CA Federation Manager

Federation Manager Agent for Windows Authentication Guide

r12.5

Contact CA Technologies

Contact CA Support

For your convenience, CA Technologies provides one site where you can access the information that you need for your Home Office, Small Business, and Enterprise CA Technologies products. At http://ca.com/support, you can access the following resources:

- Online and telephone contact information for technical assistance and customer services
- Information about user communities and forums
- Product and documentation downloads
- CA Support policies and guidelines
- Other helpful resources appropriate for your product

Providing Feedback About Product Documentation

If you have comments or questions about CA Technologies product documentation, you can send a message to techpubs@ca.com.

To provide feedback about CA Technologies product documentation, complete our short customer survey which is available on the CA Support website at http://ca.com/docs.

Contents

Chapter 1: Introduction to the CA Federation Manager Agent for Windows Authentication

This section contains the following topics:

Overview of the Federation Manager Windows Agent

The CA Federation Manager Agent for Windows Authentication lets users on systems implementing one of the Integrated Windows Authentication (IWA) protocols to federate with business partners.

When a user requests access to a protected resource, Federation Manager uses the log-on identity information from a third-party web access management (WAM) system for delegated authentication. Federation Manager redirects the request to the Federation Manager Windows Agent. The Federation Manager Windows Agent verifies the user identity, creates an open format cookie, and passes the cookie to Federation Manager. Federation Manager generates a SAML assertion and starts the federation process.

Note: See the *Federation Manager Guide* for information about delegated authentication.

IWA supports the Windows NT LAN Manager (NTLM) and Kerberos encryption protocols. On Windows systems, the Federation Manager Windows Agent can use NTLM or Kerberos. On UNIX systems, the Federation Manager Windows Agent can only use Kerberos.

The Federation Manager Windows Agent is installed on the same Windows or UNIX system that Federation Manager is installed on. The following restrictions apply:

- The Federation Manager Windows Agent is incompatible with Federation Manager implementations using the SiteMinder connector.
- The browser issuing a single sign-on (SSO) request cannot be on the same system as the Federation Manager server.

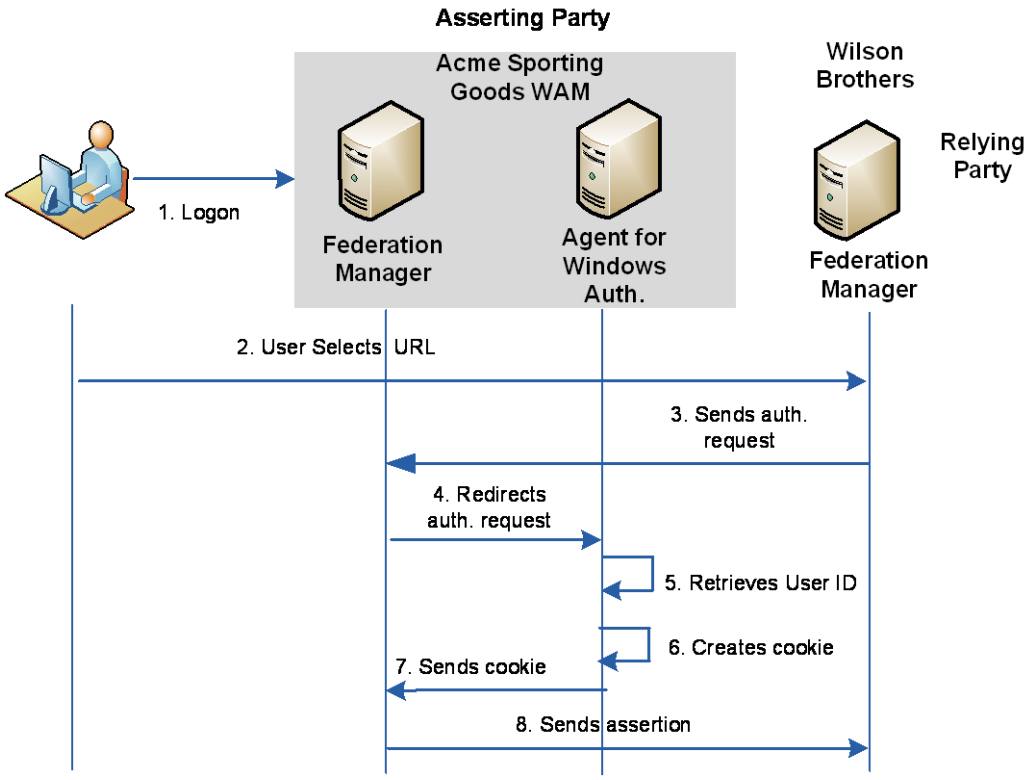
Intended Audience

The *Federation Manager Agent for Windows Authentication Guide* is intended for system and security administrators who are responsible for installing and administering authentication servers. The administrator must know about the Integrated Windows Authentication protocols—NTLM and Kerberos. In addition, the reader must be familiar with federation concepts and Federation Manager administration.

Federation Manager Windows Agent Use Case

A delegated authentication use case shows how the Federation Manager Windows Agent works. For this use case, Wilson Brothers department store wants to grant single sign-on access to employees of their supplier, Acme Sporting Goods, to provide them with special discounts. Wilson Brothers and Acme Sporting Goods have an established federated partnership. Employees of Acme Sporting Goods typically log in to their account at work with their domain user name and password. When an employee visits the Wilson Brothers Web site, the employee is granted access through one of the IWA protocols without being challenged.

The following illustration shows the role of the Federation Manager Windows Agent in a federated partnership:



The following process references the annotations in the preceding diagram:

1. The user logs in to the web access management (WAM) system at Acme Sporting Goods.
2. The user opens a browser and navigates to the URL for Wilson Brothers department store, the relying party.

   Note: The browser cannot be on the same system where Federation Manager and the Federation Manager Windows Agent are installed.
3. The relying party sends an authentication request to Federation Manager at the asserting party. Federation Manager determines that delegated authentication is specified for this partnership.
4. Federation Manager sends a request to the Agent to validate the security context for this user.
5. The Agent extracts the validated information.
6. The Agent sets the user information into an open format cookie.
7. The Agent sends the cookie to Federation Manager.
8. Federation Manager extracts the user information and sends a SAML assertion to the relying party.

The user is granted single sign-on access to the Wilson Brothers site.

Terminology

This guide uses the following terms related to Windows authentication:

Authentication Sever (AS)

The authentication server is the part of the key distribution center (KDC) that replies to the initial authentication request from the client. After the user is authenticated, the authentication server issues a ticket granting ticket (TGT). Using the TGT the user can obtain other Kerberos service tickets without having to re-enter a password.

Integrated Windows Authentication (IWA)

Integrated Windows Authentication provides Windows client application with authentication information from a user's log-on credentials. If the authentication exchange fails to identify the user, the browser prompts the user for a Windows ID and password. Integrated Windows Authentication is not a standard or an authentication protocol; it uses either the Kerberos or NTLM protocols.

Kerberos

The Kerberos authentication protocol lets users communicate safely over any network. Kerberos is also a suite of free software published by Massachusetts Institute of Technology (MIT) that implements this protocol. Kerberos uses tickets for verifying user identity. Kerberos protocol messages are protected against eavesdropping and replay attacks. Kerberos builds on symmetric key cryptography and requires a trusted third party, the key distribution center.

Key Distribution Center (KDC)

A key distribution center is part of a cryptographic system, which includes an authentication server and a ticket granting server. The purpose of a key distribution center is to reduce the risks inherent in exchanging keys. Key distribution centers often operate in systems where some users can have permission to use certain services at some times and not at others.

Keytab

A keytab is a file containing pairs of Kerberos principals and encrypted keys derived from the Kerberos password. This file is used for logging into the key distribution center.

NTLM

NTLM is an authentication protocol used in various Microsoft network implementations for single sign-on. NTLM employs a challenge-response mechanism for authentication, in which clients prove their identities without sending a password to the server. NTLM consists of three messages, commonly referred to as Type 1 (negotiation), Type 2 (challenge) and Type 3 (authentication). The responses in the Type 3 message are the most critical, because they prove to the server that the client user knows the account password.

Ticket Granting Ticket (TGT)

The ticket granting ticket (TGT) is a small, encrypted identification file with a limited validity period. After authentication, this file is granted to a user for data traffic protection by the KDC authentication server. The ticket granting ticket file contains the session key, the expiration date of the ticket, and the user IP address.

Ticket Granting Server (TGS)

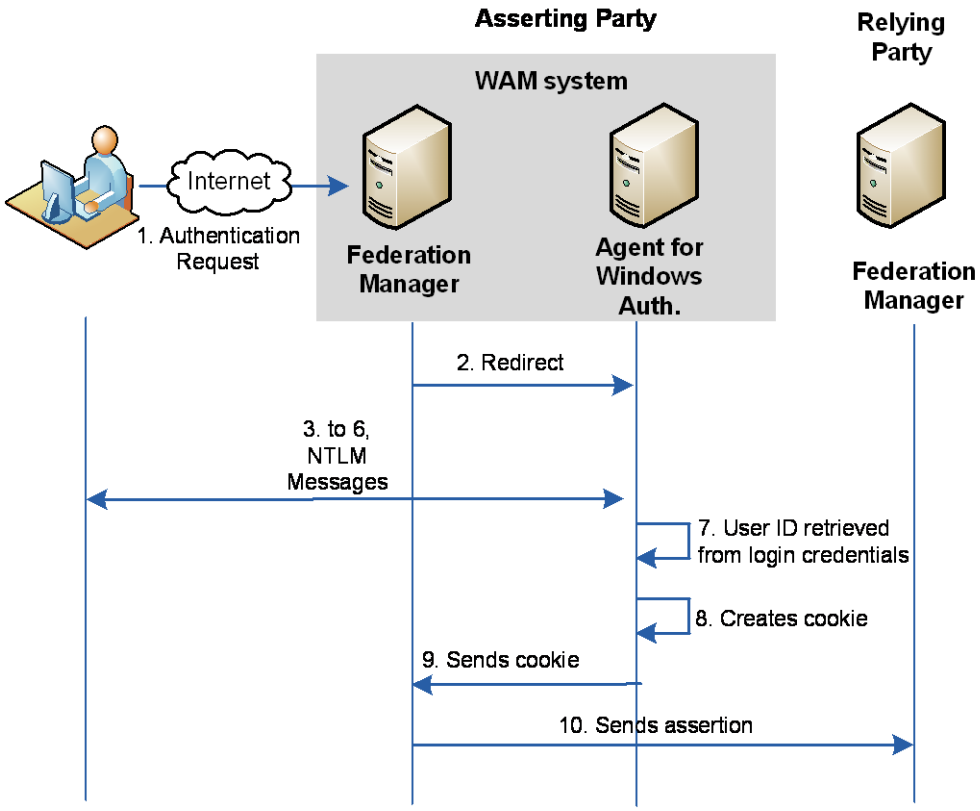
The ticket granting server is the KDC component that distributes service tickets to clients with a valid ticket granting ticket (TGT). The ticket granting server is like an application server that issues tickets as a service.

NTLM Protocol

NTLM includes various authentication and session security protocols. NTML is based on a challenge-response model, consisting of three types of messages exchanged in the following order:

1. The client sends a type 1 message (negotiation) to the server. The type 1 message specifies the features supported by the client and requested of the server.
2. The server sends a type 2 message (challenge) to the client. The primary function of this message is to challenge the identity of the client user.
3. The client sends a type 3 message (authentication) to the server. The type 3 message includes the domain and user name of the client user and responds to the challenge in the type 2 message.

The following diagram shows how Federation Manager and the Federation Manager Windows Agent use the NTLM protocol:



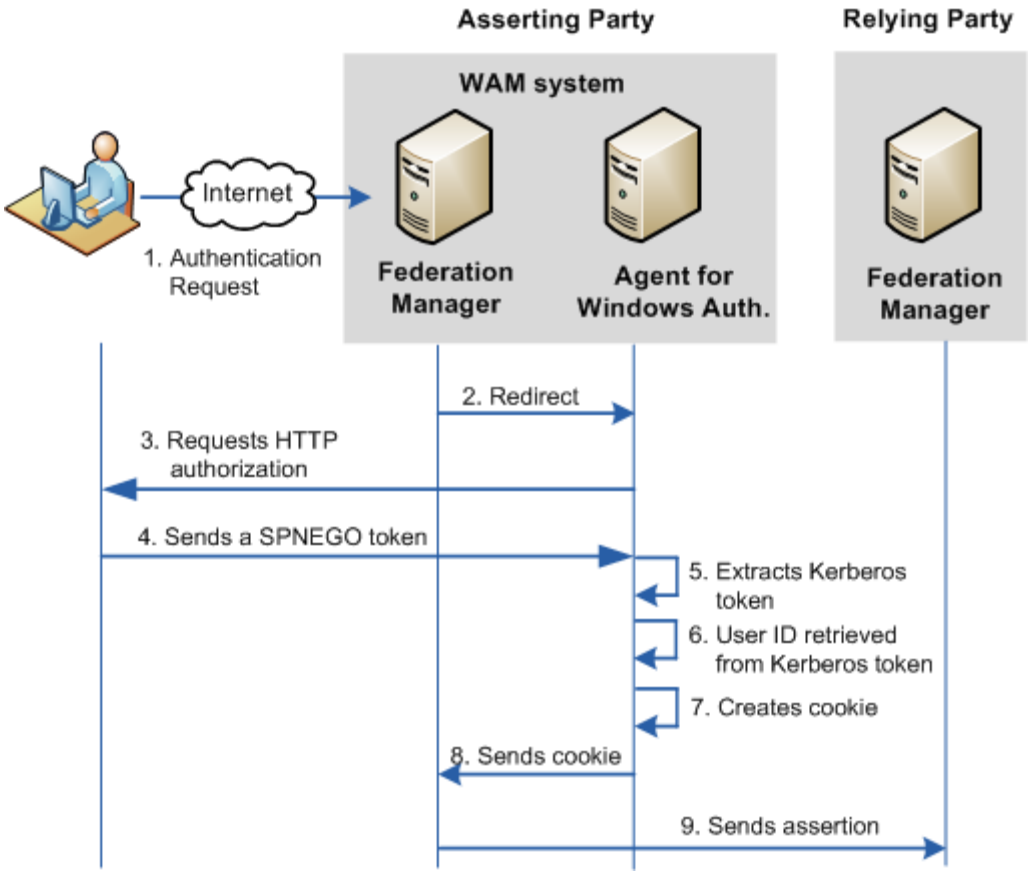
The following process references annotations in the preceding diagram:

1. An authentication request is made to Federation Manager at the asserting party.
2. Federation Manager recognizes the request as delegated authentication and redirects to the Federation Manager Windows Agent.

3. The Federation Manager Windows Agent sends a response back to the browser.
4. If the browser is configured for IWA, the browser sends an NTLM Negotiate token (type 1 message) in the authorization header to the Federation Manager Windows Agent.
5. The Federation Manager Windows Agent sends an NTLM Challenge token (type 2 message) to the browser.
6. The browser sends an NTLM Authenticate token (type 3 message) to the Federation Manager Windows Agent.
7. If a security context is associated with a user, the Federation Manager Windows Agent retrieves the user identity from the established context.
8. The Agent creates an open format cookie containing the user identity information.
9. The Agent sends the cookie to Federation Manager.
10. Federation Manager sends a SAML Assertion to the Relying Party to complete federation processing.

Kerberos Protocol

The Kerberos protocol is an elaboration of the NTLM protocol. The following illustration shows how Federation Manager and the Federation Manager Windows Agent use the Kerberos protocol:



The following process references annotations in the preceding diagram:

1. An authentication request is made to Federation Manager at the asserting party.

   Federation Manager recognizes that this request is a delegated authentication request.

2. Federation Manager redirects to the Federation Manager Windows Agent.

3. The Federation Manager Windows Agent requests an HTTP authorization from the browser.

4. If the browser is configured for IWA, it sends a SPNEGO token to the Federation Manager Windows Agent. This token allows initiators and acceptors to negotiate whether to use Kerberos or NTLM.

5. The Federation Manager Windows Agent extracts a Kerberos token from the SPNEGO token.
6. After the security context is established from the Kerberos token, the Agent retrieves the user identity information.
7. The Agent creates the open format cookie and builds a redirect URL.
8. The Agent sends the cookie to Federation Manager.
9. Federation Manager does the required processing and sends an assertion to the relying party.

Chapter 2: Deployment Prerequisites for the Federation Manager Agent

This section contains the following topics:

Deployment Overview

The Federation Manager Windows Agent has three modes of operation, depending on the choice of authentication protocol:

- NTLM mode (supported only on Windows)
- Kerberos mode (supported on Windows and UNIX)
- Kerberos mode with failover to NTLM (supported only on Windows)

You select the mode of operation in the first screen of the Agent configuration wizard.

The overall process for deployment of the Federation Manager Windows Agent includes the following steps:

1. Perform system prerequisites, which vary depending on the mode of operation and the operating environment:
   - NTLM with the Agent on Windows (see page 16)
   - Kerberos with the Agent on Windows and the KDC on Windows (see page 16)
   - Kerberos with the Agent on Windows and the KDC on UNIX (see page 17)

- Kerberos with the Agent on UNIX and the KDC on Windows (see page 17)
- Kerberos with the Agent on UNIX and the KDC on UNIX (see page 18)

2. Install the Federation Manager Windows Agent. (see page 27)
3. Configure the Federation Manager Windows Agent. (see page 33)
4. Configure the Federation Manager server for delegated authentication. (see page 39)

Prerequisites for NTLM Mode (Windows only)

The prerequisites for installing the Federation Manager Windows Agent on systems running Windows and using NTLM mode are listed following.

- Set up the domain controller on Windows for NTLM (see page 18).
- Configure Internet Explorer settings:
  - Local Intranet Properties Setup (see page 23)
  - Intranet Authentication Setup (see page 24)
  - (Optional) Browser Authentication through a Proxy Server (see page 24)
  - (Optional) Port Specification (see page 25)

Prerequisites for Kerberos Mode with Federation Manager and the KDC on Windows

The prerequisites for installing the Federation Manager Windows Agent on Windows systems using Kerberos mode with the KDC on a system running Windows are listed following.

1. Set up the domain controller for Kerberos.on Windows (see page 19).
2. Create the keytab file on Windows (see page 20).
3. Perform additional Kerberos configuration for the Federation Manager server on Windows. (see page 22)
4. Configure Internet Explorer settings:
   - Local Intranet Properties Setup (see page 23)
   - Intranet Authentication Setup (see page 24)
   - (Optional) Browser Authentication through a Proxy Server (see page 24)
   - (Optional) Port Specification (see page 25)

Prerequisites for Kerberos Mode with Federation Manager on Windows and the KDC on UNIX

The prerequisites for installing the Federation Manager Windows Agent on a system running Windows in Kerberos mode with the KDC on a UNIX system are as follows:

1. Configure the KDC for Federation Manager on the UNIX system. (see page 20)
2. Create the keytab file on the UNIX system (see page 21).
3. Perform additional Kerberos configuration for the Federation Manager server on Windows. (see page 22)
4. Configure Internet Explorer settings:
   - Local Intranet Properties setup (see page 23)
   - Intranet Authentication Setup (see page 24)
   - (Optional) Browser Authentication through a Proxy Server (see page 24)
   - (Optional) Port Specification (see page 25)

Prerequisites for Kerberos Mode with Federation Manager on UNIX and the KDC on Windows

The prerequisites for installing the Federation Manager Windows Agent on a UNIX system running in Kerberos mode with the KDC on Windows are as follows:

1. Set up the domain controller for Kerberos on Windows. (see page 19)
2. Create the keytab file on Windows (see page 20).
3. Perform additional Kerberos configuration for the Federation Manager server on UNIX (see page 22).
4. Configure Internet Explorer settings:
   - Local Intranet Properties setup (see page 23)
   - Intranet Authentication setup (see page 24)
   - (Optional) Browser Authentication through a Proxy Server (see page 24)
   - (Optional) Port Specification (see page 25)

Prerequisites for Kerberos Mode with Federation Manager and the KDC on a UNIX System

The prerequisites for installing the Federation Manager Windows Agent on a UNIX system running in Kerberos mode with the KDC on a UNIX system are as follows:

1. Configure the KDC for Federation Manager on the UNIX system (see page 20).
2. Create the keytab file on the UNIX system (see page 21).
3. Perform additional Kerberos configuration for the Federation Manager server on UNIX. (see page 22)
4. Configure Explorer settings:
   - Local Intranet Properties Setup (see page 23)
   - Intranet Authentication Setup (see page 24)
   - (Optional) Browser Authentication through a Proxy Server (see page 24)
   - (Optional) Port Specification (see page 25)

Domain Controller Setup on Windows for NTLM

Windows 2003 SP 1 Active Directory is the primary domain controller for the Windows Domain. This host provides storage for the user, service accounts, credentials, and Windows Domain services.

The Federation Manager Windows Agent generates an NTLM response message to the NTML challenge message sent by the relying party. The server at the relying party passes the challenge and the response to the domain controller. The response is an encrypted version of the challenge using the hash of the user password. The domain controller encrypts the challenge using the same hash of the password and compares it with the response generated at the asserting party. If they match, the authentication is complete. The domain controller informs the server at the relying party.

To deploy a domain controller when using NTLM

1. Promote Windows 2003 SP 1 Server to a domain controller using the Windows dcpromo utility.
2. Open the Active Directory Users and Computers dialog from Administrative tools.
3. Select Create a User Account.
4. Enter a password for creating this account.
5. Clear the option User Must Change Password at Next Logon.

The domain controller is deployed for NTLM.

Domain Controller Setup on Windows for Kerberos

When using Kerberos, the domain controller is the key distribution center (KDC) for the Kerberos Realm. In a pure Windows 2003 environment, a Kerberos Realm is equivalent to a Windows Domain. The domain controller host provides storage for the user, service accounts, credentials, the Kerberos ticketing services, and Windows Domain services.

A keytab file is required for Kerberos authentication, which lets users logged on to the Federation Manager server authenticate with the KDC without being prompted for a password. The keytab file is created with the ktpass utility. The ktpass command tool utility is a Windows support tool. The default encryption type is RC4-HMAC-NT, which can be confirmed by running ktpass /? at the command prompt. Also, be sure to confirm the Kerberos version number.

To deploy the Windows domain controller when using Kerberos

1. Promote Windows 2003 SP 1 Server to a domain controller using the Windows dcpromo utility.
2. Open the Active Directory Users and Computers dialog from Administrative tools.
3. Select Create a User Account.
4. Enter a password for this account.
5. Clear the User Must Change Password at Next Logon option.
6. Associate the Windows 2003 workstation account with a server principal name (for example, HTTP/IWAConnectorHostName.idp.com@IDP.COM).
7. Create a keytab file (see page 20).

   Use the password entered in step 4.
8. Copy the keytab file to a secure location on the Federation Manager server at the asserting party.

   Important! The keytab name with its full path must be specified in the Keytab Location field during the Federation Manager Windows Agent configuration.

The domain controller is deployed for Kerberos on systems running Windows.

KDC Configuration on a UNIX System

The UNIX server that hosts the Kerberos key distribution center (KDC) must be configured to support the Federation Manager server.

To configure Federation Manager on the UNIX KDC server

1. Open a command prompt window.
2. Enter the following command at the command-line prompt:

   ```
   usr/sbin/kadmin.local
   ```

3. Add the Federation Manager system service principal name with this command:

   ```
   addprinc -pw <password> HTTP/AgentHost Name.domainname.com@DOMAINNAME.COM
   ```

4. Create a keytab file. (see page 21)
5. Enter quit.

The configuration of Federation Manager on the UNIX KDC server is complete.

Create a Keytab File on Windows

A keytab file is required for Kerberos authentication. The keytab file can be created on a Windows system or a UNIX system.

To create the keytab file on Windows

1. Open a command-prompt window.
2. Enter the following command:

ktpass -out *output_keytab_location* -princ *SPN_name* -ptype KRB5_NT_PRINCIPAL -mapuser *username* -pass *password*

The keytab file is created.

For example:

```
ktpass -out c:\workstation.keytab -princ HTTP/
IWAConnectorHostName.idp.com@IDP.COM
-ptype KRB5_NT_PRINCIPAL -mapuser testkrb -pass password
Targeting domain controller: winkdc.idp.com
Using legacy password setting method
Successfully mapped HTTP/ IWAConnectorHostName.idp.com to testkrb.
Key created.
Output keytab to c:\workstation.keytab:
Keytab version: 0x502
keysize 67 HTTP/ IWAConnectorHostName.idp.com@IDP.COM ptype 1
(KRB5_NT_PRINCIPAL) vno 2 etype 0x17 (RC4-HMAC) keylength 16
(0xfd77a26f1f5d61d1fafd67a2d88784c7)
```

Create a Keytab File on a UNIX System

A keytab file is required for Kerberos authentication. The keytab file can be created on a Windows system or a UNIX system.

To create the keytab file on a UNIX system

1. Open a command-prompt window.
2. Enter the following command:

   ```
   ktadd -k output_keytab_location SPN name
   ```

The keytab file is created.

Additional Configuration for Kerberos on Windows

The following actions are required on the Federation Manager server when using Kerberos on Windows:

- Configure a Kerberos configuration file (krb5.ini) and place krb5.ini in the Windows system root path:
    a. Configure the KDC for the Windows 2003 Kerberos realm (domain) to use the Windows 2003 domain controller.
    b. Configure krb5.ini to use the Windows 2003 KDC keytab file containing the credentials of the workstation principal.

```
[libdefaults]
default_realm = IDP.COM
default_keytab_name = C:\WINDOWS\krb5.keytab
default_tkt_enctypes = des-cbc-md5 rc4-hmac
default_tgs_enctypes = des-cbc-md5 rc4-hmac
[realms]
IDP.COM = {
kdc = winkdc.idp.com:88
default_domain = IDP.COM
}
[domain_realm]
.idp.com = IDP.COM
```

- Deploy the Windows 2003 KDC keytab file to a secure location (as mentioned for krb5.ini).

Additional Configuration for Kerberos on UNIX

To configure Kerberos, the following commands are required on a Federation Manager server on a UNIX system:

- scp root@*KDC system name*:/etc/krb/krb.conf
- cat krb.profile
- kclient -p krb.profile

The UNIX system is configured for Kerberos authentication.

Local Intranet Properties Setup

Internet Explorer requires some specific settings to function in a single sign-on deployment. The setup for the browser requires configuring the local Intranet properties and configuring Intranet authentication. These settings apply whether you are using the Kerberos or the NTLM authentication protocol.

To configure the local Intranet properties

1. Open an Internet Explorer browser.
2. Select Tools form the Internet Explorer menu bar.
3. Select Internet Options from the drop-down menu.
4. Click the Security tab.
5. Click the Local Intranet button.
6. Click the Sites button.
7. Verify that the Include all sites that bypass the proxy server check box is selected.
8. Click the Advanced button.
9. Enter all domain names used on the Intranet, for example, AgentHostName.domainname.com.
10. Select the Advanced tab.
11. Scroll to the Security section.
12. Select Enable Integrated Windows Authentication (requires restart).
13. Restart the system.
14. Click OK.

The local Intranet properties are configured.

Intranet Authentication Setup

To function in a single-sign on solution requires some specific settings for the Internet Explorer. These client browser settings assume an Intranet environment. The setup for the browser requires configuring the local Intranet properties and configuring Intranet authentication.

To configure the Intranet authentication settings

1. Open an Internet Explorer browser.
2. Select the Tools menu from the Internet Explorer menu bar.
3. Select Internet Options from the drop-down menu.
4. Click the Security tab.
5. Click the Local Intranet button.
6. Click the Custom Level button.
7. Select the Security tab.
8. Scroll down to the User Authentication section.
9. Select Automatic logon only in Intranet zone.
10. Click OK.

Users are authenticated on the Intranet zone.

Browser Authentication through a Proxy Server

When a proxy server is inserted between the browser and the Federation Manager Windows Agent server, which is the same as the Federation Manager asserting party, authentication no longer works. In this case all URLs with relative domain names must be configured not to go through the proxy server.

To configure proxy settings when using the Federation Manager Windows Agent

1. Open an Internet Explorer browser.
2. Select the Tools menu from the Internet Explorer menu bar.
3. Select Internet Options from the drop-down menu.
4. Click the Advanced Tab.
5. Scroll down to the Security section.
6. Verify that Enable Integrate Windows Authentication is selected.
7. Click the Connections tab.

8. Click the LAN Settings button.
9. Verify that the proxy server address and port number are correct.
10. Click the Advanced button.
11. List any relevant domain name in the Exceptions field.
12. Click OK.

The browser is configured to bypass the proxy server for the specified domains.

Port Specification

If your configuration has a firewall between the Federation Manager Windows Agent and the domain controller, the following static ports must be opened to allow communication:

- Microsoft-DS traffic (445/tcp, 445/udp)
- Lightweight Directory Access Protocol (LDAP) ping (389/udp)
- Domain Name System (DNS) (53/tcp, 53/udp)
- Kerberos authentication protocol (88/tcp, 88/udp)
- NetBIOS datagram Service (138/tcp, 138/udp)
- NetBIOS-ns Service (137/tcp, 137/udp)
- epmap (135/tcp, 135/udp)

In addition, the following Local Security Authority (LSA) ports are dynamic and must be made static by modifying registry entries:

- Local Security Authority Service(NTDS) (1025/tcp, 1025/udp):: Configurable Port required for NTLM
- Local Security Authority Service(NetLogin) (1026/tcp, 1026/udp):: Configurable Port required for Kerberos

Visit the following site for information about the LSA ports:

http://support.microsoft.com/kb/224196/

Chapter 3: Installation of the Federation Manager Windows Agent

This section contains the following topics:

Installation Requirements

Consider the following installation requirements:

- The Federation Manager Windows Agent must be installed on a system where Federation Manager is already installed.
- Do not install the Federation Manager Windows Agent on a system where Federation Manager is using the SiteMinder Connector.

Important! If you upgrade to r12.5 and the Agent for Windows Authentication is installed, upgrade the Agent to the same version as Federation Manager. Otherwise, the Agent fails to work properly.

Installation Executables for r12.5

The following table identifies the installation executables for the Windows Agent for authentication. The table is organized by platform.

Note: The installation executable and folder names include the string **iwa**, which references support for Integrated Windows Authentication technology.

Platform	Installation Executable
Solaris	ca-fedmgr-iwa-12.5-sol.bin
Linux	ca-fedmgr-iwa-12.5-rhel30.bin

Platform	Installation Executable
Windows	ca-fedmgr-iwa-12.5-win32.exe

For more information about supported operating systems, see the Federation Manager Platform Support Matrix on the Technical Support site.

Install the Federation Manager Windows Agent on Windows

Run the Federation Manager Windows Agent installer from an executable located on the Technical Support site.

To locate installation kits

1. Go to the Technical Support site.
2. Log on to the site.
3. Click Download Center.
4. Search the Download Center for the installation kit, and download it to your local system.

To install the Agent on Windows

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
3. Run the installation executable for your operating platform.

   View a list of executables here (see page 27).

   The installation wizard starts.
4. Follow the prompts in the installation wizard.

   The Windows Agent is installed your system.
5. After the installation is complete, run the configuration wizard (see page 35).

Install the Federation Manager Windows Agent on UNIX

Run the Federation Manager Windows Agent from an executable located on the Technical Support site.

To locate installation kits

1. Go to the Technical Support site.
2. Log on to the site.
3. Click Download Center.
4. Search the Download Center for the installation kit, and download it to your local system.

To install the Agent on a UNIX system

1. Exit all applications that are running.
2. Navigate to where the installation executable is located.
3. Run the installation executable for your operating platform.

   View a list of executables here (see page 27).

   The installation wizard starts.
4. Follow the prompts in the installation wizard.

   The Windows Agent is installed on your system.
5. After the installation is complete, run the configuration wizard.

Unattended Installation of the Federation Manager Windows Agent on Windows

After the Windows Agent has been manually installed, you can install it on the same system, or a different system, using the unattended installation mode.

An unattended installation uses one command that points to a properties file. The default properties template file can be modified to suit your requirements.

The unattended installation process is the same on any platform. Only the executable file names differ.

Follow these steps:

1. Navigate to the directory where the installation executable is located.

   View a list of installation executables here (see page 27).

2. Enter the following command at a command prompt:
   `installation_executable -i silent -f ca-fedmanager-iwa-installer.properties`

   -f

   Specifies the name of the Windows Agent installer properties file. If the properties file is not in the same directory as the installation executable file, specify the relative path to the properties file.

   -i

   Specifies the installation mode.

   The installation executes and writes the settings in the properties file.

The unattended installation is complete.

Uninstall the Federation Manager Windows Agent from Windows

Remove the Windows Agent from your Windows system when you no longer require it.

Follow these steps:

1. Select Start, All Programs, CA, FederationManager, Uninstall Federation Manager Windows Authentication Agent.

   The wizard starts up.

2. Follow the instructions in the wizard.
3. Navigate to the Program Files\CA\FederationManager\connector directory and delete any IWA folders and subfolders, if necessary.
4. Reboot the system.

The Federation Manager Windows Agent is removed from your system.

Uninstall the Federation Manager Windows Agent from a UNIX System

Remove the Windows Agent from your UNIX system when you no longer require it.

Follow these steps:

1. Open a command window.
2. Navigate to the Federation Manager Windows Agent home directory.
3. Enter the following command:

   ./ca-federation-iwa-uninstall.sh
4. Delete any remaining folders and all subfolders, as required.

The Federation Manager Windows Agent is removed from the system.

Upgrade the Federation Manager Windows Agent to r12.5

The installation program can also upgrade your version of the Federation Manager Agent for Windows Authentication. Remeber to install the Windows Agent on a system where Federation Manager is already installed.

Important! Federation Manager and the Windows Agent must be the same version. If you upgrade to r12.5 and the Agent for Windows Authentication is installed, upgrade the Agent to the same version as Federation Manager. Otherwise, the Agent fails to work properly.

Follow these steps:

1. Confirm that Federation Manager is the same version as that of the Agent you plan to upgrade. If not, first upgrade Federation Manager.
2. Run the Windows Agent installation executable for your operating platform. View a list of executables here (see page 27).

   No further configuration required.
3. Run the configuration wizard (see page 33).

Chapter 4: Configuration of the Federation Manager Windows Agent

This section contains the following topics:

Information Required by the Configuration Wizard

After you install the Federation Manager Windows Agent, run the configuration wizard. On Windows systems, you can select the authentication protocol (Kerberos or NTLM). ON UNIX systems, Kerberos is the only supported protocol.

Note: The configuration executable and folder names include the string **iwa**, which references support for Integrated Windows Authentication technology.

The following parameters are required for NTLM and Kerberos configurations.

Important! The values specified for these parameters must match the values specified in the Deployment settings in the Federation Manager UI, which are communicated out of band.

Cookie zone

Specifies the single sign-on security zone name.

Default: FED

Limits: Alpha string

Cookie name

Specifies the name of the open format cookie.

Default: ""

Limits: Alpha string

Encryption password

Specifies the password used to derive a key to encrypt the cookie.

Default: ""

Limits: Alphanumeric string

Encryption Transformation type

Specifies the FIPS-compliant cryptographic transform.

Default: AES128/CBC/PKCS5Padding

Limits: AES128/CBC/PKCS5Padding, AES192/CBC/PKCS5Padding, AES256/CBC/PKCS5Padding, 3DES_EDE/CBC/PKCS5Padding

UseHMAC

Specifies whether to use a Hash Message Authentication Code (HMAC).

Default: false

Limits: true or false

Note: If you are on a system running Windows and you have selected the Kerberos authentication protocol, you can optionally select NTLM as the failover option.

When specifying the Kerberos protocol, provide values for the following parameters:

KDC address

Specifies the fully qualified domain name of the key distribution center (KDC).

KDC realm

Specifies the domain name of the system on which the KDC is located.

Keytab location

Specifies the path of the keytab file, which is created on the KDC system and moved to the system on which Federation Manager Windows Agent is located.

Principal

Specifies the service principal name (SPN), which uniquely identifies an instance of a service, for example, HTTP/host.abc.com. HTTP is the name of the service and host.abc.com is the name of the host on which the service resides.

The Keytab location and Principal parameters are written to the login.conf file. The other parameters are written to the IWAConnectorConfig.conf file.

Note: If you review the login.conf file, do not change the value of the isInitiator parameter.

Run the Configuration Wizard on Windows

Run the configuration wizard for the Agent for Windows Authorization after the installtion. The wizard establishes values for parameters related to authentication protocol and cookie specifications.

Follow these steps:

1. Exit all applications that are running.
2. Navigate to where the configuration command file is located:

   federation_mgr_root\connectors\IWA.
3. Double-click ca-fedmanager-iwa-config.cmd.

   The configuration wizard starts.
4. Follow the prompts provided by the wizard.

The configuration is complete.

Run the Configuration Wizard on UNIX

The configuration wizard for the Federation Manager Windows Agent establishes values for parameters related to authentication protocol and cookie specifications.

Run the configuration wizard to complete the installation process.

Follow these steps:

1. Exit all applications that are running.
2. Navigate to where the configuration command file is located:

   *federation_mgr_root/*connectors/IWA
3. Execute the script ca-fedmanager-iwa-config.sh.

   The configuration wizard starts.
4. Follow the prompts provided by the wizard to complete the configuration.

5. Source the following script so the Agent works properly:
   `. /federation_mgr_home/connectors/IWA/ca_fedmgr_iwa_env.ksh`
6. Restart the Federation Manager services:
   a. Open a command window.
   b. Run the following scripts:

      federation_mgr_home/fedmanager.sh stop

      federation_mgr_home/fedmanager.sh start

   Note: Do not stop and start the services as the root user. You must be a non-root user.

Unattended Configuration on Windows

After the Federation Manager Windows Agent has been configured using the wizard at least once, you can configure it on the same system, or a different system, using unattended mode. An unattended mode configuration uses one command that points to a properties file. You can modify the configuration properties to suit your requirements.

To configure the Federation Manager Agent in unattended mode on Windows

1. Navigate to the directory where the configuration executable is located:

   federation_mgr_root\connectors\IWA\install_config_info
2. Enter the following command at a command prompt:

   `ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties`

   -f

   Specifies the name of the Federation Manager Windows Agent configuration properties file. If the properties file is not in the same directory as the executable file, specify the relative path to the properties file.

   -i

   Specifies the configuration mode. For unattended mode, the value is silent.

The unattended configuration is complete.

Unattended Configuration on a UNIX System

After configuring the Federation Manager Windows Agent using the wizard at least once, configure it on the same system, or a different system, using unattended mode. An unattended mode configuration uses one command that points to a properties file. Modify the configuration properties file to suit your requirements.

To configure the Federation Manager Agent in unattended mode on a UNIX system

1. Navigate to the directory where the configuration executable is located:

   federation_mgr_root/connectors/IWA/install_config_info

2. Enter the following command at a command prompt:

   ```
   ca-fedmanager-iwa-confg.bin i-silent -f ca-fedmanager-iwa-config.properties
   ```

   -f

   Specifies the name of the Federation Manager Windows Agent configuration properties file. If the properties file is not in the same directory as the executable file, specify the relative path to the properties file.

   -i

   Specifies the configuration mode. For unattended mode, the value is silent.

The unattended configuration is complete.

Federation Manager Windows Agent Configuration File

After you have run the configuration wizard, the values you specified are written to the IWAConnectorConfig.conf file. You can rerun the wizard at any time to modify almost all the parameter values.

Several parameter values are not set in the configuration wizard. You can modify the file directly when you want to update the following values:

context_cleanup_interval

Specifies the interval after which the cleanup thread starts deleting the expired context. Decreasing this value leads to quicker cleanup and better memory availability.

Default: 30000-milliseconds

Limits: A lower value is recommended when you expect many incomplete requests.

context_expiration_interval

Specifies the time after which a context is assumed to be expired. For NTLM, context is valid for maximum 1 minute.

Default: 60000-milliseconds

Limits:The value of this parameter cannot be set less than 1 minute. A higher value can possibly lead to a stale context not getting cleaned up.

context_cleanup_thread_priority

Specifies the priority for the context clean up thread.

Default: 5

Limits: A higher priority is recommended when you expect many incomplete requests.

Chapter 5: Delegated Authentication Configuration

This section contains the following topics:

Delegated Authentication Setup

The Federation Manager Windows Agent works with Federation Manager to provide user authentication in an IWA context. Because the Federation Manager Windows Agent is acting as a third-party authentication service, you must configure Federation Manager to use delegated authentication.

In addition, the cookie settings on the Federation Manager Infrastructure, Deployment settings dialog must be communicated out of band to the Federation Manager Windows Agent.

To configure Federation Manager for delegated authentication

1. Login in to the Federation Manager UI.
2. Select the SAML 1.1 or SAML 2.0 partnership you want to edit. Be sure that you are editing a Producer-> Consumer or IDP -> SP partnership.
3. Navigate to one of the following steps in the partnership wizard:
   - SAML1.1: Single Sign-on
   - SAML 2.0: SSO and SLO
4. Set the Authentication Mode to Delegated.
5. Set the Delegated Authentication Type to Open Format Cookie.

   Note: The Federation Manager Windows Agent requires delegated authentication based on the open format cookie. This option is not available if you have configured Federation Manager to use the SiteMinder connector.
6. Enter the delegated authentication URL.

   Example: http://*hostname:portnum*/iwa/IWARedirect

Federation Manager is configured for delegated authentication.

Note: For more information about delegated authentication, see the *Federation Manager Guide*.

Chapter 6: Troubleshooting

This section contains the following topics:

Review the Windows Agent Trace Log File

Troubleshoot the Federation Manager Windows Agent by referring to the trace log file, IWAConnectorTrace.log.

To set up the trace log file:

1. Navigate to %FEDROOT%\connectors\IWA\Config\login.conf.
2. Open the login.conf file and make the following change:

   debug=true
3. Restart the Federation Manager services.

The log file is written to the directory %FEDROOT%\logs\connectors\IWA\IWAConnectorTrace.log.

The log file can contain any of the following messages:

Symptom:

Config file not found.

Solution:

Make sure that the IWAConnectorConfig.conf file is present in the *federation_mgr_root*\connectors\IWA\config folder.

Symptom:

Invalid authtype specified.

Solution:

Make sure the authentication type is specified as NTLM or Kerberos. Re-run the configuration wizard if necessary. Do not manually edit the configuration file to change this value.

Symptom:

NTLM is not supported on non-Windows platform.

Solution:

Re-run the configuration wizard and specify Kerberos as the authentication type. Do not manually edit the configuration file to change this value.

Symptom:

Password should be encrypted using the IWAEncryptPassword utility.

Solution:

Re-run the configuration wizard and enter the password. Do not manually edit the configuration file to change this value.

Symptom:

AuthType cannot be blank.

Solution:

Re-run the configuration wizard and select an authentication type. Do not manually edit the configuration file to change this value.

Symptom:

Encryption key cannot be blank.

Solution:

Re-run the configuration wizard and select an encryption key. Do not manually edit the configuration file to change this value.

Symptom:

Invalid Encryption Transform specified.

Solution:

Re-run the configuration wizard and specify another encryption transformation. Do not manually edit the configuration file to change this value.

Symptom:

Invalid HMAC value specified. Only true or false can be specified.

Solution:

Re-run the configuration wizard and select true or false for whether to enable HMAC. Do not manually edit the configuration file to change this value.

Symptom:

Kerberos configuration is invalid.

Solution:

Make sure the following parameters are specified correctly:

- Kerberos Realm
- KDC address
- Kerberos configuration file location (the login.conf file)

Re-run the configuration wizard if necessary. Do not manually edit the configuration file to change any of these values.

Symptom:

Context expiration interval cannot be less than 1 minute.

Solution:

Re-run the configuration wizard and specify a context expiration interval of longer than 1 minute. Do not manually edit the configuration file to change this value.

Symptom:

Invalid configuration. Server not initialized.

Solution:

Make sure the following values are specified correctly:

- Authentication type
- Encryption key
- Encryption Transform
- Kerberos Realm
- KDC Address
- Kerberos configuration file location (the login.conf file)

Re-run the configuration wizard if necessary. Do not manually edit the configuration file to change any of these values.

Symptom:

Aborting request as it is initiated with an IP address.

Solution:

Make sure that the SSO request is always initiated with a fully qualified domain name.

Symptom:

Kerberos initialization failed, please check the configuration parameters.

Solution:

Make sure the following values are specified correctly:

- Authentication type
- Encryption key
- Encryption Transform
- Kerberos Realm
- KDC Address
- Kerberos configuration file location (the login.conf file)

Re-run the configuration wizard if necessary. Do not manually edit the configuration file to change any of these values.

Symptom:

No cookie found; it is either expired or deleted.

Solution:

This message appears when the browser is configured incorrectly. Make sure that the browser configuration is complete for NTLM and that cookies are not disabled.

Symptom:

NTLM credentials cookie is not found.

Solution:

This message appears when the browser is configured incorrectly. Make sure that the browser configuration is complete for NTLM and that cookies are not disabled.

Symptom:

User domain or workstation information not found.

Solution:

This message appears when the domain name or the workstation man was not found in the NTLM type 3 message. Makes sure that this message has not been altered.

Symptom:

User has not entered the domain information.

Solution:

Make sure the browser configuration for NTLM authentication is complete. If you are using a prompt-based authentication, make user that the domain name is provided with the user name.

Symptom:

Authentication failed when attempting auth for principal *SPN_Name* to the KDC *KDC_address*, using keys in the Keytab k*eytab_path*.

Solution:

Make sure that the following parameters are correct:

- Principal Name
- KDC Address
- Keytab Path

Symptom:

User Name not found; ensure that your browser is on a machine other than the Federation Manager server.

Solution:

Make sure that the SSO request is always made from a system other than the Federation Manager server at the asserting party.

Index