CA SiteMinder Federation Standalone

Agent for Windows Authentication Guide

r12.52 SP1

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.

Documentation Changes

- No 12.52 SP1 documentation updates have been made, as a result of issues found in previous releases.
- No 12.52 documentation updates have been made, as a result of issues found in previous releases.

Contents

Chapter 1: Introduction to the Federation Agent for Windows Authentication

Overview of the Federation Agent for Windows

The Federation 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, the federation system uses the log-on identity information from a third-party web access management (WAM) system. This process of using the third-party WAM is known as delegated authentication. The federation system redirects the request to the Federation Agent. The Agent verifies the user identity, creates an open format cookie, and passes the cookie to the federation system. The system then generates a SAML assertion and passes it to the relying party.

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

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

The Federation Agent is installed on the same Windows or UNIX system where CA SiteMinder® Federation Standalone is installed. The following restrictions apply:

- The Federation Agent is incompatible with federation installations using the CA SiteMinder® Connector.
- The browser issuing a single sign-on (SSO) request cannot be on the same system as the federation system.

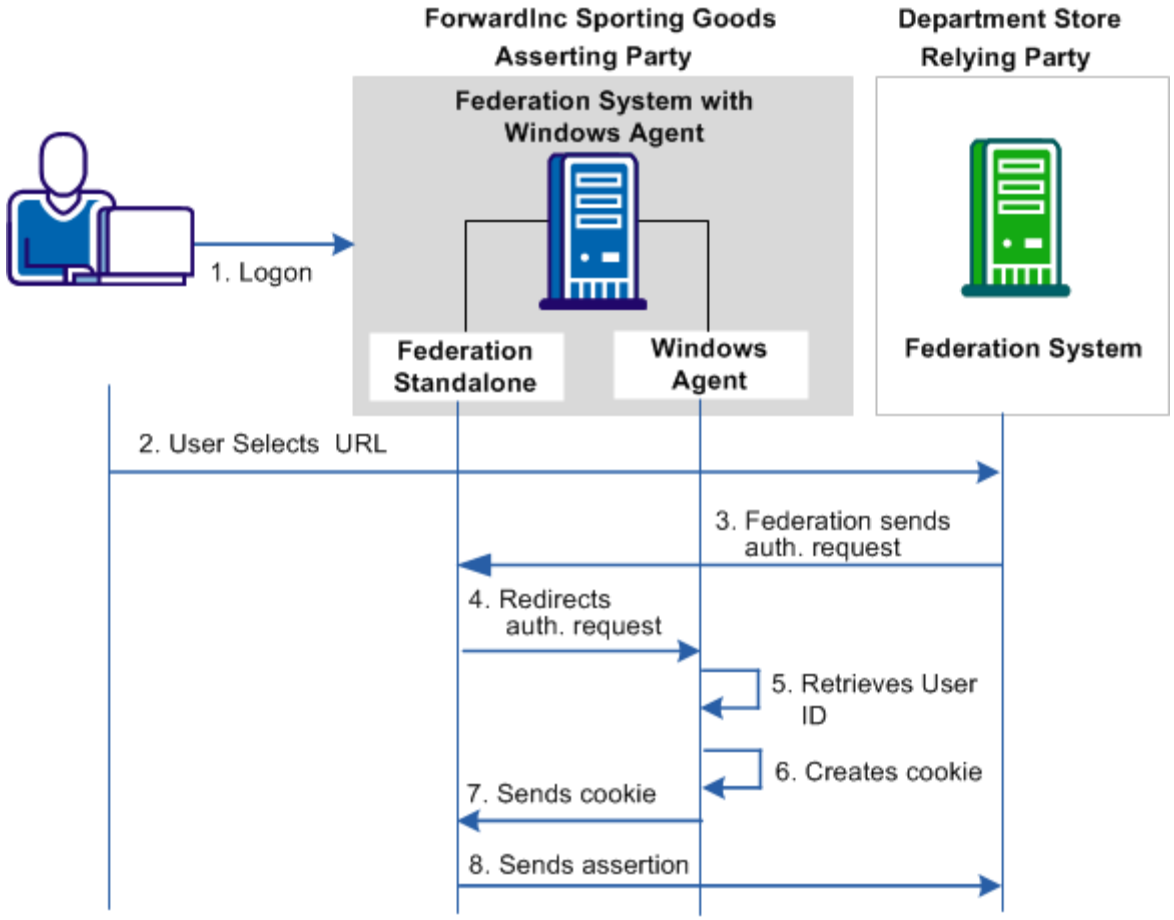
The administrator must know about the Integrated Windows Authentication protocols—NTLM and Kerberos. In addition, the reader must be familiar with federation concepts and CA SiteMinder® Federation Standalone administration.

SSO between a System using IWA and a Business Partner

A delegated authentication use case shows how the Federation Agent works. A department store wants to grant single sign-on access to employees of their supplier, ForwardInc Sporting Goods, to provide them with special discounts.

The department store and ForwardInc Sporting Goods have an established federated partnership. Employees of ForwardInc Sporting Goods typically log in to their account at work with their domain user name and password. When an employee visits the department store web site, the employee is granted access through one of the IWA protocols without being challenged.

The following graphic shows the role of the Federation Agent in a federated partnership:



The transaction as shown in the diagram is as follows:

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

   Note: The browser cannot be on the same system where the federation system with the Windows Agent is installed.
3. The relying party sends an authentication request to the asserting party. The federation system at the asserting party determines that delegated authentication is configured for this partnership.
4. The federation system sends a request to the Federation Agent. The Agent validates the security context for the user.
5. The Windows Agent extracts the validated information from the request.
6. The Windows Agent places the user information into an open format cookie.
7. The Windows Agent sends the cookie to the federation system.
8. The federation system at the asserting party extracts the user information, places it in an assertion, and sends the assertion to the relying party.

The user is granted access to the department store web site without having to log in.

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)

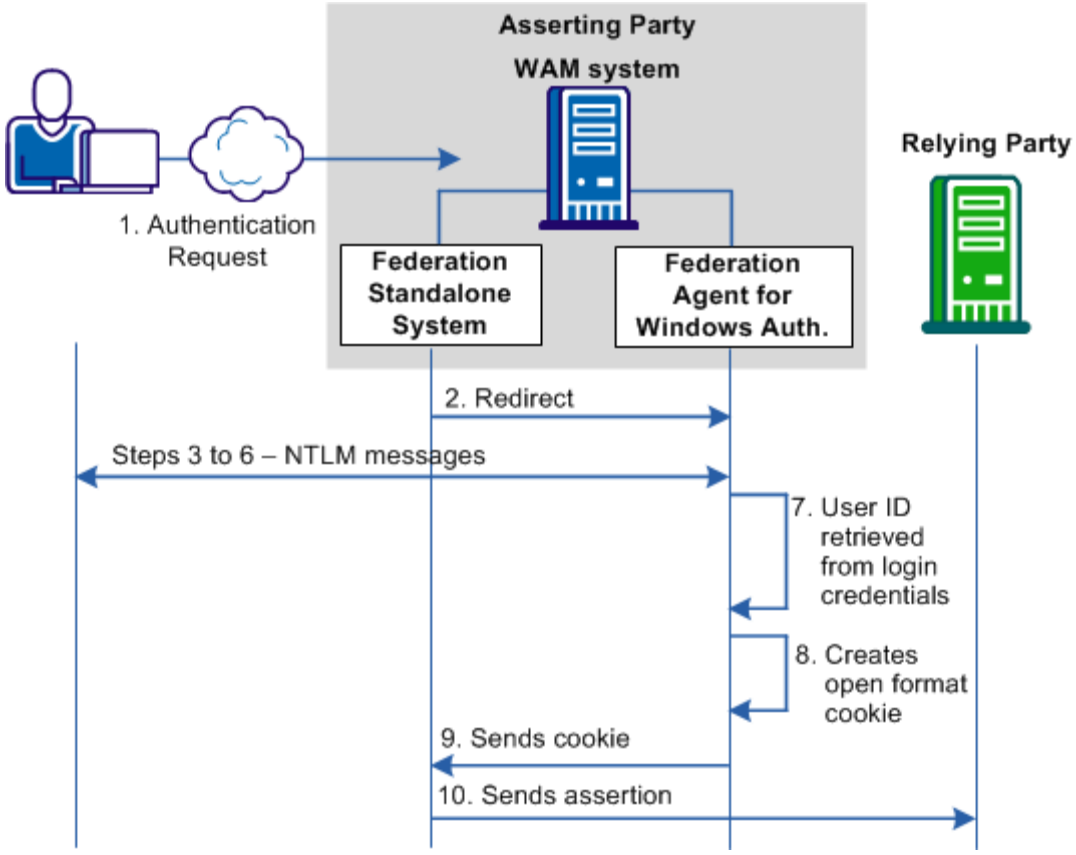
The ticket granting server is the KDC component that distributes service tickets to clients with a valid ticket granting ticket (TGT). The ticket granting server is like an application server that issues tickets as a service.

NTLM Protocol

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

1. The client sends a type 1 message (negotiation) to the server. The type 1 message specifies the features that are 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 graphic shows how the federation system with the Federation Agent use the NTLM protocol:

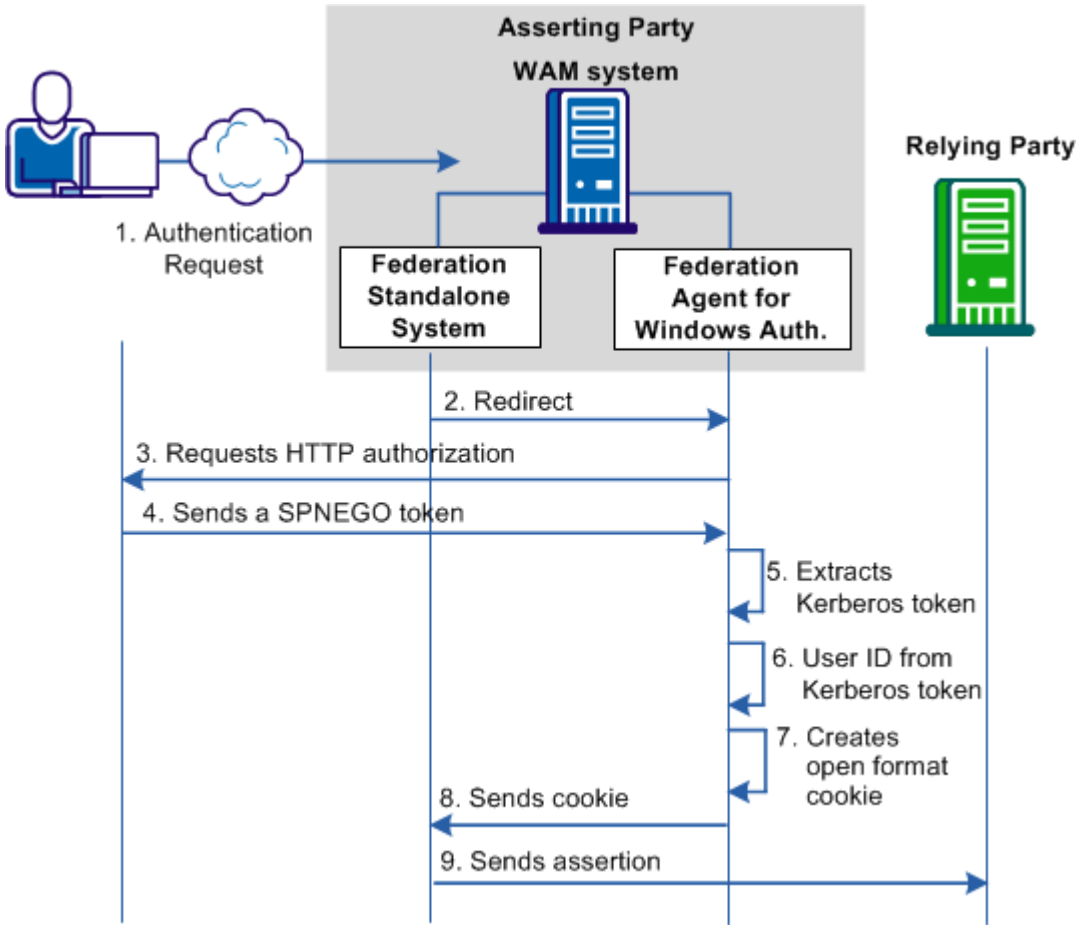


The following process references annotations in the preceding diagram:

1. An authentication request is made to federation system at the asserting party.
2. The federation system recognizes the request as a delegated authentication request and redirects to the request to the Federation Agent.
3. The 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 Agent.
5. The Federation 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 Agent.
7. If a security context is associated with a user, the Federation 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 the federation system.
10. The federation system sends an assertion to the relying party to complete federation processing.

Kerberos Protocol

The following illustration shows how the federation system with the Federation Agent use the Kerberos protocol:



The following process references annotations in the preceding diagram:

1. An authentication request is made to the federation system at the asserting party.

   The federation system recognizes that this request is a delegated authentication request.

2. The federation system redirects to the Federation Agent.
3. The Federation Agent requests an HTTP authorization from the browser.
4. If the browser is configured for IWA, it sends a SPNEGO token to the Federation Agent. This token allows initiators and acceptors to negotiate whether to use Kerberos or NTLM.
5. The Federation 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 the federation system.
9. The federation system does the required processing and sends an assertion to the relying party.

Chapter 2: Installation Prerequisites for the Federation Agent for Windows

Install the Federation Agent for Windows Authentication on the same Windows or UNIX system where is installed. The following restrictions apply:

- The Federation Agent is incompatible with federation installations using the CA SiteMinder® Connector.
- The browser issuing a single sign-on (SSO) request cannot be on the same system as the federation server.

The CA SiteMinder® Federation 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 when you run the Agent configuration wizard.

The setup process for Federation Windows Agent includes the following steps:

1. Complete installation prerequisites, which vary depending on the mode of operation and the operating environment:
   - NTLM with the Agent on Windows
   - Kerberos with the Agent on Windows and the KDC on Windows
   - Kerberos with the Agent on Windows and the KDC on UNIX
   - Kerberos with the Agent on UNIX and the KDC on Windows
   - Kerberos with the Agent on UNIX and the KDC on UNIX
2. Install the Federation Agent for Windows.
3. Configure Federation Agent for Windows. (see page 33)
4. Configure the delegated authentication for the federation system.

NTLM Mode on a Windows System

Before you install the Federation Windows Agent on a Windows system using NTLM, complete the installation prerequisites.

1. Set up the domain controller on Windows for NTLM.
2. Configure Internet Explorer settings.

Set up the Domain Controller 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 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.

Follow these steps:

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.

Configure Internet Explorer for single sign-on. The procedures apply whether you are using NTLM or Kerberos as the authentication protocol.

More information:

Internet Explorer Configuration Settings (see page 24)

Kerberos Mode for a Windows System with a Windows KDC

Complete the installation prerequisites for the Federation Agent on a Windows system using Kerberos mode. The KDC is on a Windows system. Set up the domain controller for Kerberos on Windows.

1. Set up the Domain Controller on Windows for Kerberos.
2. Complete Additional Configuration for Kerberos on Windows
3. Configure Internet Explorer Settings

Set up the Domain Controller 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 system 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, confirm the Kerberos version number.

Follow these steps:

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 by opening a command prompt window and enter the following command:

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

   Use the password entered in step 4.

   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)
```

8. Copy the keytab file to a secure location on the federation system at the asserting party.

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

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

Complete Additional Configuration for Kerberos on Windows

The following actions are required on the federation system when using Kerberos on Windows:

1. Configure a Kerberos configuration file (krb5.ini). Place the krb5.ini file 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
```

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

Configure Internet Explorer for single sign-on. The procedures apply whether you are using NTLM or Kerberos as the authentication protocol.

More information:

Internet Explorer Configuration Settings (see page 24)

Kerberos Mode for a Windows System with a UNIX KDC

Complete the installation prerequisites for the Federation Agent on a system running Windows in Kerberos mode. The KDC is on a UNIX system.

1. Configure the KDC on a UNIX System.
2. Complete Additional Configuration for Kerberos on Windows.
3. Configure Internet Explorer Settings.

Configure the KDC on a UNIX System

The UNIX server that hosts the Kerberos key distribution center (KDC) must be configured to support the federation system. Part of this process is to create a keytab file. A keytab file is required for Kerberos authentication.

Follow these steps:

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

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

3. Add the CA SiteMinder® Federation Standalone system service principal name with this command:

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

4. Create a keytab file by opening a command prompt window and enter the following command:

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

   The keytab file is created.

5. Enter quit.

The configuration of federation on the UNIX KDC server is complete.

Complete Additional Configuration for Kerberos on UNIX

To configure Kerberos, the following commands are required on a federation system 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.

Configure Internet Explorer for single sign-on. The procedures apply whether you are using NTLM or Kerberos as the authentication protocol.

More information:

Internet Explorer Configuration Settings (see page 24)

Kerberos Mode for a UNIX System with a Windows KDC

Complete the prerequisites for installing the Federation Agent on a UNIX system running in Kerberos mode. The KDC is on a Windows system.

1. Set up the Domain Controller on Windows for Kerberos.
2. Additional Configuration for Kerberos on UNIX.
3. Configure Internet Explorer Settings.

Set up the Domain Controller 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 system 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, confirm the Kerberos version number.

Follow these steps:

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 by opening a command prompt window and enter the following command:

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

   Use the password entered in step 4.

   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)
```

8. Copy the keytab file to a secure location on the federation system at the asserting party.

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

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

Complete Additional Configuration for Kerberos on UNIX

To configure Kerberos, the following commands are required on a federation system 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.

Configure Internet Explorer for single sign-on. The procedures apply whether you are using NTLM or Kerberos as the authentication protocol.

More information:

Internet Explorer Configuration Settings (see page 24)

Kerberos Mode for a UNIX System with a UNIX KDC

Complete the installation prerequisites for the Federation Agent on a UNIX system running in Kerberos mode. The KDC is on a UNIX system.

1. Configure the KDC on a UNIX System.
2. Additional Configuration for Kerberos on UNIX.
3. Configure Internet Explorer Settings.

Configure the KDC on a UNIX System

The UNIX server that hosts the Kerberos key distribution center (KDC) must be configured to support the federation system. Part of this process is to create a keytab file. A keytab file is required for Kerberos authentication.

Follow these steps:

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

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

3. Add the CA SiteMinder® Federation Standalone system service principal name with this command:

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

4. Create a keytab file by opening a command prompt window and enter the following command:

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

   The keytab file is created.

5. Enter quit.

The configuration of federation on the UNIX KDC server is complete.

Complete Additional Configuration for Kerberos on UNIX

To configure Kerberos, the following commands are required on a federation system 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.

Configure Internet Explorer for single sign-on. The procedures apply whether you are using NTLM or Kerberos as the authentication protocol.

More information:

Internet Explorer Configuration Settings (see page 24)

Internet Explorer Configuration Settings

To function in a single sign-on deployment, configure some specific Internet Explorer settings.

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.

Follow these steps:

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.

Follow these steps:

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 (Optional)

At the asserting party, when a proxy server is inserted between the browser and the federation system with the Agent, authentication no longer works. In this case all URLs with relative domain names must be configured not to go through the proxy server.

Follow these steps:

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 (Optional)

If your configuration has a firewall between the Federation 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: Install the Federation Agent for Windows Authentication

Installation Requirements

Consider the following installation requirements:

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

Important! If you upgrade CA SiteMinder® Federation Standalone to the current version, upgrade the Agent to the same version. Otherwise, the Agent fails to work properly.

Installation Executables

The following table identifies the installation executables for the Federation Agent.

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-*version*-sol.bin
Linux	ca-fedmgr-iwa-*version*-rhel30.bin
Windows	ca-fedmgr-iwa-*version*-win32.exe

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

Install the Federation Agent (Windows)

Run the installer.

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.

   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 Agent (UNIX)

Run the installer.

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.

   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 Agent

After the Federation 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 does not require any user intervention. It relies on an installation properties file that 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.
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 Agent (Windows)

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

Follow these steps:

1. Select Start, All Programs, CA, Federation Standalone, Uninstall CA SiteMinder® Federation Standalone Windows Authentication Agent.

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

The Federation Agent for Windows Authentication is removed from your system.

Uninstall the Federation Agent (UNIX)

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 Agent for Windows Authentication home directory.
3. Enter the following command:

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

The Federation Agent is removed from the system.

Upgrade the Federation Agent to r12.52 SP1

The installation program can also upgrade your version of the Federation Agent for Windows Authentication. Remember to install the Federation Agent on a system where CA SiteMinder® Federation Standalone is already installed.

Important! The Federation Agent must be the same version as CA SiteMinder® Federation Standalone. If you upgrade the federation system, upgrade the Agent. Otherwise, the Agent fails to work properly.

Follow these steps:

1. Confirm that the main federation system is the same version as that of the Agent you plan to upgrade. If not, first upgrade CA SiteMinder® Federation Standalone.
2. Run the Windows Agent installation executable for your operating platform.

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

Chapter 4: Configure the Federation Agent for Windows Authentication

Information Required by the Configuration Wizard

After you install the Federation Agent, run the configuration wizard. On a Windows system, select the authentication protocol (Kerberos or NTLM). ON a UNIX system, 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 for Kerberos configurations.

Important! The values for these parameters must match the values that are specified in the Deployment settings of the Administrative UI. Find out the value of these these settings from the CA SiteMinder® Federation Standalone administrator before you configure the Federation Agent.

Cookie zone

Specifies the single sign-on security zone name.

Default: FED

Value: An alphabetic string

Cookie name

Specifies the name of the open format cookie.

Default: ""

Value: An alphabetic string

Encryption password

Specifies the password that derives a key for encrypting the cookie.

Default: ""

Value: An 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. This file is created on the KDC system and moved to the system where the Federation Agent is installed.

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 Federation Agent after the installation. 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_installation_dir\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 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_installation_dir/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_install_dir/connectors/IWA/ca_fedmgr_iwa_env.ksh`
6. Restart the federation services:
   a. Open a command window.
   b. Run the following scripts:

      federation_install_dir/fedmanager.sh stop

      federation_install_dir/fedmanager.sh start

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

Unattended Configuration (Windows)

After you configure the Federation Agent one time using the wizard, you can configure it on the same system, or a different system, using unattended mode. An unattended mode configuration does not require user intervention. It uses a configuration properties file. You can modify the configuration properties to suit your requirements.

Follow these steps:

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

   federation_installation_dir\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 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 (UNIX)

After you configure the Federation Agent one time using the wizard, you can configure it on the same system, or a different system, using unattended mode. An unattended mode configuration does not require user intervention. It uses a configuration properties file. Modify the configuration properties file to suit your requirements.

Follow these steps:

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

   federation_installation_dir/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 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.

Modifying the Configuration File for the Federation Agent (Optional)

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

Value: 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

Value: 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

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

Chapter 5: Delegated Authentication Setup

The Federation Agent works with CA SiteMinder® Federation Standalone so users can authenticate in an IWA context. Because the Federation Agent is acting as a third-party authentication service, configure the federation system to use delegated authentication.

Follow these steps:

1. Log in in to the Administrative UI.
2. Select the SAML 1.1 or SAML 2.0 partnership you want to edit. Edit a Producer-> Consumer partnership or an 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 following information:
   - The Federation Agent requires delegated authentication that is based on the open format cookie. This option is not available if you configured the federation system to use the SiteMinder Connector.
   - The values for the cookie settings that you specified during the Agent configuration must match the values in the Deployment settings of the Administrative UI.
6. Enter the delegated authentication URL.

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

Delegated authentication is enabled.

Note: For more information about delegated authentication, see the *CA SiteMinder® Federation Standalone Guide*.

Chapter 6: Troubleshoot using the Agent Trace Log File

Troubleshoot the Federation 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 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_install_dir*\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 name 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 prompt-based authentication, make sure 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 server.

Solution:

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

Index