Information Management Software InfoSphere™ IBM

IBM® InfoSphere Information Server

IBM InfoSphere Information Server Single Sign-On (SSO) by using SAML 2.0 and Tivoli Federated Identity Manager (TFIM)

Installation and Configuration Guide

© **Copyright International Business Machines Corporation 2016, 2020. All rights reserved.**
US Government Users Restricted Rights -- Use, duplication or disclosure restricted by GSA ADP Schedule Contract with IBM Corp.

Table of Contents

About this publication

IBM InfoSphere Information Server Version 11.5 implements solutions for federated single sign-on for its web applications. This guide describes how to install and configure IBM InfoSphere Information Server with SAML 2.0 and Tivoli Federated Identity Manager (TFIM).

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 includes experience with deploying applications into an IBM® WebSphere® Application Server environment.

Publications and Prerequisites

Refer to the instructions for accessing publications online. 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:

- **InfoSphere Information Server version 11.5:** http://www.ibm.com/support/knowledgecenter/SSZJPZ_11.5.0/com.ibm.swg.im.iis.productization.iisinfsv.home.doc/topics/kc_homepage_IS.html

- **To enable your system to use the SAML web single sign-on (SSO) feature:** http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

- **TFIM software prerequisites:** http://www.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.6/com.ibm.tivoli.fim.doc_6226/ic/ic-homepage.html

Additional documentation can be found in the Useful Links section in this document.

Chapter 1: Planning the installation

In order to enable single sign on functionality to the web applications of IBM InfoSphere Information Server you will need to install and configure:

- Tivoli Federated Identity Manager (TFIM)
- Configuration of the SAML TAI, in the **WAS ND** installation of IBM InfoSphere Information Server.
  Note that **WebSphere Liberty (LWAS)** is not supported and cannot be used for this configuration.
- Establishing the Trust Relationships between TFIM and WebSphere
- Install IBM InfoSphere Information Server version 11.5.0.1 or higher. Other patches may be required. Check Chapter 4: InfoSphere Information Server Configuration - Requirements for details
- LDAP Configuration

Chapter 2: Installing TFIM

Planning the installation

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 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.

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.

Installation: 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.

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.

For more information on the software prerequisites, see http://www.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.6/com.ibm.tivoli.fim.doc_6226/ic/ic-homepage.html

Installation modes

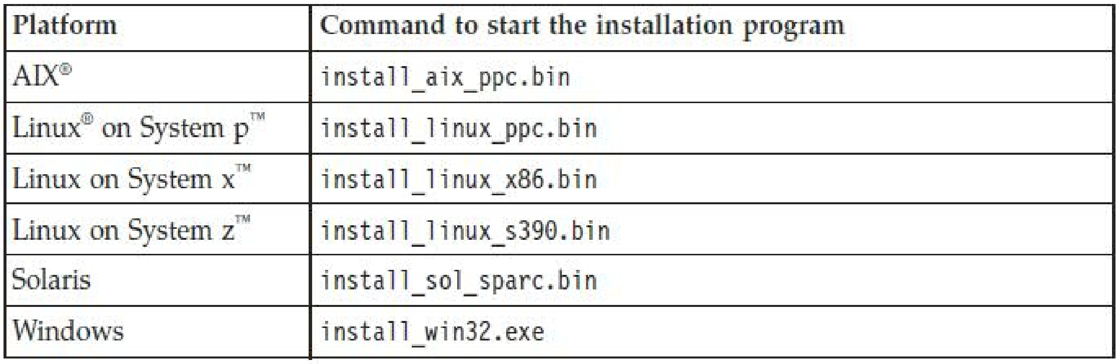
Tivoli Federated Identity Manager supports two interactive modes and one silent mode for installing each feature. The interactive modes consist of a graphical mode and a console (text-based) mode.

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 more information about creating and using response files, see http://www.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.6/com.ibm.tivoli.fim.doc_6226/ic/ic-homepage.html

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.
Commands to start the installation program in graphical mode



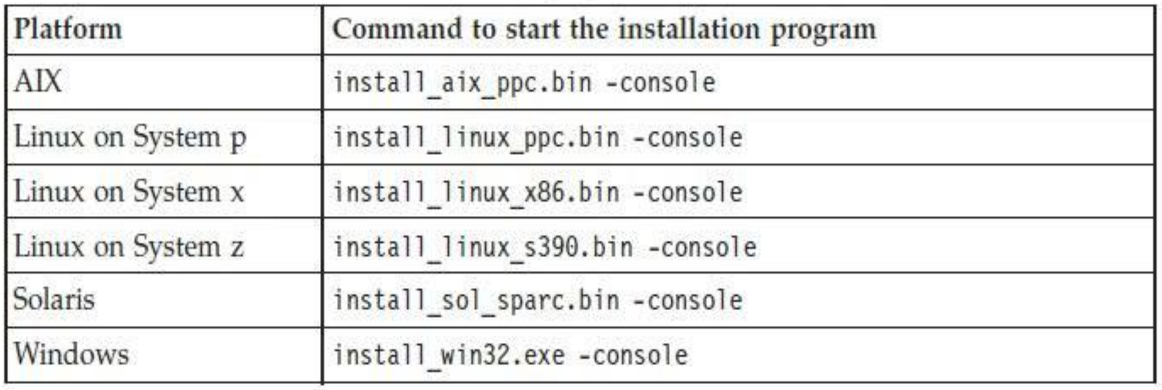
Platform	Command to start the installation program
AIX®	install_aix_ppc.bin
Linux® on System p™	install_linux_ppc.bin
Linux on System x™	install_linux_x86.bin
Linux on System z™	install_linux_s390.bin
Solaris	install_sol_sparc.bin
Windows	install_win32.exe

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.

Commands to start the installation program in 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

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 v 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 http://www.ibm.com/support/knowledgecenter/SSZSXU_6.2.2.6/com.ibm.tivoli.fim.doc_6226/ic/ic-homepage.html

WebSphere Application Server

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

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.

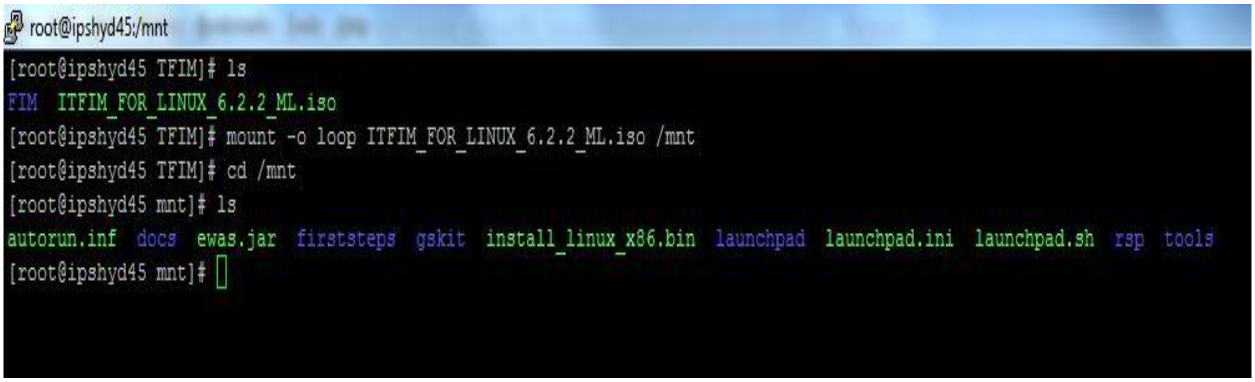
Within Tivoli Federated Identity Manager deployments, embedded WebSphere Application Server can be useful to support the Tivoli Federated Identity Manager management console component, when the management console is deployed on a separate computer that does already have WebSphere Application Server.

Installing WebSphere Application Server

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

To install the federated single sign-on feature:

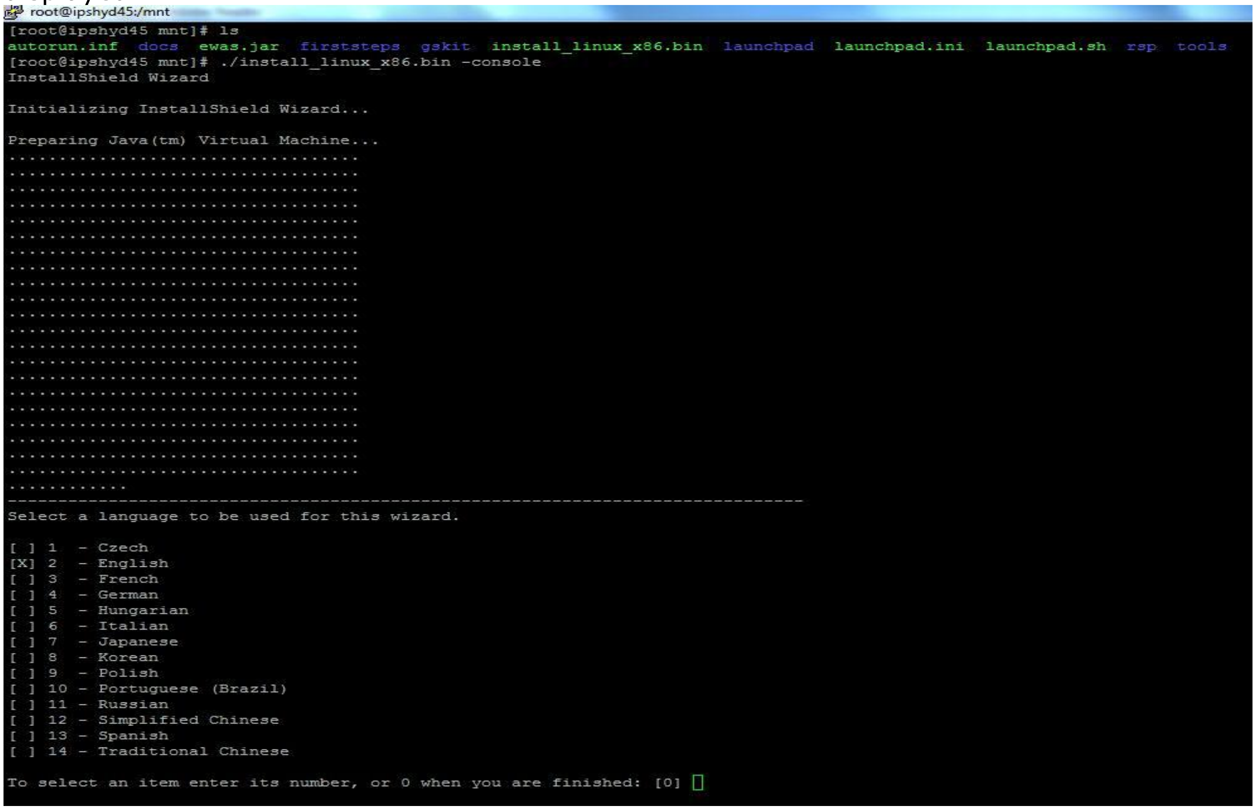
1. Insert the CD into or download the image onto the machine on which you will install the feature.



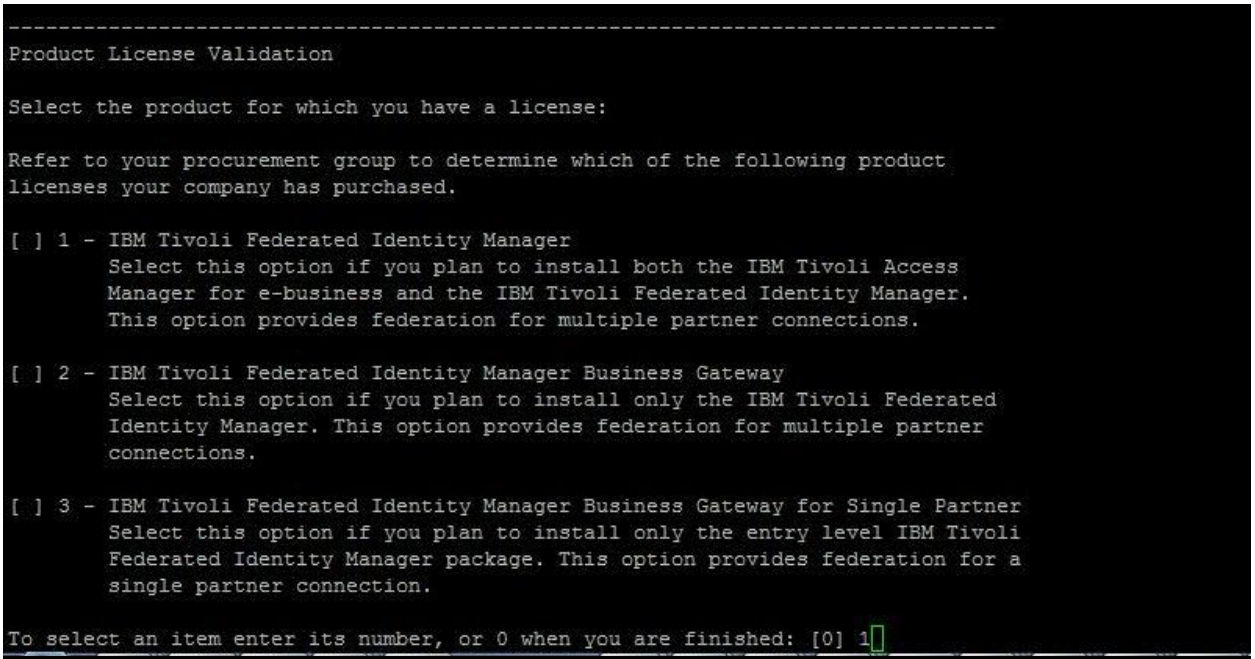
```
root@ipshyd45:/mnt
[root@ipshyd45 TFIM]# ls
FIM  ITFIM_FOR_LINUX_6.2.2_ML.iso
[root@ipshyd45 TFIM]# mount -o loop ITFIM_FOR_LINUX_6.2.2_ML.iso /mnt
[root@ipshyd45 TFIM]# cd /mnt
[root@ipshyd45 mnt]# ls
autorun.inf  docs  ewas.jar  firststeps  gskit  install_linux_x86.bin  launchpad  launchpad.ini  launchpad.sh  rsp  tools
[root@ipshyd45 mnt]# 
```

2. Use a command line to start the installation using either the graphical mode or console mode. For example, to start the installation in console mode use
   ./install_linux_x86.bin –console

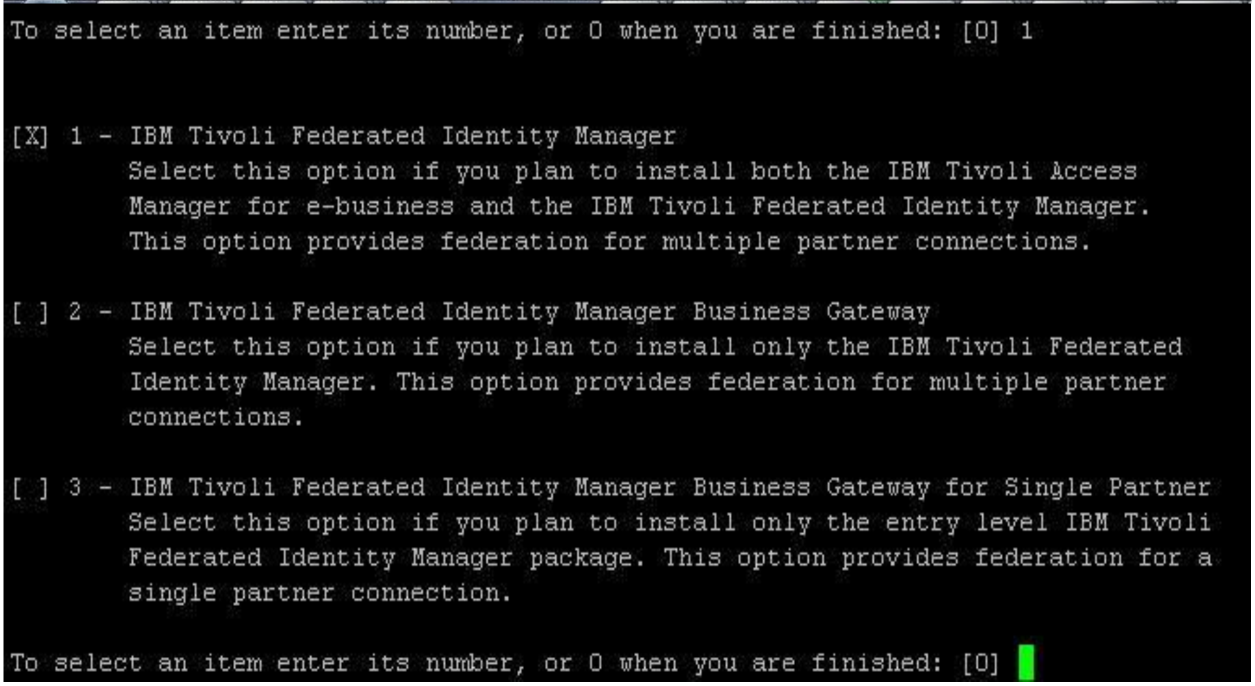
3. Select a language, and click OK. The software license agreement is displayed.



```
root@ipshyd45:/mnt
[root@ipshyd45 mnt]# ls
autorun.inf  docs  ewas.jar  firststeps  gskit  install_linux_x86.bin  launchpad  launchpad.ini  launchpad.sh  rsp  tools
[root@ipshyd45 mnt]# ./install_linux_x86.bin -console
InstallShield Wizard

Initializing InstallShield Wizard...

Preparing Java(tm) Virtual Machine...
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
....................................
............
-------------------------------------------------------------------------------
Select a language to be used for this wizard.

[ ] 1  - Czech
[X] 2  - English
[ ] 3  - French
[ ] 4  - German
[ ] 5  - Hungarian
[ ] 6  - Italian
[ ] 7  - Japanese
[ ] 8  - Korean
[ ] 9  - Polish
[ ] 10 - Portuguese (Brazil)
[ ] 11 - Russian
[ ] 12 - Simplified Chinese
[ ] 13 - Spanish
[ ] 14 - Traditional Chinese

To select an item enter its number, or 0 when you are finished: [0] 
```

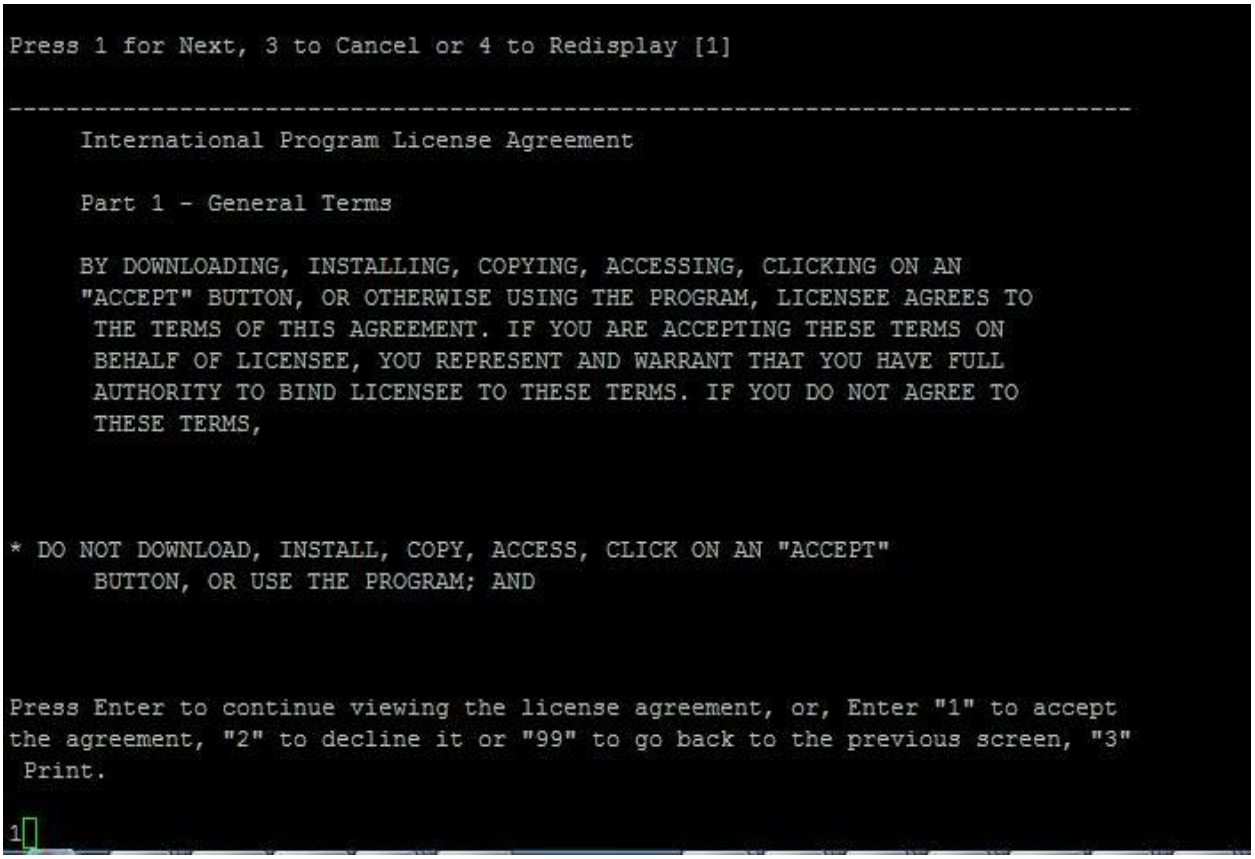


```
-------------------------------------------------------------------------------
Product License Validation

Select the product for which you have a license:

Refer to your procurement group to determine which of the following product
licenses your company has purchased.

[ ] 1 - IBM Tivoli Federated Identity Manager
        Select this option if you plan to install both the IBM Tivoli Access
        Manager for e-business and the IBM Tivoli Federated Identity Manager.
        This option provides federation for multiple partner connections.

[ ] 2 - IBM Tivoli Federated Identity Manager Business Gateway
        Select this option if you plan to install only the IBM Tivoli Federated
        Identity Manager. This option provides federation for multiple partner
        connections.

[ ] 3 - IBM Tivoli Federated Identity Manager Business Gateway for Single Partner
        Select this option if you plan to install only the entry level IBM Tivoli
        Federated Identity Manager package. This option provides federation for a
        single partner connection.

To select an item enter its number, or 0 when you are finished: [0] 1
```



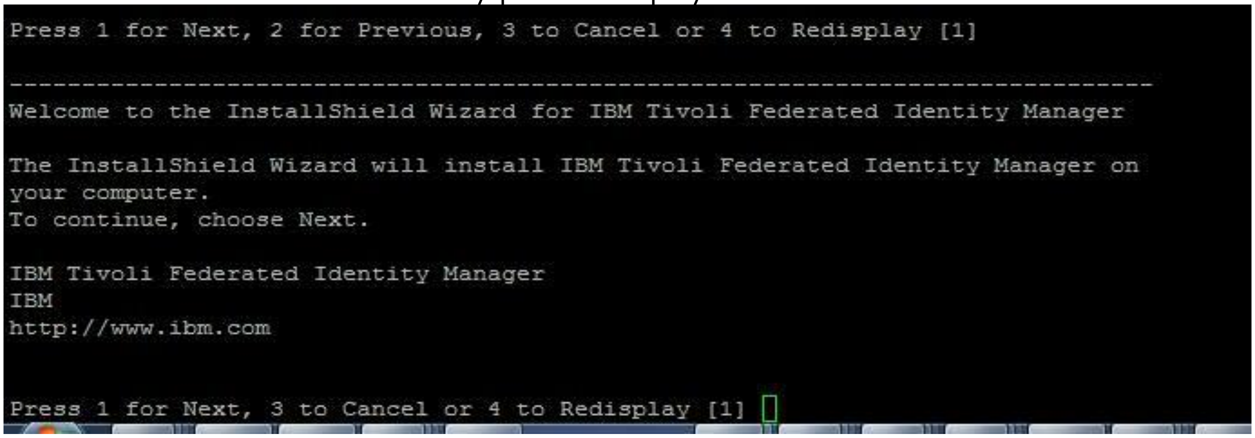
```
To select an item enter its number, or 0 when you are finished: [0] 1


[X] 1 - IBM Tivoli Federated Identity Manager
        Select this option if you plan to install both the IBM Tivoli Access
        Manager for e-business and the IBM Tivoli Federated Identity Manager.
        This option provides federation for multiple partner connections.

[ ] 2 - IBM Tivoli Federated Identity Manager Business Gateway
        Select this option if you plan to install only the IBM Tivoli Federated
        Identity Manager. This option provides federation for multiple partner
        connections.

[ ] 3 - IBM Tivoli Federated Identity Manager Business Gateway for Single Partner
        Select this option if you plan to install only the entry level IBM Tivoli
        Federated Identity Manager package. This option provides federation for a
        single partner connection.

To select an item enter its number, or 0 when you are finished: [0]
```

4. If you agree to the license terms, accept the license, and click Next. The Welcome screen is displayed.



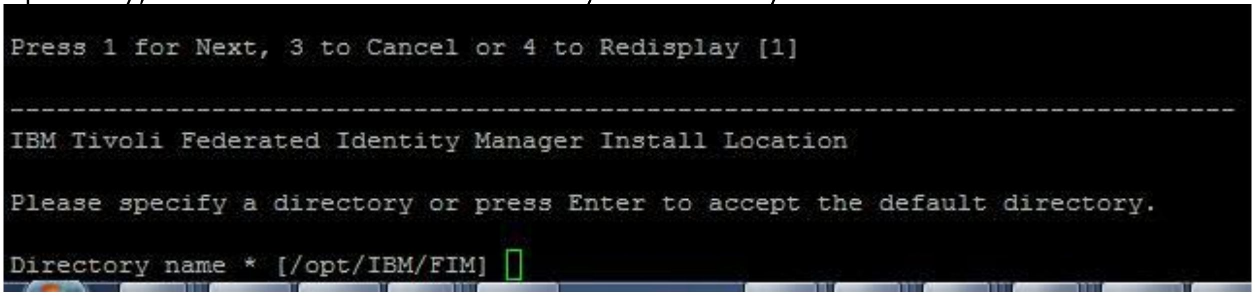
```
Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]

-------------------------------------------------------------------------------
     International Program License Agreement

     Part 1 - General Terms

     BY DOWNLOADING, INSTALLING, COPYING, ACCESSING, CLICKING ON AN
     "ACCEPT" BUTTON, OR OTHERWISE USING THE PROGRAM, LICENSEE AGREES TO
      THE TERMS OF THIS AGREEMENT. IF YOU ARE ACCEPTING THESE TERMS ON
      BEHALF OF LICENSEE, YOU REPRESENT AND WARRANT THAT YOU HAVE FULL
      AUTHORITY TO BIND LICENSEE TO THESE TERMS. IF YOU DO NOT AGREE TO
      THESE TERMS,



* DO NOT DOWNLOAD, INSTALL, COPY, ACCESS, CLICK ON AN "ACCEPT"
      BUTTON, OR USE THE PROGRAM; AND



Press Enter to continue viewing the license agreement, or, Enter "1" to accept
the agreement, "2" to decline it or "99" to go back to the previous screen, "3"
 Print.

1
```

5. Click Next. The installation directory panel is displayed.



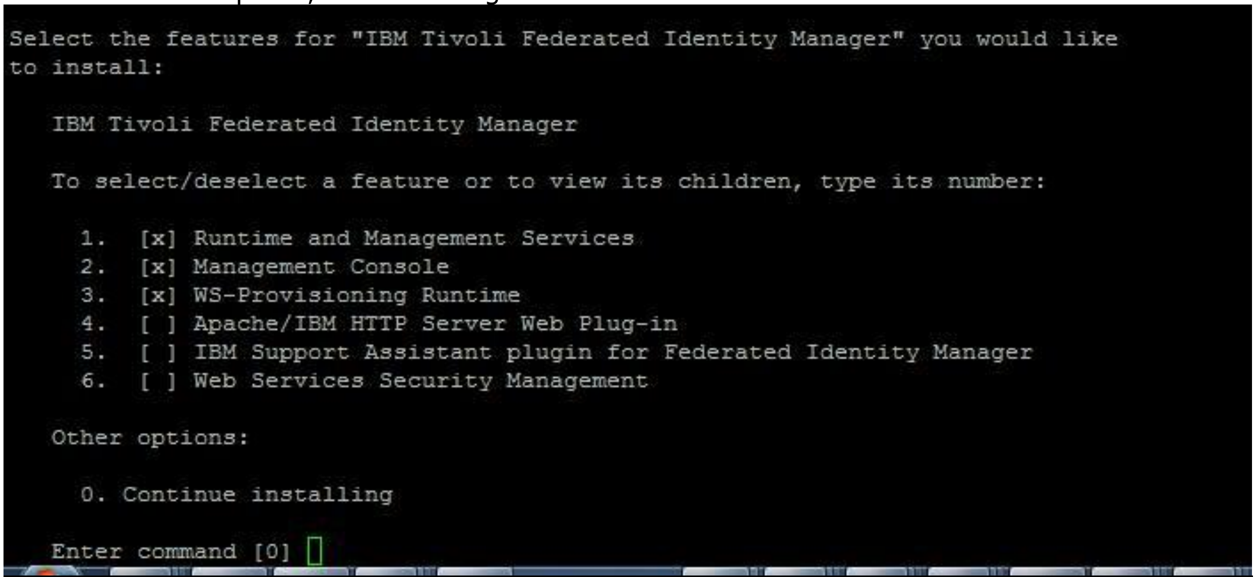
```
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

-------------------------------------------------------------------------------
Welcome to the InstallShield Wizard for IBM Tivoli Federated Identity Manager

The InstallShield Wizard will install IBM Tivoli Federated Identity Manager on
your computer.
To continue, choose Next.

IBM Tivoli Federated Identity Manager
IBM
http://www.ibm.com


Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]
```

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.

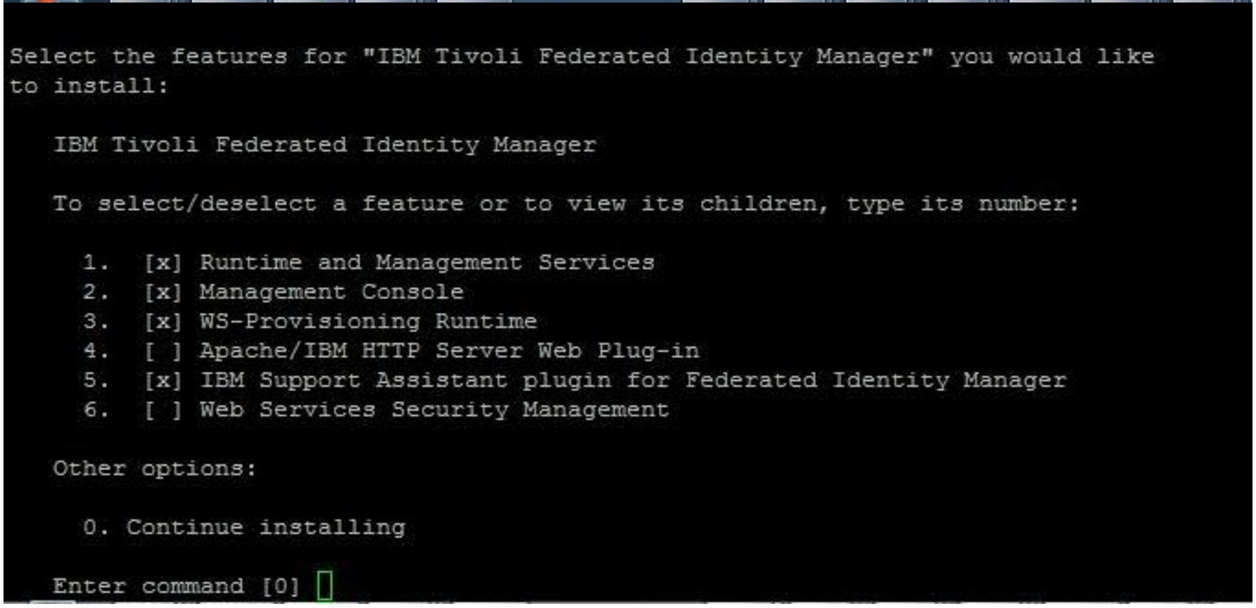


```
Press 1 for Next, 3 to Cancel or 4 to Redisplay [1]

-------------------------------------------------------------------------------
IBM Tivoli Federated Identity Manager Install Location

Please specify a directory or press Enter to accept the default directory.

Directory name * [/opt/IBM/FIM]
```

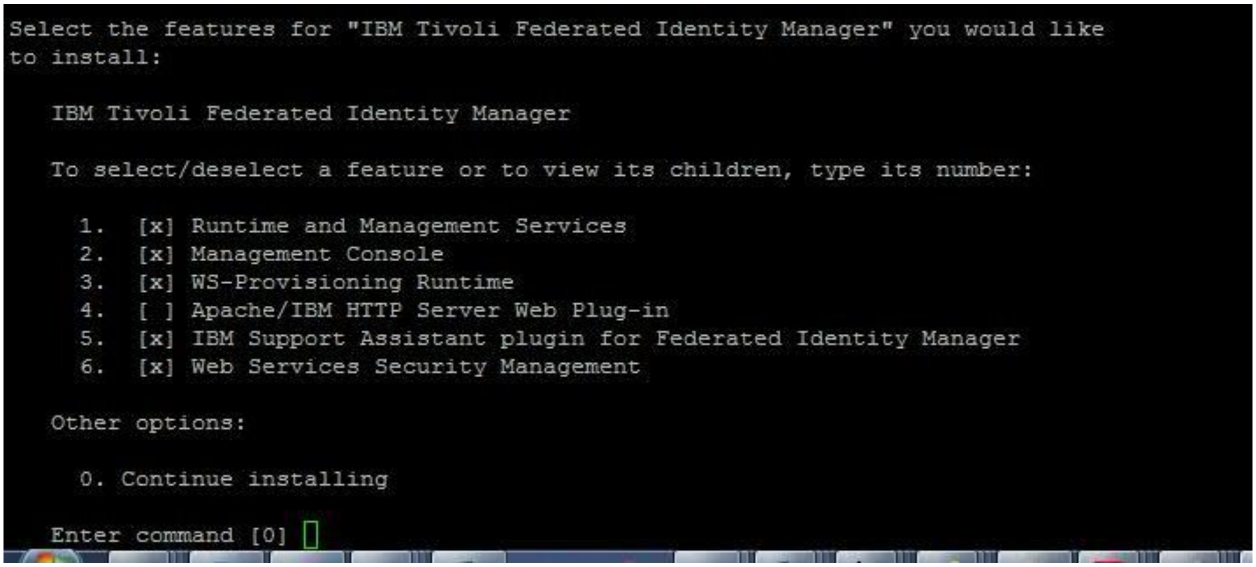
7. Select Runtime and Management Services. When you are installing the management console on the same computer, select Management console also. Click Next.



```
Select the features for "IBM Tivoli Federated Identity Manager" you would like
to install:

   IBM Tivoli Federated Identity Manager

   To select/deselect a feature or to view its children, type its number:

     1.  [x] Runtime and Management Services
     2.  [x] Management Console
     3.  [x] WS-Provisioning Runtime
     4.  [ ] Apache/IBM HTTP Server Web Plug-in
     5.  [ ] IBM Support Assistant plugin for Federated Identity Manager
     6.  [ ] Web Services Security Management

   Other options:

     0. Continue installing

   Enter command [0]
```

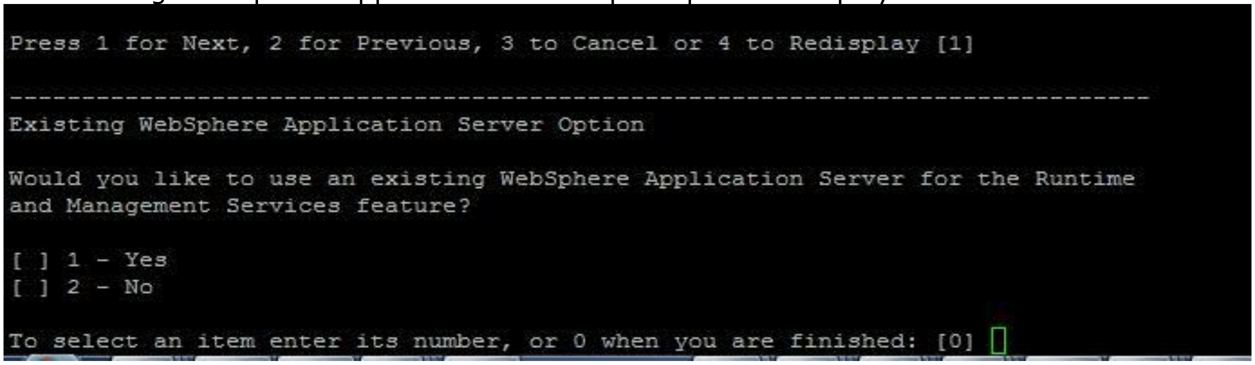


```
Select the features for "IBM Tivoli Federated Identity Manager" you would like
to install:

   IBM Tivoli Federated Identity Manager

   To select/deselect a feature or to view its children, type its number:

     1.  [x] Runtime and Management Services
     2.  [x] Management Console
     3.  [x] WS-Provisioning Runtime
     4.  [ ] Apache/IBM HTTP Server Web Plug-in
     5.  [x] IBM Support Assistant plugin for Federated Identity Manager
     6.  [ ] Web Services Security Management

   Other options:

     0. Continue installing

   Enter command [0]
```



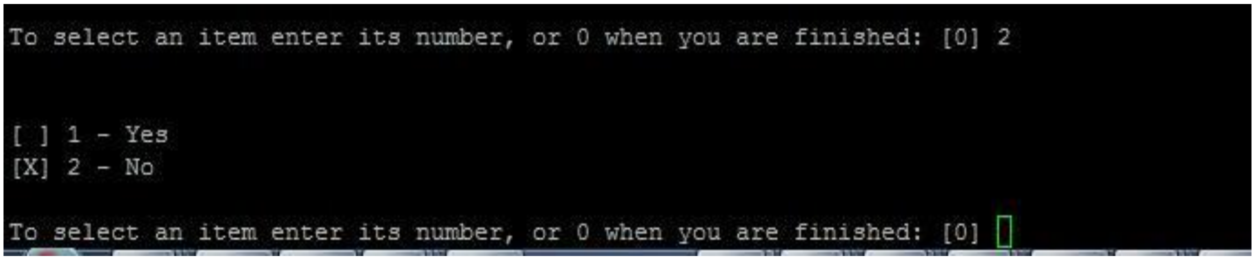
```
Select the features for "IBM Tivoli Federated Identity Manager" you would like
to install:

   IBM Tivoli Federated Identity Manager

   To select/deselect a feature or to view its children, type its number:

     1.  [x] Runtime and Management Services
     2.  [x] Management Console
     3.  [x] WS-Provisioning Runtime
     4.  [ ] Apache/IBM HTTP Server Web Plug-in
     5.  [x] IBM Support Assistant plugin for Federated Identity Manager
     6.  [x] Web Services Security Management

   Other options:

     0. Continue installing

   Enter command [0]
```

The Existing WebSphere Application Server option panel is displayed.

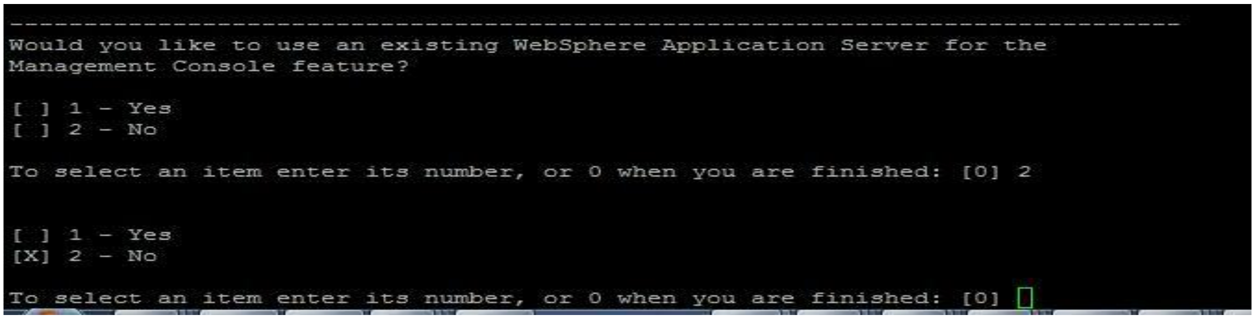


```
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

-------------------------------------------------------------------------------
Existing WebSphere Application Server Option

Would you like to use an existing WebSphere Application Server for the Runtime
and Management Services feature?

[ ] 1 - Yes
[ ] 2 - No

To select an item enter its number, or 0 when you are finished: [0]
```

8. Select 2-No to indicate that you want to install the embedded WebSphere Application Server, and click Next.



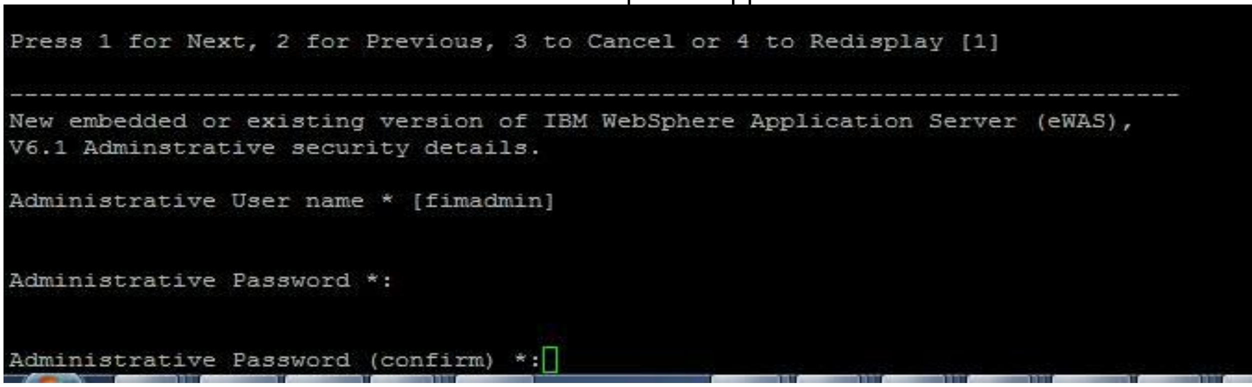
```
To select an item enter its number, or 0 when you are finished: [0] 2


[ ] 1 - Yes
[X] 2 - No

To select an item enter its number, or 0 when you are finished: [0]
```



```
-------------------------------------------------------------------------------
Would you like to use an existing WebSphere Application Server for the
Management Console feature?

[ ] 1 - Yes
[ ] 2 - No

To select an item enter its number, or 0 when you are finished: [0] 2


[ ] 1 - Yes
[X] 2 - No

To select an item enter its number, or 0 when you are finished: [0]
```

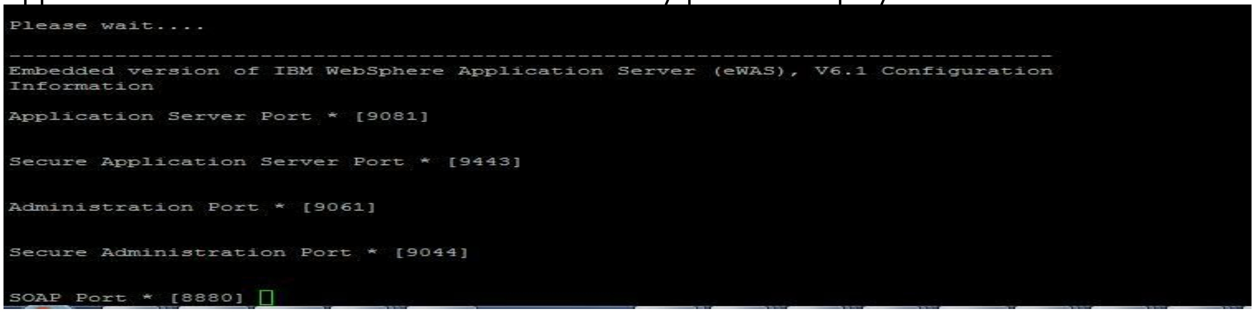
9. Enter the requested information:

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.



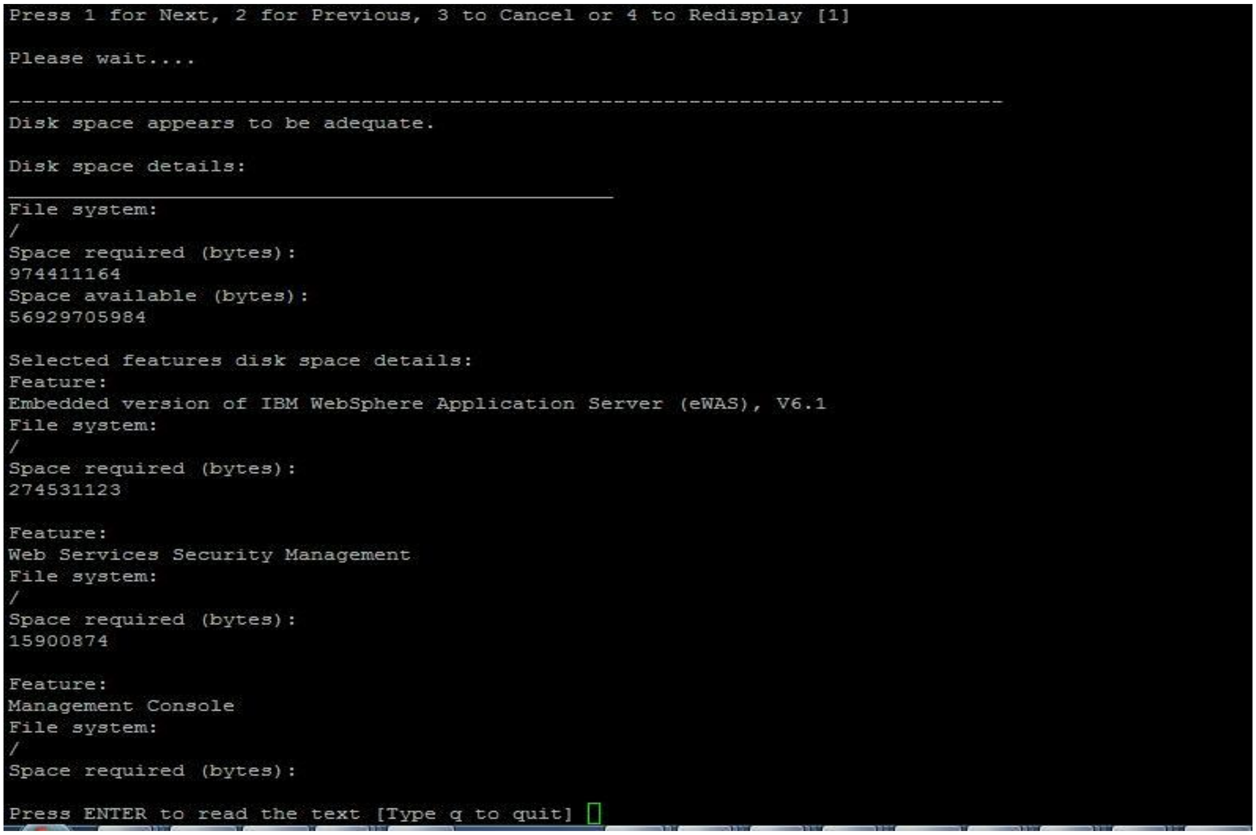
```
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

-------------------------------------------------------------------------------
New embedded or existing version of IBM WebSphere Application Server (eWAS),
V6.1 Adminstrative security details.

Administrative User name * [fimadmin]


Administrative Password *:


Administrative Password (confirm) *:
```

b. Enter the port information that will be used with this installation of WebSphere Application Server. Click Next. The Disk Summary panel is displayed.

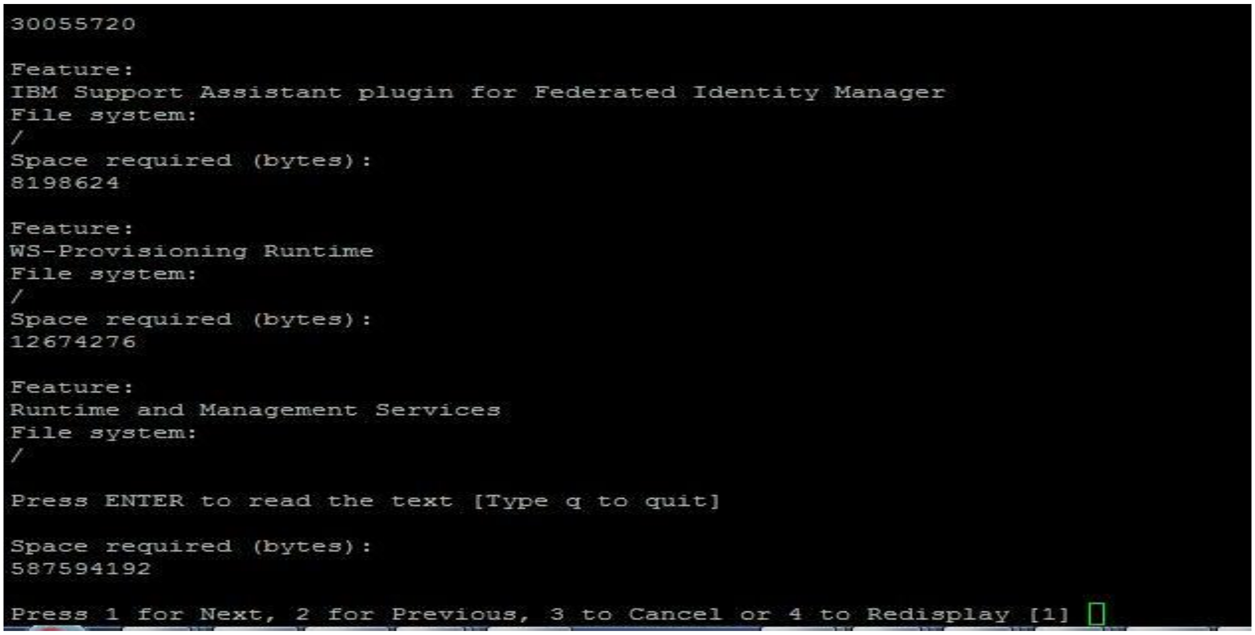


```
Please wait....

-------------------------------------------------------------------------------
Embedded version of IBM WebSphere Application Server (eWAS), V6.1 Configuration
Information

Application Server Port * [9081]

Secure Application Server Port * [9443]

Administration Port * [9061]

Secure Administration Port * [9044]

SOAP Port * [8880]
```

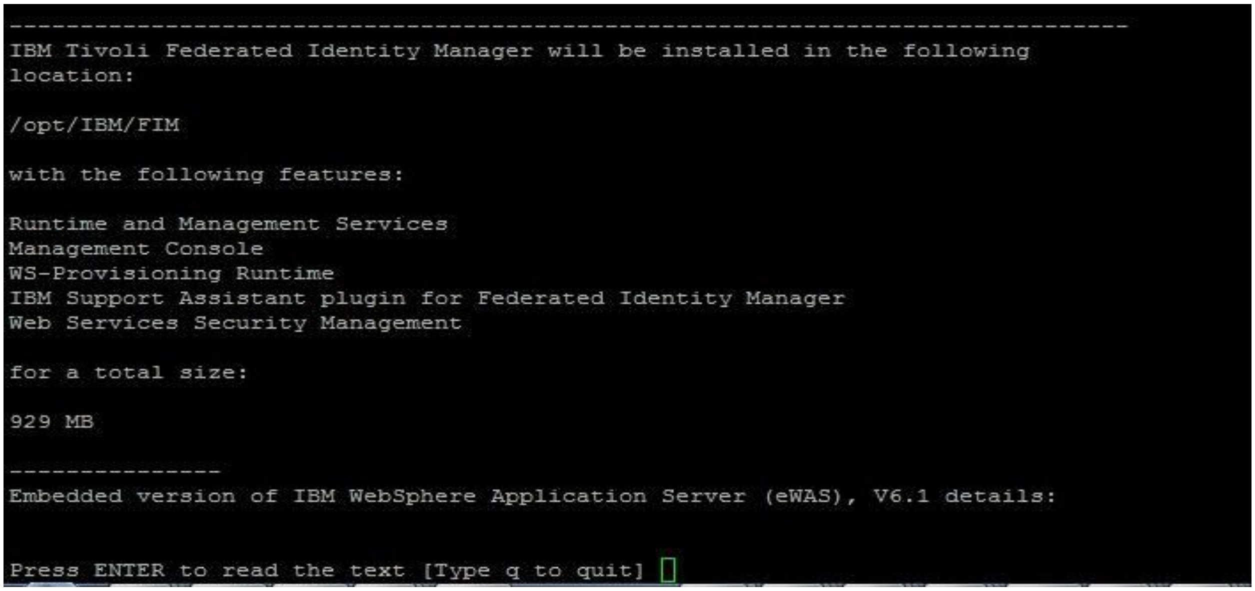
10. Verify that adequate free space is available, and click Next. The installation summary screen is displayed.



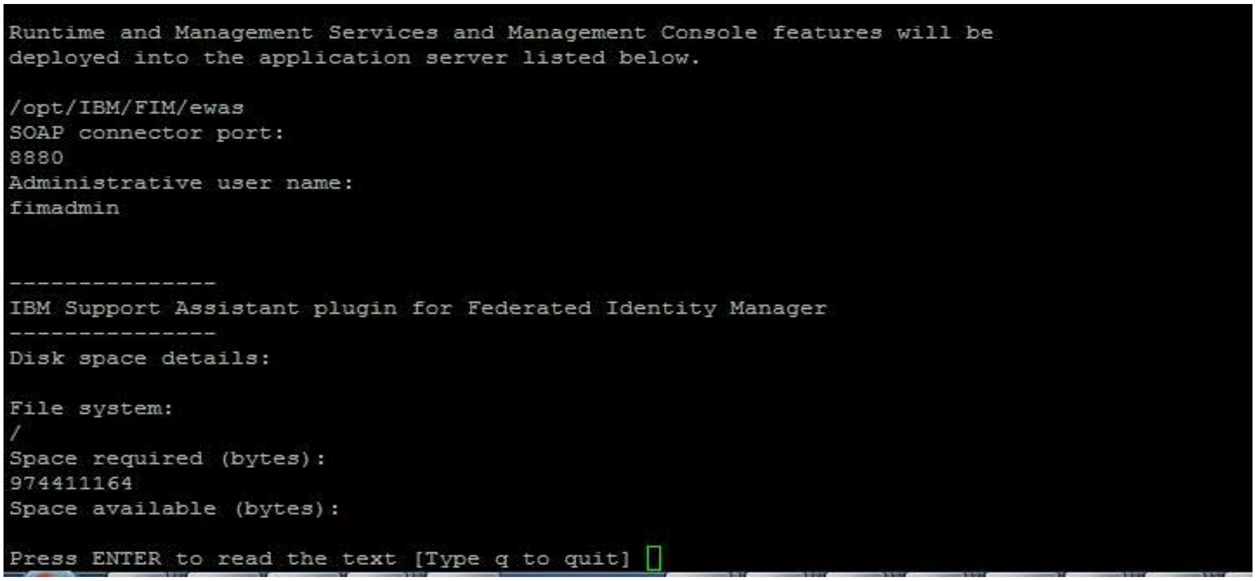
```
Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]

Please wait....

-------------------------------------------------------------------------------
Disk space appears to be adequate.

Disk space details:
________________________________________________
File system:
/
Space required (bytes):
974411164
Space available (bytes):
56929705984

Selected features disk space details:
Feature:
Embedded version of IBM WebSphere Application Server (eWAS), V6.1
File system:
/
Space required (bytes):
274531123

Feature:
Web Services Security Management
File system:
/
Space required (bytes):
15900874

Feature:
Management Console
File system:
/
Space required (bytes):

Press ENTER to read the text [Type q to quit]
```



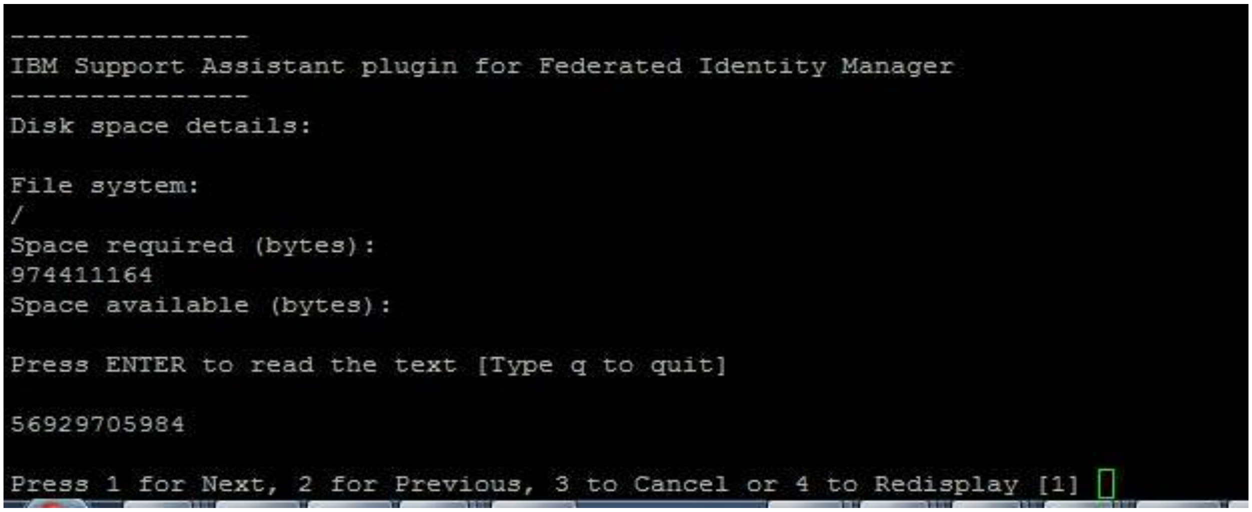
```
30055720

Feature:
IBM Support Assistant plugin for Federated Identity Manager
File system:
/
Space required (bytes):
8198624

Feature:
WS-Provisioning Runtime
File system:
/
Space required (bytes):
12674276

Feature:
Runtime and Management Services
File system:
/

Press ENTER to read the text [Type q to quit]

Space required (bytes):
587594192

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```



```
-----------------------------------------------------------------------------
IBM Tivoli Federated Identity Manager will be installed in the following
location:

/opt/IBM/FIM

with the following features:

Runtime and Management Services
Management Console
WS-Provisioning Runtime
IBM Support Assistant plugin for Federated Identity Manager
Web Services Security Management

for a total size:

929 MB

---------------
Embedded version of IBM WebSphere Application Server (eWAS), V6.1 details:


Press ENTER to read the text [Type q to quit]
```

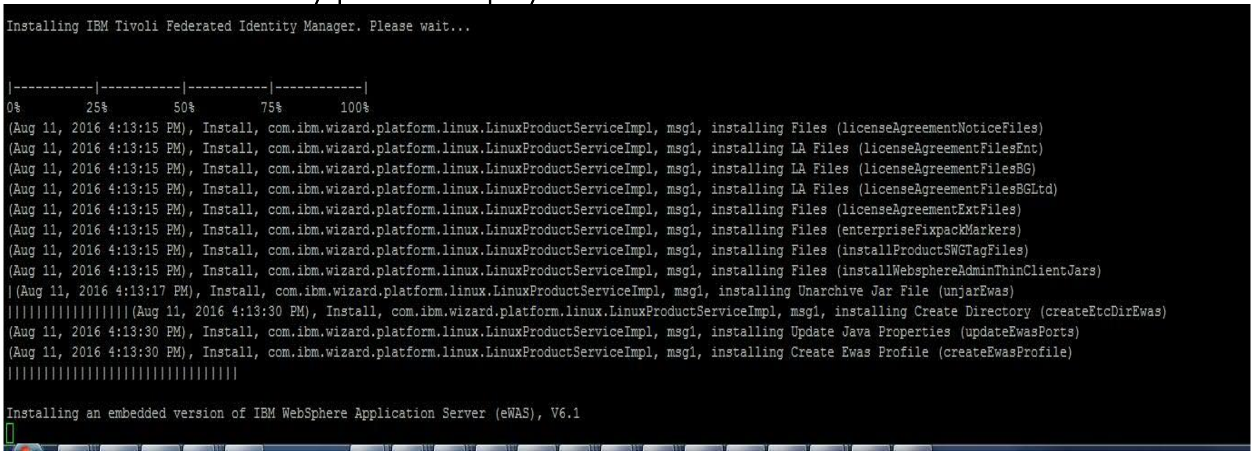


```
Runtime and Management Services and Management Console features will be
deployed into the application server listed below.

/opt/IBM/FIM/ewas
SOAP connector port:
8880
Administrative user name:
fimadmin


---------------
IBM Support Assistant plugin for Federated Identity Manager
---------------
Disk space details:

File system:
/
Space required (bytes):
974411164
Space available (bytes):

Press ENTER to read the text [Type q to quit]
```

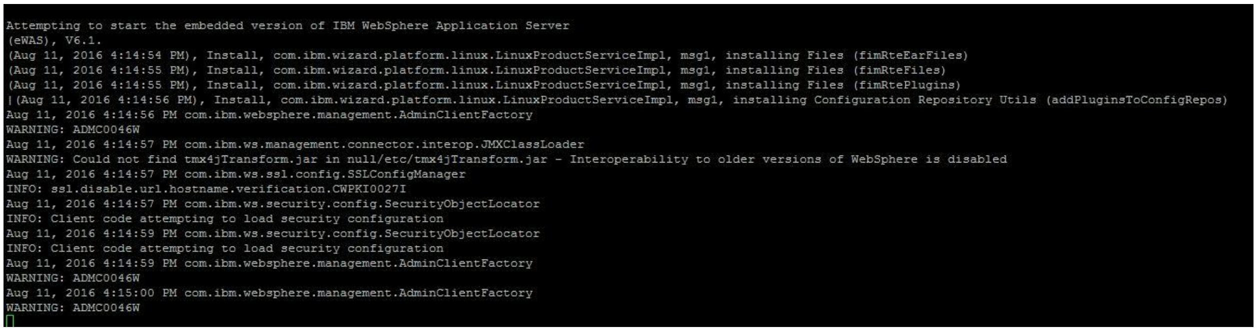


```
---------------
IBM Support Assistant plugin for Federated Identity Manager
---------------
Disk space details:

File system:
/
Space required (bytes):
974411164
Space available (bytes):

Press ENTER to read the text [Type q to quit]

56929705984

Press 1 for Next, 2 for Previous, 3 to Cancel or 4 to Redisplay [1]
```

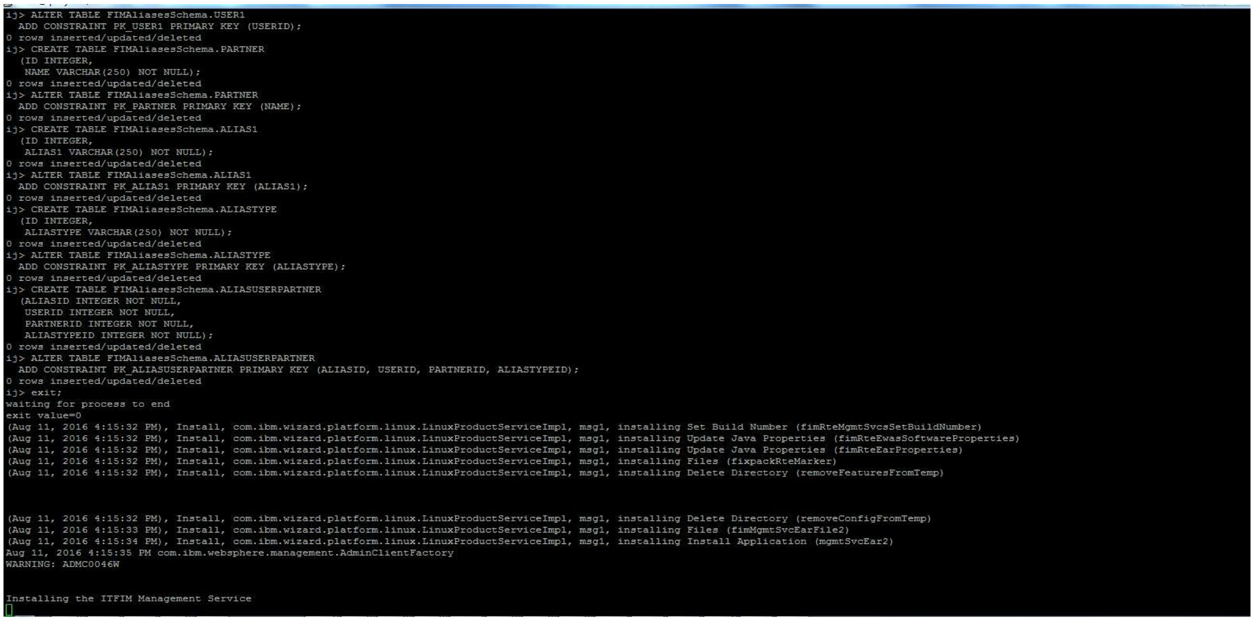
11. Verify that the information is correct, and click Next. The files are installed. This might take a few minutes. A status bar displays the installation progress. When file installation completes, an installation summary panel is displayed.



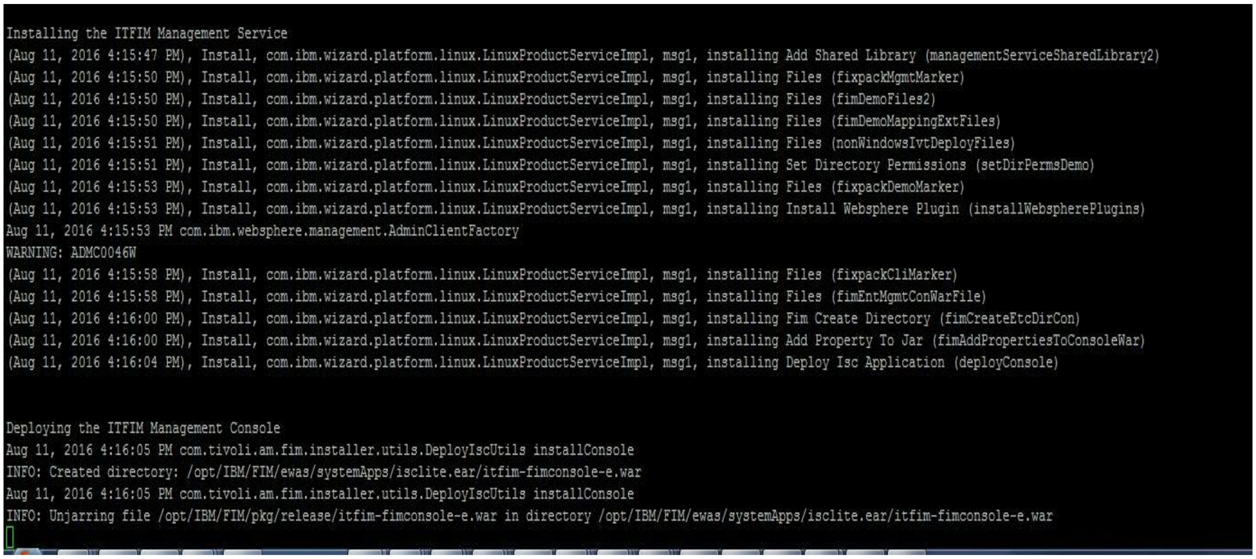
```
Installing IBM Tivoli Federated Identity Manager. Please wait...


|-----------|-----------|-----------|------------|
0%         25%         50%         75%        100%
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (licenseAgreementNoticeFiles)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing LA Files (licenseAgreementFilesEnt)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing LA Files (licenseAgreementFilesBG)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing LA Files (licenseAgreementFilesBGLtd)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (licenseAgreementExtFiles)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (enterpriseFixpackMarkers)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (installProductSWGTagFiles)
(Aug 11, 2016 4:13:15 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (installWebsphereAdminThinClientJars)
|(Aug 11, 2016 4:13:17 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Unarchive Jar File (unjarEwas)
||||||||||||||||(Aug 11, 2016 4:13:30 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Create Directory (createEtcDirEwas)
(Aug 11, 2016 4:13:30 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Update Java Properties (updateEwasPorts)
(Aug 11, 2016 4:13:30 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Create Ewas Profile (createEwasProfile)
|||||||||||||||||||||||||||||||||

Installing an embedded version of IBM WebSphere Application Server (eWAS), V6.1
```



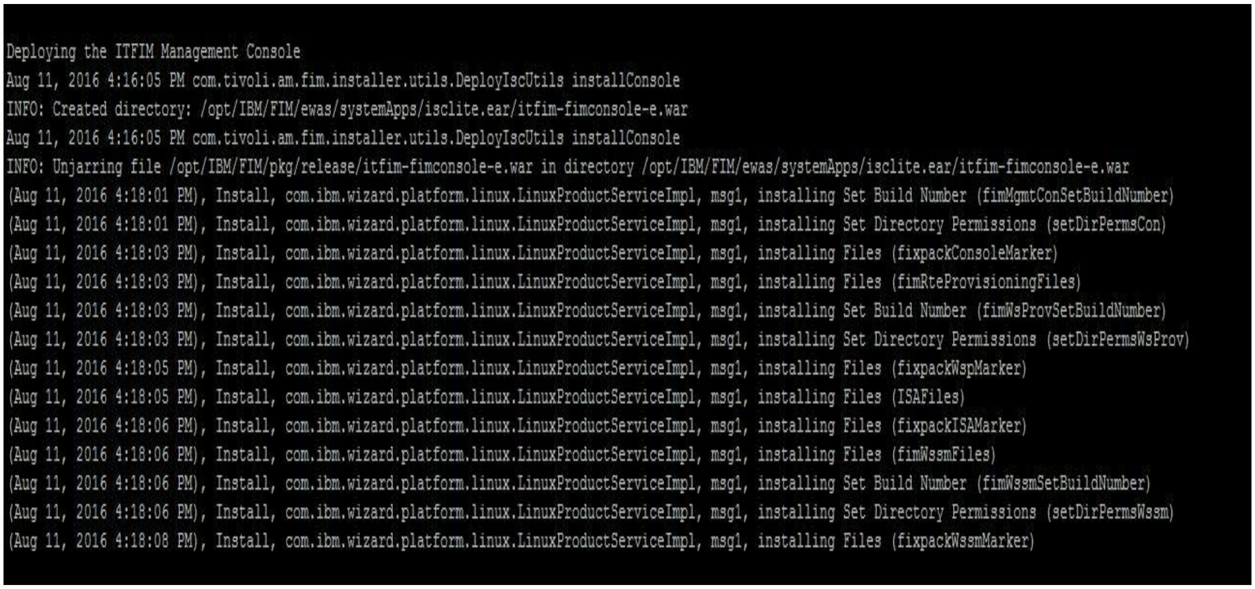
```
Attempting to start the embedded version of IBM WebSphere Application Server
(eWAS), V6.1.
(Aug 11, 2016 4:14:54 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimRteEarFiles)
(Aug 11, 2016 4:14:55 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimRteFiles)
(Aug 11, 2016 4:14:55 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimRtePlugins)
|(Aug 11, 2016 4:14:56 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Configuration Repository Utils (addPluginsToConfigRepos)
Aug 11, 2016 4:14:56 PM com.ibm.websphere.management.AdminClientFactory
WARNING: ADMC0046W
Aug 11, 2016 4:14:57 PM com.ibm.ws.management.connector.interop.JMXClassLoader
WARNING: Could not find tmx4jTransform.jar in null/etc/tmx4jTransform.jar - Interoperability to older versions of WebSphere is disabled
Aug 11, 2016 4:14:57 PM com.ibm.ws.ssl.config.SSLConfigManager
INFO: ssl.disable.url.hostname.verification.CWPKI0027I
Aug 11, 2016 4:14:57 PM com.ibm.ws.security.config.SecurityObjectLocator
INFO: Client code attempting to load security configuration
Aug 11, 2016 4:14:59 PM com.ibm.ws.security.config.SecurityObjectLocator
INFO: Client code attempting to load security configuration
Aug 11, 2016 4:14:59 PM com.ibm.websphere.management.AdminClientFactory
WARNING: ADMC0046W
Aug 11, 2016 4:15:00 PM com.ibm.websphere.management.AdminClientFactory
WARNING: ADMC0046W
```



```
ij> ALTER TABLE FIMAliasesSchema.USER1
  ADD CONSTRAINT PK_USER1 PRIMARY KEY (USERID);
0 rows inserted/updated/deleted
ij> CREATE TABLE FIMAliasesSchema.PARTNER
  (ID INTEGER,
   NAME VARCHAR(250) NOT NULL);
0 rows inserted/updated/deleted
ij> ALTER TABLE FIMAliasesSchema.PARTNER
  ADD CONSTRAINT PK_PARTNER PRIMARY KEY (NAME);
0 rows inserted/updated/deleted
ij> CREATE TABLE FIMAliasesSchema.ALIAS1
  (ID INTEGER,
   ALIAS1 VARCHAR(250) NOT NULL);
0 rows inserted/updated/deleted
ij> ALTER TABLE FIMAliasesSchema.ALIAS1
  ADD CONSTRAINT PK_ALIAS1 PRIMARY KEY (ALIAS1);
0 rows inserted/updated/deleted
ij> CREATE TABLE FIMAliasesSchema.ALIASTYPE
  (ID INTEGER,
   ALIASTYPE VARCHAR(250) NOT NULL);
0 rows inserted/updated/deleted
ij> ALTER TABLE FIMAliasesSchema.ALIASTYPE
  ADD CONSTRAINT PK_ALIASTYPE PRIMARY KEY (ALIASTYPE);
0 rows inserted/updated/deleted
ij> CREATE TABLE FIMAliasesSchema.ALIASUSERPARTNER
  (ALIASID INTEGER NOT NULL,
   USERID INTEGER NOT NULL,
   PARTNERID INTEGER NOT NULL,
   ALIASTYPEID INTEGER NOT NULL);
0 rows inserted/updated/deleted
ij> ALTER TABLE FIMAliasesSchema.ALIASUSERPARTNER
  ADD CONSTRAINT PK_ALIASUSERPARTNER PRIMARY KEY (ALIASID, USERID, PARTNERID, ALIASTYPEID);
0 rows inserted/updated/deleted
ij> exit;
waiting for process to end
exit value=0
(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Build Number (fimRteMgmtSvcsSetBuildNumber)
(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Update Java Properties (fimRteEwasSoftwareProperties)
(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Update Java Properties (fimRteEarProperties)
(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackRteMarker)
(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Delete Directory (removeFeaturesFromTemp)



(Aug 11, 2016 4:15:32 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Delete Directory (removeConfigFromTemp)
(Aug 11, 2016 4:15:33 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimMgmtSvcEarFile2)
(Aug 11, 2016 4:15:34 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Install Application (mgmtSvcEar2)
Aug 11, 2016 4:15:35 PM com.ibm.websphere.management.AdminClientFactory
WARNING: ADMC0046W


Installing the ITFIM Management Service
```

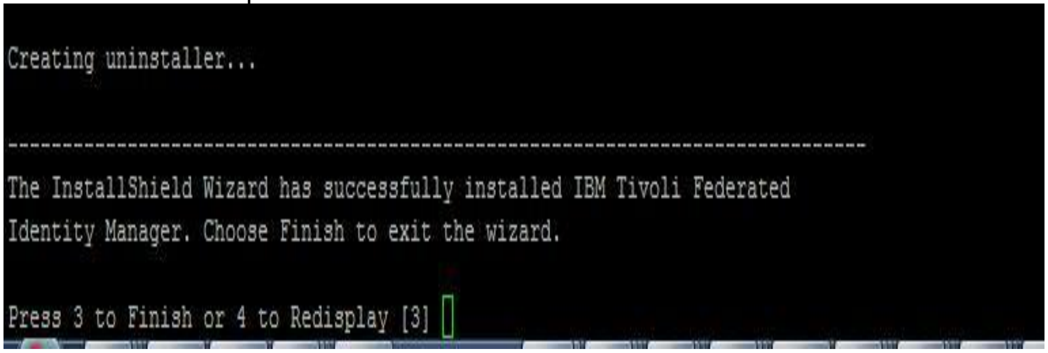


```
Installing the ITFIM Management Service
(Aug 11, 2016 4:15:47 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Add Shared Library (managementServiceSharedLibrary2)
(Aug 11, 2016 4:15:50 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackMgmtMarker)
(Aug 11, 2016 4:15:50 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimDemoFiles2)
(Aug 11, 2016 4:15:50 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimDemoMappingExtFiles)
(Aug 11, 2016 4:15:51 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (nonWindowsIvtDeployFiles)
(Aug 11, 2016 4:15:51 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Directory Permissions (setDirPermsDemo)
(Aug 11, 2016 4:15:53 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackDemoMarker)
(Aug 11, 2016 4:15:53 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Install Websphere Plugin (installWebspherePlugins)
Aug 11, 2016 4:15:53 PM com.ibm.websphere.management.AdminClientFactory
WARNING: ADMC0046W
(Aug 11, 2016 4:15:58 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackCliMarker)
(Aug 11, 2016 4:15:58 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimEntMgmtConWarFile)
(Aug 11, 2016 4:16:00 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Fim Create Directory (fimCreateEtcDirCon)
(Aug 11, 2016 4:16:00 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Add Property To Jar (fimAddPropertiesToConsoleWar)
(Aug 11, 2016 4:16:04 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Deploy Isc Application (deployConsole)


Deploying the ITFIM Management Console
Aug 11, 2016 4:16:05 PM com.tivoli.am.fim.installer.utils.DeployIscUtils installConsole
INFO: Created directory: /opt/IBM/FIM/ewas/systemApps/isclite.ear/itfim-fimconsole-e.war
Aug 11, 2016 4:16:05 PM com.tivoli.am.fim.installer.utils.DeployIscUtils installConsole
INFO: Unjarring file /opt/IBM/FIM/pkg/release/itfim-fimconsole-e.war in directory /opt/IBM/FIM/ewas/systemApps/isclite.ear/itfim-fimconsole-e.war
```



```
Deploying the ITFIM Management Console
Aug 11, 2016 4:16:05 PM com.tivoli.am.fim.installer.utils.DeployIscUtils installConsole
INFO: Created directory: /opt/IBM/FIM/ewas/systemApps/isclite.ear/itfim-fimconsole-e.war
Aug 11, 2016 4:16:05 PM com.tivoli.am.fim.installer.utils.DeployIscUtils installConsole
INFO: Unjarring file /opt/IBM/FIM/pkg/release/itfim-fimconsole-e.war in directory /opt/IBM/FIM/ewas/systemApps/isclite.ear/itfim-fimconsole-e.war
(Aug 11, 2016 4:18:01 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Build Number (fimMgmtConSetBuildNumber)
(Aug 11, 2016 4:18:01 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Directory Permissions (setDirPermsCon)
(Aug 11, 2016 4:18:03 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackConsoleMarker)
(Aug 11, 2016 4:18:03 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimRteProvisioningFiles)
(Aug 11, 2016 4:18:03 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Build Number (fimWsProvSetBuildNumber)
(Aug 11, 2016 4:18:03 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Directory Permissions (setDirPermsWsProv)
(Aug 11, 2016 4:18:05 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackWspMarker)
(Aug 11, 2016 4:18:05 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (ISAFiles)
(Aug 11, 2016 4:18:06 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackISAMarker)
(Aug 11, 2016 4:18:06 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fimWssmFiles)
(Aug 11, 2016 4:18:06 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Build Number (fimWssmSetBuildNumber)
(Aug 11, 2016 4:18:06 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Set Directory Permissions (setDirPermsWssm)
(Aug 11, 2016 4:18:08 PM), Install, com.ibm.wizard.platform.linux.LinuxProductServiceImpl, msg1, installing Files (fixpackWssmMarker)
```

12. Click Finish. The Tivoli Federated Identity Manager runtime and management services installation is complete.



```
Creating uninstaller...


-------------------------------------------------------------------------------
The InstallShield Wizard has successfully installed IBM Tivoli Federated
Identity Manager. Choose Finish to exit the wizard.

Press 3 to Finish or 4 to Redisplay [3]
```

Configuration of a single sign-on federation

The topics in the Configuration section provide a step-by-step guide to configuring a single sign-on federation. The management console provides wizards to guide you through many of the configuration tasks.

Complete the configuration tasks in the following order:

- Identity provider and service provider roles
- Domain Configuration
- Selecting Point of Contact Server
- Configuring WebSphere as Point of Contact Server
- Manage Federations
- Manage Federation Partners

Identity provider and service provider roles

Each partner in a federation has a role. The role is either Identity Provider or Service Provider.

- **Identity provider:**
  An identity provider is a federation partner that vouches for the identity of a user. The Identity Provider authenticates the user and provides an authentication token (that is, information that verifies the authenticity of the user) to the service provider. The identity provider either directly authenticates the user, such as by validating a user name and password, or indirectly authenticates the user, such as by validating an assertion about the user’s identity as presented by a separate identity provider. The identity provider handles the management of user identities in order to free the service provider from this responsibility.

- **Service Provider:**
  A service provider is a federation partner that provides services to the end user. Typically, service providers do not authenticate users but instead request authentication decisions from an identity provider. Service providers rely on identity providers to assert the identity of a user, and typically certain attributes about the user that are managed by the identity provider. Service providers may also maintain a local account for the user along with attributes that are unique to their service. Service providers can maintain a local account for the user, which can be referenced by an identifier for the user.

Some federation protocols use different terminology to refer to the service provider role:

- **Relying party:** The Information Card protocol specification uses the term Relying Party to describe the service provider role. When you configure the Information Card federation, using the Tivoli Federated Identity Manager wizard, you will choose the Service Provider role for your Relying Party.

- **Consumer:** The OpenID protocol specification uses the term Consumer to describe the service provider role. When you configure the OpenID, using the Tivoli Federated Identity Manager wizard, you will choose the Service Provider role for your Consumer.

Before installing Tivoli Federated Identity Manager, you will need to know whether you will be the identity provider or the service provider in each of the federations that you will configure. You will also want to understand the point of contact server options for your role.

Domain Configuration

A Tivoli Federated Identity Manager domain is a deployment of the Tivoli Federated Identity Manager runtime component to either a WebSphere single server or a WebSphere cluster. There is one domain per WebSphere cluster. In a single server environment, there can be only one domain. Each domain is managed independently. You can use installation of the Tivoli Federated Identity Manager management console to manage multiple domains. You can manage only one domain at a time. The domain that is being managed is known as the active domain.

When Tivoli Federated Identity Manager is installed, no domains exist. You will use the management console to create a domain. When you installed Tivoli Federated Identity Manager the management service was deployed to a WebSphere server (single server mode) or WebSphere Deployment Manager (WebSphere cluster mode). You will connect with this management service and choose a WebSphere server or cluster to which you will deploy the Tivoli Federated Identity Manager runtime component. When the runtime is deployed and configured, you are ready to configure additional features such as federated single sign-on or Web services security management.

In a WebSphere Network Deployment environment, the deployment and configuration of the Tivoli Federated Identity Manager runtime to cluster members is an automated process. It is not necessary to perform additional installation of Tivoli Federated Identity Manager or Tivoli Access Manager software onto the WebSphere cluster computers. Deployment and configuration of the runtime application to distributed cluster members is performed by the Tivoli Federated Identity Manager management service utilizing the application deployment services of the WebSphere Deployment Manager.

The management console provides a wizard to guide you through the creation of the domain. The following sections list the properties that the wizard prompts you to supply.

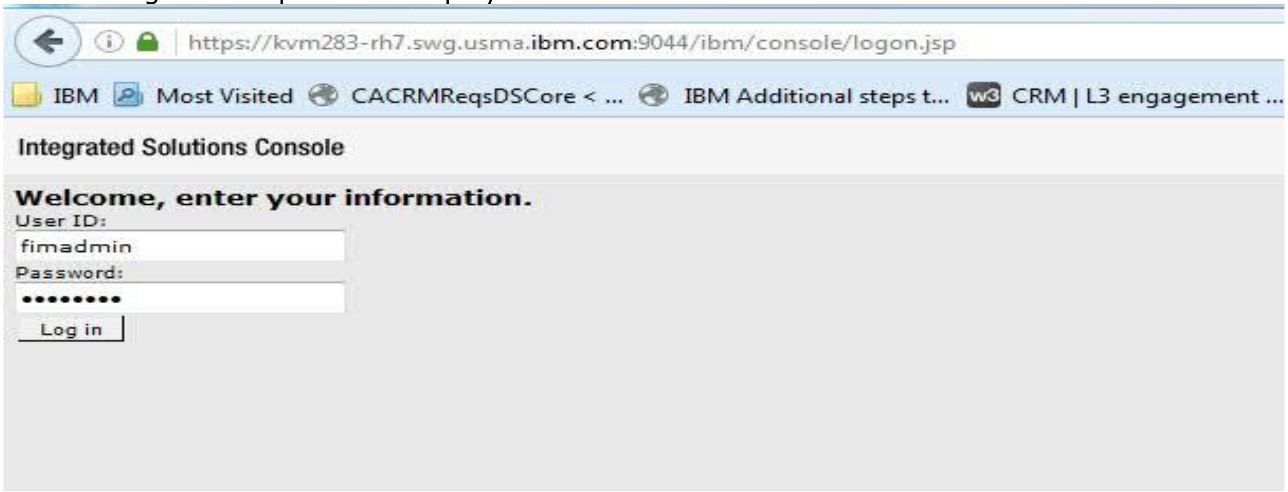
Creating and deploying a new domain

You must create a domain and deploy a runtime application for each instance of the Tivoli Federated Identity Manager. This task is a prerequisite for configuration of additional Tivoli Federated Identity Manager features such as federated single sign-on or Web services security management.

A wizard prompts you to supply the necessary configuration properties.

1. Verify that the WebSphere Application Server application is running.
2. Log in to the WebSphere console and click Tivoli Federated Identity Manager → Getting Started.

3. The Getting Started portlet is displayed.



https://kvm283-rh7.swg.usma.ibm.com:9044/ibm/console/logon.jsp

IBM | Most Visited | CACRMReqsDSCore < ... | IBM Additional steps t... | CRM | L3 engagement ...

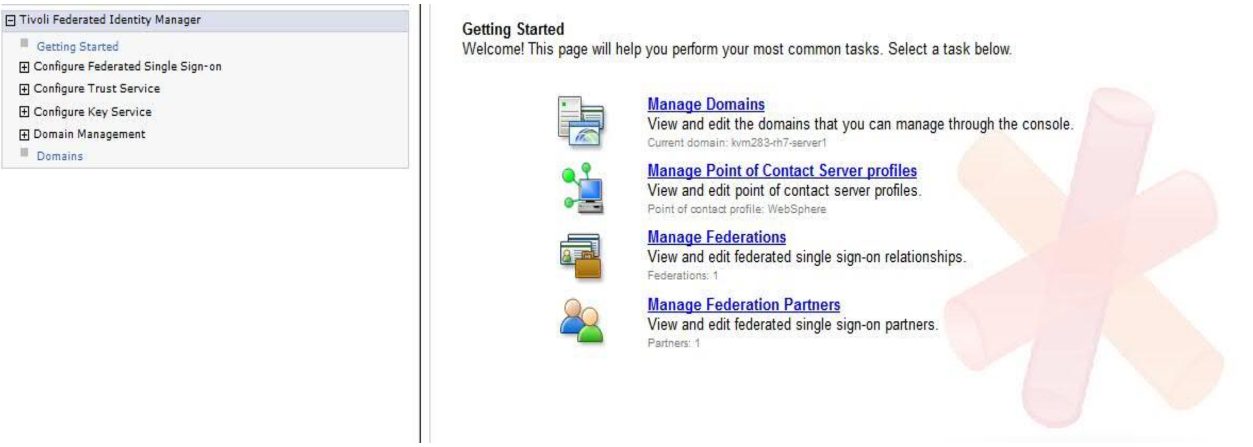
Integrated Solutions Console

Welcome, enter your information.

User ID: fimadmin

Password: ••••••••

Log in



⊟ Tivoli Federated Identity Manager
- Getting Started
- ⊞ Configure Federated Single Sign-on
- ⊞ Configure Trust Service
- ⊞ Configure Key Service
- ⊞ Domain Management
- Domains

Getting Started

Welcome! This page will help you perform your most common tasks. Select a task below.

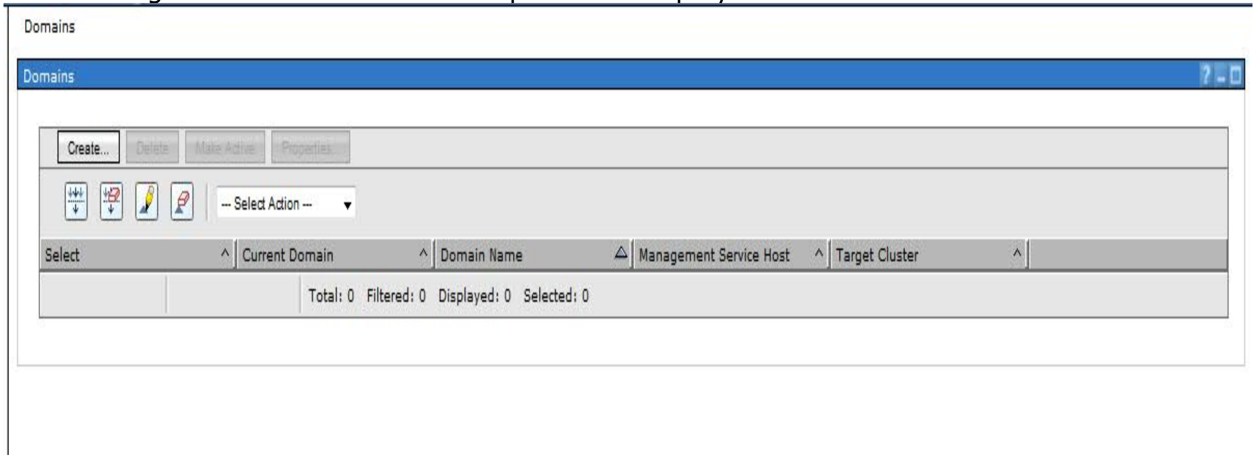
Manage Domains
View and edit the domains that you can manage through the console.
Current domain: kvm283-rh7-server1

Manage Point of Contact Server profiles
View and edit point of contact server profiles.
Point of contact profile: WebSphere

Manage Federations
View and edit federated single sign-on relationships.
Federations: 1

Manage Federation Partners
View and edit federated single sign-on partners.
Partners: 1

4. Click Manage Domains. The Domains portlet is displayed



Domains

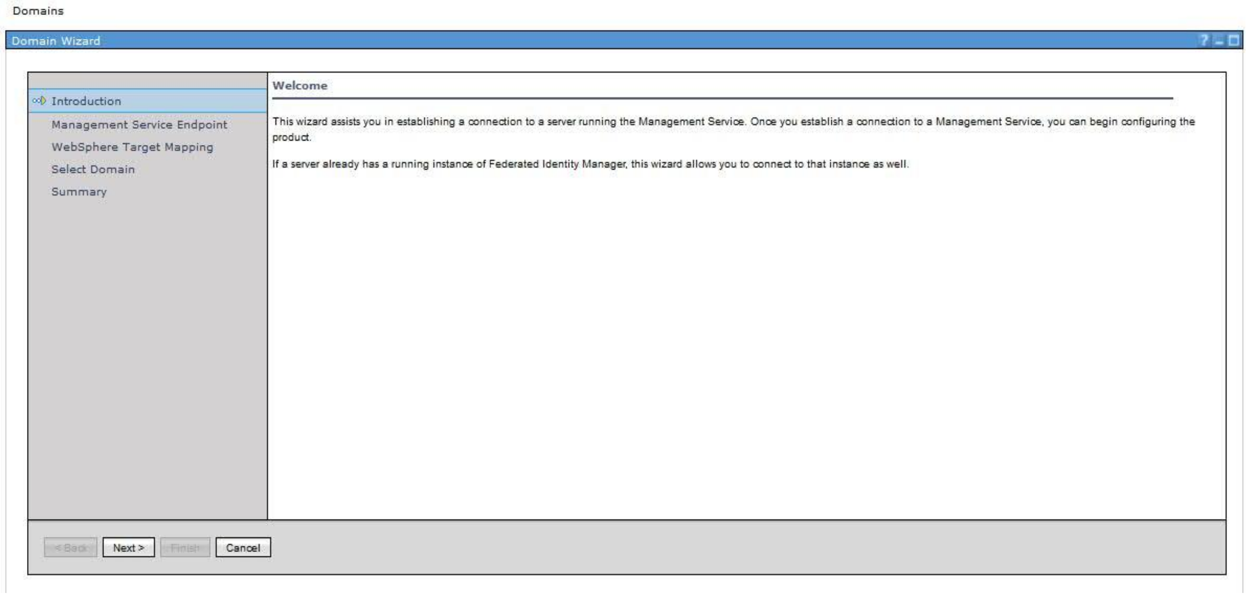
Domains

Create... | Delete | Make Active | Properties

-- Select Action --

Select	Current Domain	Domain Name	Management Service Host	Target Cluster
	Total: 0 Filtered: 0 Displayed: 0 Selected: 0			

5. Click Create. The Domain Wizard displays the Welcome panel.

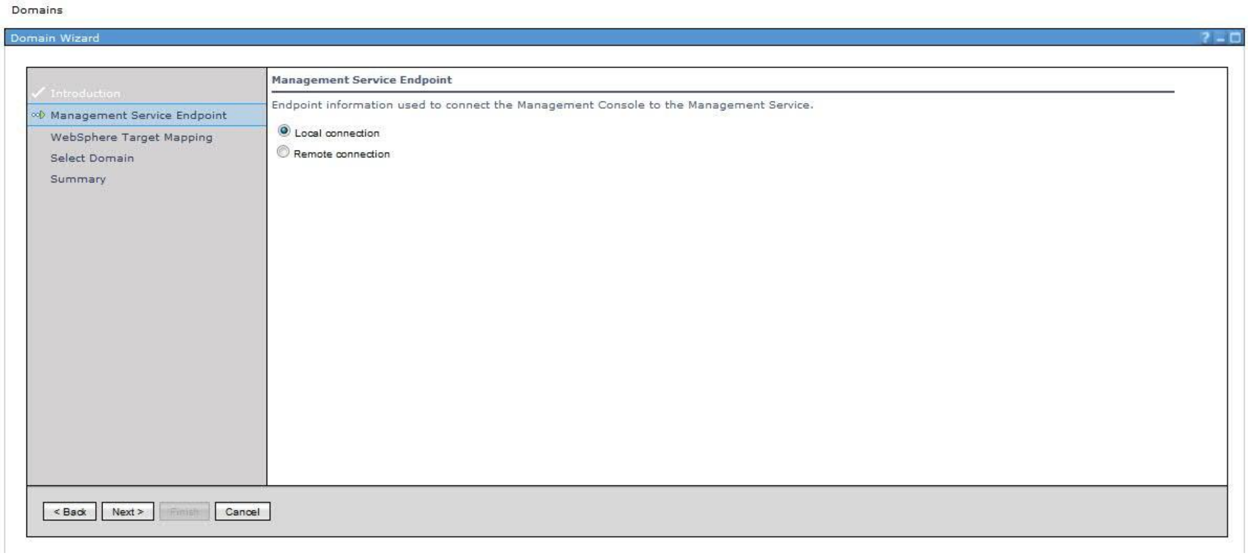


Welcome

This wizard assists you in establishing a connection to a server running the Management Service. Once you establish a connection to a Management Service, you can begin configuring the product.

If a server already has a running instance of Federated Identity Manager, this wizard allows you to connect to that instance as well.

6. Click Next. The Management Service Endpoint panel is displayed.



Management Service Endpoint

Endpoint information used to connect the Management Console to the Management Service.

● Local connection

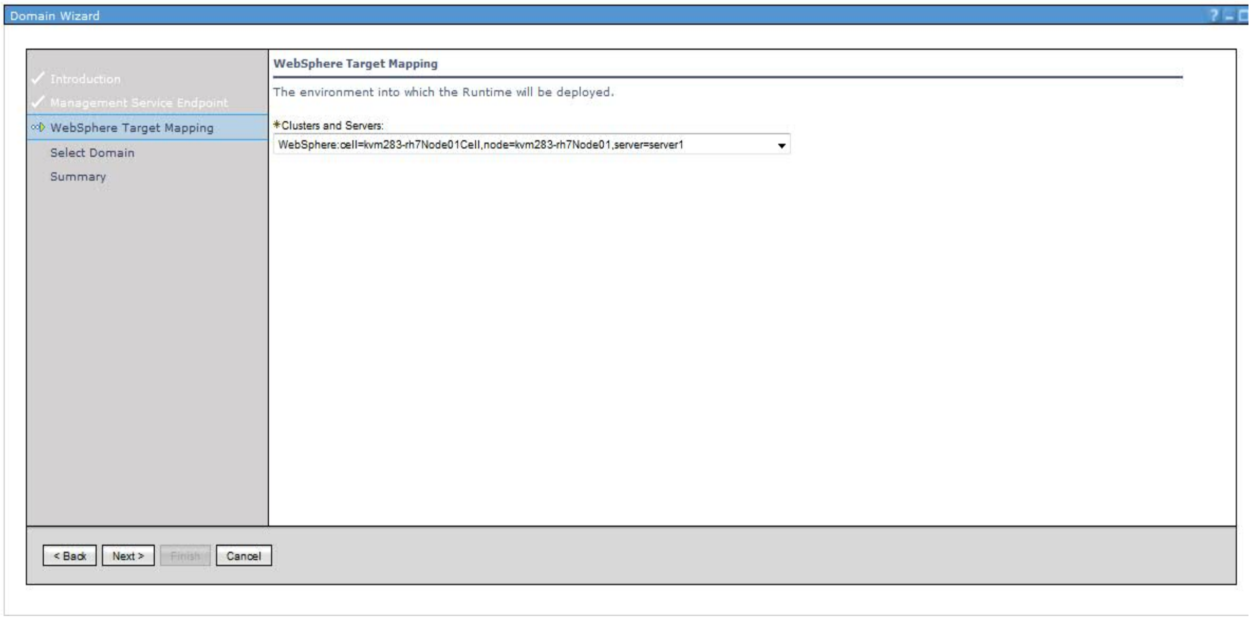
○ Remote connection

7. Enter values for the specified properties and click Next.

8. Click Next. The WebSphere Target Mapping panel is displayed. Select or enter the name of your server or cluster. When finished, click Next.

- When the WebSphere environment consists of a single server, the panel displays a Server name menu with a default name.

- When the WebSphere environment consists of a cluster, the panel displays the Cluster Name menu. This menu lists the names of clusters defined in the cell. Select the name of the cluster to use.

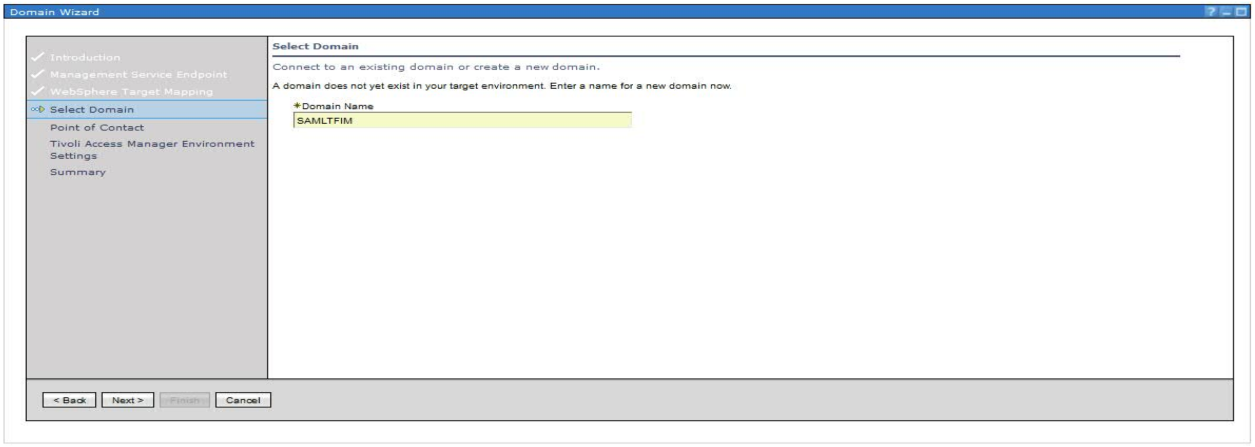


WebSphere Target Mapping

The environment into which the Runtime will be deployed.

*Clusters and Servers:
WebSphere:cell=kvm283-rh7Node01Cell,node=kvm283-rh7Node01,server=server1

9. The Select Domain panel is displayed. A default name is provided. Accept it or enter a name for the new domain.



Domain Wizard
✓ Introduction
✓ Management Service Endpoint
✓ WebSphere Target Mapping
Select Domain
Point of Contact
Tivoli Access Manager Environment Settings
Summary
< Back
Next >
Finish
Cancel

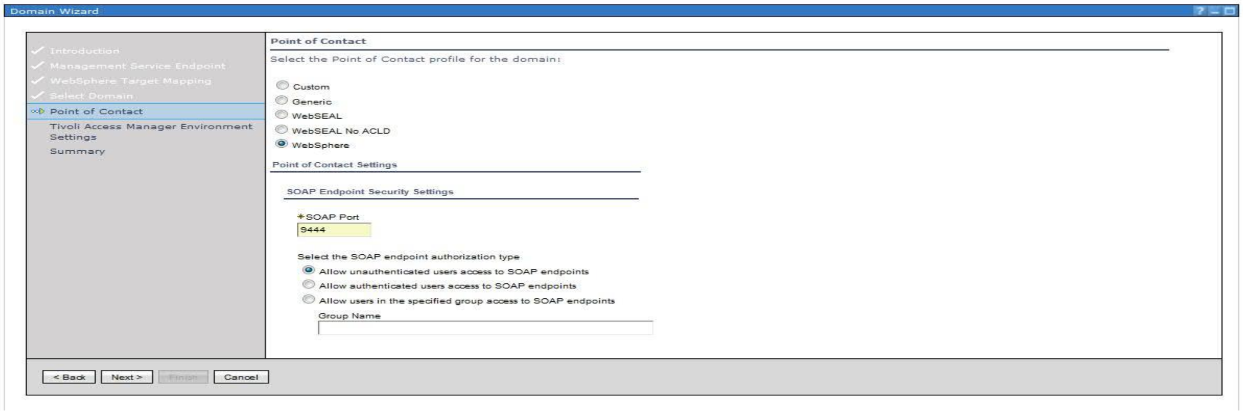
Select Domain

Connect to an existing domain or create a new domain.

A domain does not yet exist in your target environment. Enter a name for a new domain now.

*Domain Name
SAMLTFIM

10. Select WebSphere as Point of Contact for the domain.



Domain Wizard
✓ Introduction
✓ Management Service Endpoint
✓ WebSphere Target Mapping
✓ Select Domain
Point of Contact
Tivoli Access Manager Environment Settings
Summary
< Back
Next >
Finish
Cancel

Point of Contact

Select the Point of Contact profile for the domain:

○ Custom
○ Generic
○ WebSEAL
○ WebSEAL No ACLD
● WebSphere

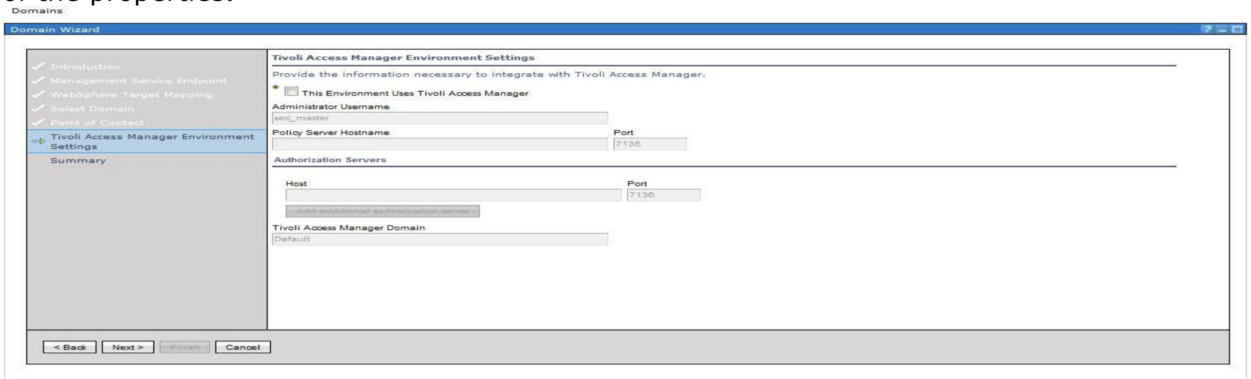
Point of Contact Settings

SOAP Endpoint Security Settings

*SOAP Port
9444

Select the SOAP endpoint authorization type
● Allow unauthenticated users access to SOAP endpoints
○ Allow authenticated users access to SOAP endpoints
○ Allow users in the specified group access to SOAP endpoints
Group Name

11. The Tivoli Access Manager Environment Settings panel is displayed. Select or deselect This Environment Uses Tivoli Access Manager as appropriate. Click Next. Provide values for the rest of the properties.



Tivoli Access Manager Environment Settings

Provide the information necessary to integrate with Tivoli Access Manager.

* □ This Environment Uses Tivoli Access Manager

Administrator Username: sec_master

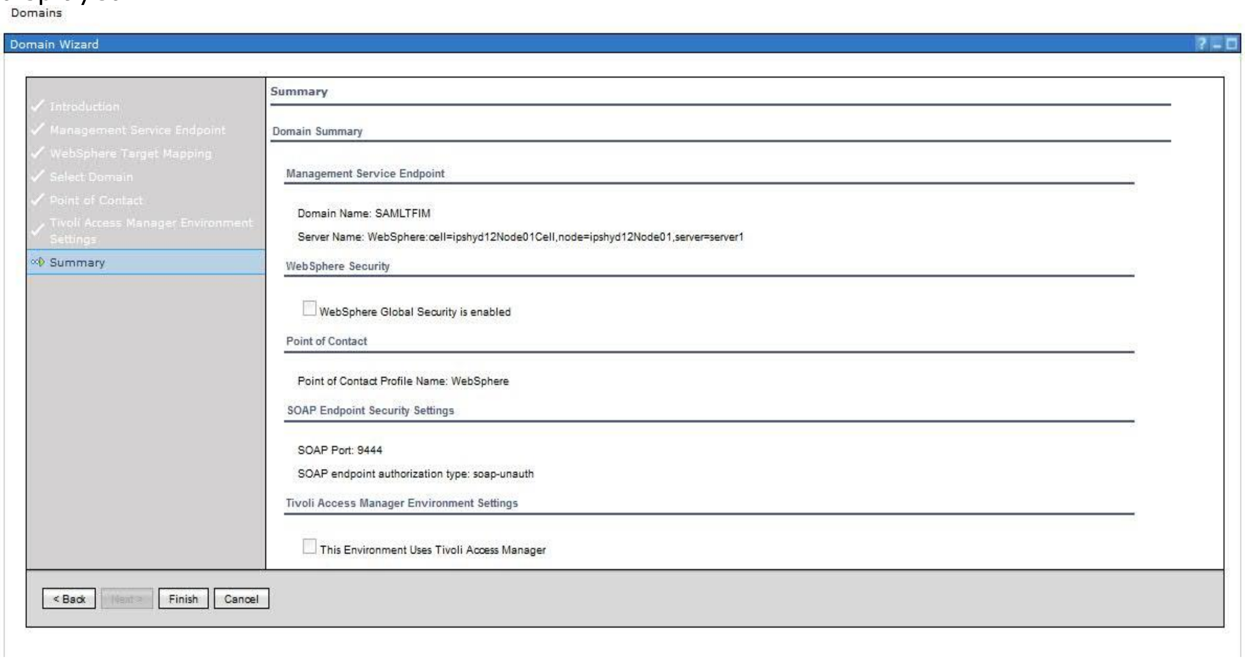
Policy Server Hostname: Port: 7135

Authorization Servers

Host: Port: 7136

Tivoli Access Manager Domain: Default

12. The Summary panel is displayed. Verify that the domain information is correct and click Finish. The domain is created and the domain wizard exits. The Create Domain Complete panel is displayed.



Summary

Domain Summary

Management Service Endpoint

Domain Name: SAMLTFIM

Server Name: WebSphere:cell=ipshyd12Node01Cell,node=ipshyd12Node01,server=server1

WebSphere Security

□ WebSphere Global Security is enabled

Point of Contact

Point of Contact Profile Name: WebSphere

SOAP Endpoint Security Settings

SOAP Port: 9444

SOAP endpoint authorization type: soap-unauth

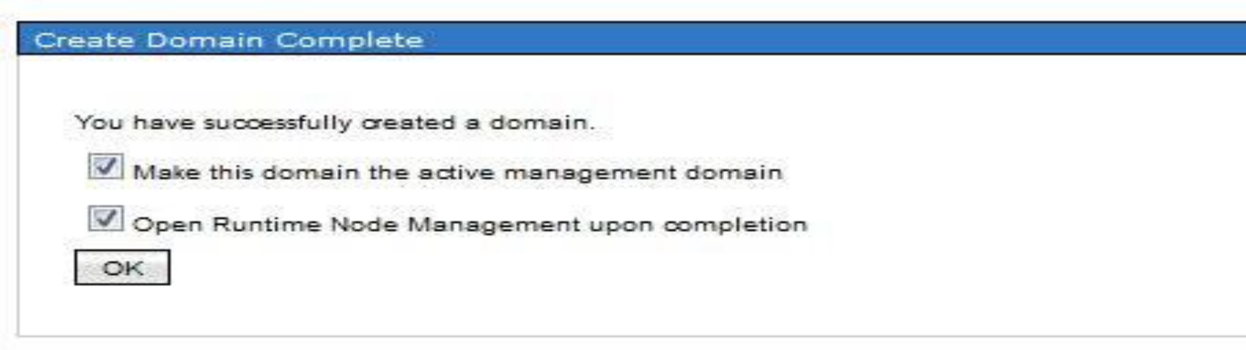
Tivoli Access Manager Environment Settings

□ This Environment Uses Tivoli Access Manager

13. Select both of the check boxes on the Create Domain Complete panel and click OK. You must complete both of the tasks as part of the initial creation and deployment of the Tivoli Federated Identity Manager management service and runtime:

    - Make this domain the active management domain

- Open Runtime Node Management upon completion



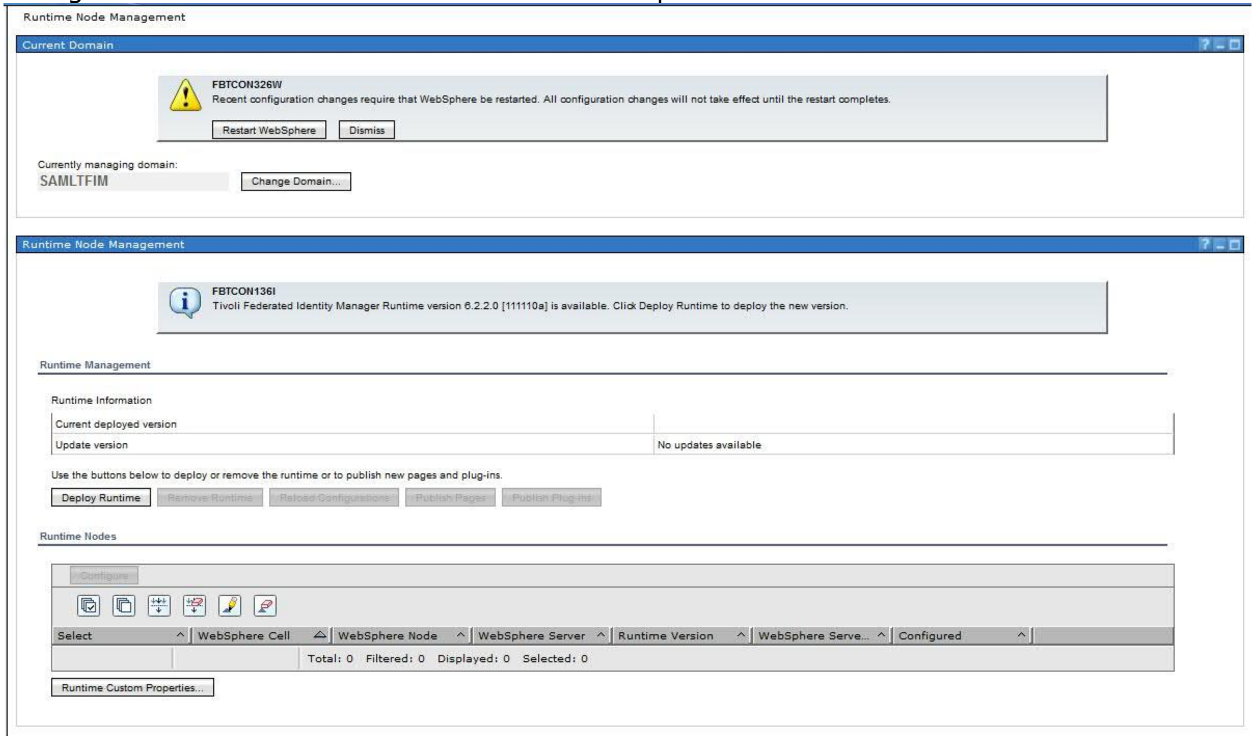
Create Domain Complete

You have successfully created a domain.

☑ Make this domain the active management domain

☑ Open Runtime Node Management upon completion

14. A message "Recent configuration changes require WebSphere be restarted. All configuration changes will not take effect until the restart completes."



Runtime Node Management

Current Domain

FBTCON326W
Recent configuration changes require that WebSphere be restarted. All configuration changes will not take effect until the restart completes.

Currently managing domain: SAMLTFIM

Runtime Node Management

FBTCON136I
Tivoli Federated Identity Manager Runtime version 6.2.2.0 [111110a] is available. Click Deploy Runtime to deploy the new version.

Runtime Management

Runtime Information

Current deployed version	
Update version	No updates available

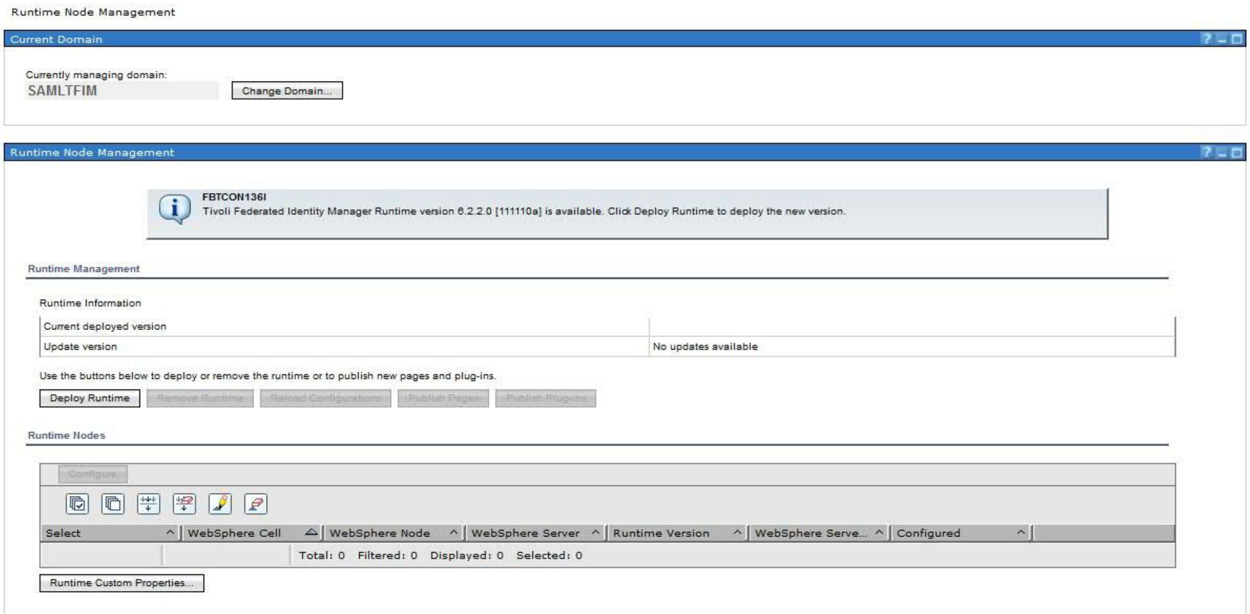
Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Runtime Nodes

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Serve...	Configured
		Total: 0 Filtered: 0 Displayed: 0 Selected: 0				

15. Click the Restart WebSphere button.

16. The Current Domain portlet and the Runtime Node Management portlet are displayed. In the Runtime Node Management portlet, click Deploy Runtime. A message is displayed:



Runtime Node Management

Current Domain

Currently managing domain:
SAMLTFIM
Change Domain...

Runtime Node Management

FBTCON136I
Tivoli Federated Identity Manager Runtime version 6.2.2.0 [111110a] is available. Click Deploy Runtime to deploy the new version.

Runtime Management

Runtime Information

Current deployed version	
Update version	No updates available

Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Deploy Runtime | Remove Runtime | Reload Configurations | Publish Pages | Publish Plug-ins

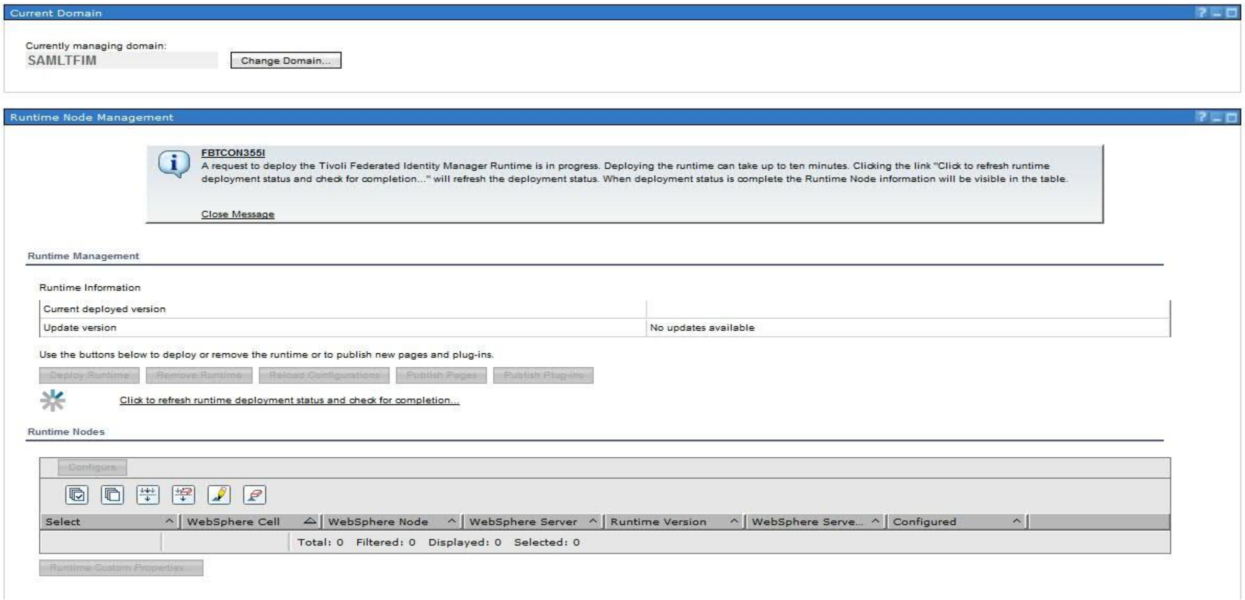
Runtime Nodes

Configure

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Serve...	Configured
		Total: 0 Filtered: 0 Displayed: 0 Selected: 0				

Runtime Custom Properties...

FBTCON355I - A request to deploy the Tivoli Federated Identity Manager Runtime is in progress.



Current Domain

Currently managing domain:
SAMLTFIM
Change Domain...

Runtime Node Management

FBTCON355I
A request to deploy the Tivoli Federated Identity Manager Runtime is in progress. Deploying the runtime can take up to ten minutes. Clicking the link "Click to refresh runtime deployment status and check for completion..." will refresh the deployment status. When deployment status is complete the Runtime Node information will be visible in the table.

Close Message

Runtime Management

Runtime Information

Current deployed version	
Update version	No updates available

Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Deploy Runtime | Remove Runtime | Reload Configurations | Publish Pages | Publish Plug-ins

Click to refresh runtime deployment status and check for completion...

Runtime Nodes

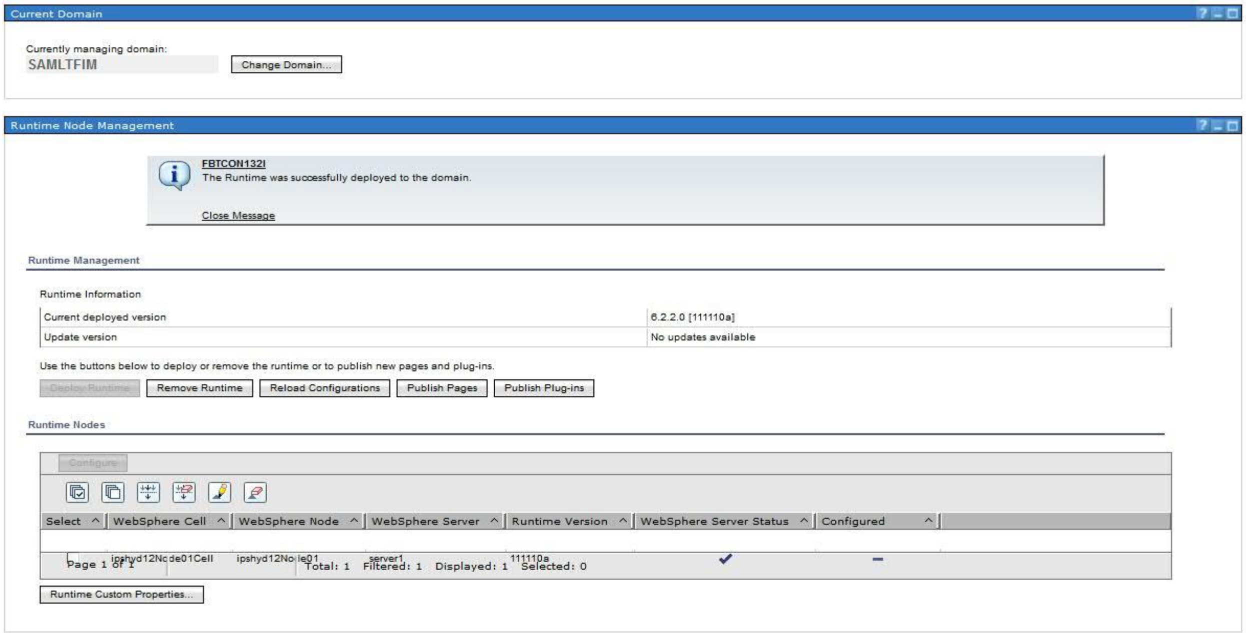
Configure

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Serve...	Configured
		Total: 0 Filtered: 0 Displayed: 0 Selected: 0				

Runtime Custom Properties...

The following link is displayed:
Click to refresh runtime deployment status and check for completion.
The Deploy operation may take several minutes. During this time, you can click the link to check for completion. When the deployment is complete, then clicking on the link will return the message:

FBTCON132I The Runtime was successfully deployed to the domain.



Currently managing domain: SAMLTFIM

FBTCON132I
The Runtime was successfully deployed to the domain.

Runtime Management

Runtime Information

Current deployed version	6.2.2.0 [111110a]
Update version	No updates available

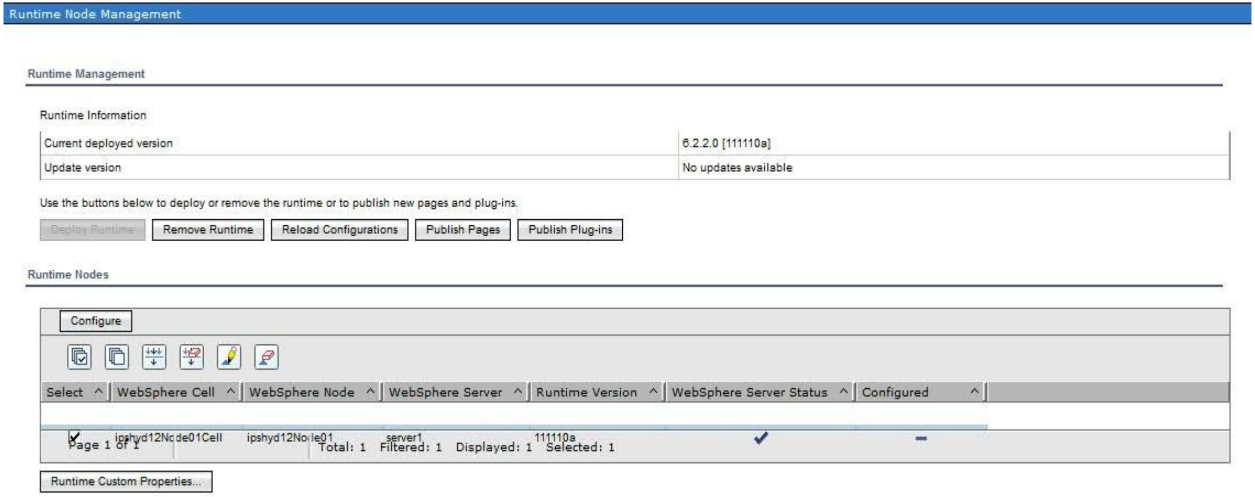
Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Runtime Nodes

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Server Status	Configured
	ipshyd12Node01Cell	ipshyd12Node01	server1	111110a	✓	–

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 0

17. The Runtime Node Management portlet is redrawn. An entry for the runtime is added to the Runtime Nodes table for each node in the domain. Also, the Configure button is activated.



Runtime Management

Runtime Information

Current deployed version	6.2.2.0 [111110a]
Update version	No updates available

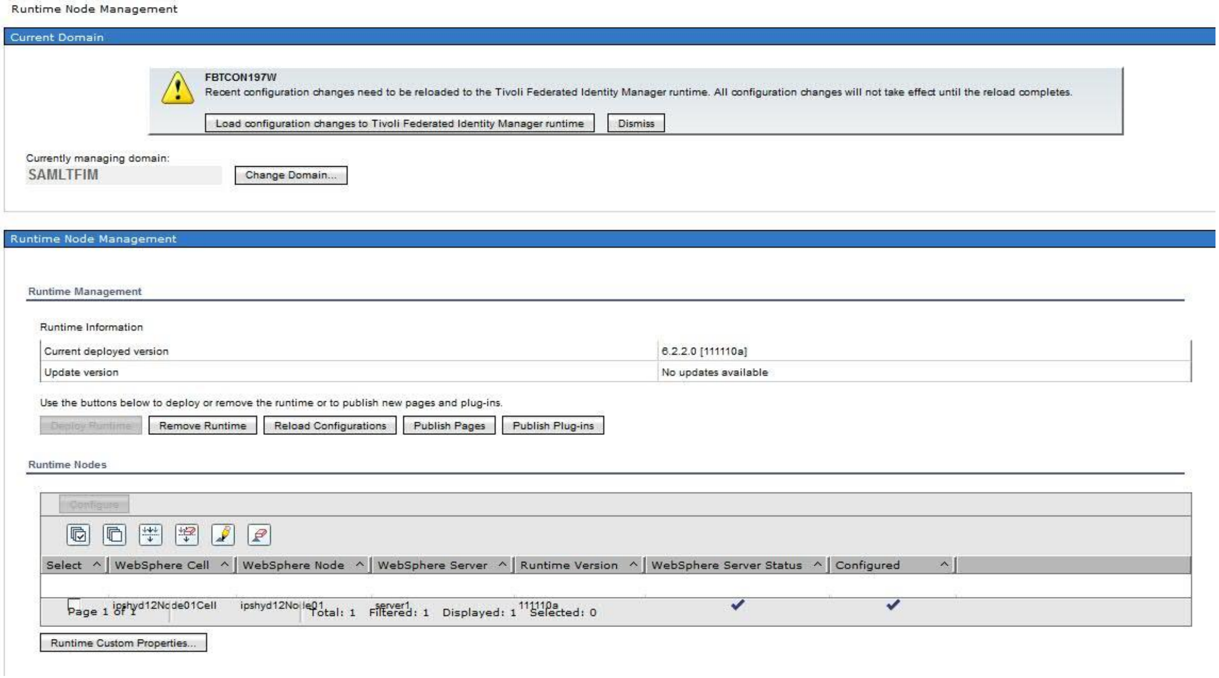
Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Runtime Nodes

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Server Status	Configured
☑	ipshyd12Node01Cell	ipshyd12Node01	server1	111110a	✓	–

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 1

18. In the Runtime Node table, select the check box for your node and click Configure. The runtime application is configured into the environment.



FBTCON197W
Recent configuration changes need to be reloaded to the Tivoli Federated Identity Manager runtime. All configuration changes will not take effect until the reload completes.

Currently managing domain: SAMLTFIM

Runtime Information

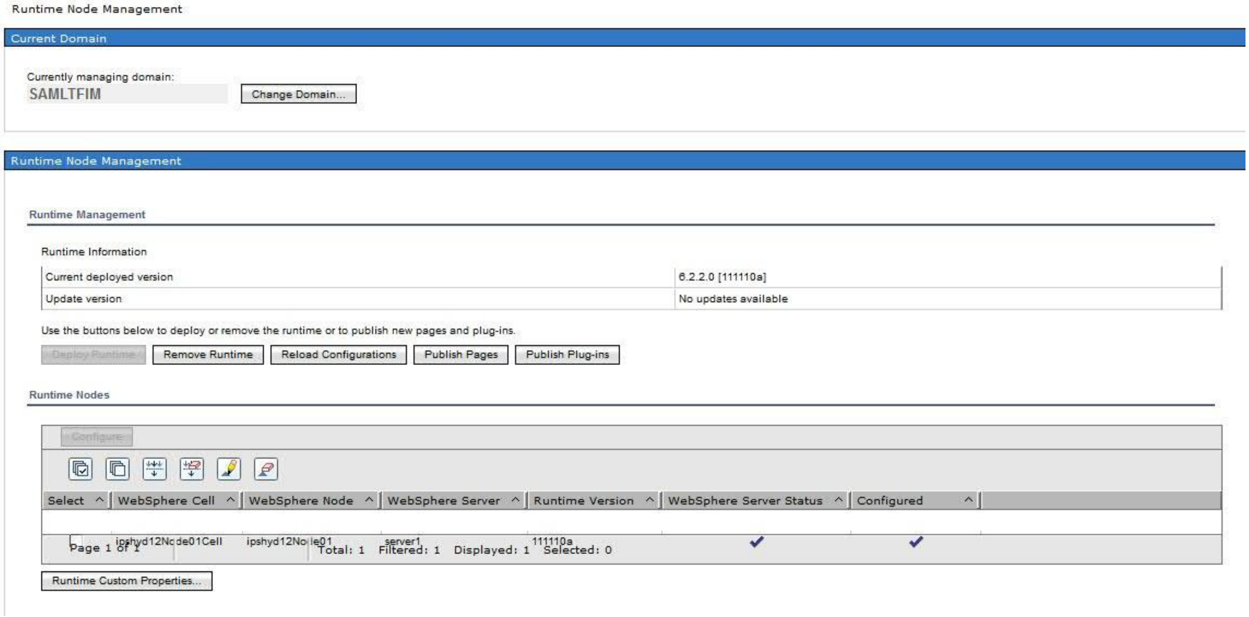
Current deployed version	6.2.2.0 [111110a]
Update version	No updates available

Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Server Status	Configured
□	ipshyd12Node01Cell	ipshyd12Node01	server1	111110a	✓	✓

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 0

19. When all nodes are configured, click the Load configuration changes to the Tivoli Federated Identity Runtime button. The button is located in the Current Domain portlet.



Currently managing domain: SAMLTFIM

Runtime Information

Current deployed version	6.2.2.0 [111110a]
Update version	No updates available

Use the buttons below to deploy or remove the runtime or to publish new pages and plug-ins.

Select	WebSphere Cell	WebSphere Node	WebSphere Server	Runtime Version	WebSphere Server Status	Configured
□	ipshyd12Node01Cell	ipshyd12Node01	server1	111110a	✓	✓

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 0

20. In a WebSphere non-clustered (standalone server) environment, the domain creation and deployment is now complete. Continue with the appropriate instructions for your scenario.

Domain Configuration

Selecting a point of contact server

Tivoli Federated Identity Manager is not directly involved in user authentication or the creation of an application session. Instead, Tivoli Federated Identity Manager relies on a point of contact server.

The point of contact server is a proxy or application server that interacts with a user, performs the authentication and manages sessions. In a typical deployment, the point of contact is located at the edge of a protected network in front of a firewall, such as in a DMZ.

The point of contact server provides endpoints, which are the locations to and from which messages are sent and received. Each endpoint has a URL, so that the endpoints can be accessed by external users as Web sites on the Internet. The point of contact receives access requests and provides the authentication service. It serves as the first component capable of evaluating the authentication credentials of the user that is requesting access to the protected network. It also manages the users' session lifecycle, from session creation, to session access, to session deletion (such as in response to session logout services).
The choice of type of point of contact server to use is determined by the security architecture and network topology requirements. Tivoli Federated Identity Manager supports four options for the point of contact server:

- IBM WebSphere Application Server
- Tivoli Access Manager WebSEAL
- Generic point of contact server
- A custom point of contact server

WebSphere as point of contact server

If you intend to use IBM WebSphere Application Server, your configuration options change depending on whether you are the identity provider partner or the service provider partner.

Identity Provider options

When you use IBM WebSphere Application Server as the point of contact server and you are the identity provider in a federation, you have the following options for the type of authentication to use:

- Forms authentication using any supported user registry
- SPNEGO (Simple and Protected GSSAPI Negotiation Mechanism) using TAI (Trust Association Interceptor) authentication and using Microsoft Active Directory as the user registry

Service Provider options

When you use IBM WebSphere Application Server as the point of contact server and you are the service provider in a federation, single sign-on is enabled using Lightweight Third-Party Authentication (LTPA). You have the following options for hosting applications that will be used in the federation that is configured in Tivoli Federated Identity Manager:

- IBM WebSphere Application Server, either the same server on which Tivoli Federated Identity Manager is installed or on a separate server running either WebSphere Application Server version 5.1 or 6.x.
- Microsoft Internet Information Services server 6.0 with the Tivoli Federated Identity Manager Web Server plug-in installed
- IBM HTTP Server 6.1 with the Tivoli Federated Identity Manager Web Server plug-in installed
- Apache HTTP Server 2.0 or 2.2 with the Tivoli Federated Identity Manager Web Server plug-in installed

Configuring WebSphere as point of contact server

Tivoli Federated Identity Manager can be installed with either an embedded WebSphere server or into an existing WebSphere environment. When you install the embedded server, and use WebSphere as a point of contact server, the installation automates much of the configuration. When you install into an existing WebSphere environment, and want to use WebSphere as a point of contact server, you must manually configure the WebSphere and IHS servers to fit your deployment.

When configured as a point of contact server, WebSphere provides authentication services. The authentication services are specific to the federation role (identity provider or service provider).

WebSphere as point of contact for identity providers

Form-based authentication

In this configuration, the identity provider uses any user registry that is supported by WebSphere Application Server with form-based authentication to authenticate users who are requesting single sign-on. All of the identity provider's users must exist in the supported user registry. When users try to use single sign-on to access a resource (such as a Web application), Tivoli Federated Identity Manager presents a login form. The login form is provided with Tivoli Federated Identity Manager.

An unauthenticated user who triggers a single sign-on request to a service provider resource will be authenticated against the configured WebSphere Application Server user registry.

Configuring form-based authentication

If you are using WebSphere Application Server as your point of contact server with form-based authentication, there are several configuration tasks that you will need to complete.
The configuration tasks include:

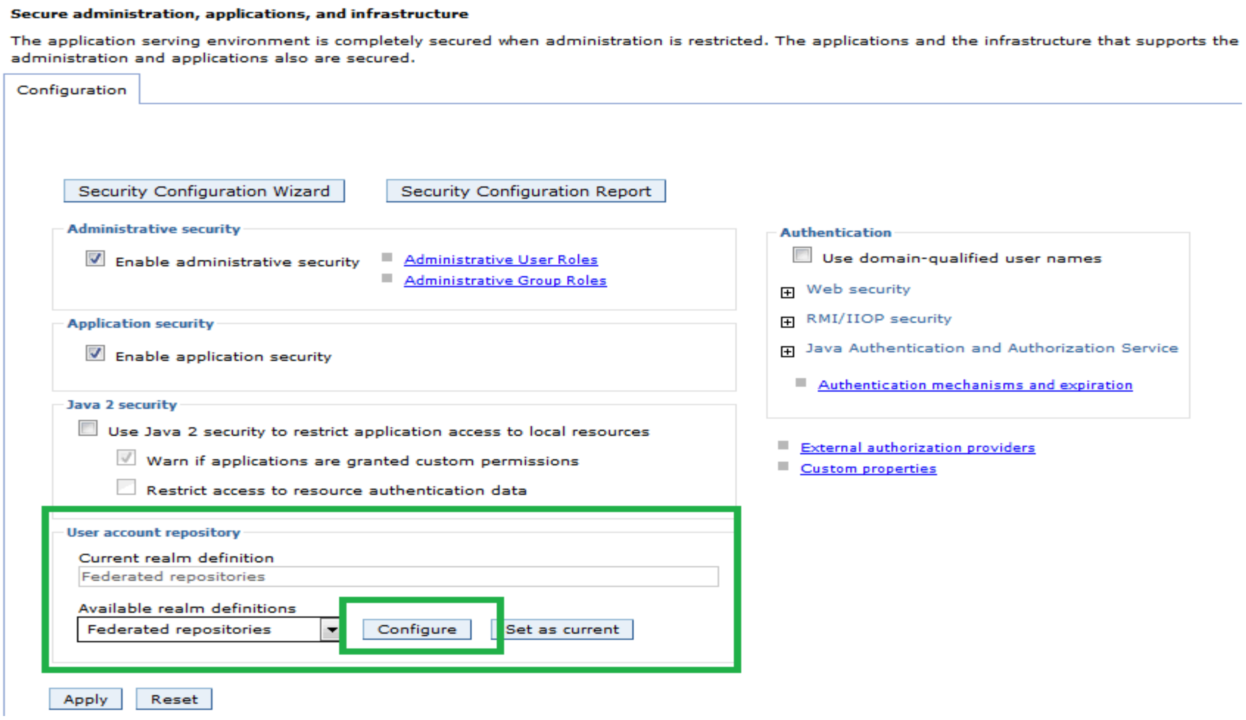
1. "Selecting and installing the user registry"
2. "Configuring the user registry"
3. "Adding single sign-on users"
4. "Adding administrative users"
5. "Configuring user registry for embedded WebSphere"
6. "Configuring an SSL connection to the user registry"
7. "Customizing the login form"

1. Selecting and installing the user registry

Select an LDAP repository. Federated with and LDAP component is also a viable option.

2. Configuring the user registry

- In Security > Secure administration, applications, and infrastructure:



Secure administration, applications, and infrastructure

The application serving environment is completely secured when administration is restricted. The applications and the infrastructure that supports the administration and applications also are secured.

Administrative security

☑ Enable administrative security

- Administrative User Roles
- Administrative Group Roles

Application security

☑ Enable application security

Java 2 security

☐ Use Java 2 security to restrict application access to local resources

☑ Warn if applications are granted custom permissions

☐ Restrict access to resource authentication data

User account repository

Current realm definition: Federated repositories

Available realm definitions: Federated repositories

Authentication

☐ Use domain-qualified user names

⊞ Web security

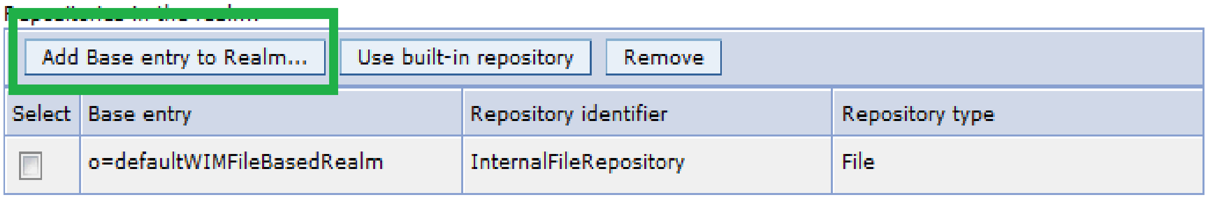
⊞ RMI/IIOP security

⊞ Java Authentication and Authorization Service

- Authentication mechanisms and expiration

- External authorization providers
- Custom properties

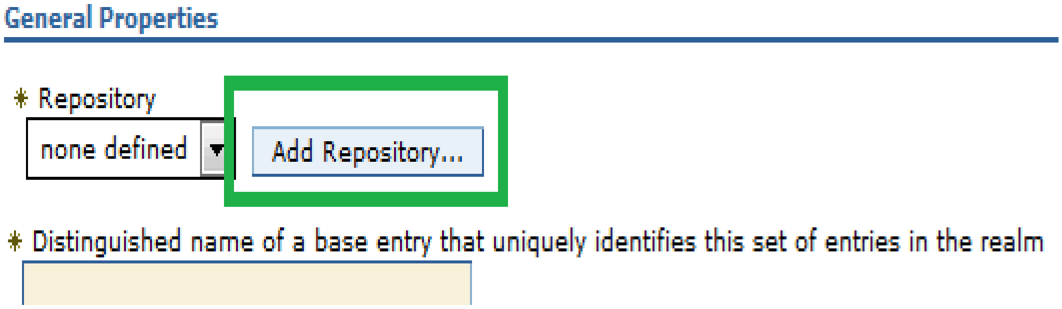
- Click 'Configure'. Click 'Add Base entry to Realm...'



Repositories in the realm:

Select	Base entry	Repository identifier	Repository type
☐	o=defaultWIMFileBasedRealm	InternalFileRepository	File

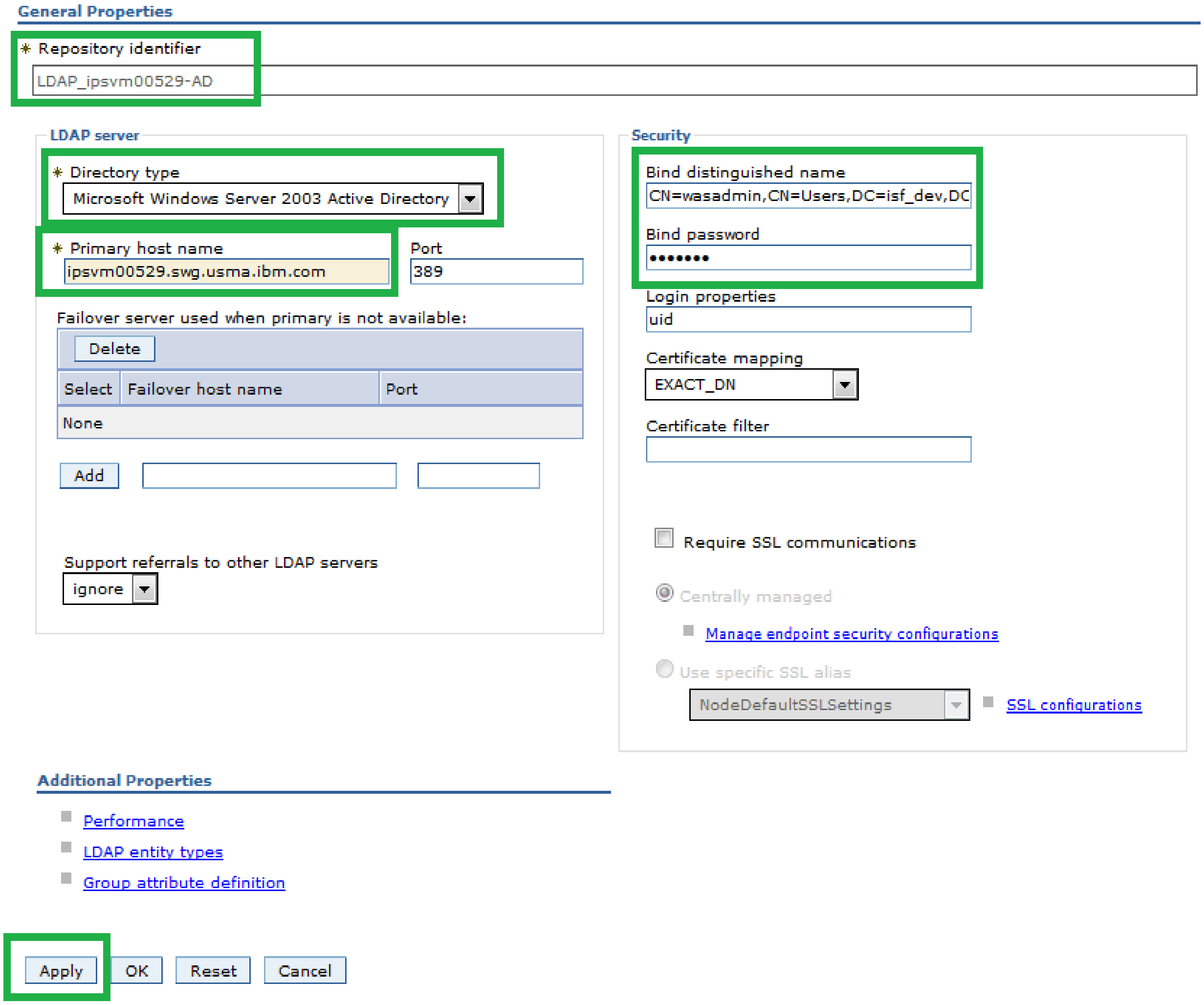
- Click 'Add Repository...'



* Repository: none defined

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm:

- Configured LDAP to point at the AD machine:



* Repository identifier: LDAP_ipsvm00529-AD

* Directory type: Microsoft Windows Server 2003 Active Directory

* Primary host name: ipsvm00529.swg.usma.ibm.com

Port: 389

Failover host name: None

Support referrals to other LDAP servers: ignore

Bind distinguished name: CN=wasadmin,CN=Users,DC=isf_dev,DC

Bind password: •••••••

Login properties: uid

Certificate mapping: EXACT_DN

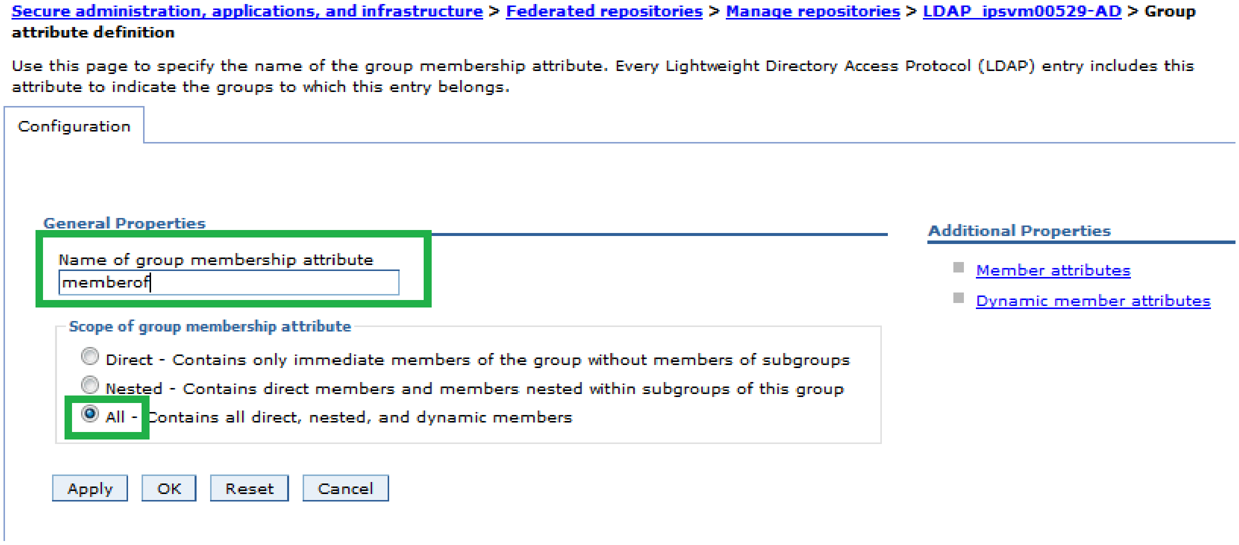
Certificate filter:

☐ Require SSL communications

● Centrally managed

○ Use specific SSL alias: NodeDefaultSSLSettings

- 'Group attribute definition' settings:



Secure administration, applications, and infrastructure > Federated repositories > Manage repositories > LDAP_ipsvm00529-AD > Group attribute definition

Use this page to specify the name of the group membership attribute. Every Lightweight Directory Access Protocol (LDAP) entry includes this attribute to indicate the groups to which this entry belongs.

General Properties

Name of group membership attribute
memberof

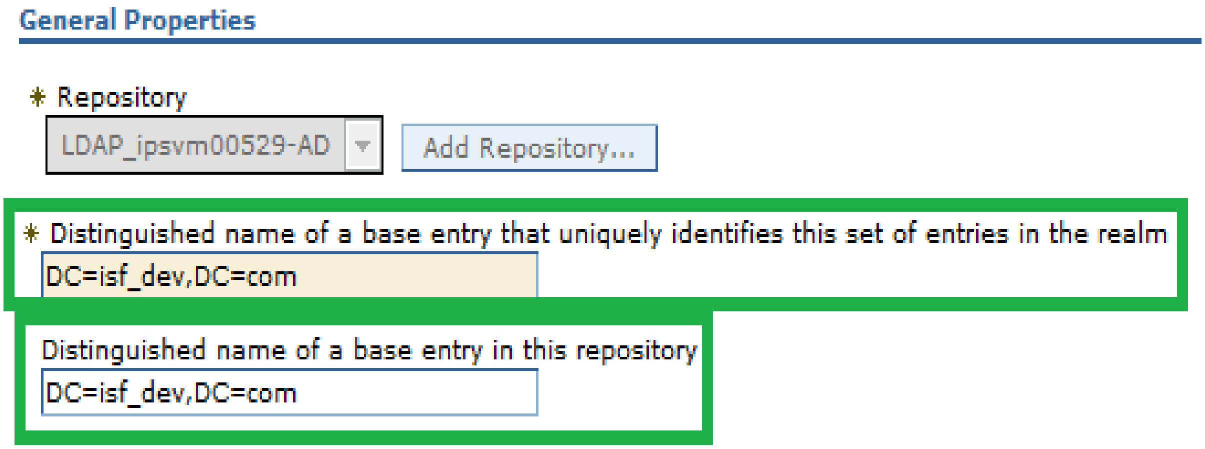
Scope of group membership attribute

○ Direct - Contains only immediate members of the group without members of subgroups
○ Nested - Contains direct members and members nested within subgroups of this group
● All - Contains all direct, nested, and dynamic members

Additional Properties

- Member attributes
- Dynamic member attributes

- Click 'Apply'. Click 'Save directly to the master configuration'
- Click 'Apply'. Click 'Save directly to the master configuration'
- In 'General Properties' added "DC=isf_dev,DC=com"



General Properties

* Repository
LDAP_ipsvm00529-AD

* Distinguished name of a base entry that uniquely identifies this set of entries in the realm
DC=isf_dev,DC=com

Distinguished name of a base entry in this repository
DC=isf_dev,DC=com

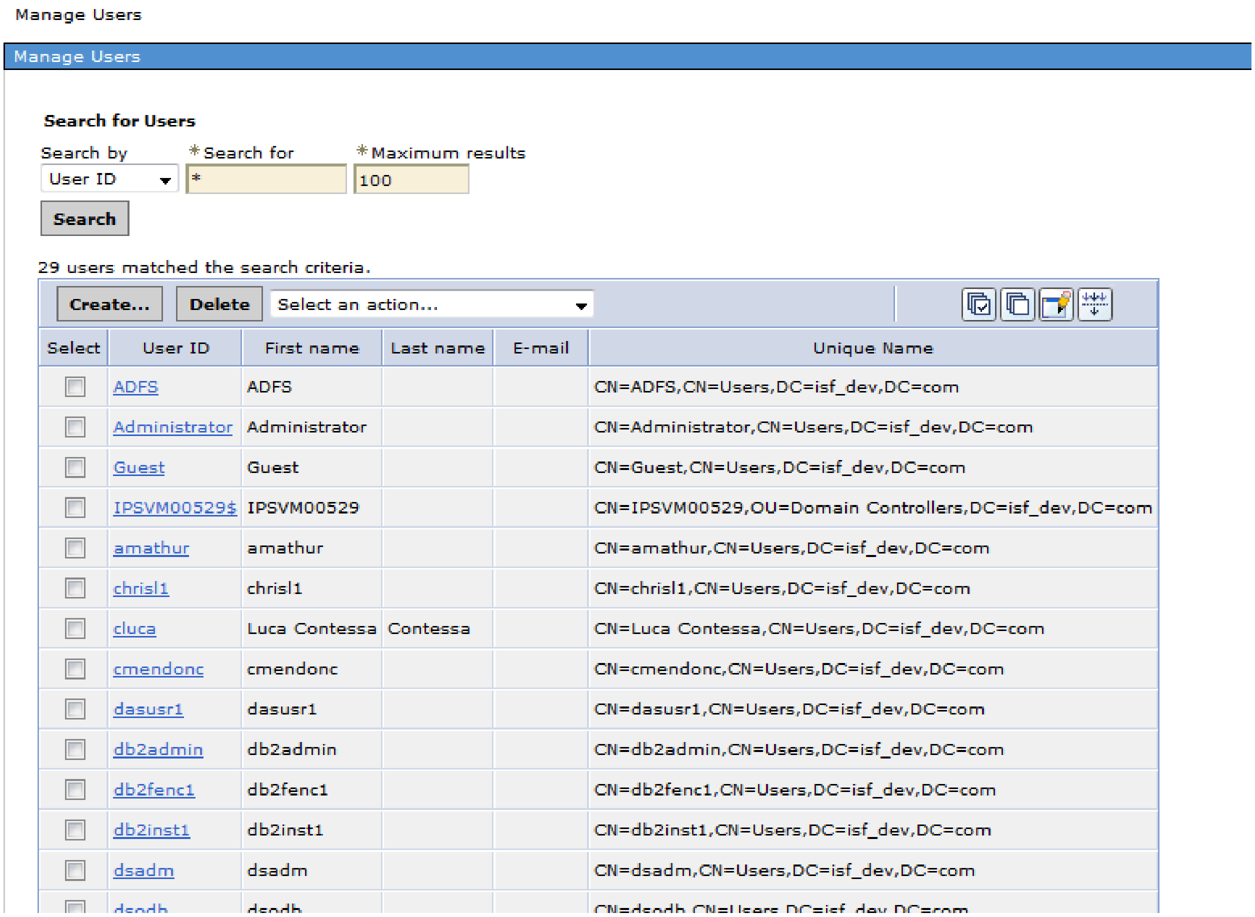
- Click 'Set as Current' on 'Secure administration, applications, and infrastructure'
- Restart the TFIM WAS.

```
/opt/IBM/FIM/ewas/profiles/itfimProfile/bin/stopServer.sh
/opt/IBM/FIM/ewas/profiles/itfimProfile/bin/startServer.sh
```

```
[root@kvm283-rh7 /]# cd /opt/IBM/FIM/ewas/profiles/itfimProfile/bin/
[root@kvm283-rh7 bin]# ./stopServer.sh server1
ADMU0116I: Tool information is being logged in file
           /opt/IBM/FIM/ewas/profiles/itfimProfile/logs/server1/stopServer.log
ADMU0128I: Starting tool with the itfimProfile profile
ADMU3100I: Reading configuration for server: server1
Realm/Cell Name: <default>
Username: fimadmin
```

```
    Password:
    ADMU3201I: Server stop request issued. Waiting for stop status.
    ADMU4000I: Server server1 stop completed.

    [root@kvm283-rh7 bin]# ./startServer.sh server1
    ADMU0116I: Tool information is being logged in file
              /opt/IBM/FIM/ewas/profiles/itfimProfile/logs/server1/startServer.log
    ADMU0128I: Starting tool with the itfimProfile profile
    ADMU3100I: Reading configuration for server: server1
    ADMU3200I: Server launched. Waiting for initialization status.
ADMU3000I: Server server1 open for e-business; process id is 9935
```

- Login to TFIM console. The list of Users now uses the LDAP registry:



Manage Users

Manage Users

Search for Users

Search by: User ID

* Search for: *

* Maximum results: 100

Search

29 users matched the search criteria.

Select	User ID	First name	Last name	E-mail	Unique Name
□	ADFS	ADFS			CN=ADFS,CN=Users,DC=isf_dev,DC=com
□	Administrator	Administrator			CN=Administrator,CN=Users,DC=isf_dev,DC=com
□	Guest	Guest			CN=Guest,CN=Users,DC=isf_dev,DC=com
□	IPSVM00529$	IPSVM00529			CN=IPSVM00529,OU=Domain Controllers,DC=isf_dev,DC=com
□	amathur	amathur			CN=amathur,CN=Users,DC=isf_dev,DC=com
□	chrisl1	chrisl1			CN=chrisl1,CN=Users,DC=isf_dev,DC=com
□	cluca	Luca Contessa	Contessa		CN=Luca Contessa,CN=Users,DC=isf_dev,DC=com
□	cmendonc	cmendonc			CN=cmendonc,CN=Users,DC=isf_dev,DC=com
□	dasusr1	dasusr1			CN=dasusr1,CN=Users,DC=isf_dev,DC=com
□	db2admin	db2admin			CN=db2admin,CN=Users,DC=isf_dev,DC=com
□	db2fenc1	db2fenc1			CN=db2fenc1,CN=Users,DC=isf_dev,DC=com
□	db2inst1	db2inst1			CN=db2inst1,CN=Users,DC=isf_dev,DC=com
□	dsadm	dsadm			CN=dsadm,CN=Users,DC=isf_dev,DC=com
□	dsodb	dsodb			CN=dsodb,CN=Users,DC=isf_dev,DC=com

3. Adding single sign-on users

N/A. Users already exist.

4. Adding administrative users

N/A. Admin user already exists.

5. Configuring user registry for embedded WebSphere

N/A. Already done previously.

6. Configuring an SSL connection to the user registry

This step is optional.

7. Customizing the login form

Customization of the login form pages is optional.

Manage Federations

Establishing a SAML federation

Complete the following tasks to configure your federation:

1. Gathering your federation configuration information
2. Creating your role in the federation
3. Providing guidance to your partner
4. Obtaining federation configuration data from your partner
5. Adding your partner
6. Providing federation properties to your partner

1. Gathering your federation configuration information

The Federation wizard prompts you for information that is used in your federation. Before starting the wizard, prepare for the configuration process by gathering your configuration information using the appropriate worksheet.

SAML 2.0 identity provider worksheet

If you will be the identity provider in the federation and will use SAML 2.0, record your configuration information in the following tables. An example of values follows:

Field	**Value**	**Notes**
Federation name	TFIM	'-' and '_' not allowed characters in name
Role	Identity Provider	
Company name, Company URL, and contact name and information.		
Federation Protocol	SAML 2.0	
Point of contact server URL	https://kvm283-rh7.swg.usma.ibm.com:9443	
SAML 2.0 profile options	Basic	
Select Signing Key	Defaults	
Select which outgoing messages and assertions you will sign	Defaults	
Select Signing Key	Defaults	
Encryption Key		
Message Options: - Message Lifetime in seconds - Artifact Lifetime in second - Session Timeout	Defaults	
Require Consent to Federate	Do not require consent to federate. (Check box is not selected.)	
SOAP Endpoint	https://kvm283-rh7.swg.usma.ibm.com:8880/sps/TFIM/saml20/soap	
Amount of time before the issue date that an assertion is considered valid	Default	
Amount of time the assertion is valid after being issued	Default	
Identity mapping options	XSLT file	When it asked to import the XSLT file, copy and imported file from **/opt/IBM/FIM/examples/mapping_rules/ip_saml_20.xsl**

2. Creating your role in the federation

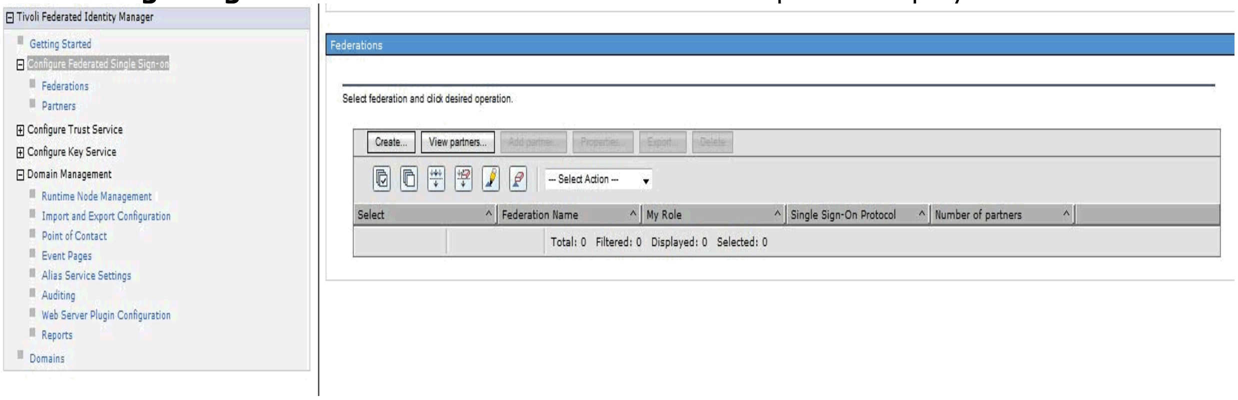
Use the console to create a federation. To begin, the Federation Wizard prompts you to supply the necessary information about your role in the federation.

Note: During the configuration, you may be asked to restart WebSphere Application Server. Make sure the server has restarted completely before continuing with the task.

3. Providing guidance to your partner

To create a federation:

1. Log in to the console and click **Tivoli Federated Identity Manager** → **Configure Federated Single Sign-on** → **Federations**. The Federations portlet displays several action buttons



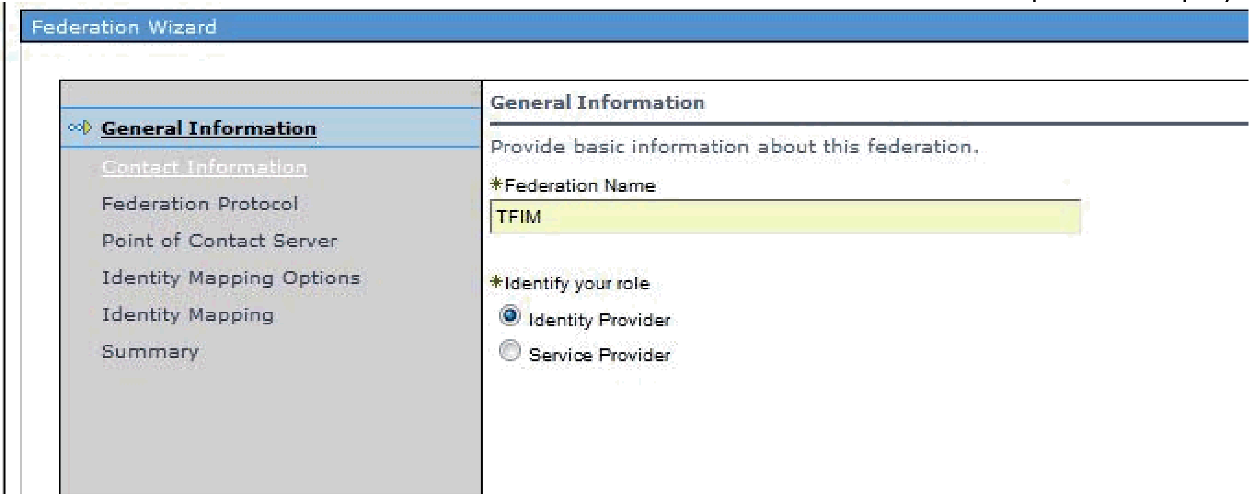
⊟ Tivoli Federated Identity Manager
- Getting Started
- ⊟ Configure Federated Single Sign-on
  - Federations
  - Partners
- ⊞ Configure Trust Service
- ⊞ Configure Key Service
- ⊟ Domain Management
  - Runtime Node Management
  - Import and Export Configuration
  - Point of Contact
  - Event Pages
  - Alias Service Settings
  - Auditing
  - Web Server Plugin Configuration
  - Reports
- Domains

Federations

Select federation and click desired operation.

Select	Federation Name	My Role	Single Sign-On Protocol	Number of partners
	Total: 0 Filtered: 0 Displayed: 0 Selected: 0			

2. Click **Create**. The Federation Wizard starts. The General Information panel is displayed.



Federation Wizard

General Information

Provide basic information about this federation.

*Federation Name

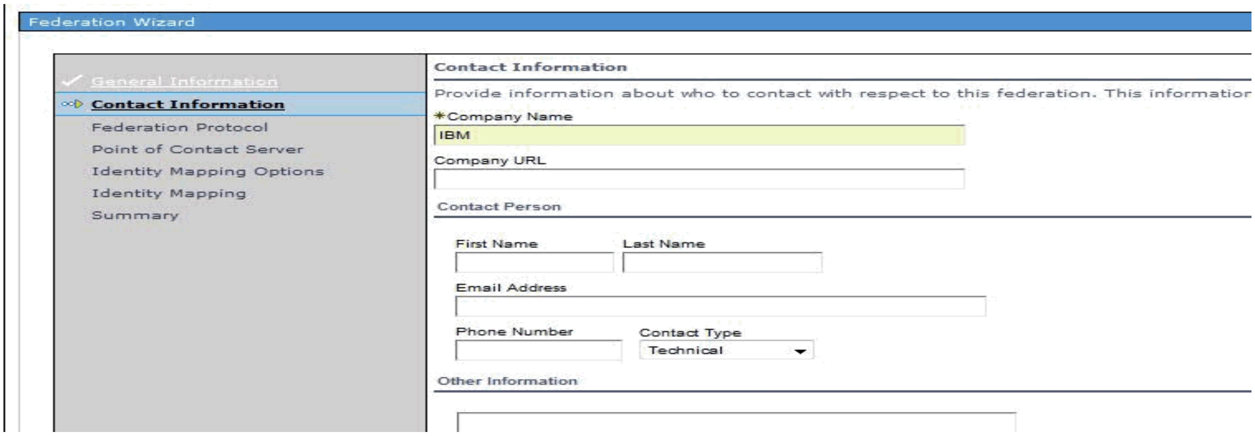
TFIM

*Identify your role

● Identity Provider

○ Service Provider

3. Use your worksheet to complete the panels that are displayed by the Federation wizard. Use your completed worksheet as a guide for completing the fields that are displayed. If you need to go back to a previous panel, click **Back**. If you want to end the configuration, click **Cancel**. Otherwise, click **Next** after you complete each panel.



Federation Wizard

Contact Information

Provide information about who to contact with respect to this federation. This informatio

*Company Name

IBM

Company URL

Contact Person

First Name

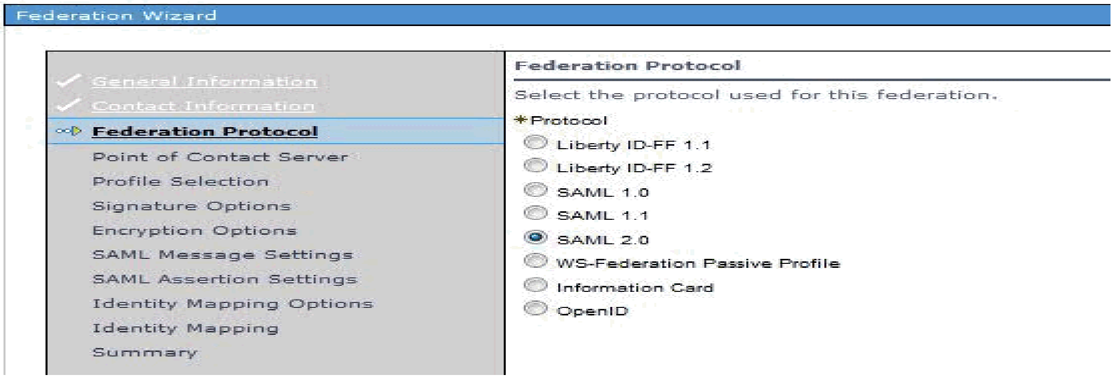
Last Name

Email Address

Phone Number

Contact Type: Technical

Other Information

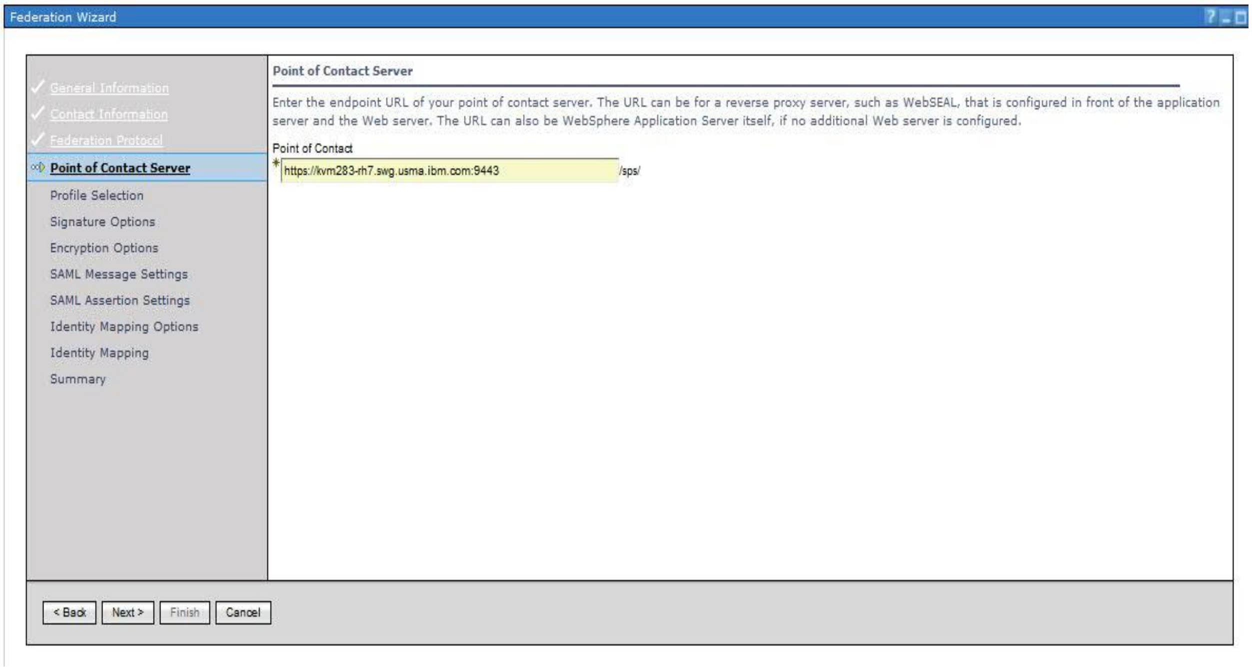


Federation Protocol

Select the protocol used for this federation.

* Protocol

○ Liberty ID-FF 1.1
○ Liberty ID-FF 1.2
○ SAML 1.0
○ SAML 1.1
● SAML 2.0
○ WS-Federation Passive Profile
○ Information Card
○ OpenID

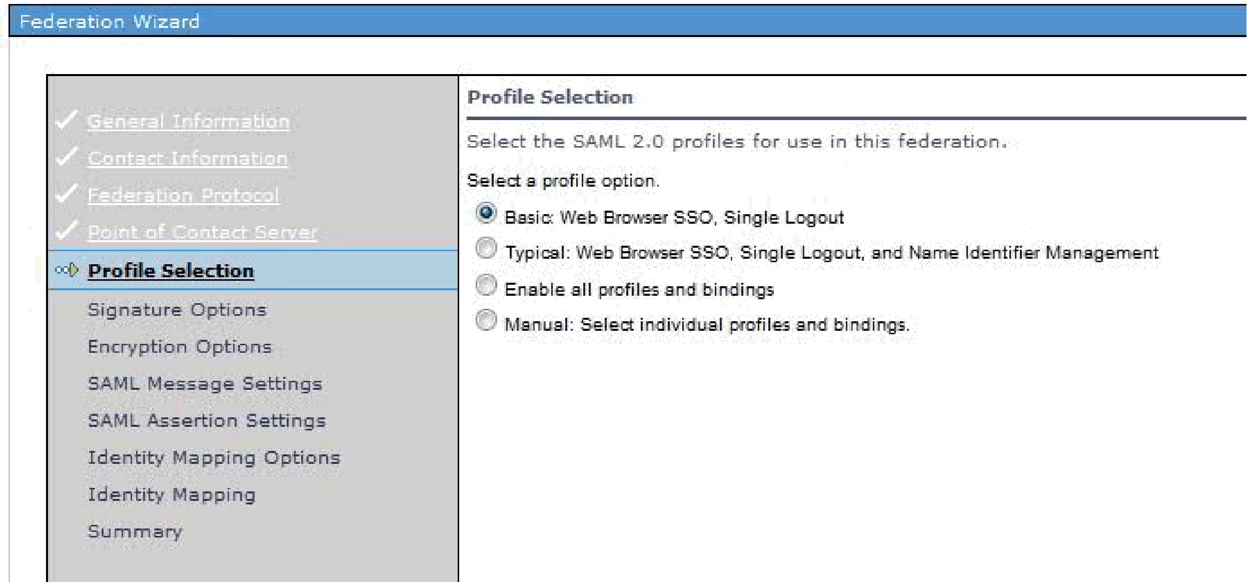


Point of Contact Server

Enter the endpoint URL of your point of contact server. The URL can be for a reverse proxy server, such as WebSEAL, that is configured in front of the application server and the Web server. The URL can also be WebSphere Application Server itself, if no additional Web server is configured.

Point of Contact

* https://kvm283-rh7.swg.usma.ibm.com:9443 /sps/

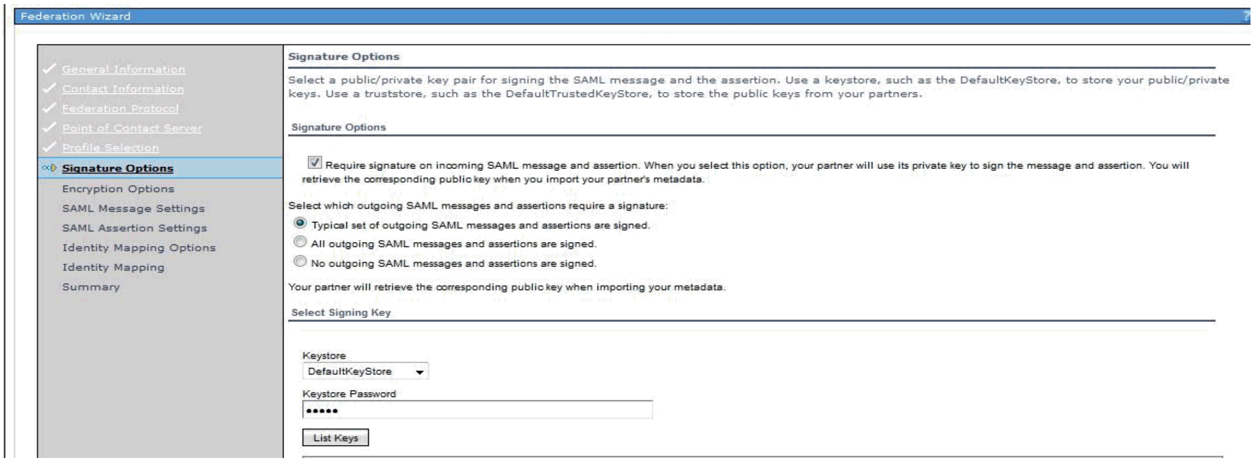


Profile Selection

Select the SAML 2.0 profiles for use in this federation.

Select a profile option.

● Basic: Web Browser SSO, Single Logout
○ Typical: Web Browser SSO, Single Logout, and Name Identifier Management
○ Enable all profiles and bindings
○ Manual: Select individual profiles and bindings.



Signature Options

Select a public/private key pair for signing the SAML message and the assertion. Use a keystore, such as the DefaultKeyStore, to store your public/private keys. Use a truststore, such as the DefaultTrustedKeyStore, to store the public keys from your partners.

Signature Options

☑ Require signature on incoming SAML message and assertion. When you select this option, your partner will use its private key to sign the message and assertion. You will retrieve the corresponding public key when you import your partner's metadata.

Select which outgoing SAML messages and assertions require a signature:

● Typical set of outgoing SAML messages and assertions are signed.

○ All outgoing SAML messages and assertions are signed.

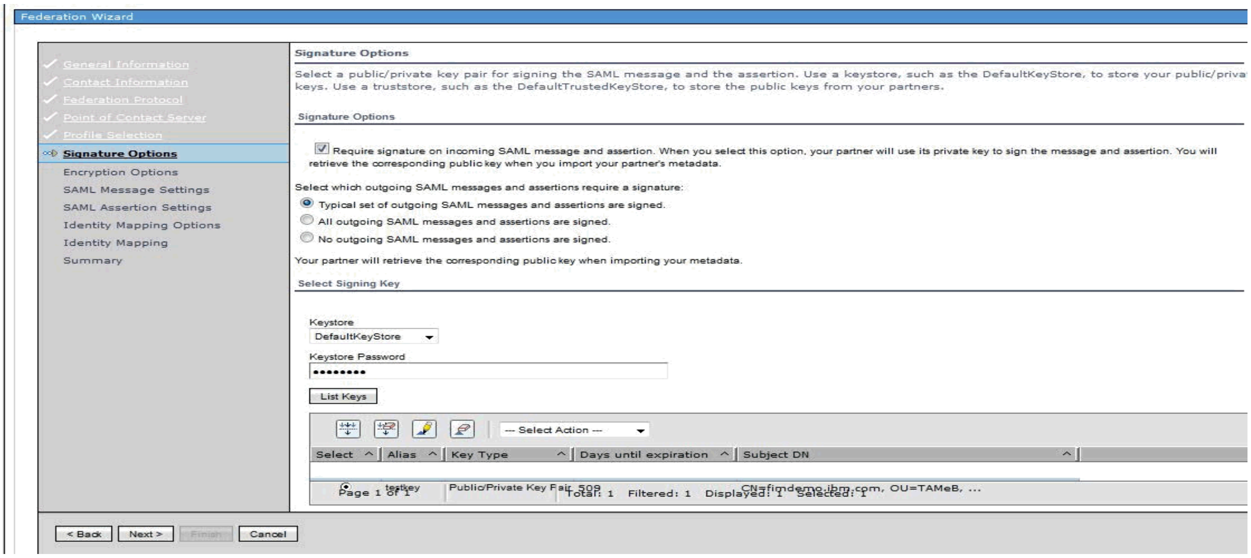
○ No outgoing SAML messages and assertions are signed.

Your partner will retrieve the corresponding public key when importing your metadata.

Select Signing Key

Keystore: DefaultKeyStore

Keystore Password: •••••



Signature Options

Select a public/private key pair for signing the SAML message and the assertion. Use a keystore, such as the DefaultKeyStore, to store your public/priva keys. Use a truststore, such as the DefaultTrustedKeyStore, to store the public keys from your partners.

Signature Options

☑ Require signature on incoming SAML message and assertion. When you select this option, your partner will use its private key to sign the message and assertion. You will retrieve the corresponding public key when you import your partner's metadata.

Select which outgoing SAML messages and assertions require a signature:

● Typical set of outgoing SAML messages and assertions are signed.

○ All outgoing SAML messages and assertions are signed.

○ No outgoing SAML messages and assertions are signed.

Your partner will retrieve the corresponding public key when importing your metadata.

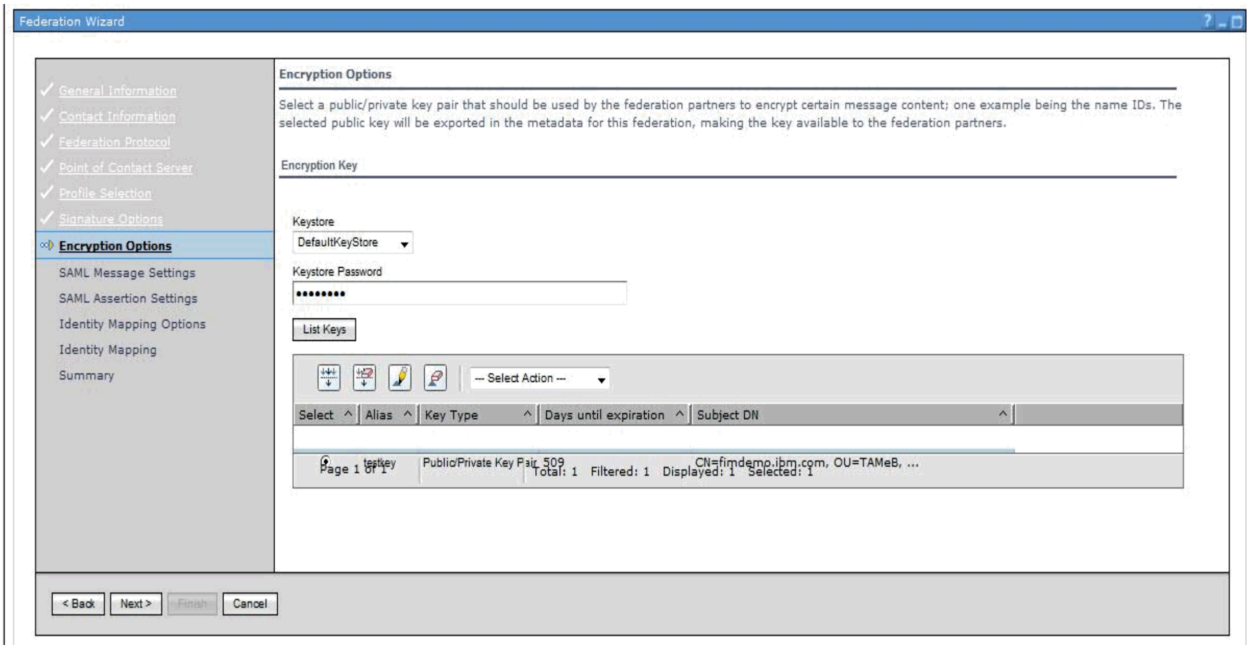
Select Signing Key

Keystore: DefaultKeyStore

Keystore Password: ••••••••

Select	Alias	Key Type	Days until expiration	Subject DN
●	testkey	Public/Private Key Pair 509		CN=fimdemo.ibm.com, OU=TAMeB, ...

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 1



Encryption Options

Select a public/private key pair that should be used by the federation partners to encrypt certain message content; one example being the name IDs. The selected public key will be exported in the metadata for this federation, making the key available to the federation partners.

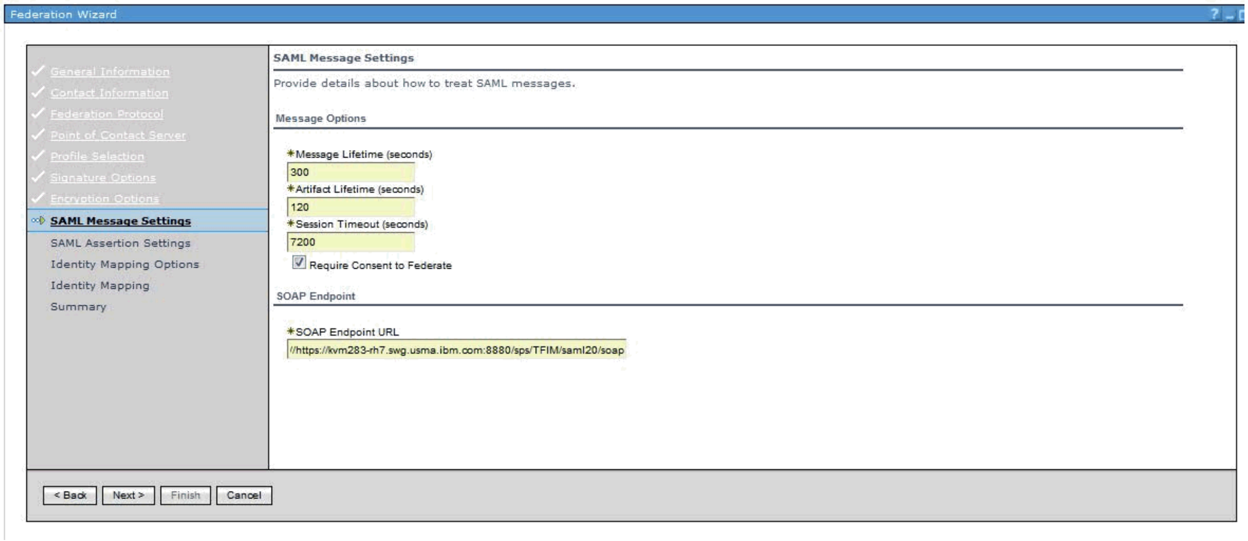
Encryption Key

Keystore: DefaultKeyStore

Keystore Password: ••••••••

Select	Alias	Key Type	Days until expiration	Subject DN
●	testkey	Public/Private Key Pair 509		CN=fimdemo.ibm.com, OU=TAMeB, ...

Page 1 of 1 Total: 1 Filtered: 1 Displayed: 1 Selected: 1



SAML Message Settings

Provide details about how to treat SAML messages.

Message Options

*Message Lifetime (seconds): 300

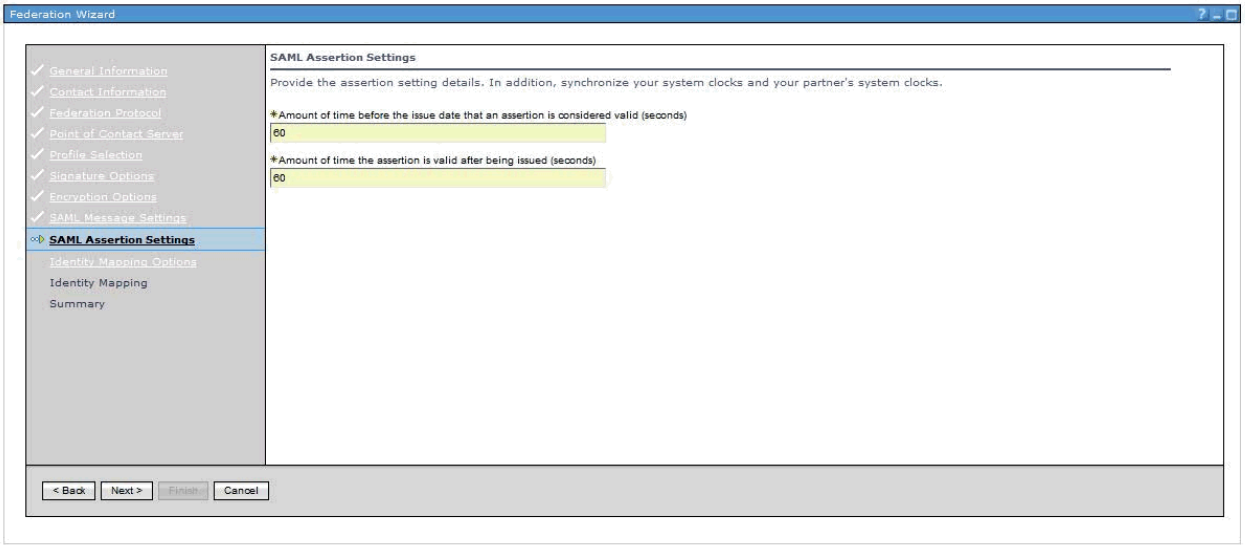
*Artifact Lifetime (seconds): 120

*Session Timeout (seconds): 7200

☑ Require Consent to Federate

SOAP Endpoint

*SOAP Endpoint URL: //https://kvm283-rh7.swg.usma.ibm.com:8880/sps/TFIM/saml20/soap

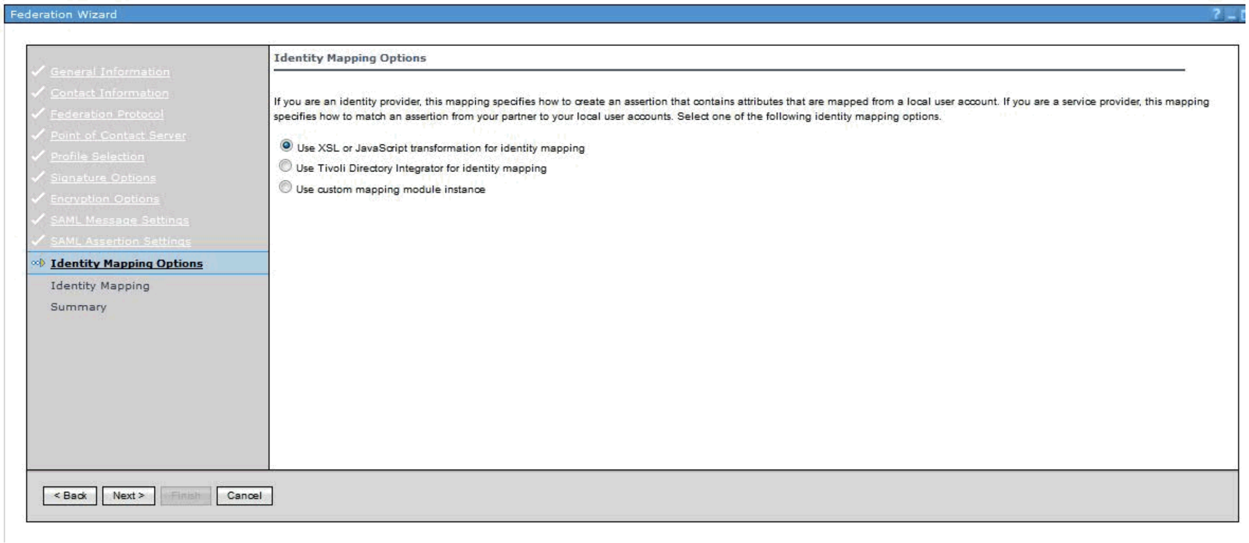


SAML Assertion Settings

Provide the assertion setting details. In addition, synchronize your system clocks and your partner's system clocks.

*Amount of time before the issue date that an assertion is considered valid (seconds): 60

*Amount of time the assertion is valid after being issued (seconds): 60



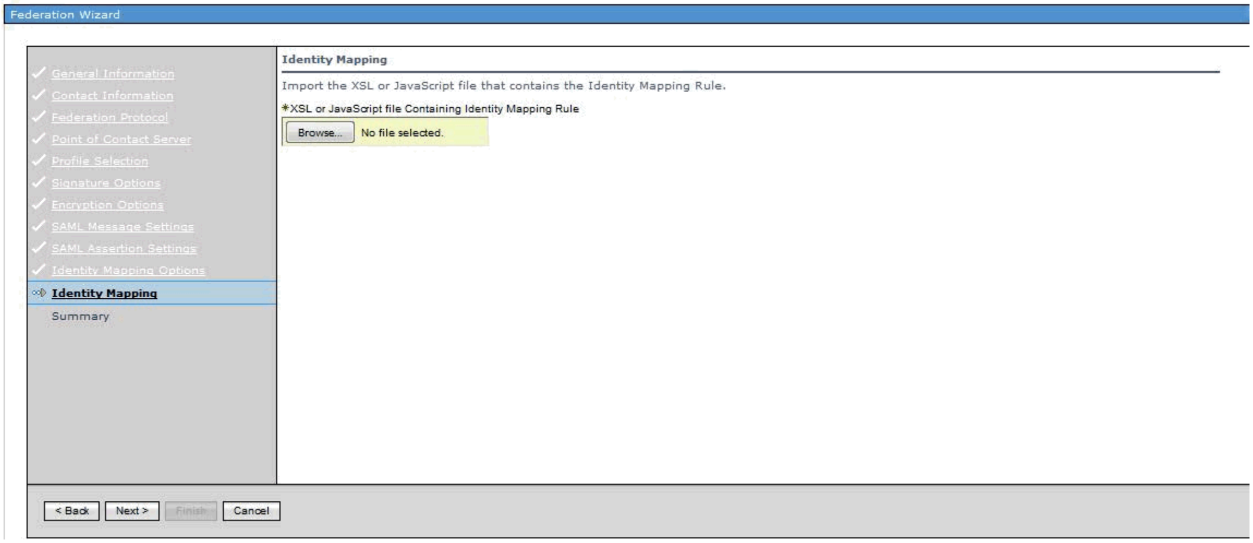
Identity Mapping Options

If you are an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If you are a service provider, this mapping specifies how to match an assertion from your partner to your local user accounts. Select one of the following identity mapping options.

● Use XSL or JavaScript transformation for identity mapping

○ Use Tivoli Directory Integrator for identity mapping

○ Use custom mapping module instance

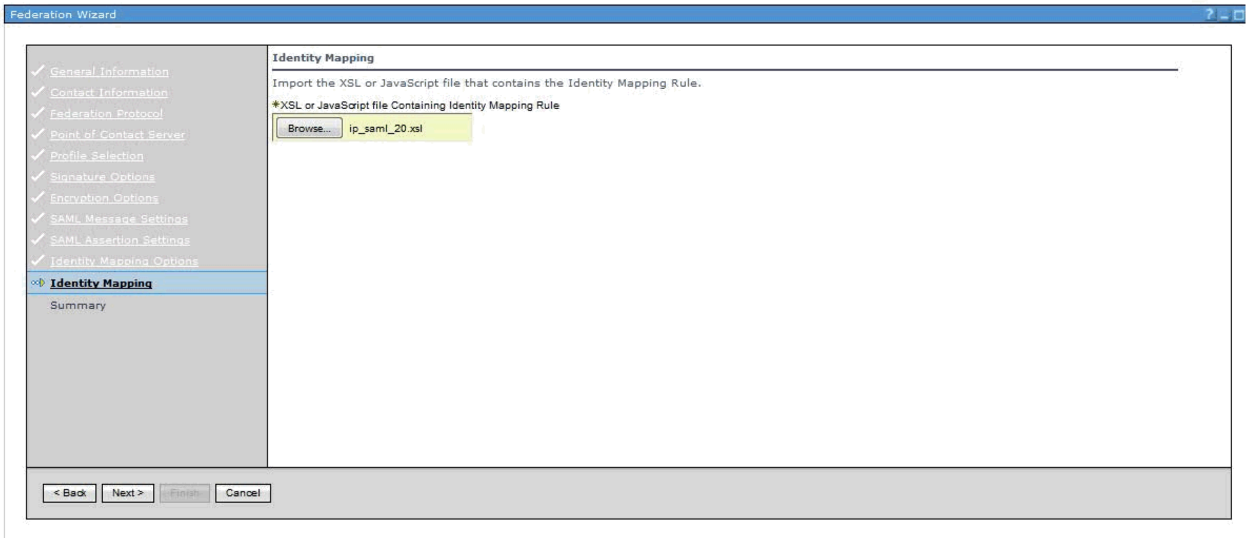


Identity Mapping

Import the XSL or JavaScript file that contains the Identity Mapping Rule.

*XSL or JavaScript file Containing Identity Mapping Rule

Browse... No file selected.



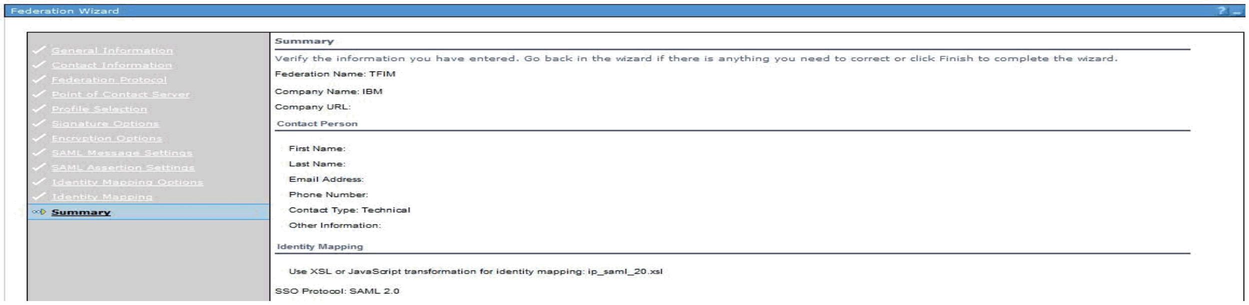
Identity Mapping

Import the XSL or JavaScript file that contains the Identity Mapping Rule.

*XSL or JavaScript file Containing Identity Mapping Rule

Browse... ip_saml_20.xsl

4. When you have completed all configuration panels, the Summary panel is displayed. Verify that the configuration settings are correct and click **Finish**. The Create Federation Complete portlet is displayed.



Summary

Verify the information you have entered. Go back in the wizard if there is anything you need to correct or click Finish to complete the wizard.

Federation Name: TFIM

Company Name: IBM

Company URL:

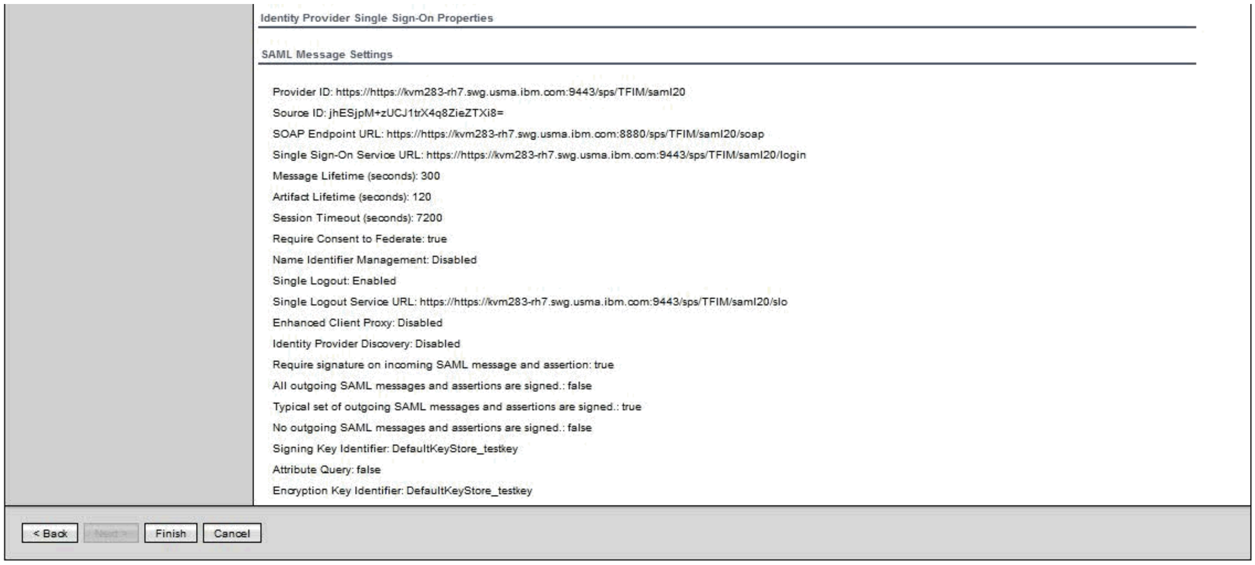
Contact Person

First Name:
Last Name:
Email Address:
Phone Number:
Contact Type: Technical
Other Information:

Identity Mapping

Use XSL or JavaScript transformation for identity mapping: ip_saml_20.xsl

SSO Protocol: SAML 2.0



Identity Provider Single Sign-On Properties

SAML Message Settings

Provider ID: https://https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20

Source ID: jhESjpM+zUCJ1trX4q8ZieZTXi8=

SOAP Endpoint URL: https://https://kvm283-rh7.swg.usma.ibm.com:8880/sps/TFIM/saml20/soap

Single Sign-On Service URL: https://https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20/login

Message Lifetime (seconds): 300

Artifact Lifetime (seconds): 120

Session Timeout (seconds): 7200

Require Consent to Federate: true

Name Identifier Management: Disabled

Single Logout: Enabled

Single Logout Service URL: https://https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20/slo

Enhanced Client Proxy: Disabled

Identity Provider Discovery: Disabled

Require signature on incoming SAML message and assertion: true

All outgoing SAML messages and assertions are signed.: false

Typical set of outgoing SAML messages and assertions are signed.: true

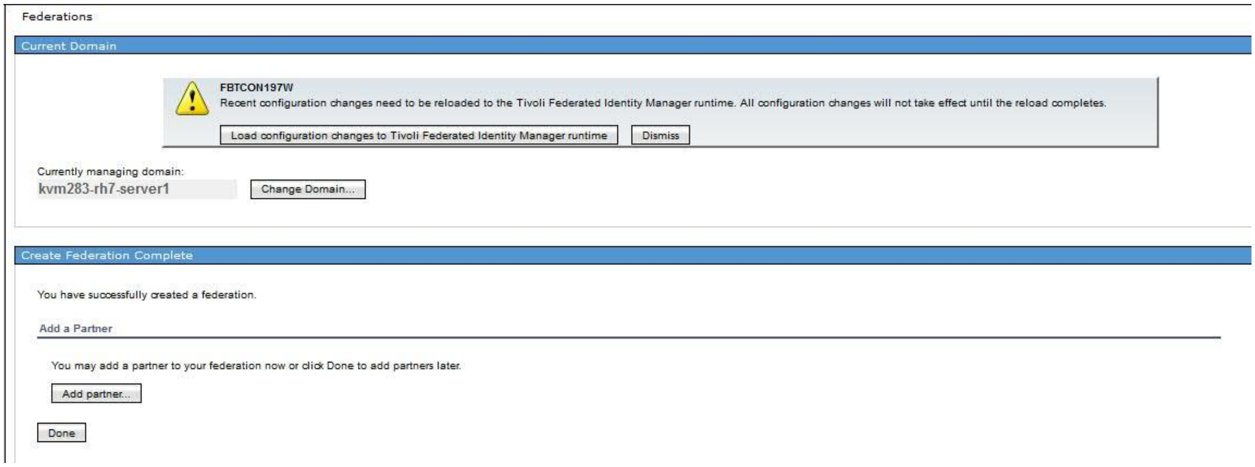
No outgoing SAML messages and assertions are signed.: false

Signing Key Identifier: DefaultKeyStore_testkey

Attribute Query: false

Encryption Key Identifier: DefaultKeyStore_testkey

< Back
Next >
Finish
Cancel



Federations

Current Domain

FBTCON197W
Recent configuration changes need to be reloaded to the Tivoli Federated Identity Manager runtime. All configuration changes will not take effect until the reload completes.

Load configuration changes to Tivoli Federated Identity Manager runtime
Dismiss

Currently managing domain:
kvm283-rh7-server1

Create Federation Complete

You have successfully created a federation.

Add a Partner

You may add a partner to your federation now or click Done to add partners later.

5. Add your partner now or later.

   - Click **Add partner** to start the Partner Wizard and add your partner's configuration using the steps described below.

4. Obtaining federation configuration data from your partner

You must obtain configuration information from your partner before you can add that partner to a federation.

Here the partner is WebSphere SAML TAI. The SAML TAI data can be obtained as below.

```
[root@kvm283-rh7 /]# cd /opt/IBM/WebSphere/AppServer/profiles/InfoSphere/bin
[root@kvm283-rh7 bin]# ./wsadmin.sh -lang jython
Realm/Cell Name: <default>
Username: wasadmin
Password:
WASX7209I: Connected to process "server1" on node kvm283-rh7Node01 using SOAP
connector;  The type of process is: UnManagedProcess
WASX7031I: For help, enter: "print Help.help()"
```

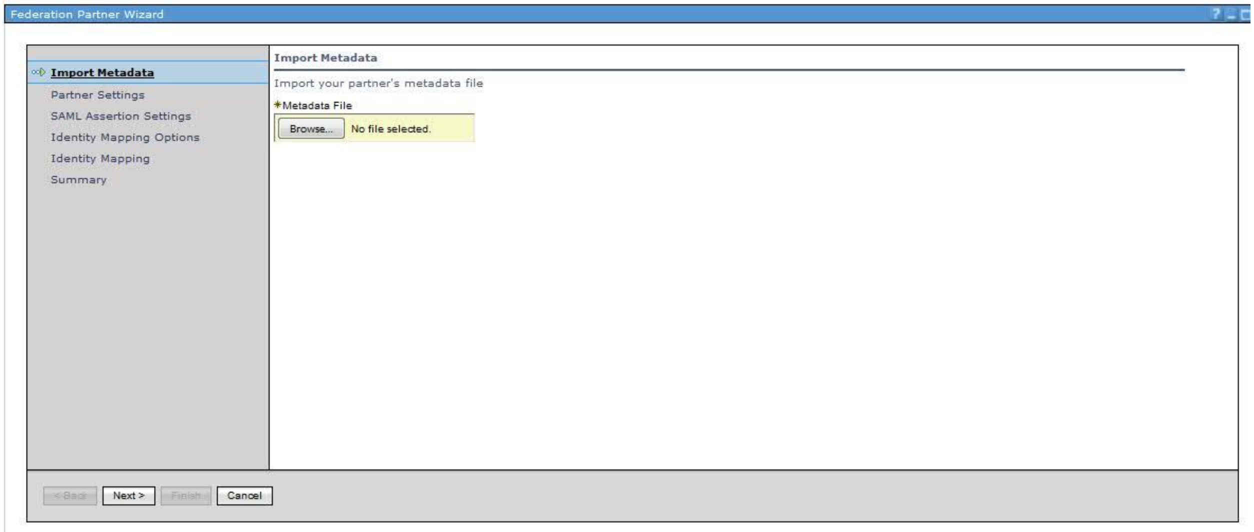
```
wsadmin>AdminTask.exportSAMLSpMetadata('-spMetadataFileName /opt/IBM/spdata.xml -
ssoId 1')
'true'
wsadmin>quit
```

That produced file /opt/IBM/spdata.xml with the metadata TFIM needed on the SAML TAI Service Provider.

5. Adding your partner

Follow these steps:

1. Make sure you have gathered the partner information as described in the worksheets. For example, if you are using a metadata file from your partner, copy the file to an easily accessible location on your computer.
   For instance, copy the spdata.xml file to your local Windows system, as that's where the TFIM partner creation wizard looks for it. So that the metadata import is successful.



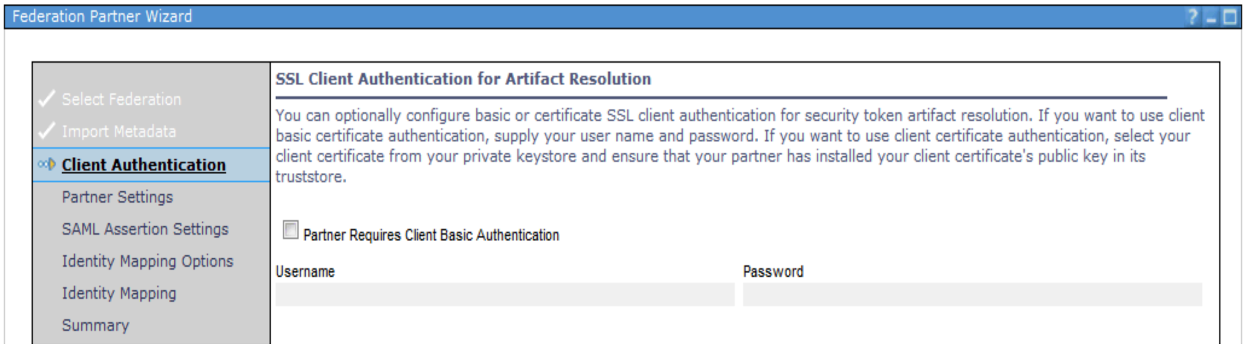
Import Metadata

Import your partner's metadata file

*Metadata File

Browse... No file selected.

2. Client Authentication is optional, leave blank if not needed:



SSL Client Authentication for Artifact Resolution

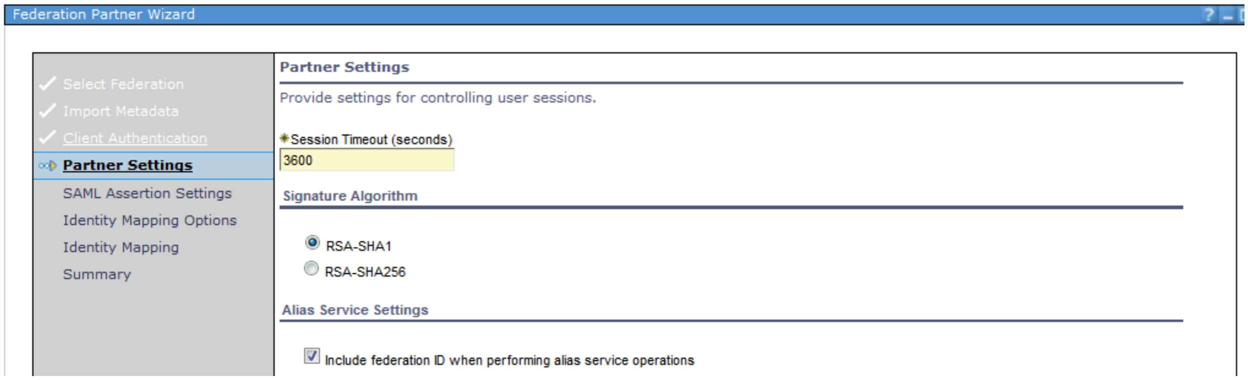
You can optionally configure basic or certificate SSL client authentication for security token artifact resolution. If you want to use client basic certificate authentication, supply your user name and password. If you want to use client certificate authentication, select your client certificate from your private keystore and ensure that your partner has installed your client certificate's public key in its truststore.

□ Partner Requires Client Basic Authentication

Username

Password

3. Partner Settings, leave defaults:



Partner Settings

Provide settings for controlling user sessions.

*Session Timeout (seconds)
3600

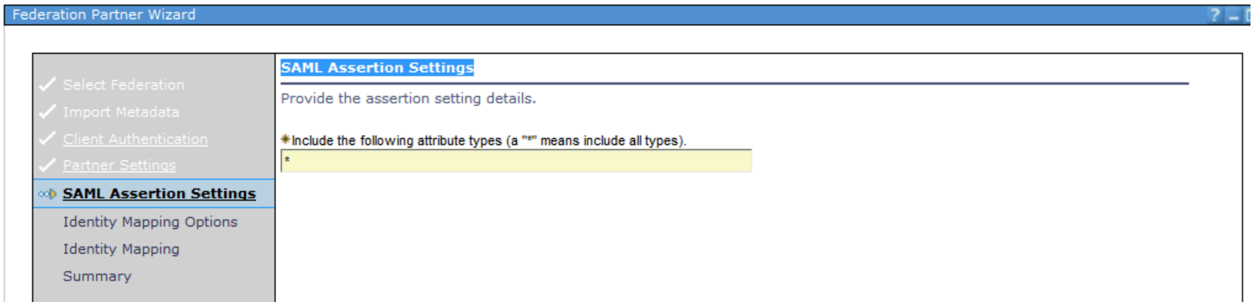
Signature Algorithm

● RSA-SHA1
○ RSA-SHA256

Alias Service Settings

☑ Include federation ID when performing alias service operations

4. SAML Assertion Settings: use default values:

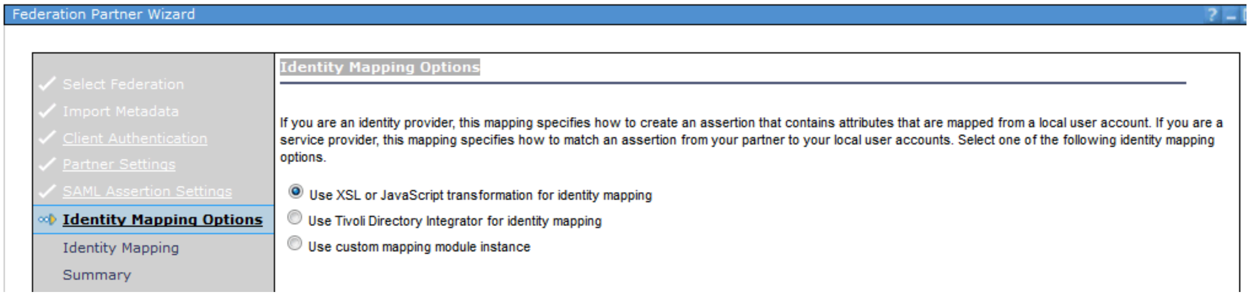


SAML Assertion Settings

Provide the assertion setting details.

Include the following attribute types (a "" means include all types).
*

5. Identity Mapping Options: use default values:

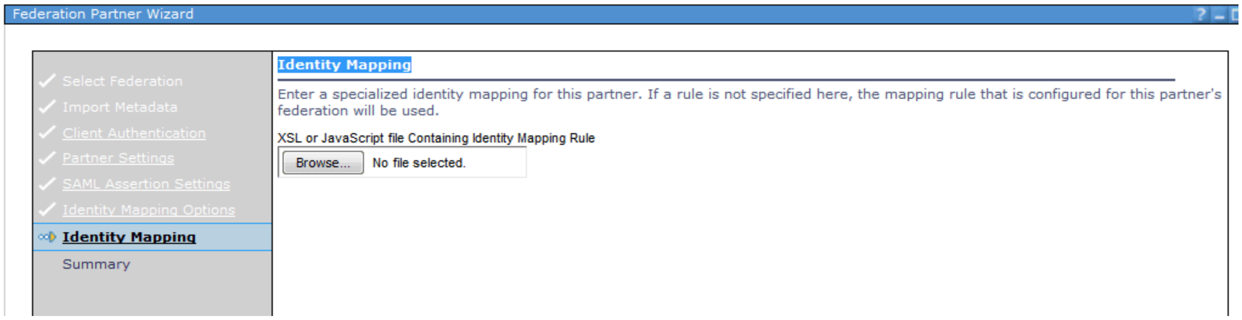


Identity Mapping Options

If you are an identity provider, this mapping specifies how to create an assertion that contains attributes that are mapped from a local user account. If you are a service provider, this mapping specifies how to match an assertion from your partner to your local user accounts. Select one of the following identity mapping options.

● Use XSL or JavaScript transformation for identity mapping
○ Use Tivoli Directory Integrator for identity mapping
○ Use custom mapping module instance

6. Identity Mapping: leave blank. It will use the rule(s) you setup in the Federation itself:

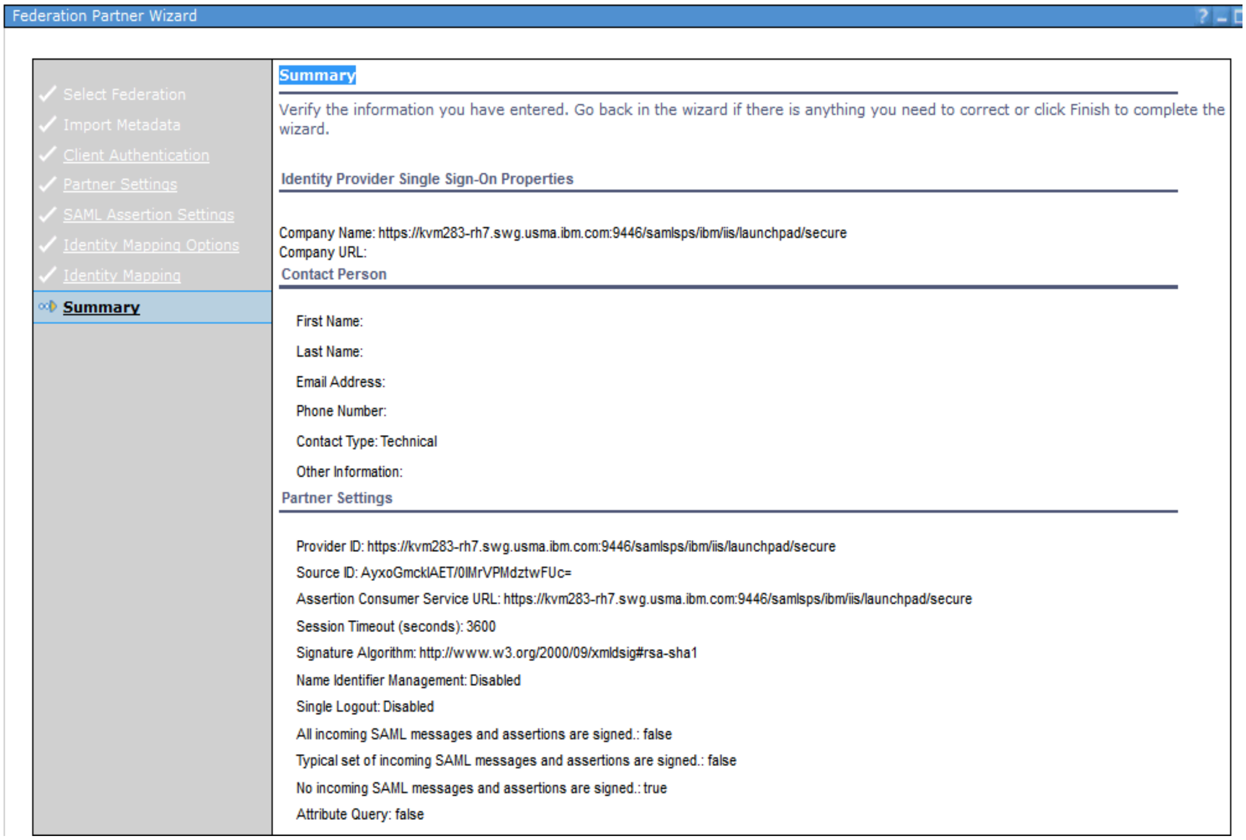


Identity Mapping

Enter a specialized identity mapping for this partner. If a rule is not specified here, the mapping rule that is configured for this partner's federation will be used.

XSL or JavaScript file Containing Identity Mapping Rule
Browse... No file selected.

7. Summary:



Summary

Verify the information you have entered. Go back in the wizard if there is anything you need to correct or click Finish to complete the wizard.

Identity Provider Single Sign-On Properties

Company Name: https://kvm283-rh7.swg.usma.ibm.com:9446/samlsps/ibm/iis/launchpad/secure
Company URL:

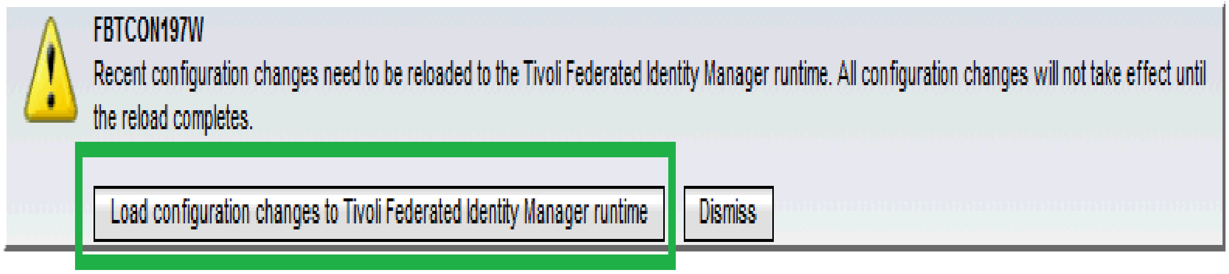
Contact Person

First Name:
Last Name:
Email Address:
Phone Number:
Contact Type: Technical
Other Information:

Partner Settings

Provider ID: https://kvm283-rh7.swg.usma.ibm.com:9446/samlsps/ibm/iis/launchpad/secure
Source ID: AyxoGmcklAET/0IMrVPMdztwFUc=
Assertion Consumer Service URL: https://kvm283-rh7.swg.usma.ibm.com:9446/samlsps/ibm/iis/launchpad/secure
Session Timeout (seconds): 3600
Signature Algorithm: http://www.w3.org/2000/09/xmldsig#rsa-sha1
Name Identifier Management: Disabled
Single Logout: Disabled
All incoming SAML messages and assertions are signed.: false
Typical set of incoming SAML messages and assertions are signed.: false
No incoming SAML messages and assertions are signed.: true
Attribute Query: false

8. Click ‘Finish’.
9. Click ‘Enable Partner’.
10. Click ‘Load config…’.



FBTCON197W
Recent configuration changes need to be reloaded to the Tivoli Federated Identity Manager runtime. All configuration changes will not take effect until the reload completes.

Load configuration changes to Tivoli Federated Identity Manager runtime
Dismiss

6. Providing federation properties to your partner:

When your partner wants to add you as a partner to their federation configuration, you must provide your partner with the necessary information.

The steps differ according to whether you provide a metadata file or provide the information manually.

- **Metadata file method**

  If your partner can import your data, you can use the metadata file method with either SAML 1.x or SAML 2.0 federation.

1. Use the console to generate a metadata file that contains the necessary federation configuration and a key for validating response message signatures, if you require validation of the signatures. Follow the instructions in "Exporting federation properties."
2. You may also need to provide your partner with the appropriate keys and certificates for your role and SAML standard in the federation.

Exporting federation properties

When you want to join a partner's federation, you must supply your federation configuration properties. You can export your federation properties to a file and share them with your partner.

1. Log in to the console and click **Tivoli Federated Identity Manager → Configure Federated Single Sign-on → Federations**.

2. The Federations panel is displayed. Select a federation from the table.

3. Click **Export**. The browser displays a message window that prompts you to save the file containing the exported data. Click **OK.** The browser download window prompts for a location where to save the file.

4. Select a directory and metadata file name and click **Save**. Metadata file names have the following syntax:

   *federationname_companyname*_metadata.xml

   For example, for a federation named *TFIM* and a company named *IBM*, the metadata file would be named:

   *TFIM_IBM*_metadata.xml

   Place the file in an easily accessible location. You will need to provide this file to your partner, when your partner wants to import configuration information for the federation.

Chapter 3: WAS SAML TAI (Service Provider)

Overview of installation and configuration

IBM WebSphere Application Server — and stack products running on top of a WebSphere Application Server platform — has had a customizable authentication framework since V5.1 based on the **Trust Association Interceptor (TAI)** interface. There are multiple product implementations of this interface. In 2012, the WebSphere Application Server full profile edition shipped a new **Security Assertion Markup Language (SAML)** TAI that is available on WebSphere Application Server versions 7.0, 8.0 and 8.5.

The actors involved are:

- **Identity Provider (IdP)**
- **Service Provider (SP)** sometime known as the Relying Party, or RP.

The job of the IdP is to authenticate the end user (exactly how the IdP does this is immaterial), and to produce some assertions or claims about the user. These assertions are digitally signed by the IdP. The SAML specification defines the format of these assertions. The SP receives the assertions and, if the SP is satisfied that the assertions came from a trusted IdP, logs the user in based upon some parts of the assertion.

The WebSphere SAML TAI does not truly support a Service Provider (SP) initiated authentication path. For a SP initiated authentication, the SP generates a SAML Request which it sends to the SAML IdP. Essentially the user accesses the protected URI without an LTPA token, the SAML TAI intercepts, the TAI doesn't find a SAML token and the TAI error page is triggered. The SAML TAI configuration however specifies the IdP login page in the TAI error page property (e.g. sso_1.sp.login.error.page). This URL is therefore invoked. The IdP URL points back to the SAML TAI via another URL specified as a RelayState parameter. And that RelayState parameter URL itself contains a RelayState parameter that points at the post authentication target URL.

The mentioned steps are depicted in Figure 1 below:

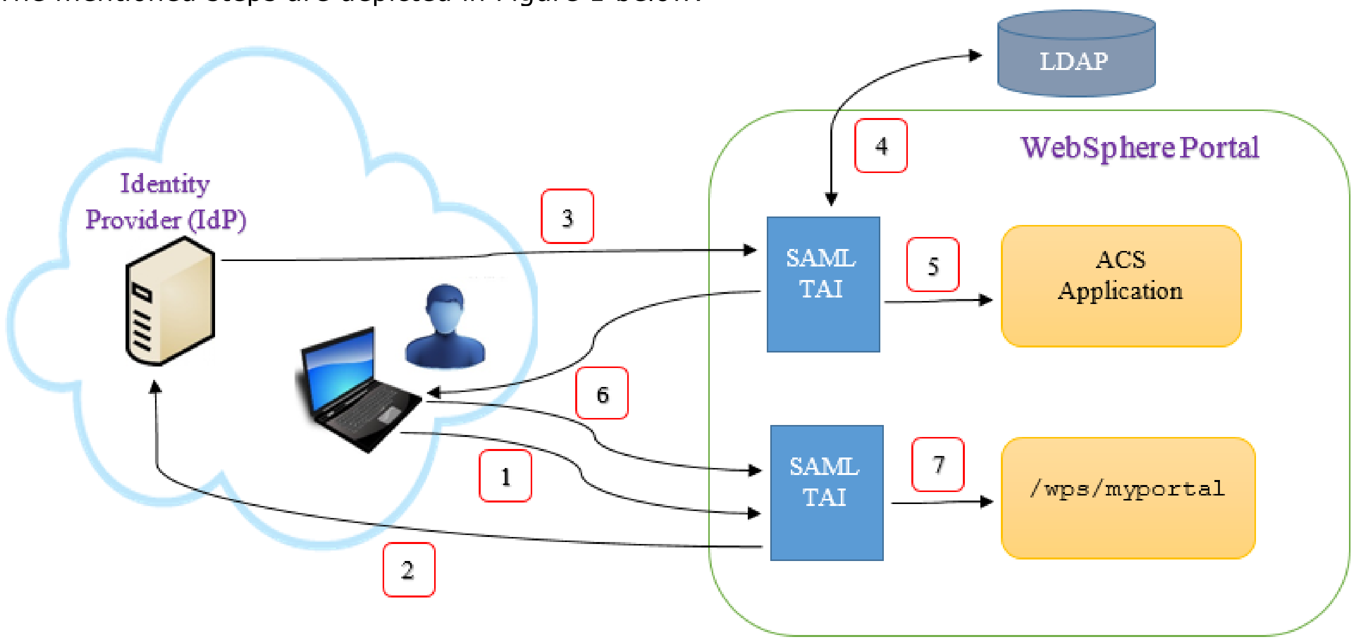


Figure 1.

1. The user starts the process by following a link to the application’s URL at the SP. For example, this would be https://portal.uac.com/wps/myportal.
2. The SAML TAI is called twice. Because this URL is not the ACS, the TAI does not initially intercept the request. The Web Inbound configuration looks for a LtpaToken2 cookie. None is found. The SAML TAI is called a second time. Based on some data in the incoming request and the TAI configuration, the TAI returns an HTTP 302 redirects to the correct IdP. A cookie is set by the TAI. This is set to the value of the **original referrer URL**, which in this example is https://portal.uac.com/wps/myportal. As discussed above, the user authenticates to the IdP.
3. Based on configuration in the IdP and the original URL provided to the IdP, a SAML response is created and sent via an HTTP Post redirect to an Assertion Consumer Service (ACS) in the SP. This SAML response is signed by the IdP.
4. The SAML TAI consumes the SAML response and logs the user in. In this example, the user identity exists in the UAC LDAP. Know, however, that this is not a requirement for SAML Web SSO. A JAAS subject is created in memory, and various WebSphere Application Server security tokens are created, including an SSOToken, which is also known as the LtpaToken2. From this SSOToken, a LtpaToken2 cookie is created.
5. With the user logged in, the request is dispatched to the ACS. It is an application whose sole purpose is to redirect the user to the correct landing page after being logged in by the SAML TAI. The ACS has a Java™ EE security constraint defined, in order to cause the WebSphere Application Server container security and the SAML TAI to be called. An ACS application is shipped as part of the support for the SAML TAI.
6. The ACS redirects the user to the landing page for the application (possibly based upon something in request, or possibly based on configuration). In this example, this URL is: https://portal.uac.com/wps/myportal. This HTTP redirection includes the new LtpaToken2 cookie. The browser follows the redirection and resends the LtpaToken2.
7. The SAML TAI is called again, this time to check if there is a SAML response in the request. There is not, but there is a LtpaToken2 cookie, so the standard Web Inbound login configuration processing occurs

Installation

Before you can use the SAML Web SSO feature, you must:

1. **Install the SAML Assertion Consumer Service (ACS) application on the IIS application server.** This server will be referenced by the URLs specified on the `sso_.sp.acsUrl` SAML TAI custom properties.
2. **Enable the SAML TAI**

For both steps, follow the instructions in the WebSphere Knowledge Center article on installing and enabling the WAS SAML TAI "Enabling your system to use the SAML web single sign-on (SSO) feature" here: http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/twbs_enablesamlsso.html

Make sure to have installed the SAML ACS Application (in step 1. above) before continuing.

To enable the SAML TAI (step 2.), you can use either the `wsadmin` command utility or the WAS administrative console. If enabling SAML TAI using the WAS administrative console:

a. Log on to the WebSphere Application Server administrative console.
b. If your WAS ND environment is not clustered:

- Click **Security->Global security**.
- Expand Web and SIP security and click **Trust association**.

c. If your WAS ND environment is clustered:

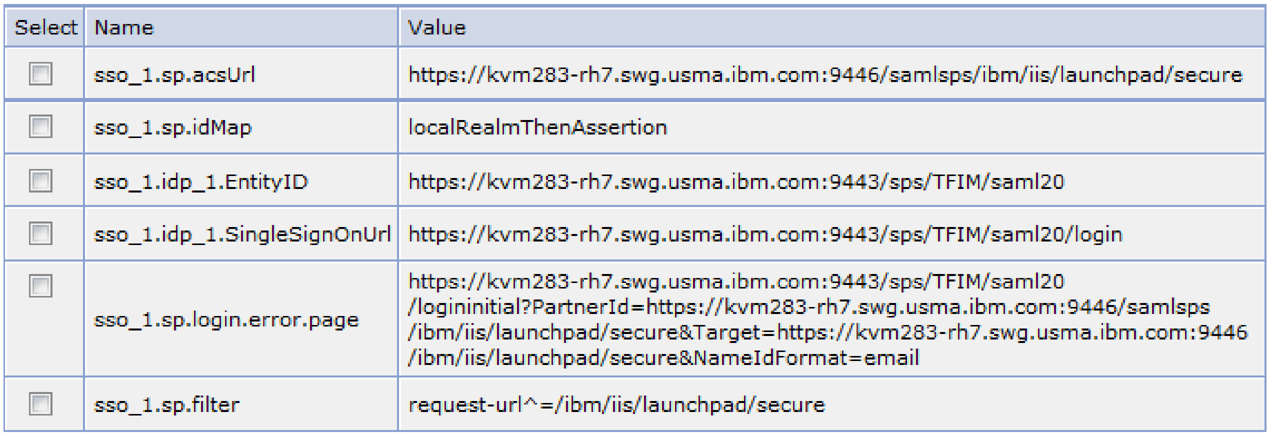
- Click **Security->Security domains -> IBM_Information_Server_sd.**
- Click and expand **Trust association**. Select Customize for this domain

d. Select the **Enable trust association** check box and click **Interceptors**.
e. Click New and enter `com.ibm.ws.security.web.saml.ACSTrustAssociationInterceptor` in the Interceptor class name field.
f. Do not remove the existing interceptor `com.ibm.iis.isf.j2ee.impl.was.security.WASTrustAssociationInterceptor2`. This interceptor is created by the IIS installation, and is used by ISF for trusted session management.
g. Under Custom properties of the new interceptor, provide the following custom property information:

NAME	VALUE
sso_1.sp.acsUrl	https://**<ACSServer:port>**/samlsps/ibm/iis/launchpad/secure
sso_1.sp.idMap	localRealmThenAssertion
sso_1.idp_1.EntityID	http://**<IdPDomain:port>**/sps/TFIM/saml20
sso_1.idp_1.SingleSignOnUrl	https://**<IdPDomain:port>**/sps/TFIM/saml20/login
sso_1.sp.login.error.page	https://**<IdPDomain:port>**/sps/TFIM/saml20/logininitial?PartnerId=https://**<ACSServer:port>**/samlsps/ibm/iis/launchpad/secure&Target=https://**<ACS-SERVER:port>**/ibm/iis/launchpad/secure&NameIdFormat=email
sso_1.sp.filter	request-url^=/ibm/iis/launchpad/secure

Some fields in the example above contain the <ACS-SERVER:port> placeholder. Modify the server name and port with the ones from your IIS installation, that is, the host name of the system where WebSphere Application Server and IIS are installed and the Web server SSL port number (WC_defaulthost_secure).

An example of the SAML TAI properties follows:



Select	Name	Value
□	sso_1.sp.acsUrl	https://kvm283-rh7.swg.usma.ibm.com:9446/samlsps/ibm/iis/launchpad/secure
□	sso_1.sp.idMap	localRealmThenAssertion
□	sso_1.idp_1.EntityID	https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20
□	sso_1.idp_1.SingleSignOnUrl	https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20/login
□	sso_1.sp.login.error.page	https://kvm283-rh7.swg.usma.ibm.com:9443/sps/TFIM/saml20/logininitial?PartnerId=https://kvm283-rh7.swg.usma.ibm.com:9446/samlsps/ibm/iis/launchpad/secure&Target=https://kvm283-rh7.swg.usma.ibm.com:9446/ibm/iis/launchpad/secure&NameIdFormat=email
□	sso_1.sp.filter	request-url^=/ibm/iis/launchpad/secure

Changing the landing URL page after a successful TFIM login

The default configuration described in this document uses the IIS Secure Launchpad application as the target location after a successful login to TFIM. To change the landing URL where users are forwarded after a successful TFIM login, follow these instructions. This example uses the IIS Information Governance Catalog (IGC) application as the new landing page.

1. Modify the SAML TAI property `sso_1.sp.login.error.page`.
   It should contain the new Target application, like for example:

   https://<IdPDomain:port>/sps/TFIM/saml20/logininitial?PartnerId=https://<ACSServer:port>/samlsps/ibm/iis/launchpad/secure&Target=https://<ACS-SERVER:port>/ibm/iis/igc&NameIdFormat=email

2. Disable the cookie `'WasSamlSpReqURL'` containing the Secure Launchpad URL. By default, WAS and SAML provide this cookie in the request to the IdP, which forces TFIM to always redirect to the original requester (i.e. the Secure Launchpad), regardless how the `Target` flag has been configured. To remove the cookie `WasSamlSpReqURL`, create the following property in the SAML TAI configuration:

   `sso_1.sp.preserveRequestState` and set it `false`.

The example below highlights the modified SAML TAI properties:

NAME	VALUE
sso_1.sp.acsUrl	https://**<ACSServer:port>**/samlsps/ibm/iis/launchpad/secure
sso_1.sp.idMap	localRealmThenAssertion
sso_1.idp_1.EntityID	http://**<IdPDomain:port>**/sps/TFIM/saml20
sso_1.idp_1.SingleSignOnUrl	https://**<IdPDomain:port>**/sps/TFIM/saml20/login
sso_1.sp.login.error.page	https://<IdPDomain:port>/sps/TFIM/saml20/logininitial?PartnerId=https://<ACSServer:port>/samlsps/ibm/iis/launchpad/secure&Target=https://<ACS-SERVER:port>/ibm/iis/igc&NameIdFormat=email
sso_1.sp.filter	request-url^=/ibm/iis/launchpad/secure
sso_1.sp.preserveRequestState	false

3. By default, the IIS ISF framework checks for cross-site request forgery attacks, and will deny the forwarding to a URL other than the Secure Launchpad. ISF provides a IIS repository flag where you specify the list of allowed *Referer domain names* that will be ignored by the check for cross-site forgery attack.

   From the `<IIS_HOME>\ASBServer\bin` folder run the command:
   ```
   ./iisAdmin.sh -set -key com.ibm.iis.isf.security.AllowedRefererDomainNames
                 -value "<domain of the TFIM server>"
   ```
   for example:
   ```
   ./iisAdmin.sh -set -key com.ibm.iis.isf.security.AllowedRefererDomainNames
                 -value "IdPDomain.com"
   ```

   This TFIM domain is specified in the SAML TAI property `sso_1.sp.login.error.page (<IdPDomain>)`. Specify the root domain of TFIM. Do not use additional subdomains, as the domain will not be recognized by the cross-site request forgery attack test. For example, use "isf_dev.com" and not "fs.isf_dev.com".

   Should you receive an error in your WAS log indicating a "`Possible Cross-Site Request Forgery Attack`", this domain is found in the HTTP Referer Header, in the WAS error. For example, if the WAS error you are getting is:

   ```
   https://kvmrh7.ibm.com:9446/ibm/iis/igc HTTP Referer Header:
   https://fs.isf_dev.com/sps/TFIM/logininitial....
   Possible Cross-Site Request Forgery Attack.
   ```

   set the Registry key `com.ibm.iis.isf.security.AllowedRefererDomainNames` to `"isf_dev.com"`.

4. Make sure you leave the IIS registry keys as described in the InfoSphere Information Server Configuration chapter in this document:

   ```
   ./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
   com.ibm.iis.isf.security.SAMLSecureURL=/ibm/iis/launchpad/secure
   com.ibm.iis.isf.security.SAML=true
   ```

5. Restart WAS.

Chapter 4: InfoSphere Information Server Configuration

Requirements

IBM InfoSphere Information Server Version 11.5.0.1 or higher implements solutions for federated single sign-on for its web applications. However, you will also need to:

- Use of WebSphere ND version 8.5.5.5 or higher. Note that currently WebSphere Liberty (LWAS) does not support a SAML configuration and therefore cannot be used for this purpose.

- If using IIS version 11.5.0.1 GA, installation of the following patches is required:
    - ISF Patch JR57496
    - If you are using the Information Governance Catalog Console (IGC), installation of Governance Rollup 7 Patch, or higher, is also required

- If using IIS version 11.5.0.2 GA, or higher, no additional patches or fixes are necessary.

Configuration

There are two InfoSphere Information Server repository key-value pairs that are used to enable and activate the SAML configuration and provide the proper redirection to the configured IdP provider login page:

- `com.ibm.iis.isf.security.SAML`
- `com.ibm.iis.isf.security.SAMLSecureURL`

Setting `com.ibm.iis.isf.security.SAML` to 'true' will enable the SAML forwarding behavior. This basically allows the redirection of the un-authorized user to the configured SAML IdP login page.

The `com.ibm.iis.isf.security.SAMLSecureURL` is the URI where an un-authenticated user is redirected when trying to access a protected IIS application. Set this value to the IIS secure Launchpad URI (“`/ibm/iis/launchpad/secure`”). The URI contains the short address of the web application, and cannot contain server or port information.

To list the existing IIS Repository settings, use:

```
    cd /opt/IBM/InformationServer/ASBServer/bin
    ./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
```

To turn on SAML principal forwarding use:

```
    ./iisAdmin.sh -set –key com.ibm.iis.isf.security.SAML -value true
```

To change the URI for redirection after an IdP login:

```
    ./iisAdmin.sh -set -key com.ibm.iis.isf.security.SAMLSecureURL –value
"/ibm/iis/launchpad/secure"
```

To unset the URL and the SAML forwarding (e.g. turn off forwarding):

```
    ./iisAdmin.sh -unset -key com.ibm.iis.isf.security.SAMLSecureURL
    ./iisAdmin.sh -unset -key com.ibm.iis.isf.security.SAML
```

You will need to restart WAS for any of the above changes to take effect.

Chapter 5: LDAP Configuration

Overview of installation and configuration

You need to configure the LDAP access to Active Directory underlying the SAML IdP, either as a Federated Repository or Stand-alone LDAP Repository. Note that the SAML Assertion only provides identity information that InfoSphere Information Server can use for authentication. It does not provide other information needed for authorization, such as group memberships. So, even though the SAML Assertion can be configured to provide additional user info, the WAS SAML TAI cannot process such additional information at this time.

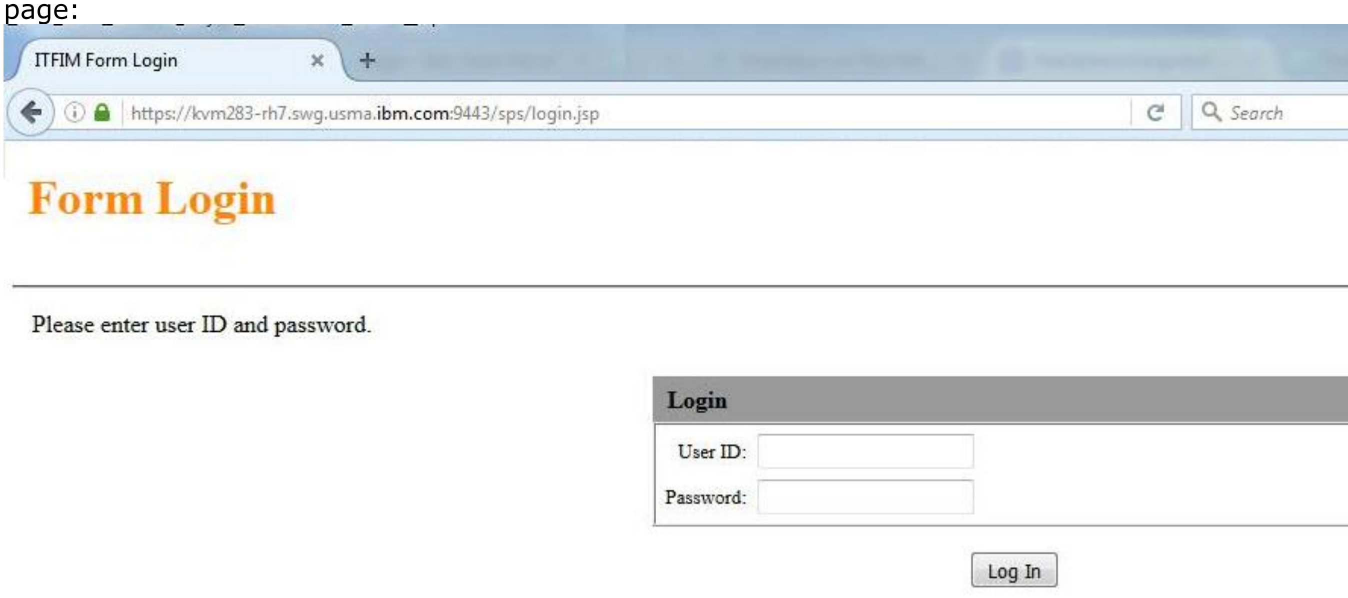
The SAML TAI provides a mapping between the authenticated user id and the LDAP user id (when the TAI idMap parm is set, e.g. sso_1.sp.idMap = localRealmThenAssertion). When this mapping takes place InfoSphere Information Server can obtain user authentication data via the SAML assertion, then obtain the needed and additional user information via LDAP.

Chapter 6: User scenarios and standard behavior

Once the system is completely configured and running, we expect the following scenarios and operations behavior:

Single Sign-On:

1. **Accessing the IIS Secure Launchpad:**
   Access the IIS Secure Launchpad via: https://<IISServer>:<port>/ibm/iis/launchpad/secure
   If not already authenticated via the configured IdP, user is redirected to the TFIM IdP Login page:



Form Login

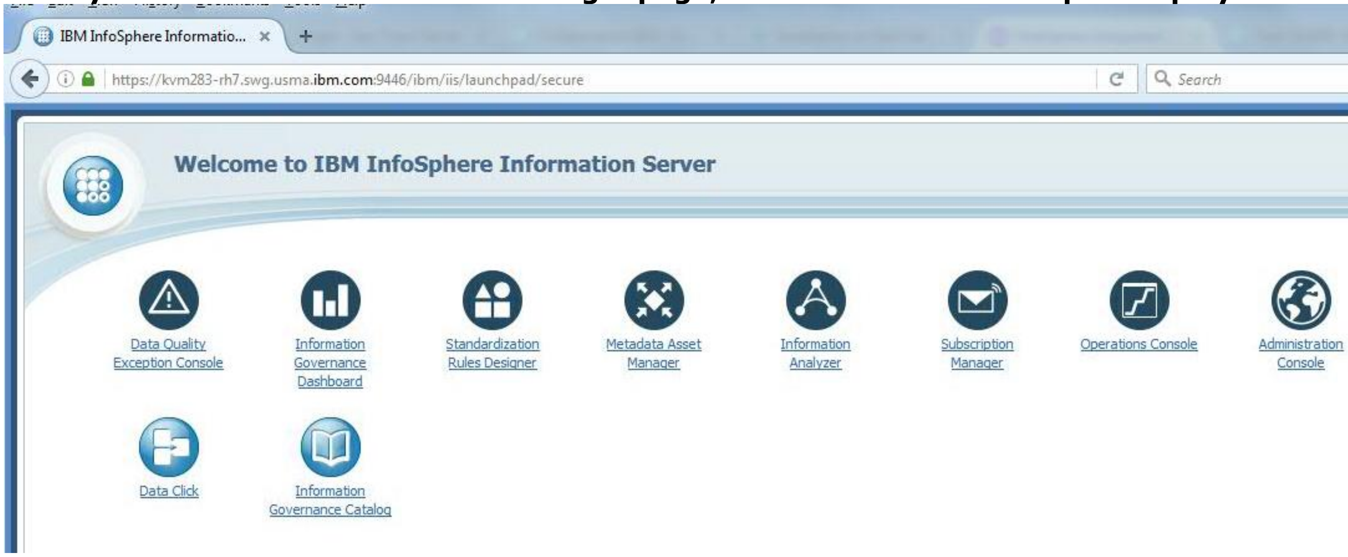
Please enter user ID and password.

Login

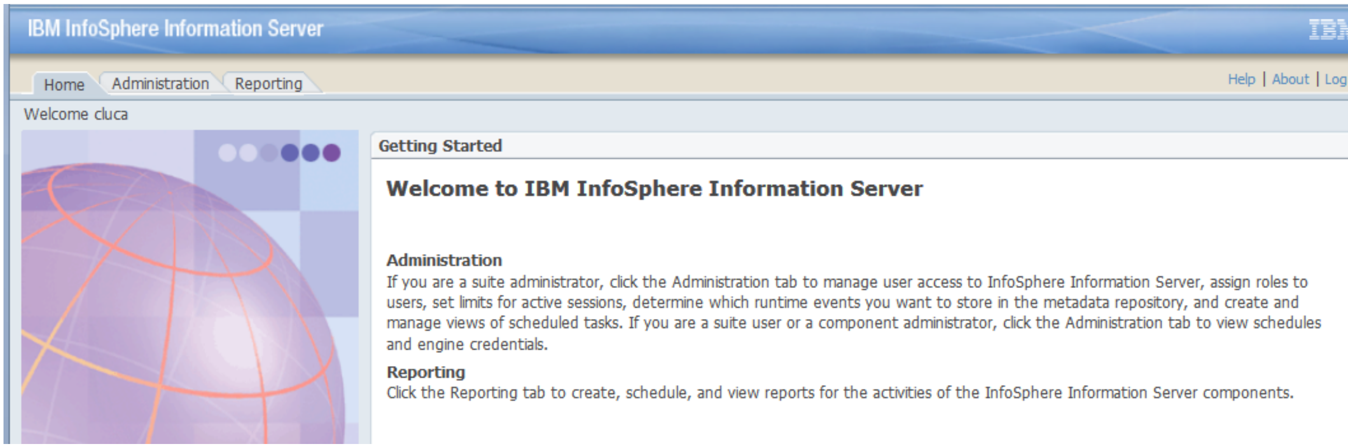
User ID:

Password:

2. **Once you authenticate via the TFIM Login page, the IIS Secure Launchpad displays**:


IBM InfoSphere Informatio...
https://kvm283-rh7.swg.usma.ibm.com:9446/ibm/iis/launchpad/secure
Search
Welcome to IBM InfoSphere Information Server
Data Quality Exception Console
Information Governance Dashboard
Standardization Rules Designer
Metadata Asset Manager
Information Analyzer
Subscription Manager
Operations Console
Administration Console
Data Click
Information Governance Catalog

3. **Once authenticated, invoke any of the IIS web applications** without a request for further authentication.



Welcome cluca

Getting Started

Welcome to IBM InfoSphere Information Server

Administration
If you are a suite administrator, click the Administration tab to manage user access to InfoSphere Information Server, assign roles to users, set limits for active sessions, determine which runtime events you want to store in the metadata repository, and create and manage views of scheduled tasks. If you are a suite user or a component administrator, click the Administration tab to view schedules and engine credentials.

Reporting
Click the Reporting tab to create, schedule, and view reports for the activities of the InfoSphere Information Server components.

Single Log Out (SLO):

1. Once the user has logged out from one of the IIS web applications, the active WAS LTPA token is invalidated and user is therefore logged out from all of the active IIS web applications running within instances of the same web browser type (Internet Explorer, FireFox, etc.).
2. Once logged out, the user is redirected to the SAML IdP login to renew the authentication.
3. Once a WAS LTPA token or the SAML token expires (via time-out), it cannot be used for any further interaction by any of the IIS web applications. The token expiration essentially acts as a logout for each of the active web applications. User is redirected to the IdP login page when this scenario occurs.

Chapter 7: Troubleshooting notes and issues

Unsupported Functions

IIS and the SAML configuration do not support the following functions and tasks:

- IIS trusted and system user authentication.
- IIS thick clients, like the IIS Windows Console
- IIS command line clients
- ISD Web Services as deployed by the IIS ISD Console.

Information Server 11.7.x web applications not supporting SAML SSO

In InfoSphere Information Server version 11.7.x, the following web applications do not recognize and adhere to the SAML 2.0 SSO login protocol. An explicit login to these applications is necessary even after an SSO login:

- Information Governance Catalog New
- Governance Monitor (New)
- Enterprise Search (New)

Known issues

Due to the different nature of the IIS applications, you may encounter the following behavior in particular situations:

- The IIS application Standardization Rules Designer (SRD), after a logout, does not return to the main SAML IdP login screen to renew the authentication, but shows its proprietary SRD login screen instead. However, the Single Log Out feature still functions correctly, as it invalidates the active WAS LTPA token.

  Solution: After a logout from the SRD application, when the SRD proprietary login screen shows, do not login onto the SRD application directly, but manually redirect your browser to the IIS Secure Launchpad via https://<IISServer>:<port>/ibm/iis/launchpad/secure or to your SAML IdP login screen to properly login with SSO via SAML.

- Within one instance of a browser, if you have multiple browser tabs open running different IIS applications, a logout from one application in one browser tab may not be immediately reflected in the applications running on other background tabs. Applications in these background tabs may show an error and may fail to automatically redirect you to the SAML IdP login screen.

  Solution: Refresh the browser window (F5 key) of these secondary tabs to redirect you to the SAML login screen.

- The WAS LTPA token or the SAML token may expire and a time-out will occur after the configured amount of time. This event produces the same behavior as a logout event, where the expired LTPA token is not valid any longer. When this happens, some IIS applications may report an error to the user. A similar error may occur when you have multiple browser tabs open with IIS applications running in them.

Solution: This behavior is expected, especially in the browser background tabs. Refresh the browser window (F5 key) of these secondary tabs to redirect you to the SAML login screen.

Troubleshooting notes

There following notes will help you avoid usual pitfalls and describe expected behavior when working with a SAML installation:

1. If you **set or reset the two InfoSphere Information Server repository key-value pairs**
   ```
    com.ibm.iis.isf.security.SAML
    com.ibm.iis.isf.security.SAMLSecureURL
   ```
   you need to restart WAS in order for the change in the repository keys to be acknowledged.

2. **Installing and Configuring the WebSphere SAML TAI** - Deploying the application using the ' installSamlACS.py' script
   You may find issues deploying the SAML TAI application, as in the following example:

   ```
   cd C:\IBM\WebSphere\AppServer\profiles\saml\bin
   C:\IBM\WebSphere\AppServer\profiles\saml\bin>wsadmin -f installSamlACS.py install
   ipsvm00529Node02 server1

    WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
   connector;  The type of process is: UnManagedProcess
    WASX7303I: The following options are passed to the scripting environment and are
   available as arguments that are stored in the argv variable: "[install,
   ipsvm00529Node02, server1]"
    WASX7011E: Cannot find file "installSamlACS.py"
   ```

   However, "installSamlACS.py" is in `C:\IBM\WebSphere\AppServer\bin`, not the profile bin. So, you need to run the command from the `AppServer\bin` dir:

   ```
   cd C:\IBM\WebSphere\AppServer\bin
   C:\IBM\WebSphere\AppServer\bin>wsadmin -f installSamlACS.py install ipsvm00529Node02
   server1

   WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
   connector;  The type of process is: UnManagedProcess
   WASX7303I: The following options are passed to the scripting environment and are
   available as arguments that are stored in the argv variable: "[install,
   ipsvm00529Node02, server1]"
   Installing Saml ACS service...
   Deploying WebSphereSamlSP.ear
   ADMA0073W: Custom permissions are found in the [("java.security.AllPermission" "<all
   permissions>" "<all actions>")] policy file. Custom permissions can compromise the
   integrity of Java 2 Security.
       WASX7327I: Contents of was.policy file:
              grant codeBase "file:${application}" {
              permission java.security.AllPermission;
             };
   ADMA5016I: Installation of WebSphereSamlSP started.
   ADMA5058I: Application and module versions are validated with versions of deployment
   ```

```
targets.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
ADMA5081I: The bootstrap address for client module is configured in the WebSphere
Application Server repository.
ADMA5053I: The library references for the installed optional package are created.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
ADMA5001I: The application binaries are saved in
C:\IBM\WebSphere\AppServer\profiles\saml\wstemp\Script15430e2fa33\workspace\cells\ips
vm00529Node02Cell\applications\WebSphereSamlSP.ear\WebSphereSamlSP.ear
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
SECJ0400I: Successfully updated the application WebSphereSamlSP with the
appContextIDForSecurity information.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
ADMA5005I: The application WebSphereSamlSP is configured in the WebSphere Application
Server repository.
ADMA5113I: Activation plan created successfully.
ADMA5011I: The cleanup of the temp directory for application WebSphereSamlSP is
complete.
ADMA5013I: Application WebSphereSamlSP installed successfully.
```

3. **Exporting the SAML TAI Service Provider metadata from a Windows WebSphere**
   When exporting the SAML TAI SP information from a Windows WebSphere system, you may run in some syntax issues:

```
cd C:\IBM\WebSphere\AppServer\profiles\saml\bin
C:\IBM\WebSphere\AppServer\profiles\saml\bin>wsadmin -lang jython

WASX7209I: Connected to process "server1" on node ipsvm00529Node02 using SOAP
connector;  The type of process is: UnManagedProcess
WASX7031I: For help, enter: "print Help.help()"
wsadmin>AdminTask.exportSAMLSpMetadata('-spMetadataFileName c:\tmp\spdata.xml -ssoId
1')
WASX7015E: Exception running command: "AdminTask.exportSAMLSpMetadata('-
spMetadataFileName c:\tmp\spdata.xml -ssoId 1')"; exception information:
com.ibm.websphere.management.cmdframework.CommandException: Unable to write c:
mp\spdata.xml
```

The Windows wsadmin command still needs the Unix style path information:

```
wsadmin>AdminTask.exportSAMLSpMetadata('-spMetadataFileName /tmp/spdata.xml -ssoId
1')
'true'
wsadmin>quit

C:\IBM\WebSphere\AppServer\profiles\saml\bin>dir C:\tmp\spdata.xml
 Volume in drive C has no label.
 Volume Serial Number is 5ED6-13CF
 Directory of C:\tmp
     04/19/2016  08:21 PM               694 spdata.xml
                    1 File(s)            694 bytes
```

4. **Information Server commands, operations, and web applications not working after configuration of SAML and SSO**
   If you are using IS 11.5.0.1 with the ISF 11.5 RUP4 patch installed, after configuration of SAML and SSO, some operations and functions may not work, as for example:
   - Invocation of the ASBAgent (node agent) NodeAgents.sh/bat reports error

- Utility command istool.sh/bat report errors
- Invocation of Information Server web applications, even after a validated Identity Provider login, redirects the user to the Identity Provider login screen, if the user does not have DataStage/QualityStage User and DataClick Author/User roles.

Solution: Install ISF Patch JR57496, as recommended in the Requirements paragraph in this document.

5. **Information Server web applications are not working with SSO when using IS 11.5.0.1 with Patch JR57496, or when using IIS 11.5.0.2**

You may encounter issues with the web applications behavior in SSO mode, if you have IIS 11.5.0.1 and Patch JR57496, or IIS 11.5.0.2. For example:

- IA and DataClick icons are not displayed in the secure launchpad screen
- You are unable to launch any web clients from the secure launchpad, if the user has only Suite User and IGC User roles.
- After successful login to the IdP, attempt to launch any web application redirects the browser to the IdP login page.

Solution: Verify the existing IIS Repository settings, using:

```
    cd /opt/IBM/InformationServer/ASBServer/bin
    ./iisAdmin.sh -display -key com.ibm.iis.isf.security.SAML*
```

Make sure you have both registry keys defined:
`com.ibm.iis.isf.security.SAML` has value `true`
`com.ibm.iis.isf.security.SAMLSecureURL` has a value, like `"/ibm/iis/launchpad/secure"`

To turn on SAML principal forwarding use:

```
    ./iisAdmin.sh -set -key com.ibm.iis.isf.security.SAML -value true
```

To change the default URI for redirecting an un-authenticated user:

```
    ./iisAdmin.sh -set -key com.ibm.iis.isf.security.SAMLSecureURL -value
"/ibm/iis/launchpad/secure"
```

Note that the URL specified for `com.ibm.iis.isf.security.SAMLSecureURL` can only contain the URL short address of the web application, without server or port specified, as for example in `"/ibm/iis/launchpad/secure"`.
You will need to restart WAS for any of the above changes to take effect.

Useful links

The following documents and links can provide additional information and explanations on SAML and WebSphere Application Server with a SAML environment:

SAML

- Video presentation on SAML and SPNEGO concepts: "BP104 -- Simplifying The S's: Single Sign-On, SPNEGO and SAML -- Gabriella Davis, The Turtle Partnership -- Chris Miller, Connectria" - http://w3.tap.ibm.com/medialibrary/media_view?id=243931

WebSphere application Server

- A good overview of WebSphere authentication: "IBM WebSphere Developer Technical Journal: Advanced authentication in WebSphere Application Server" - http://www.ibm.com/developerworks/websphere/techjournal/0508_benantar/0508_benantar.html
- “Understanding the WebSphere Application Server SAML Trust Association Interceptor” - http://www.ibm.com/developerworks/websphere/techjournal/1307_lansche/1307_lansche.html
- “Identity federation using SAML and WebSphere software” - http://www.ibm.com/developerworks/library/ws-SAMLWAS/
- This WAS Portal example is not completely applicable to WebSphere Application Server, but contains some useful insights: “Step by step guide to implement SAML 2.0 for Portal 8.5” - https://developer.ibm.com/digexp/docs/docs/customization-administration/step-step-guide-implement-saml-2-0-portal-8-5/
- Knowledge Center doc on the SAML TAI properties. “SAML web single sign-on (SSO) trust association interceptor (TAI) custom properties” - http://www.ibm.com/support/knowledgecenter/SSAW57_8.5.5/com.ibm.websphere.nd.doc/ae/rwbs_samltaiproperties.html

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 character set (DBCS) information, contact the IBM Intellectual Property Department in your country or send inquiries, in writing, to:

Intellectual Property Licensing
Legal and Intellectual Property Law
IBM Japan Ltd.
19-21, Nihonbashi-Hakozakicho, Chuo-ku
Tokyo 103-8510, Japan

The following paragraph does not apply to the United Kingdom or any other country where such provisions are inconsistent with local law: INTERNATIONAL BUSINESS MACHINES CORPORATION PROVIDES THIS PUBLICATION "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF NON-INFRINGEMENT, MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE. Some states do not allow disclaimer of express or implied warranties in certain transactions, therefore, this statement 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
J46A/G4
555 Bailey Avenue
San Jose, CA 95141-1003 U.S.A.

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

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

Any performance data contained herein was determined in a controlled environment. Therefore, the results obtained in other operating environments may vary significantly. Some measurements may have been made on development-level systems and there is no guarantee that these measurements will be the same on generally available systems. Furthermore, some 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.

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

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

Trademarks

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

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

Microsoft, Windows, 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 and logos are 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.