstallation wizard.

About this task

To create a response file for installing or uninstalling the component:

Procedure

1. Launch the installation or uninstallation wizard for the desired operating system platform and specify the name of a file to be used to record the options taken.

   Installation

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

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

   Linux on xSeries®
   ./install_linux_x86.bin `-options-record` *response_file_name*

   Linux on zSeries®
   ./install_linux_s390.bin `-options-record` *response_file_name*

   HP-UX
   ./install_hpux_ia64.bin `-options-record` *response_file_name*

   Windows
   install_win32.exe `-options-record` *response_file_name*
2. Proceed through the program panels and specify the desired values for the various options.
3. After completing the panels, click **Finish** to create the response file.

4. Review the response file created to verify that the values specified are correct. Some response files might contain macros rather than the data that was entered. In these cases, you might need to edit the file using a text editor.
5. Make the response file available to the people or processes that will use it to install or uninstall the component.

Using a response file

After a response file has been created, the response file can be used with the installation wizard to install the component in a predetermined manner.

About this task

To install the component using a response file from the command line:

Procedure

1. Open a command prompt.
2. Launch the installation wizard for the desired operating system platform specifying the response file that has been created.

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

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

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

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

   HP-UX
   ./install_hpux_ia64.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.

What to do next

Alternately, the wizard can be launched from a script or batch file as part of an automated process.

Appendix A. Upgrading to version 6.2.1

The procedure you must follow to upgrade a previous version of Tivoli Federated Identity Manager to Tivoli Federated Identity Manager version 6.2.1 depends on whether your existing environment was installed using an existing version of WebSphere Application Server or the embedded version of WebSphere Application Server.

About this task

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 63
- "Enabling Java calls made from XSLT files after upgrading" on page 65
- "Upgrading LDAP" on page 65
- "Migration information for cluster environment" on page 66

Upgrading on an existing WebSphere Application Server installation

Use these instructions to upgrade Tivoli Federated Identity Manager from a previous version that was installed on an existing version of WebSphere Application Server to version 6.2.1, which will also be installed on an existing version of WebSphere Application Server.

Before you begin

Before continuing with this upgrade procedure:

- Ensure that your installation is at level 6.0.1.1 or higher, 6.1.1.0 or higher, or 6.2.0 or higher. To check your installation level, log into the console and check the version number on the Welcome page.
- If your installation is not at the required level, download the appropriate fix pack using the Download section of the Tivoli Federated Identity Manager Support site at: http://www.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html. Follow the fix pack installation instructions. Then return to these upgrade instructions.

About this task

Attention: This upgrade procedure requires that you install version 6.2.1 on an existing version of WebSphere Application Server where the previous version was installed.

Procedure

1. Make a note of your existing domain properties.
   a. On the existing system, log into the console.
   b. Click **Tivoli Federated Identity Manager → Domains**
   c. Select a domain and then click **Properties**.

Note: You will need this information later, when using the domain wizard, to recreate the connection between the administration console and the management service.

2. Backup the configuration of your existing environment, which was installed on an existing version of WebSphere Application Server.
   a. Using the console, export the existing configuration by clicking **Tivoli Federated Identity Manager → Domain Management**.
   b. Click **Import and Export Configuration**, select the appropriate domain, and then click **Export Configuration**
   c. When prompted, specify the location where the exported configuration JAR file is to be saved. Click **OK**. The saved configuration is your backup. It will not be used in the upgrade.
3. Uninstall the previous version of Tivoli Federated Identity Manager. Refer to the procedures in Appendix I, "Uninstalling," on page 89.
4. Install Tivoli Federated Identity Manager version 6.2.1.

   Attention:
   - You must install version 6.2.1 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**.
5. When the installation is completed, restart the WebSphere Application Server where the runtime and management service component is installed.
6. When the server restarts, activate and deploy the domain, as follows:
   a. Log into the console and click **Tivoli Federated Identity Manager → Domains**.
   b. Click **Create** to create a domain. The Domain creation wizard prompts you for domain information. Supply the information that you noted in step 1 on page 61.

      For instructions on creating a domain, see the *IBM Tivoli Federated Identity Manager Configuration Guide*..
   c. At the end of the domain wizard, select the check box to make the domain active.
   d. 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.

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

      1) Select **Tivoli Federated Identity Manager > Domains**
      2) Select your domain. Verify that it is the active domain.
      3) Select **Properties**.
      4) 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 and click **Unconfigure**.
      5) You can now return to the Domain properties portlet to enter the properties. Select **Tivoli Federated Identity Manager > Domains**
      6) Select your domain. Verify that it is the active domain.
      7) Select **Properties**.

8) Enter the Tivoli Access Manager properties.
9) Click OK.

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

Note: If the following error is displayed, 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.
```

f. Click **Deploy Runtime**.

7. If your previous system had version 6.0.1.x installed, you must run the tfimcfg tool to configure properties for the WebSEAL point of contact server.

What to do next

The upgrade procedure should now be complete.

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

- "Enabling Java calls made from XSLT files after upgrading" on page 65
- "Migration information for cluster environment" on page 66

Upgrading on an embedded WebSphere Application Server installation

Use these instructions to upgrade Tivoli Federated Identity Manager from a previous version that was installed on the embedded version of WebSphere Application Server to version 6.2.1, which will also be installed on the embedded version of WebSphere Application Server.

Before you begin

Before continuing with this upgrade procedure:

- Ensure that your installation is at level 6.1.1.1 or higher. To check your installation level, log into the console and check the version number on the Welcome page.
- If your installation is not at the required level, download the appropriate fix pack using the Download section of the Tivoli Federated Identity Manager Support site at: http://www-306.ibm.com/software/sysmgmt/products/support/IBMTivoliFederatedIdentityManager.html. Follow the fix pack installation instructions. Then return to these upgrade instructions.
- Ensure that you have copies of the SSL certificates that you use in your current environment and that you will continue to use in your new environment.

About this task

Attention: This upgrade procedure requires that you install version 6.2.1 on the embedded version of WebSphere Application Server.

Procedure

1. Make a note of your existing domain properties:
   a. On the existing system, log into the console.
   b. Click **Tivoli Federated Identity Manager → Domains**.

c. Select a domain and then click **Properties**.

Note: You will need this information later, when using the domain wizard, to recreate the connection between the administration console and the management service.

2. Backup the configuration of your existing environment, which was installed on an embedded version of WebSphere Application Server.
   a. Using the console, export the existing configuration by clicking **Tivoli Federated Identity Manager → Domain Management → Import and Export Configuration → Export Configuration**
   b. When prompted, specify the location where the exported configuration JAR file is to be saved. Click **OK**. You will use this file to import your configuration into your 6.2.1 version installation.
3. Uninstall the previous version of Tivoli Federated Identity Manager. Refer to the procedures in Appendix I, "Uninstalling," on page 89.
4. Install Tivoli Federated Identity Manager version 6.2.1.

   Attention: During the installation, when you are given the option to use an existing version of WebSphere Application Server, select **No**.
5. When the installation is completed, restart the WebSphere Application Server where the runtime and management service component is installed.
6. When the server restarts, create and deploy a domain.
   a. Log into the console and click **Tivoli Federated Identity Manager → Domains**.
   b. Click **Create** to create a domain. The Domain creation wizard prompts you for domain information. Supply the information that you noted above.

      For further instructions on creating a domain, see the *IBM Tivoli Federated Identity Manager Configuration Guide*.
   c. At the end of the domain wizard, select the check box to make the domain active.
7. Import the configuration that you exported in step 2.
   a. Using the console, import the configuration by clicking **Tivoli Federated Identity Manager → Domain Management → Import and Export Configuration → Import Configuration**
   b. Select the domain name of the domain into which the configuration archive is to be imported.
   c. In the **Configuration Archive** field, enter the fully qualified path name to the exported JAR file, such as /tmp/fimconfig_20061011–114614–0500.jar. Or, use **Browse** to locate the file.
   d. Click **Import Configuration**.
   e. Deploy the runtime when prompted.
8. Review your configuration to ensure that the importing process completed successfully.
9. 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.

   Note: In some upgrade scenarios, properties for Tivoli Access Manager are not automatically migrated. For these scenarios, you must manually enter the properties.
   a. Select **Tivoli Federated Identity Manager > Domains**
   b. Select your domain. Verify that it is the active domain.

c. Select **Properties**.
d. If the properties for Tivoli Access Manager are missing, you must first unconfigure the runtime before updating the properties:
   1) Select **Tivoli Federated Identity Manager > Domain Management > Runtime Node Management**
   2) Select the runtime in the table and click **Unconfigure**.
e. You can now return to the Domain properties portlet to enter the properties. Select **Tivoli Federated Identity Manager > Domains**
f. Select your domain. Verify that it is the active domain.
g. Select **Properties**.
h. Enter the Tivoli Access Manager properties.
i. Click OK.

10. Replace the SSL certificates on the version 6.2.1 system with the SSL certificates and configuration that you intend to use. Refer to the procedures in the *IBM Tivoli Federated Identity Manager Configuration Guide*.

What to do next

When the upgrade procedure is completed successfully, continue with "Enabling Java calls made from XSLT files after upgrading" as appropriate for your environment.

Enabling Java calls made from XSLT files after upgrading

In your previous installation of Tivoli Federated Identity Manager you might have made Java calls from your XSLT files. To keep these calls working properly after you upgrade to version 6.2.1, you must place the .jar file that contains the XSLT extension class in your ext subdirectory.

About this task

Note: Starting from version 7 of WebSphere Application Server, you cannot enable Java calls from XSLT files. The recommended migration path, where Java is required, is to implement and deploy a Java mapping module.

Complete the following procedure.

Procedure

1. Locate your .jar file that contains the XSLT extension class.
2. Move the .jar file to the appropriate directory.

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

   HP-UX, Linux, Solaris
   /opt/IBM/WebSphere/AppServer/java/jre/lib/ext/

   Windows
   C:\Program Files\IBM\WebSphere\AppServer\java\jre\lib\ext\

3. 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 previous versions of Tivoli Federated Identity Manager, the LDAP alias service only created aliases for user accounts that existed in the LDAP server.

In Tivoli Federated Identity Manager Version 6.2.1, the LDAP alias service stores aliases for any user identifier. However, the LDAP attribute used to store the user identifier differs from earlier versions. Consequently, a migration step must be run to preserve any existing aliases from these earlier product versions.

Use the LDAP upgrade tool to complete the migration process. Run from the command line, the tool provides the following capabilities:

- Migrating user aliases to Tivoli Federated Identity Manager Version 6.2.1
- Performing a "reverse migration" to earlier versions
- Migrating directly
- Producing an LDIF file with the required changes

The jar file for the LDAP migration update tool can be found at `FIM_install_directory/tools/ldap/itfim-ldap.jar`.

Use the tool to create an LDIF file, which is manually reviewed and applied to the LDAP server.

Issue the following command:

```
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/fim621-migration.ldif
```

Note: The entry parameters for the LDAP upgrade tool resemble the parameters in the ldapsearch command.

Other parameters are available to pass to this tool:

- `-reverse` performs a reverse migration.
- `-deleteAbandonedEntries` deletes any entries that refer to a DN that no longer exists. This process occurs before the migration step.
- `-Z` enables the SSL connection to the LDAP server.

Migration information for cluster environment

Due to a change in the naming of the Tivoli Federated Identity Manager runtime when deployed into WebSphere clusters, there might be a need to manually update some application information for the runtime.

The Tivoli Federated Identity Manager 6.2.1 installation supports an automated migration feature that detects the presence of a previous version of Tivoli Federated Identity Manager. There is a limitation with the automation feature that occurs when Tivoli Federated Identity Manager has been deployed into a WebSphere cell that supports multiple WebSphere clusters.

In Tivoli Federated Identity Manager 6.1.1, the runtime was deployed to a cluster as application name **ITFIMRuntime-<*clustername*>**. For each cluster in the cell there could be a **ITFIMRuntime-<*clustername*>** application deployed to it.

In Tivoli Federated Identity Manager 6.2.1, 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. This means that there is one **ITFIMRuntime** application for the cell, and the module-to-server mappings specify where it is installed.

When the runtime is deployed for Tivoli Federated Identity Manager Version 6.2.1, the deployment program checks for the existence of an **ITFIMRuntime-<*clustername*>** application. When one is found, the program migrates the application information to the newly deployed **ITFIMRuntime** application. When that step is complete, the program removes the **ITFIMRuntime-<*clustername*>** application.

When there is more than one I**TFIMRuntime-<*clustername*>** application installed, the deployment program migrates only the one for the cluster into which the new **ITFIMRuntime** application has been deployed. The rest of the older runtime applications are deleted. At a later step in the deployment, 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 updating effectively installs the **ITFIMRuntime** into each of the other clusters.

There may be some application information from a **ITFIMRuntime-<*clustername*>** deployment that needs to be manually updated in the **ITFIMRuntime** application for Tivoli Federated Identity Manager Version 6.2.1. For example, when there is more than one cluster in a cell, update the *security role to user/group mappings*.

Appendix B. tfimcfg reference

The tfimcfg command can be used to configure LDAP settings for the Integrated Solutions Console installation, and also to configure WebSEAL as a Point of Contact server.

tfimcfg usage

```
TFIM Autoconfiguration Tool Version 6.1.0 [060316a]

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

   -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

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 the tfimcfg tool is run to configure an LDAP server, the tool also creates several user accounts. The user accounts are needed by the single sign-on demonstration application.

When you run **tfimcfg** to set up the LDAP accounts for the administration console user, you call tfimcfg with the parameters:

```
-action ldapconfig
```

This action creates the demonstration user accounts.

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 is unable to read the keystores generated by the Tivoli Access Manager PDJrteCfg. When this error occurs, you should either use an IBM JVM or else apply the latest JRE patches from Sun. If the problem persists after applying the patches from Sun, use an IBM JVM for the configuration.

tfimcfg LDAP properties reference

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

ldap.hostname
The LDAP server host name. Default: `localhost`

ldap.port
The LDAP port number. Default: `389`

The default value is for non-SSL communication. When you have configured the LDAP server to communicate using SSL, the default port is 636.

ldap.suffix.add
Boolean value that specifies whether tfimcfg adds suffixes to the LDAP server as needed. Supports IBM Tivoli Directory Server Versions 6.1, 6.0 and 5.2 only.

Default:

```
ldap.suffix.add=true
```

ldap.suffix.user.configuration
ldap.organization.configuration
Boolean values that specify whether tfimcfg creates LDAP containers to store Tivoli Federated Identity Manager users and groups. The Tivoli Federated Identity Manager users and groups are:

- Tivoli Federated Identity Manager server users and groups
- Tivoli Federated Identity Manager Installation Verification Tool (IVT) users and groups

When you do not need those users and groups, or you already have LDAP containers that you will use for those users and groups, 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
Boolean value that 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
Boolean value that specifies whether tfimcfg creates the `secAuthority=Default` suffix for Tivoli Access Manager.

- When 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, the tfimcfg program ignores the value of the ldap.suffix.tam.configuration property.

ldap.fim.configuration
Boolean value that specifies whether tfimcfg configures LDAP for the Tivoli Federated Identity Manager alias service.

Default value: `true`.

ldap.ivt.sp.configuration
Boolean value that 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
Boolean value that specifies whether tfimcfg creates users and groups for the identity provider in the Installation Verification Tool (IVT) application.

Default value: `true`.

ldap.modify.acls
Boolean value that specifies whether tfimcfg attaches appropriate ACLs (access control lists) to the LDAP server. These ACLs grant read and write access to the Tivoli Federated Identity Manager administrative users created by tfimcfg.

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

When this is set to `false`, you must attach the ACLs manually.

Default value: `true`.

ldap.admin.dn
The DN used by the LDAP administrator to issue bind requests.

Default: `cn=root`

ldap.admin.password
The password for the LDAP administrator.

Default: `passw0rd`

ldap.security.enabled
Boolean value that specifies whether communication with the LDAP server must use SSL.

Default: `false`.

ldap.security.trusted.jks.filename
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, you can 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
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

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

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

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

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 output from tfimcfg configuration of LDAP

The following figure shows sample output from the running of tfimcfg.

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
```

Here is sample output 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 output from tfimcfg.jar

Modifying the Object Class of Users Created by tfimcfg Utility

The **tfimcfg** utility, when invoked with the argument **-action ldapConfig** creates a set of demonstration users in LDAP. The object classes of these *demo* users are, however, incompatible with WebSphere's default 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` . WebSphere's search parameters for IBM Tivoli Directory Server, however, require that user entries contain objectclass `ePerson`. Due to this mis-match of object class, the demonstration users cannot be located by WebSphere in the user registry.

A workaround for this situation is to modify the object classes of users created by the tfimcfg utility.

To add this object class to the list of object classes:

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 to read:

```
ldap.user.objectclasses=person,ePerson,organizationalPerson,
  inetOrgPerson
```

4. Invoke tfimcfg -action ldapConfig.

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 embeddedWebSphere

If you installed the embedded version of WebSphere Application Server, the federated repository was configured as your user registry. If you want to use a user registry other than the default federated repository, you will need to modify the WebSphere Application Server settings.

About this task

To enable WebSphere to use your user registry:

Procedure

1. Log in to the console. Select **Security → Secure administration, applications, and infrastructure**. The Configuration tab is displayed.
2. Click on **Security Configuration Wizard** to change the user registry used by the WebSphere runtime.
3. The **Specify extent of protection panel** is displayed. Verify that the check box **Enable application security** is selected. Click **Next**.
4. The **Secure the application serving environment** panel is displayed. Select the appropriate option for the user registry you will use:
   - **Federated repositories**
   - **Standalone LDAP registry**
   - **Local operating system**
   - **Standalone custom registry**
5. Click **Next**. The **Configure user repository** panel is displayed. Specify values for each of the registry configuration settings. Refer to the online help for descriptions of the fields presented.
6. Click **Next** and finish the wizard. Save your configuration changes.
7. Stop and then restart the WebSphere Application Server. You must use the same administrative name you used to log in and make these changes.
8. From the console, select **Tivoli Federated Identity Manager → Manage Configuration → Domain properties**.
9. 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.
10. Save the changes.
11. Stop the WebSphere Application Server.
12. Restart the WebSphere Application Server.

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

Find information about removing and then reinstalling the runtime and management services feature.

When you install a Tivoli Federated Identity Manager runtime and management services feature, you use the management console to deploy and configure it. The configure task creates a Tivoli Access Manager identity for the system that hosts the Tivoli Federated Identity Manager runtime and management services feature. This Tivoli Access Manager configuration completes the same set of configuration steps taken by Tivoli Access Manager administrators who use the Tivoli Access Manager commands pdjrte and SvrSslCfg to add applications into a Tivoli Access Manager domain.

When you want to remove the runtime and management services feature, you must first unconfigure and undeploy the existing runtime and management services feature. The unconfiguration task removes the user identity for Tivoli Access Manager, and the undeployment task removes the Tivoli Federated Identity Manager runtime from the list of WebSphere Application Server applications.

It is important to understand that the unconfiguration of the Tivoli Federated Identity Manager runtime and management services feature does not remove the configuration of the Tivoli Access Manager pdjrte feature. This Tivoli Access Manager feature contains the keys and certificates that are used when an application identity (such as the Tivoli Federated Identity Manager runtime and management services feature) contacts the Tivoli Access Manager policy server.

Note: Tivoli Federated Identity Manager cannot remove the pdjrte configuration because it could still be in use by another Tivoli Access Manager application.

When you choose to reinstall the Tivoli Federated Identity Manager runtime and management services feature, you must complete the deployment and configuration steps. When you configure the runtime and management services feature, the configuration inherits the existing Tivoli Access Manager pdjrte feature settings. The pdjrte settings are specific to the keys and certificates used by the Tivoli Access Manager policy server at the time that the pdjrte was itself configured.

- If the Tivoli Access Manager settings have changed since the original pdjrte configuration, the pdjrte must be reconfigured before the Tivoli Federated Identity Manager configuration will result in successful operation.
- If you want to configure Tivoli Federated Identity Manager against a different policy server, you must first reconfigure the Tivoli Access Manager pdjrte to work with the policy server.

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

Reconfiguration of a node when Tivoli Access Manager has been reconfigured.

About this task

Configuration can fail when Tivoli Access Manager has been configured more than one time. Tivoli Access Manager configuration includes creation of a key (certificate) and placement of knowledge of that key in the Tivoli Access Manager policy server. If you have configured Tivoli Access Manager more than once, your certificate will not match the certificate knowledge in the policy server.

Procedure

To clear the Tivoli Access Manager certificate settings, to enable configuration, remove two 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.

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

About this task

When installing as non-root:

- Clean out the /tmp directory. Ensure that files and directories have been removed from the /tmp directory to avoid conflicts during the installation. For example, remove the itfim-wizard-install-optional.log file if it exists in the /tmp directory.
- When installing the Web plug-ins, modify the variables as described in the following procedure. If you do not modify the environment variables, the Web plug-in will not function properly after installation.

Procedure

On the system where you will install the Web plug-in, make the following changes:

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

At a command prompt, 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**. Then right-click in the folder and click **Properties**.
2. Click the **Advanced** tab.
3. Click **Environment variables**.
4. Click **New**.
5. In the **Variable name** field, type a name.
6. In the **Variable value** field, type `C:\Program Files\IBM\FIM\webpi`.
7. Click **OK**.
8. Edit the **PATH** variable using the value `%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

On UNIX or Linux systems, you must perform additional configuration steps in order to run Tivoli Federated Identity Manager as a non-root user.

About this task

Note: These configuration steps are not required on Windows systems.

These instructions assume that you have successfully installed Federated Identity Manager and its prerequisites in the usual manner, as user root. You will now modify the installations to run as a non-root user.

The non-root user is required to administer WebSphere Application Server and Integrated Solutions Console.

Note: When installing the product as a non-root user, ensure that the ID of the user matches the WebSphere Application Server user ID.

These instructions assume the following user and group:

- User: wasadmin
- Group: wasgroup

Note: When WebSphere Application Server Global Security is enabled, the registry used to authenticate 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, so attempts to access the local operating system registry will fail if WebSphere Application Server is running as a non-root user with security enabled.

To run Tivoli Federated Identity Manager as a non-root user, complete the following instructions

Procedure

1. As user root, install the following:
   a. WebSphere Application Server 6.1
   b. Integrated Solutions Console
   c. Tivoli Federated Identity Manager management service and runtime
   d. Tivoli Federated Identity Manager management console
2. Enable the WebSphere Application Server 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. Ensure that all servers and the node agent are stopped. As part of the chmod commands described in the WebSphere documentation, execute the following command for each node that needs 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 machine, execute the following commands to change the permissions of the Tivoli Federated Identity Manager files:

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

Appendix I. Uninstalling

Find information about different options for uninstalling Tivoli Federated Identity Manager.

Before beginning the uninstallation procedures, you will want to be familiar with how the features can be uninstalled and then decide which uninstallation mode you will use.

1. Decide which mode to use: interactive or silent uninstallation.
   - "Interactive uninstallation modes"
   - "Silent uninstallation mode" on page 91
2. Decide which Tivoli Federated Identity Manager components to remove.
3. Follow the instructions in the appropriate section.
   - "Uninstalling (interactive modes)" on page 91
   - "Uninstalling (silent mode)" on page 94

Note: When uninstalling the product, you do not have to uninstall or roll back any fix packs.

Interactive uninstallation modes

Find information about the graphical and console uninstallation modes.

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

Graphical mode

Tivoli Federated Identity Manager provides a graphical user interface uninstallation program. Each uninstallation program presents a series of panels that prompt for the information that is required to complete the task.

Table 21. Commands to start the uninstallation program

Platform	Commands to start the uninstallation program
AIX, Linux, or Solaris	**Runtime and management services** `/opt/IBM/FIM/_uninst/uninstaller.bin` **Management console** `/opt/IBM/FIM/_uninst/uninstaller.bin` **WS-Provisioning runtime** `/opt/IBM/FIM/_uninst/uninstaller.bin` **Web services security management** `/opt/IBM/FIM/_uninst/uninstaller.bin`

Table 21. Commands to start the uninstallation program (continued)

Platform	Commands to start the uninstallation program
Windows	**Runtime and management services** `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe` **Management console** `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe` **WS-Provisioning runtime** `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe` **Web services security management** `C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`

Note: For uninstallation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

Console mode

Tivoli Federated Identity Manager supports an alternate uninstallation mode, for use when uninstalling in a non-graphical environment, such as on a server system that does not have a video card. This mode is called *console mode*.

Console mode uninstallation accomplishes the same tasks and requires the same user input as required by the graphical uninstallation.

You can choose console mode by adding the `-console` command line option when calling the uninstallation launcher.

Table 22. Commands to start the uninstallation program

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

Note: For uninstallation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

Silent uninstallation mode

Find information about using a script for the silent uninstallation mode.

Tivoli Federated Identity Manager supports a *silent mode* uninstallation. In this mode, you are not required to provide any input. Instead, input values are read from a file. This permits the feature to be uninstalled with a common set of options using a script. In order to use silent mode, you must first create a file that contains the input values. This file is called a *response file*.

For information about creating and using response files, see "Uninstalling (silent mode)" on page 94.

Uninstalling (interactive modes)

Learn how to uninstall the Tivoli Federated Identity Manager features at the same time on the same server, or individually on separate servers.

You can uninstall the Tivoli Federated Identity Manager features using graphical mode or console mode.

The following procedures describe the interactive uninstallation modes. For information about silent mode, see "Uninstalling (silent mode)" on page 94.

Preparing to uninstall the runtime and management services feature

Learn what tasks you need to perform before you uninstall the runtime and management services feature.

About this task

You must first unconfigure and undeploy the runtime and management services and the Tivoli Federated Identity Manager domain before you can remove the software.

Procedure

1. Verify that the WebSphere Application Server is running.
2. Verify that Tivoli Access Manager policy server is running.
3. Verify that the LDAP server is running.
4. Unconfigure the Tivoli Federated Identity Manager runtime and management services as follows:
   a. Unconfigure the runtime and management services. This step removes the configuration between the Tivoli Federated Identity Manager runtime and management services and the Tivoli Access Manager security domain.
   b. Undeploy the runtime and management services. This action removes the Tivoli Federated Identity Manager runtime and management services from the WebSphere Application Server list of installed applications.
   c. Delete the domain.

   See the *IBM Tivoli Federated Identity Manager Administration Guide* for directions on unconfiguring and undeploying the runtime, and for deleting the domain.

Results

When these tasks are complete, you are ready to run the uninstallation program. You can run the program interactively or in silent mode:

- To run the program interactively, see "Uninstalling the Tivoli Federated Identity Manager features."
- To run the program in silent mode, see "Uninstalling (silent mode)" on page 94.

Uninstalling the Tivoli Federated Identity Manager features

Learn how to uninstall the runtime and management services, management console, or WS-Provisioning runtime feature using either the graphical mode or console mode.

About this task

To uninstall one or more Tivoli Federated Identity Manager features:

Procedure

1. Start the WebSphere Application Server, if it is not already started.
2. Use a command line to start the uninstallation using either the graphical mode or console mode.

Table 23. Commands to start the uninstallation program in graphical mode

Platform	Uninstallation command
AIX, Linux, or Solaris	`/opt/IBM/FIM/_uninst/uninstaller.bin`
Windows	`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`

Table 24. Commands to start the uninstallation program in console mode

Platform	Command to start the uninstallation program
AIX, Linux, or Solaris	`/opt/IBM/FIM/_uninst/uninstaller.bin -console`
Windows	`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console`

Note: For uninstallation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

3. Select a language. Click **OK**. The Welcome screen is displayed.
4. Click **Next**. The list of installed features is displayed.
5. Select the check box for the features you want to uninstall, and click **Next**.

   The WebSphere Application Server security panel is displayed.
6. 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. Click **Next**.

   Administration security was either enabled or disabled when you installed the WebSphere Application Server prerequisite for this Tivoli Federated Identity Manager installation.
7. If you did not enable WebSphere Application Server security, skip this step. Continue with step 8 on page 93. If you enabled security, the WebSphere security settings panel is displayed.

   You are prompted to supply additional information about the WebSphere Application Server configuration.

a. Enter the requested values.
b. When finished, click **Next**. The WebSphere Application Server information panel is displayed.

8. Specify the **WebSphere Application Server installation directory**. Optionally, click **Browse** to select a directory on the file system. Specify the port number in the **WebSphere Application Server SOAP connector port** field, and click **Next**. The summary screen is displayed.
9. Verify that the information is correct, and click **Next**. The files are removed. This might take a few minutes. A status bar displays the installation progress. When file removal completes, a removal summary panel is displayed.
10. Click **Finish**.

    The Tivoli Federated Identity Manager uninstallation is complete.
11. If you have uninstalled Tivoli Federated Identity Manager from a Windows system, you must restart the system.
12. When you choose to completely remove Tivoli Federated Identity Manager from a computer, you must manually delete the application installation directory. For example:
    - AIX, Linux, or Solaris

      `/opt/IBM/FIM`
    - Windows

      `C:\Program Files\IBM\FIM`

    Attention: Do not delete this directory unless you are removing **all** Tivoli Federated Identity Manager features.

Uninstalling the Web services security management feature

Learn how to uninstall the Web services security management feature using either the graphical mode or console mode.

About this task

To uninstall the Web services security management feature:

Procedure

1. Use a command line to start the uninstallation using either the graphical mode or console mode.

Table 25. Commands to start the uninstallation program in graphical mode

Platform	Uninstallation command
AIX, Linux, or Solaris	`/opt/IBM/FIM/_uninst/uninstaller.bin`
Windows	`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe`

Table 26. Commands to start the uninstallation program in console mode

Platform	Command to start the uninstallation program
AIX, Linux, or Solaris	`/opt/IBM/FIM/_uninst/uninstaller.bin -console`
Windows	`C:\Program Files\IBM\FIM\_uninst\uninstaller.exe -console`

Note: For uninstallation commands for the z/OS platform, see the *Tivoli Federated Identity Manager for z/OS Program Directory.*

2. Select a language. Click **OK**. The Welcome screen is displayed.
3. Click **Next**. The list of installed features is displayed.
4. Select the check box for the Web services security management feature, and click **Next**.

   The WebSphere Application Server security panel is displayed.
5. Verify that the information is correct, and click **Next**. The files are removed. This might take a few minutes. A status bar displays the installation progress. When file removal completes, a removal summary panel is displayed.
6. Click **Finish**. The Web services security management uninstallation is complete.

   Attention: Do not delete the `_uninst_wssm` directory after uninstalling the Web services security management feature. Only after all Tivoli Federated Identity Manager features have been removed can the directory structure be removed.

Uninstalling (silent mode)

Learn how to create and use a response file to uninstall the Tivoli Federated Identity Manager features at the same time on the same server, or individually on separate servers.

Note: Examples of response files are included in the /rsp directory on the Tivoli Federated Identity Manager CD.

The following procedures for the silent uninstallation mode describe creating a response files and using the response files.

Preparing to uninstall the runtime and management services feature

Learn what tasks you need to perform before you uninstall the runtime and management services feature.

About this task

You must first unconfigure and undeploy the runtime and management services and the Tivoli Federated Identity Manager domain before you can remove the software.

Procedure

1. Verify that the WebSphere Application Server is running.
2. Verify that Tivoli Access Manager policy server is running.
3. Verify that the LDAP server is running.
4. Unconfigure the Tivoli Federated Identity Manager runtime and management services as follows:
   a. Unconfigure the runtime and management services. This step removes the configuration between the Tivoli Federated Identity Manager runtime and management services and the Tivoli Access Manager security domain.
   b. Undeploy the runtime and management services. This action removes the Tivoli Federated Identity Manager runtime and management services from the WebSphere Application Server list of installed applications.
   c. Delete the domain.

   See the *IBM Tivoli Federated Identity Manager Administration Guide* for directions on unconfiguring and undeploying the runtime, and for deleting the domain.

Results

When these tasks are complete, you are ready to run the uninstallation program. You can run the program interactively or in silent mode:

- To run the program interactively, see "Uninstalling the Tivoli Federated Identity Manager features" on page 92.
- To run the program in silent mode, see "Uninstalling (silent mode)" on page 94.

Creating a response file for uninstallation

Learn how to create a response file to uninstall the product.

About this task

A response file records the actions to be performed by the uninstallation wizard.

Note: If you want to uninstall individual features, you will need to create a response file for each feature.

To create a response file for uninstalling the features:

Procedure

1. Open a command prompt.
2. Launch the uninstallation wizard for the desired operating system platform, and specify the name of a file to be used to record the options taken.

   Runtime and management services, management console, or WS-Provisioning runtime

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst/uninstaller.bin
     -options-record response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst\uninstaller.exe
     -options-record response_file_filename.rsp
     ```

   Web services security management

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst_wssm/uninstaller.bin
      -options-record response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst_wssm\uninstaller.exe
       -options-record response_file_filename.rsp
     ```

3. Proceed through the program panels, and specify the desired values for the various options.
4. After completing the panels, click **Finish** to create the response file.
5. Open the response file in a text editor.
6. Ensure that the features you want to uninstall are selected. Locate the *feature_name*.active= statement for each feature. `True` indicates that feature will be uninstalled. `False` indicates that it will not be uninstalled.
7. Review the rest of the response file to verify that the remaining values specified are correct. Some response files might contain macros rather than the data that was entered. In these cases, you might need to change these entries.
8. Make the response file available to the people or processes that will use it to uninstall the features.

Uninstalling using a response file

Learn how to use a response file to uninstall the product.

About this task

After a response file has been created, you can use the response file with the uninstallation wizard to uninstall the feature in a predetermined manner.

To uninstall the feature using a response file from the command line:

Procedure

1. Open a command prompt.
2. Launch the uninstallation wizard for the desired operating system platform specifying the response file that has been created.

   Runtime and management services

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst/uninstaller.bin
      -silent -options response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst\uninstaller.exe
       -silent -options response_file_filename.rsp
     ```

   Management console

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst/uninstaller.bin
      -silent -options response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst\uninstaller.exe
       -silent -options response_file_filename.rsp
     ```

   WS-Provisioning runtime

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst/uninstaller.bin -silent
      -silent -options response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst\uninstaller.exe
       -silent -options response_file_filename.rsp
     ```

   Web services security management

   - AIX, Linux, or Solaris

     ```
     /opt/IBM/FIM/_uninst/uninstaller.bin
      -silent -options response_file_filename.rsp
     ```

   - Windows

     ```
     C:\Program Files\IBM\FIM\_uninst\uninstaller.exe
       -silent -options response_file_filename.rsp
     ```

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

What to do next

Alternately, the wizard can be launched from a script or batch file as part of an automated process.

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 grant 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
3-3-12, Roppongi, Minato-ku, Tokyo 106-8711 Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law:
INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement may not apply to you.

This information could include technical inaccuracies or typographical errors. Changes are periodically made to the information herein; these changes will be incorporated in new editions of the 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 information 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 measurements 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 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.

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 http://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.

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.

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

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

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

Glossary

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.

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 that a self-posting form be used to establish and use a trusted session between two partners in a federation. Contrast with *browser artifact*.

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), which 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.

metadata
Data that describes a particular piece of information, such as settings for a configuration.

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.

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.

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 invoke services across the Internet.

SOAP back channel
Communications that take place directly between two SOAP endpoints.

SPNEGO
Simple and Protected GSS API Negotiation Mechanism

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, SOAP is used to transfer the data, 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

GC27-2718-00