



# IWA IdP Integration Kit

Version 2.4

## User Guide

**Ping**Identity®

© 2010 Ping Identity® Corporation. All rights reserved.

PingFederate IWA IdP Integration Kit *User Guide*

Version 2.4

August, 2010

Ping Identity Corporation  
1099 18th Street, Suite 2950  
Denver, CO 80202  
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)

Fax: 303.468.2909

Web Site: [www.pingidentity.com](http://www.pingidentity.com)

### **Trademarks**

Ping Identity, the Ping Identity logo, PingFederate, and the PingFederate icon are trademarks or registered trademarks of Ping Identity Corporation. All other trademarks or registered trademarks are the properties of their respective owners.

### **Disclaimer**

This document is provided for informational purposes only, and the information herein is subject to change without notice. Ping Identity Corporation does not provide any warranties and specifically disclaims any liability in connection with this document.

# Contents

- Introduction.....4**
  - Intended Audience .....4
  - System Requirements.....4
  - Upgrade Information .....4
  - ZIP Manifest.....5
- SSO Processing.....6**
  - Multi-Domain Support .....7
  - Starting SSO from Outside a Trusted Domain.....7
- Installation and Configuration.....8**
  - Step 1: Install the Integration Kit .....8
  - Step 2: Modify the IWA Environment .....9
    - Integrating NTLM Authentication.....9
    - Integrating Kerberos Authentication .....10
  - Step 3: Configure the Adapter in PingFederate .....11
  - Step 4: Configure User Browsers .....14
    - Internet Explorer 6.0 or Higher .....15
    - Firefox 2.0 or Higher.....18
- Troubleshooting .....18**
  - Checking Default IE Browser Settings .....19

# Introduction

The PingFederate Integrated Windows Authentication (IWA) IdP Integration Kit provides an Identity Provider (IdP) adapter for PingFederate. This kit allows a PingFederate IdP server to perform single sign-on (SSO) to Service Provider (SP) applications based on IWA credentials.

The IWA Adapter authenticates a user in the specified domain using either the Kerberos v5 or Windows NT LAN Manager (NTLM) protocol, depending on what type of credential token the client Web browser sends back.

## Intended Audience

This document is intended for system administrators with experience using the Windows Server domain controller in conjunction with configuration and maintenance of Microsoft Active Directory. Basic knowledge of networking and user-management configuration with IWA is assumed. Please consult the documentation provided with your server tools if you encounter any difficulties in areas not directly associated with PingFederate or the IWA Integration Kit.

## System Requirements

The following prerequisites must be met to implement this Kit:

- PingFederate 4.1 or higher

---

**Important:** For cluster configurations, the load balancer(s) must be configured to use “sticky sessions” (keep-alive connections) to PingFederate servers using the IWA Adapter.

---

- J2SE JDK 1.6.0\_19 or higher

---

**Note:** This Java update version corrects a Kerberos channel-binding issue that prevented the IWA Adapter from working with an incoming channel-binding request from a Microsoft initiator.

---

- Internet Explorer 6.0 or higher, or Firefox 2.0 or higher (for the end users)
- End-user platform must be Windows-based
- Windows Server 2003 or 2008 for the domain controller

## Upgrade Information

If you are upgrading an existing deployment of this integration kit prior to version 2.4, Kerberos authentication will continue to work as configured. However, to support the latest NTLM authentication, additional configuration is required (see [“Integrating NTLM Authentication”](#) on page 9).

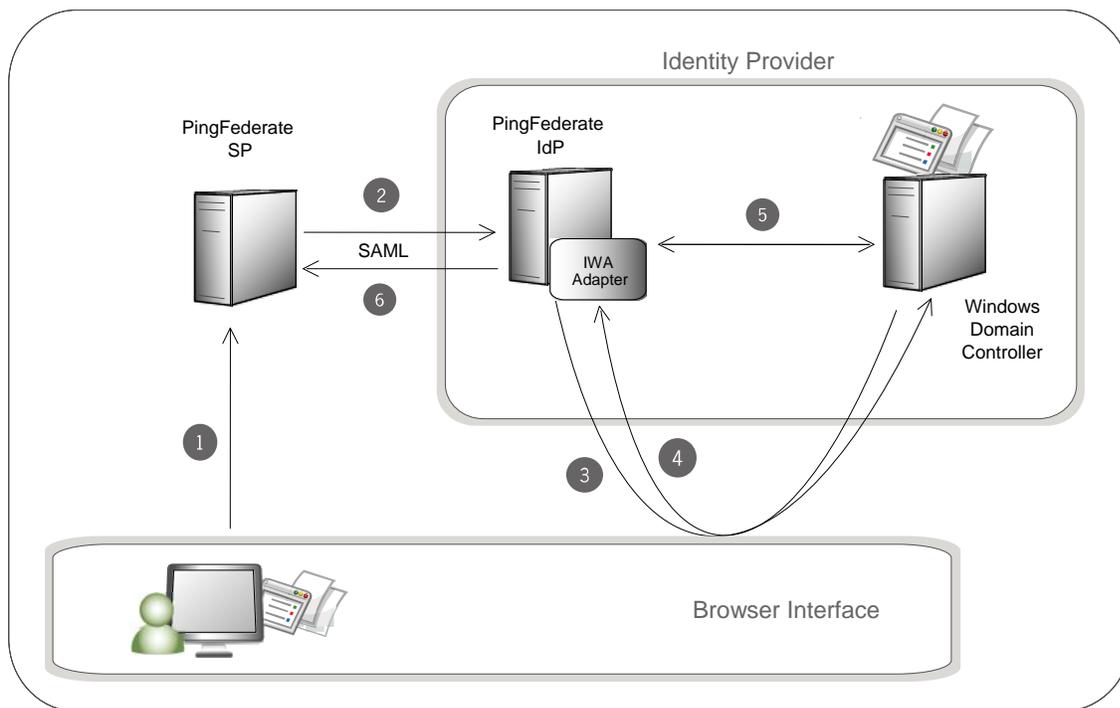
## ZIP Manifest

The distribution ZIP file for the IWA IdP Integration Kit contains the following:

- `\config` – contains configuration script:
  - `SetComputerPass.vbs` – Visual Basic script for setting a password via command line on a Computer account in Active Directory
- `\docs` – contains additional documentation:
  - `Legal.pdf` – copyright and license information
  - `IWA_IdP_Integration_Kit_Qualification_Statement.pdf` – testing and platform information
  - `IWA_IdP_Integration_Kit_User_Guide.pdf` – this document
- `\dist` – contains libraries needed to run the adapter:
  - `pf-iwa-authn-adapter-2.4.jar` – the IWA Adapter JAR file
  - `jcifs-krb5-1.3.12-PF.jar` – the Java Common Interface File System (JCIFS) library
  - `jespa-1.0.14.jar` – Java software library that provides advanced integration with Microsoft Active Directory.

# SSO Processing

The following figure shows a basic SP-initiated SSO scenario in which PingFederate servers authenticate users to an SP application using the IWA Adapter:



## Sequence

1. The user initiates SSO from an SP application through the PingFederate SP server.

---

**Note:** This SP-initiated scenario represents one use case in which both the IdP and SP are using PingFederate (or the SP has deployed some other SAML-enabled federation capability). You can also deploy the IWA Adapter to enable IdP-initiated SSO: in this case the user would request access to the SP resource at the IdP site, and the processing sequence would not include the next step.

---

2. The PingFederate SP server generates a SAML `AuthnRequest` to the PingFederate IdP server.
3. The PingFederate IdP server requests user authentication using the IWA Adapter if the user is not already logged on. The IWA Adapter challenges the browser for authentication.
4. The browser obtains a Kerberos Service Ticket or NTLM token (depending on which method is available) from the domain controller and passes the ticket/token to the IWA Adapter.
5. The IWA Adapter validates the Kerberos ticket or NTLM token:

If a Kerberos ticket is received, the IWA Adapter accesses the domain controller and validates the ticket using the credentials defined in the adapter's configuration (see "[Installation and Configuration](#)" on page 8).

If an NTLM token is received, the IWA Adapter invokes the NTLM authentication filter which performs authentication using the NETLOGON service.

If validation succeeds, the PingFederate IdP server retrieves the username and domain from the ticket or token.

6. The PingFederate IdP server generates a SAML assertion with the username and/or domain of the authenticated user and passes it to the PingFederate SP server.

## Multi-Domain Support

If your network uses multiple domains in a single server forest, you can configure the IWA Adapter for just one domain in the forest (see “[Installation and Configuration](#)” on page 8). This configuration requires transient, two-way trust among domains, which is established by default when subdomains or separate domains are created within the same forest.

If you are configuring only one domain, then you also need to configure only one Service Principal Name (see “[Integrating Kerberos Authentication](#)” on page 10).

If your network topology consists of multiple forests *without* a trust relationship between them, then you must configure multiple domains in the adapter setup. In addition, your applications will require passing a parameter as part of the `startSSO` query string, to determine the domain. For IdP-initiated SSO, the domain must be sent as the parameter `IWADomain`, while for SP-initiated SSO `RequestedAuthnCtx` must be used. For example:

### (IdP-initiated SSO)

```
https://<PF_host>:<port>/idp/startSSO.ping?PartnerSpId=<Connection_Id>&
IWADomain=europe.example.com
```

### (SP-initiated SSO)

```
https://<PF_host>:<port>/sp/startSSO.ping?PartnerIdpId=<Connection_Id>&
RequestedAuthnCtx=europe.example.com
```

where: `<PF_host>` is the domain name (or IP address) of the machine running PingFederate,  
`<port>` is the PingFederate port (refer to the *PingFederate Administrator's Manual*), and  
`<connection_id>` is the Connection ID of the SP connection.

## Starting SSO from Outside a Trusted Domain

The IWA Adapter uses NTLM to prompt users to log on using their network credentials if they attempt to initiate an SSO without being logged on to a domain configured in the adapter setup, or to a domain trusted by a configured domain.



User Name must be sent in the form of <DOMAIN>\<USERNAME>.

---

**Note:** If a user is already authenticated in a different NTLM domain, one that is not trusted or configured in the adapter setup, then the browser may attempt to send the user's credentials automatically as NTLM headers. In this case, the browser will consume two of the allowed number of logon attempts. (The number of attempts is configurable in the adapter setup.)

---

## Installation and Configuration

This section describes how to:

- Install the IWA Integration Kit.
- Modify your IWA environment for both Kerberos and NTLM to interact with the IWA Adapter.
- Configure the PingFederate IWA Adapter.
- Update end-user browsers.

### Step 1: Install the Integration Kit

1. If applicable, remove any previous releases of the IWA or NTLM Adapters from the directory:  
`<pf-server>\pingfederate\server\default\deploy`

These libraries may include any or all of the following files:

- `pf4-iwa-authn-adapter-1.0.jar`
  - `pf4-ntlm-authn-adapter-1.0.jar`
  - `pf-iwa-authn-adapter-2.x.jar`
  - `jcifs-1.1.9.jar`
2. Unzip the distribution ZIP file and copy the following files to the same `server\default\deploy` directory of your PingFederate server installation:
    - `dist\pf-iwa-authn-adapter-2.4.jar`
    - `dist\jcifs-krb5-1.3.12-PF.jar`
    - `dist\jespa-1.0.14.jar`
  3. Start or restart PingFederate.

4. If PingFederate is deployed in a server-cluster environment, ensure that you repeat this installation on all PingFederate nodes.

Also, see the “**Important**” note under “[System Requirements](#)” on page 4.

For more information about deploying PingFederate in a cluster and updating configurations, see the *PingFederate Server Cluster Guide*.

## Step 2: Modify the IWA Environment

To integrate PingFederate and the IdP Adapter into your IWA environment, several domain-controller configuration changes are required to enable both NTLM and Kerberos authentication.

---

**Note:** You must have Domain Administrator permissions.

---

### Integrating NTLM Authentication

To use NTLM authentication, you must create a Computer account in Active Directory and separately assign a password that will be needed for the IWA Adapter settings later.

---

**Note:** If you have multiple domains and wish to use Domain Local groups with group-based access control, only the groups in the same domain as the new service account will be in scope.

---

To create a Computer account and a password:

1. On the domain controller, open Active Directory Users and Computers.

---

**Tip:** If you have previously set up a domain account to enable Kerberos authentication using the PingFederate IWA Adapter, you may use the same account *if* it is a Computer account (not a User account). In that case, skip the next step.

---

2. Create a New→Computer account for the PingFederate IWA Adapter.
3. Set a password for the account.

You will need to know the password during configuration of the IWA Adapter in PingFederate.

#### On Windows Server 2003:

- a. Determine the account distinguished name (DN).

The account DN is required for setting the password in the next step.

Normally, the DN can be derived from the account name and domain. For example if the service account name is PINGAGENT in an Active Directory domain called `example.com`, then the DN would be:

```
CN=PINGAGENT, CN=Computers, DC=example, DC=com
```

If you are not sure about the DN or prefer to display it for copy/paste, you can use the ADSI (Active Directory Services Interfaces) Edit snap-in for the Microsoft Management Console to show AD entries by DN.

- b. As an Administrator on the domain controller, run the Visual Basic script `SetComputerPass.vbs` located in the `conf` directory of this distribution:  
`C:\>cscript SetComputerPass.vbs <pf_adapter_DN>`

where: `<pf_adapter_DN>` is the DN of the Active Directory account set up in the previous steps.

At the Password prompt, enter a strong (preferably random) password and make a note of it.

---

**Note:** For Windows Server 2003 there is no Microsoft-standard tool for setting passwords manually on a Computer account. This third-party VBScript is provided for that purpose.

---

#### **On Windows Server 2008:**

- a. Access ADSI Edit and locate the account used by the IWA Adapter.
- b. Right click the account name and select Reset Password.
- c. In the Reset Password window, use a strong (preferably random) password and make a note of it.

## **Integrating Kerberos Authentication**

Follow the procedure below to:

- Create a domain account for the IWA Adapter (configured later). You may wish to use the same account set up for NTLM authentication.
- Set the Service Principal Name (SPN) of the IdP PingFederate server for the account.

The Windows utility required for this setting, `setspn`, is distributed with Windows Server Support Tools. For Windows Server 2003 the tools are located on the installation CD under `...\support\tools` or available at the following URL:

<http://www.microsoft.com/downloads/details.aspx?FamilyId=6EC50B78-8BE1-4E81-B3BE-4E7AC4F0912D&displaylang=en>

Or you can download only the `setspn` utility from:

<http://www.microsoft.com/downloads/details.aspx?familyid=5fd831fd-ab77-46a3-9cfe-ff01d29e5c46&displaylang=en>

#### **To enable IWA authentication using Kerberos:**

1. Create a domain account that PingFederate can use to contact the Kerberos Key Distribution Center (KDC).

Alternatively, you can use the Computer account set up for NTLM authentication.

The account should belong to the “Domain Users” group. We recommend that the password be set with no expiration.

2. Use the Windows utility `setspn` (see the introduction to this section) to register SPN directory properties for the account by executing the following command on the domain controller:

```
setspn -a HTTP/<pf-idp.domain.name> <pf-server-account-name>
```

where: `<pf-idp.domain.name>` is the fully qualified domain name of the PingFederate server and `<pf-server-account-name>` is the domain account defined in the IWA Adapter configuration.

---

**Note:** “HTTP” must be capitalized and followed by a forward-slash (/).

---

3. Verify that the registration was successful by executing the following command:

```
setspn -l <pf-server-account-name>
```

This will give you a list of SPNs for the account. Verify that `HTTP/<pf-idp.domain.name>` is one of them.

---

**Note:** After making an SPN change, any end-users already authenticated must re-authenticate (close the browser or log off and back on) before attempting SSO.

---

### Step 3: Configure the Adapter in PingFederate

1. Log on to the PingFederate administration console and click **Adapters** under My IdP Configuration on the Main Menu.
2. On the Manage IdP Adapter Instances screen, click **Create New Adapter Instance**.
3. On the Adapter Type screen, enter an Adapter Instance Name and Adapter Instance Id, and select IWA IdP Adapter 2.4 as the Adapter Type.
4. Click **Next**.

**Configuring IdP Adapter** [Help](#) | [Support](#) | [About](#) | [Logout \(Administrator\)](#)

[Main](#) | [Manage IdP Adapter Instances](#) | [Create Adapter Instance](#)

[Type](#) | [\\* IdP Adapter](#) | [Adapter Attributes](#) | [Summary](#)

Complete the configuration necessary to look up user security contexts in your environment. This configuration was designed into the adapter for use at your site.

This adapter uses Integrated Windows Authentication (IWA) to leverage a Windows Domain login for Web authentication.

**Windows Domain(s)** (Domain(s) participating in IWA authentication. Click 'Add a new row ...' below to enter information. Then click 'Update' to validate the defined domain.)

Domain (FQDN)	Domain Controller (Host name)	Kerberos Username	Kerberos Password	NTLM Username	NTLM Password	DNS Servers (A comma-separated list of IP addresses)	Intranet IP Range(s) (CIDR notation using comma separators as needed. E.g.: 172.16.0.0/11,172.16.29.0/24)	Action
								<a href="#">Add a new row to 'Windows Domain(s)'</a>

Field Name	Field Value	Description
Error URL Redirect	<input type="text"/>	The URL for browser redirect when an error occurs or authentication fails.

[Show Advanced Fields](#)

5. On the IdP Adapter screen, click **Add a new row to 'Windows Domain(s)'** under Action.
6. Enter the fully qualified domain name (FQDN) of your IWA Windows domain.  
For example:  
corporation.companydomain.com
7. (Optional) Specify the Domain Controller host name or IP address for your IWA Windows Domain.  
Host names are not fully qualified (they do not include the domain). For example:  
Fn\_dc1  
If unspecified, the IWA Adapter uses a DNS lookup to find the domain controller.
8. In the Kerberos Username and Kerberos Password fields, respectively, enter the ID and password for the Adapter's Kerberos domain account (see "[Integrating Kerberos Authentication](#)" on page 10).
9. In the NTLM Username and NTLM Password fields, respectively, enter the ID and password for the Adapter's NTLM domain account (see "[Integrating NTLM Authentication](#)" on page 9).
10. (Optional) If PingFederate is deployed outside of the domain, enter a comma-separated list of DNS servers (IP addresses) for the domain being configured.
11. Specify the Intranet IP Range(s) for the domain in Classless Inter-Domain Routing (CIDR) format.  
This information is required to determine if a user is coming from outside the domain, in which case NTLM authentication is used as Kerberos will not be available.

12. Click **Update** in the Action column.
13. (Optional) Repeat steps 5 through 12 as needed, for any additional IWA domains.

---

**Note:** Depending on your network infrastructure, it may not be necessary to configure multiple domains (see [“Multi-Domain Support”](#) on page 7).

**Note:** To enable a failover domain controller within a domain, add the domain again, changing the Domain Controller host entry.

---

14. (Optional) Enter a URL in the Error URL Redirect field.

This is an error “landing” page in the IdP domain that the end user will see if authentication fails for any reason. PingFederate adds an `errorMessage` query parameter to the URL, containing information that can be displayed to the user.

If the field is blank, the browser displays its generic error page.

15. (Optional) Click **Show Advanced Fields** and make any desired changes to the default settings.

Refer to the screen descriptions in the administrative console. The following table provides supplemental information and instructions.

Field	More Information
Auto Config Kerberos	Clear this checkbox if an administrator will configure the <code>krb5.conf</code> file manually.
Force TCP	If you choose this option, ensure that you restart PingFederate after saving the configuration.
KDC Timeout	The default value is recommended but may be adjusted as needed. The new timeout will take effect only after PingFederate is restarted, after you save the configuration.
<code>jcifs.smb.client.soTimeout</code>	The default value is recommended but may be adjusted as needed.
<code>jcifs.netbios.cachePolicy</code>	The default value is recommended but may be adjusted as needed.
Challenge Retries	For more information about the Challenge Retries field, see <a href="#">“Starting SSO from Outside a Trusted Domain”</a> on page 7.
Kerberos Only Authentication	By default, the IWA Adapter authenticates a user to PingFederate via the standard IWA method: first by using Kerberos, then, if Kerberos fails, by falling back to NTLM. As needed for increased security, you can restrict authentication to Kerberos by clicking this checkbox.

Field	More Information
Authentication Context Value	This may be any value agreed to with your SP partner. Standard URIs are defined in the SAML specifications (see the OASIS document <a href="#">saml-authn-context-2.0-os.pdf</a> ).
NTLM Log Level	Change this value as needed to have the Adapter write more or less information into a separate log file maintained for NTLM processing. This log, <code>iwa-ntlm.log</code> , is located in the directory: <code>&lt;pf_install&gt;/pingfederate/log</code> <b>Note:</b> Logging for Kerberos authentication processing is maintained in the PingFederate server log in the same directory.

16. Click **Next**.

17. On the Adapter Attributes screen, select one or more attributes (exported from the adapter to PingFederate) to be used in constructing a unique identifier (Pseudonym) for account linking.

Refer to the “Key Concepts” chapter in the PingFederate *Administrator’s Manual* for information about account linking (or click **Help** on this screen). To ensure correct PingFederate performance under all circumstances, a Pseudonym selection is required regardless of whether an SP partner actually uses account linking.

You may also choose to mask attribute values in PingFederate log files. More information is available on the **Help** page.

18. Click **Next**.

19. On the Summary screen, click **Done**.

20. On the Manage IdP Adapter Instances screen, click **Save**.

You can now use the adapter instance for SP partner connections. (See “IdP Adapter Mapping” in the PingFederate *Administrator’s Manual*.)

---

**Important:** Do not configure more than one instance of the IWA adapter; multiple instances are not supported in the PingFederate runtime engine.

---

## Step 4: Configure User Browsers

This section contains configuration information needed for client-side browsers at your site in order to use IWA with PingFederate.

---

**Note:** If the browser is not properly configured, users may be prompted to authenticate manually to IWA applications using their network credentials, rather than automatically via SSO.

---

## Internet Explorer 6.0 or Higher

The browser setup for IE may require the following modifications of Internet Options (in the Tools menu).

---

**Tip:** This configuration is not necessary under certain conditions, as described in the **Note** at the beginning of each step.

**Important:** Other Internet Options required for IWA generally are part of the default IE installation. If you are setting up IWA, as well as the Adapter, and you encounter errors at runtime, you may need to verify that the defaults have not been changed (see “[Checking Default IE Browser Settings](#)” on page 19).

---

### To configure IE for PingFederate:

1. Under the Security tab for the Local intranet, add to the list of accessible Web sites the fully qualified domain name that is part of the PingFederate URL used to start SSO (<pf-idp.domain.name>).

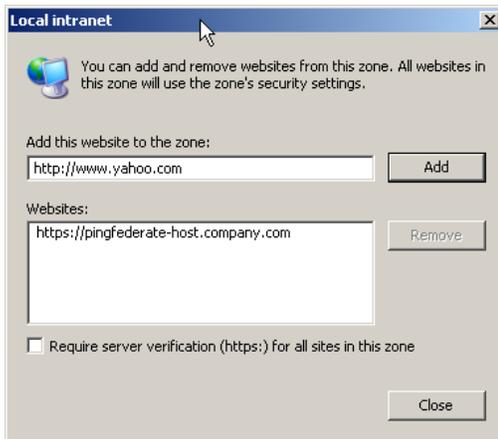
---

**Note:** This step may be skipped if <pf-idp.domain.name> is internal and not fully qualified. For example, if it is pingfederate, you can skip the step. However, if <pf-idp.domain.name> is pingfederate.company.com, then you must add the domain to the **Sites** list, as described in the following substeps.

---



- a. Click **Sites**.
- b. In the next dialog box, ensure that **Include all sites that bypass the proxy server** is checked, and then click **Advanced**.



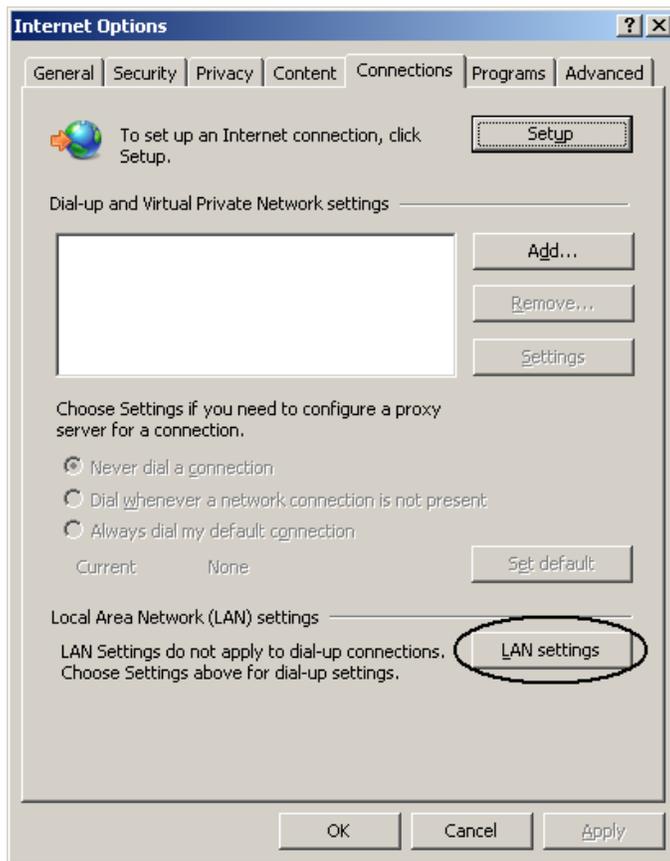
- c. Enter `<pf-idp.domain.name>` and click **Add**.
  - d. Click **Close** and then click **OK** to close the dialog boxes.
2. Verify proxy settings.

---

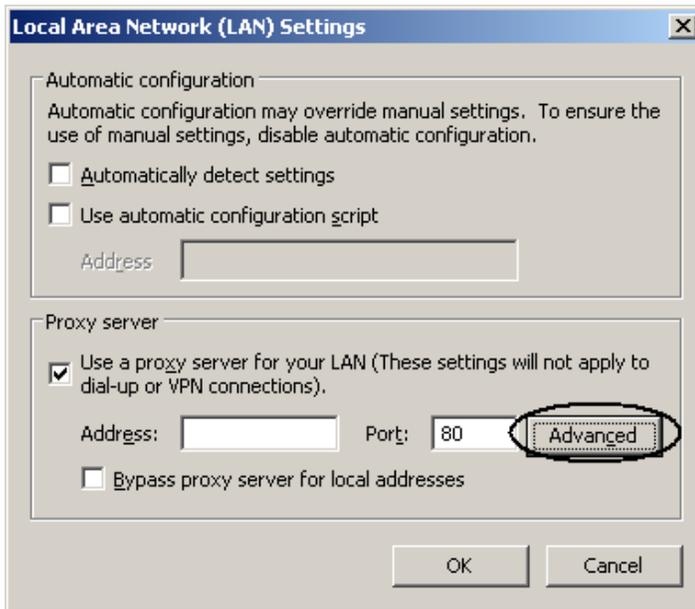
**Note:** Skip this step if a proxy is not used.

---

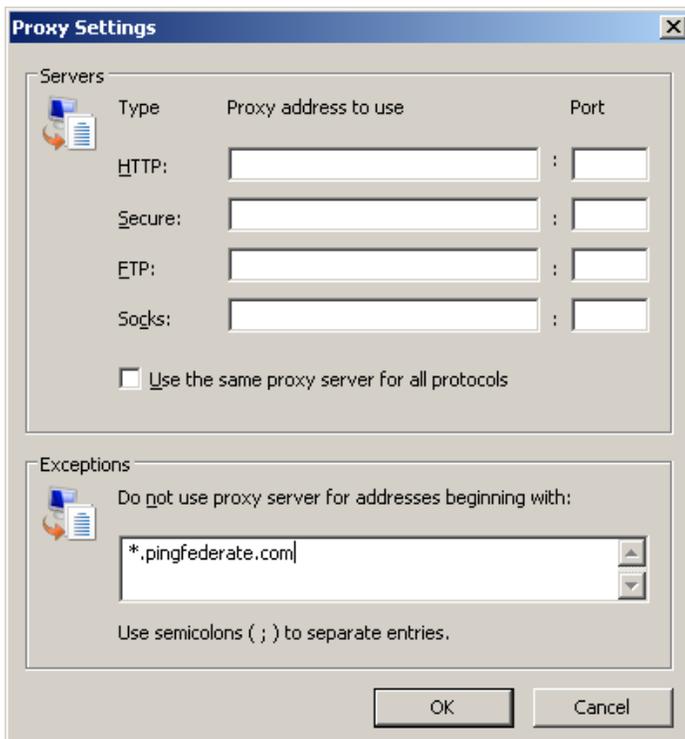
- a. Click the **Connections** tab in the Internet Options dialog.



- b. Click **LAN Settings**.



- c. In the LAN Settings dialog, ensure **Use a proxy server for your LAN is checked** and click **Advanced**.



- d. In the **Proxy Settings** dialog box, enter the PingFederate IdP server's fully qualified domain name in the Exceptions field.
- e. Click **OK** twice to return to Internet Options.

## Firefox 2.0 or Higher

1. Enter `about:config` into the address bar.
2. On the configuration-setting page, find the following properties and set their values to the fully qualified domain name of the PingFederate server:
  - `network.negotiate-auth.trusted-uris` (for Kerberos)
  - `network.automatic-ntlm-auth.trusted-uris` (for NTLM)

## Troubleshooting

The following table lists potential problems administrators might encounter during the setup or deployment of the IWA Adapter, along with possible solutions.

---

**Tip:** Additional troubleshooting information is available at the Ping Identity [Customer Portal](http://www.pingidentity.com/support-and-downloads/portal.cfm) ([www.pingidentity.com/support-and-downloads/portal.cfm](http://www.pingidentity.com/support-and-downloads/portal.cfm)) under **Answers**.

---

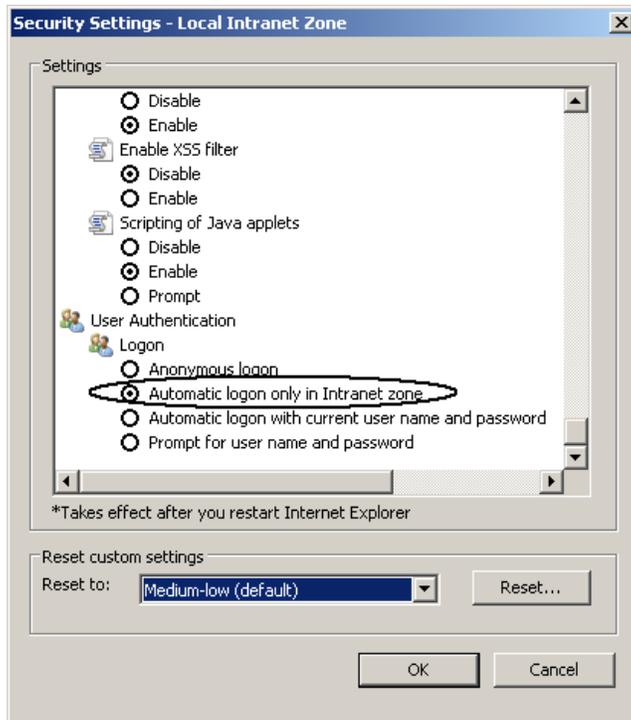
Problem	Possible Solution
The VBScript used to set the password on the IWA Adapter Computer account on Windows Server 2003 returns the error: ActiveX component can't create object: 'ScriptPW.Password'	Ensure the operating system running the script contains a required Windows library, <code>scriptpw.dll</code> , or run the script on the domain controller.  For example, while it is possible to run the script on other workstations with the right administrative permissions, operating systems such as Vista and Windows 7 do not contain the required library.
Remote users (outside the domain) need to log on a second time to reach an IWA resource, or they receive a browser error.	Ensure you have entered in the adapter configuration a CIDR list of IPs used by the domain.
SSO via the IWA Adapter does not work with server clustering.	Ensure that the load balancer uses keep-alive connections for all PingFederate servers (see the <i>Server Clustering Guide</i> ). This restriction is due to NTLM design; however, the same is true for Kerberos authentication.
SSO fails with a "FULL HEAD" warning in the server log.	Increase the <code>headerBufferSize</code> in the Jetty configuration file <code>jboss-service.xml</code> , located in the directory: <code>&lt;pf_install&gt;pingfederate\server\default\deploy\jetty.sar\META-INF</code>

Problem	Possible Solution
<p>Kerberos authentication is not working—always fails over to NTLM.</p>	<p>Ensure the SPN for the Adapter service account is unique (see <a href="#">“Integrating Kerberos Authentication”</a> on page 10).</p> <p>If the SPN is okay, ensure end-user browser settings are correct (see <a href="#">“Step 4: Configure User Browsers”</a> on page 14 and <a href="#">“Checking Default IE Browser Settings”</a> on page 19).</p> <p>There can be a variety of other reasons for Kerberos issues. Customers with support contracts can find additional information at the <a href="#">Customer Portal</a> under <b>Answers</b>.</p>
<p>The error "Failed to locate authority for name: ...." appears in <code>iwa-ntlm.log</code>.</p>	<p>Try setting the DNS Server field in the adapter configuration.</p>
<p>The exception "account used is a Computer Account" appears in <code>iwa-ntlm.log</code>.</p>	<p>This error indicates that there is a problem with the account used for NTLM authentication. To resolve this issue, first try resetting the password using a complex value that exceeds strong password requirements (see <a href="#">“Integrating NTLM Authentication”</a> on page 6. (Do not use a password that matches the account name.)</p> <p>If resetting the password does not resolve the error, delete the account and create a new one (see the section referenced above). Use a completely different account name with no more than 15 alphanumeric characters, and set a complex password that exceeds strong password requirements.</p>

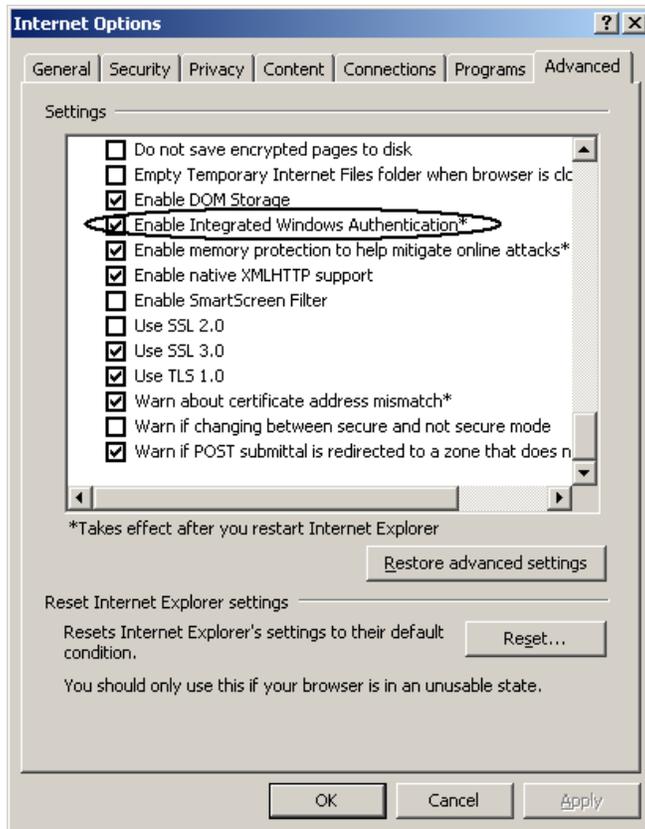
## Checking Default IE Browser Settings

If users have persistent browser errors when requesting IWA-protected applications via PingFederate, first verify that client browsers are configured correctly for both IE and Firefox (see [“Step 4: Configure User Browsers”](#) on page 14”). If those settings are correct, ensure IE default settings for IWA support have not been changed, as described in the following steps:

1. In Tools→Internet Options under the Security tab, verify intranet authentication:
  - a. Click **Custom Level**.



- b. In the Security Settings dialog box, scroll down to User Authentication and ensure that **Automatic logon only in the Intranet zone** is selected.
  - c. Click **OK** to close dialog box.
2. Verify that IWA is enabled:
    - a. Click the **Advanced** tab.
    - b. Scroll down to the Security section.



- c. Ensure that **Enable Integrated Windows Authentication** is selected.
- d. Click **OK**.