

Integrated Windows Authentication (IWA) Integration Kit



Contents

Integrated Windows Authentication (IWA) Integration Kit.....	3
Overview of the SSO flow.....	3
Multi-domain support.....	4
Starting SSO from outside a trusted domain.....	5
Setup.....	5
Install or upgrade the integration kit.....	5
Integrating NTLM authentication.....	6
Integrating Kerberos authentication.....	7
Configure PingFederate access to the domain account.....	8
Configure the adapter in PingFederate.....	8
Configure user browsers.....	11
Internet Explorer 9.0 or higher.....	15
Configure IE for PingFederate.....	18
Firefox browser.....	21
Troubleshooting.....	21
Checking default IE browser settings.....	23
Release notes.....	24
Changelog.....	24
Known issues and limitations.....	26
Download manifest.....	26

Integrated Windows Authentication (IWA) Integration Kit

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

ⓘ Attention:

Updates and support have ended for this integration. The availability of this user guide and the related product download is intended only for those who have existing solutions using this integration.

ⓘ Note:

If using only Kerberos in the deployment (not NTLM), it is recommended to use the Kerberos adapter that ships with PingFederate instead of this kit.

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.

Before you start, you should be familiar with the following parts of the PingFederate documentation:

- [Identity provider SSO configuration](#)
- [Managing IdP adapters](#)

System requirements

- PingFederate 7.x or later

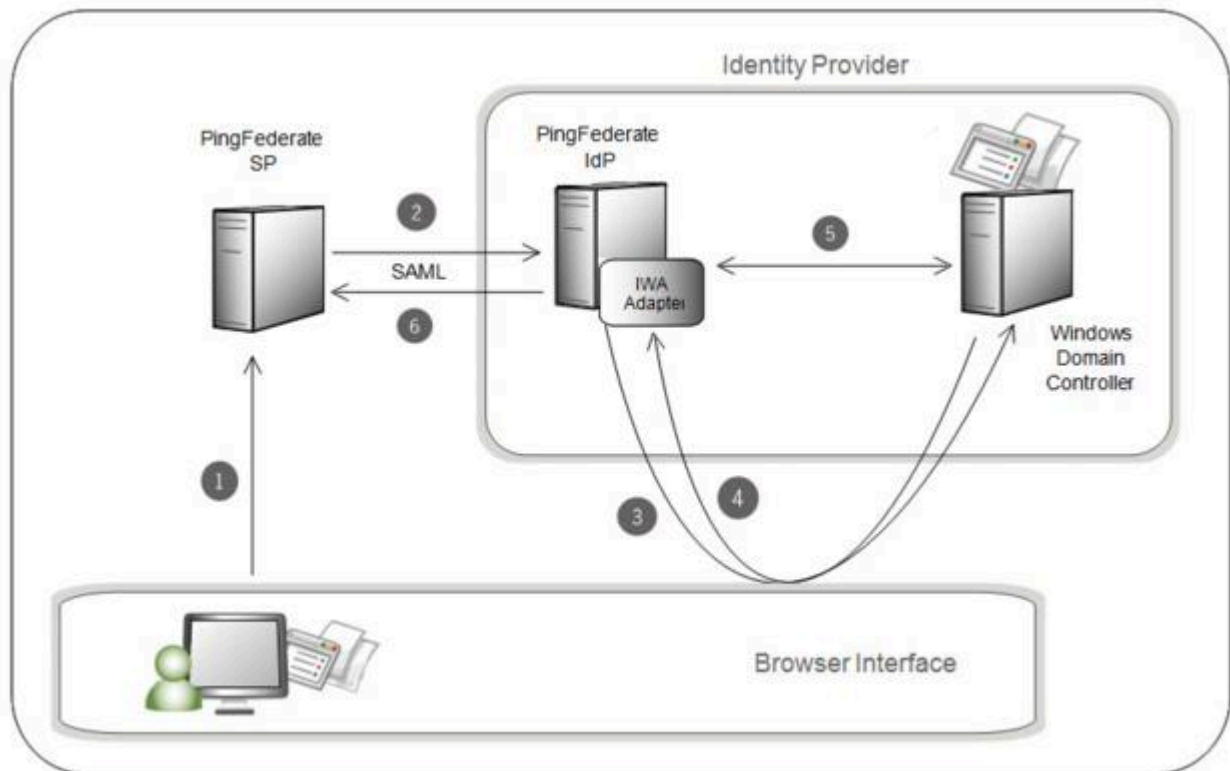
ⓘ Important:

For cluster configurations, the load balancer(s) must be configured to use “sticky sessions” (keep-alive connections) to PingFederate servers using the IWA Adapter, when the default NTLM failover is enabled. Kerberos-only authentication does not require sticky sessions. However, when NTLM failover is enabled and access is attempted from either off-network locations or via non-Kerberos enabled browsers, the IWA adapter will automatically attempt NTLM authentication, which will eventually cause some users to fail to authenticate unless sticky sessions are enabled.

- For end users, Internet Explorer 9.0 or higher, the latest version of Firefox (version 21 or later), or the latest version of Google Chrome (version 27 or later)
- Windows Server 2008, 2008 R2, or 2012 for the domain controller

Overview of the SSO flow

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



Processing Steps

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 steps 1 and 2.

2. The PingFederate SP server generates a SAML `AuthnRequest` to the PingFederate IdP server.
3. The PingFederate IdP server requests user authentication if the user is not already logged on.
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 PingFederate.
5. PingFederate validates the Kerberos ticket or NTLM token: If a Kerberos ticket is received, PingFederate accesses the domain controller and validates the ticket using the Domain/Kerberos Realm defined in PingFederate and selected in the adapter's configuration (see [Installation and configuration](#)).

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](#) on page 4
 - [Starting SSO from outside a trusted domain](#) on page 5

Multi-domain support

If your network uses multiple domains in a single server forest, you can configure the IWA Adapter for only one domain in the forest (see [Installation and configuration](#)). This configuration requires a trust relationship among domains, which is established by default when subdomains or separate domains are created within the same forest.

Note: You only need to configure one domain within PingFederate if there is a trust relationship with the other domains you want to use. For more information, see [How Domain and Forest Trusts Work](#) in the Microsoft documentation.

If you are configuring only one domain, then you also need to configure only one Service Principal Name (see [Integrating Kerberos authentication](#) on page 7).

If your network topology consists of multiple forests *without* a trust relationship between them, then you must configure multiple adapter instances, each instance mapped to a separate domain, and then map those adapter instances to your SP connections that authenticate using IWA.

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 consumes two of the allowed number of logon attempts. (The number of attempts is configurable in the adapter setup.)

Setup

Install or upgrade the integration kit

About this task

Note: The IWA Integration Kit version 3.x and higher is not compatible with earlier adapter versions (2.6 and older). If you have upgraded to PingFederate 7.x or higher from a version that includes configured IWA adapters, you must delete (step 2 below) any existing IWA adapter instances prior to installation (reconfigure new instances later, as needed). If you are upgrading the IWA Integration Kit 3.x, skip step 2 in the following procedure and continue to step 3.

Steps

1. Stop the PingFederate server if it is running.

- If you are upgrading from version 2.6 and older, remove any previous releases of the IWA or NTLM Adapters from the directory:

```
<PF_install>/server/default/deploy
```

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

- pf4-iwa-authn-adapter-*.jar
- pf4-ntlm-authn-adapter-*.jar
- pf-iwa-authn-adapter-*.jar
- jcifs-*.jar
- jcifs-krb5-*.jar
- jespa-*.jar
- jespa-*.jar

Also, remove any existing `krb5.conf` file from the directory:

```
<PF_install>/pingfederate/server/default/data/adapter-config
```

- If you are upgrading from version 3.0, remove the following files from the directory `<PF_install>/server/default/deploy`:

- jespa-*.jar
- jcifs*.jar
- pf-iwa-authn-adapter-*.jar

- From the integration kit `dist` directory, copy the following file into `<PF_install>/server/default/deploy`:

- pf-iwa-authn-adapter-3.2.0.jar

- Optional: Copy the following file from the `dist` directory:

```
kerberos.only.error.template.html
```

into the directory:

```
<PF_install>/pingfederate/server/default/conf/template
```

Note: This user-facing HTML template can be used to standardize authentication behavior across browsers. For more information about this template, see step 15 in [Configure the adapter in PingFederate](#) on page 8.

- Restart the PingFederate server.
- 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](#).

For more information about deploying PingFederate in a cluster and updating configurations, see the PingFederate [Server Clustering Guide](#).

Integrating NTLM authentication

To integrate NTLM authentication, you must create a Computer account in Active Directory and separately assign a password that is needed for the IWA Adapter settings and the AD Domain/Kerberos Realm configuration later.

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

- [Create a computer account and password](#) on page 7

Create a computer account and password

Steps

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

i 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. The service account name (NTLM Username) configured must be 15 characters or less.

i Important: If PingFederate is deployed in a clustered environment, repeat steps 2 and 3 to create multiple NTLM accounts for each node in the cluster. You will need to specify the index of the cluster node associated with each account during configuration of the IWA Adapter in PingFederate.

3. Set a password for each account created.

You need to know the password(s) during configuration of the IWA Adapter and the AD Domain/Kerberos Realm in PingFederate.

On Windows Server

- a. Access ADSI Edit.
- b. Bind to the directory partition and locate the account used by the IWA Adapter.

i Note: For more information, see [ADSI Edit](#) in the Microsoft documentation.

- c. Right-click the account name and select Reset Password.
- d. In the Reset Password window, use a strong (preferably random) password and make a note of it.

Integrating Kerberos authentication

i Note: If using only Kerberos in the deployment (not NTLM), it is recommended to use the Kerberos adapter that ships with PingFederate instead of this kit.

Follow the procedure below to:

- Create a domain account for PingFederate to use for Kerberos authentication. If you have previously set up a domain Computer account to enable NTLM authentication using the PingFederate IWA Adapter, you can use the same account if you are using both NTLM and Kerberos authentication.

i Tip: If you have previously set up a domain Computer account to enable NTLM authentication using the PingFederate IWA Adapter, you can use the same account if you are using both NTLM and Kerberos authentication.

- Set the Service Principal Name (SPN) of the IdP PingFederate server for the account.
- [Enable IWA authentication using Kerberos](#) on page 8

Enable IWA authentication using Kerberos

Steps

1. Create a domain user 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` to register SPN directory properties for the account by executing the following command on the domain controller:

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

where:

- `<pf-idp.domain.name>` is the canonical name of the PingFederate server. For more information on "canonical name", see <https://tools.ietf.org/html/rfc2181#section-10>.
- `<pf-server-account-name>` is the domain account you want to use for Kerberos authentication.

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 gives 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.

Configure PingFederate access to the domain account

About this task

To integrate both NTLM and Kerberos authentication, you must give PingFederate access to the domain account.

Steps

1. Click Active Directory Domains/Kerberos Realms on the PingFederate Main Menu to configure access for PingFederate to the domain accounts you created for NTLM and Kerberos authentication (see [Integrating NTLM authentication](#) on page 6 and [Integrating Kerberos authentication](#) on page 7).
2. Enter the domain account credentials for PingFederate to use when contacting the domain controller(s) or KDC(s) for verifying user authentication (see [Configuring Active Directory domains or Kerberos realms](#) in the PingFederate documentation).

Configure the adapter in PingFederate

Steps

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 Instance**.

3. On the Type screen, enter an Instance Name and Instance Id.

The Name is any you choose for identifying this Adapter Instance. The ID is used internally and may not contain spaces or non-alphanumeric characters.

4. Select IWA IdP Adapter 3.2 as the Type and click **Next**.
5. On the IdP Adapter screen, click **Add a new row to 'NTLM Details'** under Action .
6. In the NTLM Username and NTLM Password fields, respectively, enter the ID and password for the NTLM domain account (see [Integrating NTLM authentication](#) on page 6).

Important: For clustered PingFederate environments, add credentials corresponding to those set up for separate NTLM accounts (see [Integrating NTLM authentication](#) on page 6). Be sure you enter the corresponding index number for the server node in the **Node Index** field (see step 9).

7. If PingFederate is deployed outside of the domain, enter the comma-separated list of DNS servers (IP addresses) for the domain being configured.
8. Optional: If you use Active Directory Sites & Services (ADSS) to define groups of sites and site links for domains, specify the site name.

For more information, see [Windows Server - IT administrator content for current and previous releases](#) in the Microsoft documentation.
9. If you are running PingFederate in a clustered environment, enter the index number for the engine node you want to define. Specifying this number allows you to configure separate credentials for each node in a cluster.

Note: Not specifying a node index causes nodes to share the NTLM credentials when accessing the domain controller, which may cause runtime issues. For more information, see [Troubleshooting](#) on page 21.

Tip: A list of server nodes and the assigned index number can be found on the Cluster Management screen (see [Console configuration push](#) in the PingFederate documentation), or you can find the index numbers for each `pf.cluster.node.index` property in the `<pf_install>/pingfederate/bin/run.properties` file for each server node.

For more information about clustering, see the PingFederate [Server Clustering Guide](#).

10. Click **Update** in the Action column.
11. Optional: Repeat steps 5 through 10 as needed, for any additional engine nodes.
12. Indicate which authentication types are supported for this adapter instance.

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 just Kerberos or just NTLM.

Note: If your operating environment supports non-IE browsers or off-network authentication, select both Kerberos and NTLM authentication.

13. Select the **Domain/Realm Name** for your IWA Windows domain. Domain and Realm names are configured by accessing the Active Directory Domains/Kerberos Realms option from the PingFederate Main Menu (see Using AD Domains and Kerberos Realms in the PingFederate *Administrator's Manual*).

A Domain or Realm must be configured for use with the IWA Adapter. If the Domain or Realm you want does not appear, click **Manage Active Directory Domains/Kerberos Realms** to add it.

14. Optional: Enter a URL for redirecting the user if there are errors. This URL has an `errorMessage` query parameter appended to it, which contains a brief description of the error that occurred. The error page can optionally display this message on the screen to provide guidance on remedying the problem.

Note: In the case of an error, if you define an Error URL and the adapter instance is included in a composite adapter, the user is redirected to the Error URL rather than continuing on to the next adapter in the chain. Leave this field blank to have the adapter continue on to the next adapter (see [Composite Adapter](#) in the PingFederate documentation.)

When employing the `errorMessage` query parameter in a custom error page, adhere to Web-application security best practices to guard against common content injection vulnerabilities. If no URL is specified, the appropriate default error landing page appears. (For more information, see [Customizable user-facing screens](#) in the PingFederate documentation.)

Note: If you define an error redirect URL, errors are sent to the error URL as well as logged in the PingFederate server log, but are not logged to the PingFederate audit log.

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
Kerberos Only Error Template (checkbox)	When selected, displays a template to provide standardized information to the end user, avoiding browser unpredictability if Kerberos fails. <div data-bbox="654 993 1430 1066" style="border: 1px solid black; padding: 5px; margin-top: 10px;"> <p>Note: If you select this box, you must copy the file to the <code>pingfederate/server/default/conf/template</code> directory.</p> </div> <p>The template uses the Velocity template engine and can be modified in a text editor to suit your particular branding and informational needs. For example, you can give the user the option to try again should authentication fail. For more information on Velocity templates, see Customizable user-facing screens in the PingFederate documentation.</p>
jcifs.smb.client.soTimeout	The default value is recommended but may be adjusted as needed. Length of time, in milliseconds after which sockets are closed to prevent the client from holding server resources unnecessarily. NTLM Authentication only.
jcifs.netbios.cachePolicy	The default value is recommended but may be adjusted as needed. How long (in seconds) the server will cache NetBIOS names. The names are cached to reduce redundant name queries. NTLM Authentication only.
NTLM Challenge Retries	Maximum number of user-logon retries allowed for NTLM. For more information about the NTLM Challenge Retries field, see Starting SSO from outside a trusted domain on page 5.

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 Authentication Context for the OASIS Security Assertion Markup Language(SAML) V2.0) PDF.
NTLM Log Level	<p>Indicates the level of information written to the NTLM log. Values are 0 – nothing; 1 – critical; 2 – basic; 3 – more detail; 4 – for debugging only.</p> <p>Change this value as needed to have the Adapter write more or less information into a log file maintained for NTLM processing. This log, <code>server.log</code>, is located in the directory:</p> <pre><pf_install>/pingfederate/log</pre>

Note: Logging for Kerberos authentication processing is also maintained in the PingFederate `server.log` file.

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.

For information about account linking, see [Key concepts](#) in the PingFederate documentation. 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.

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 9.0 or higher](#) on page 11
- [Firefox browser](#) on page 15

Internet Explorer 9.0 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 23).

Configure IE for PingFederate

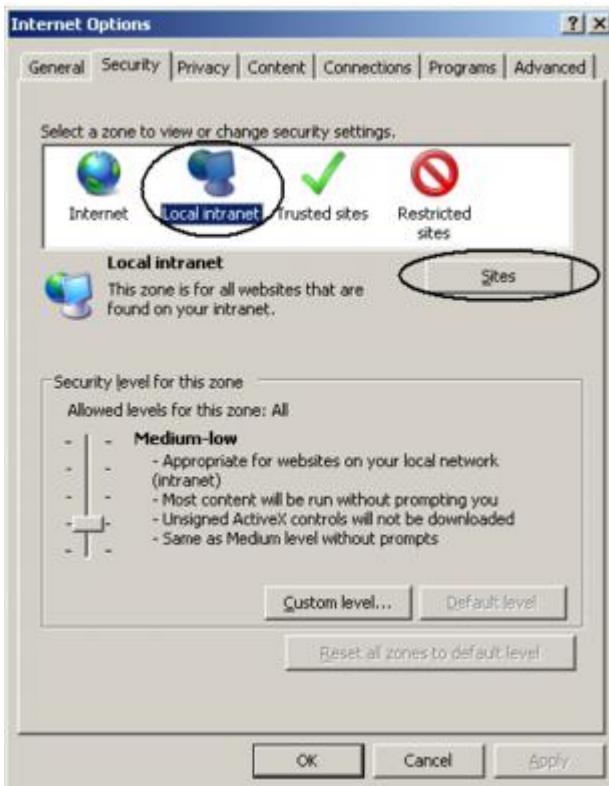
About this task

Steps

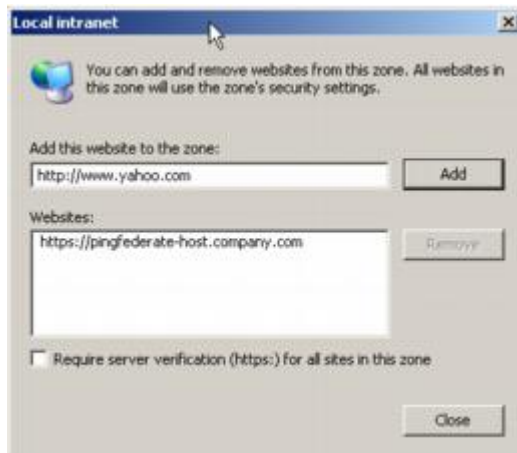
1. Under the Security tab for the Local intranet, add to the list of accessible Web sites the fully qualified domain name that is part of the PingFederate URL used to start SSO (<pf-idp.domain.name>).

 **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.



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

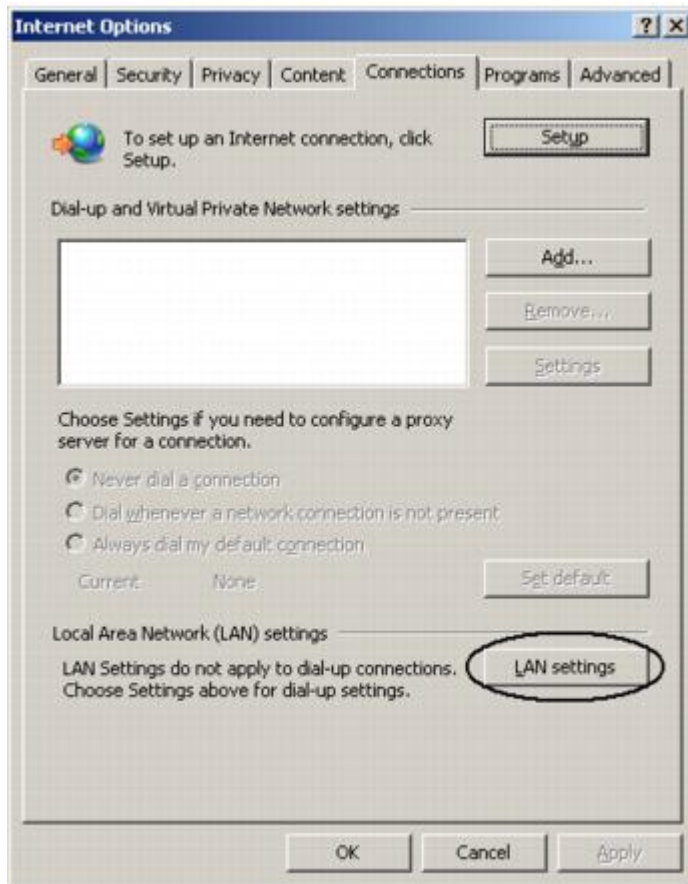


- Enter `<pf-idp.domain.name>` and click **Add**.
- Click **Close** and then click **OK** to close the dialog boxes.

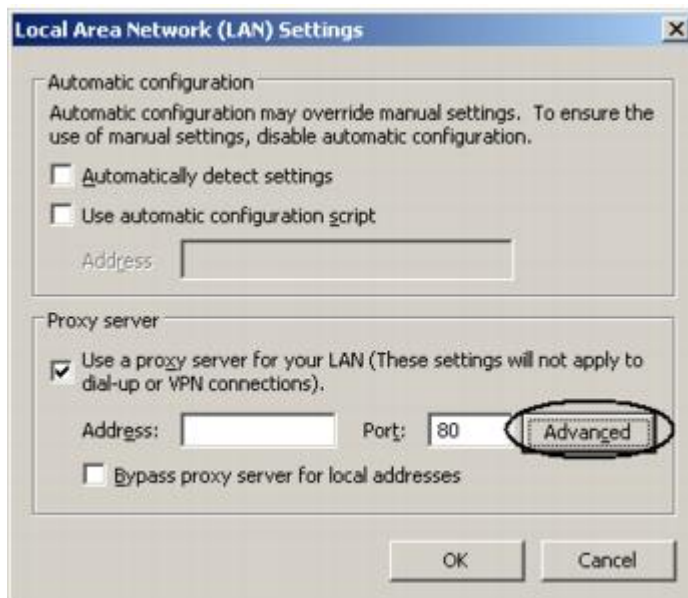
2. Verify proxy settings.

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

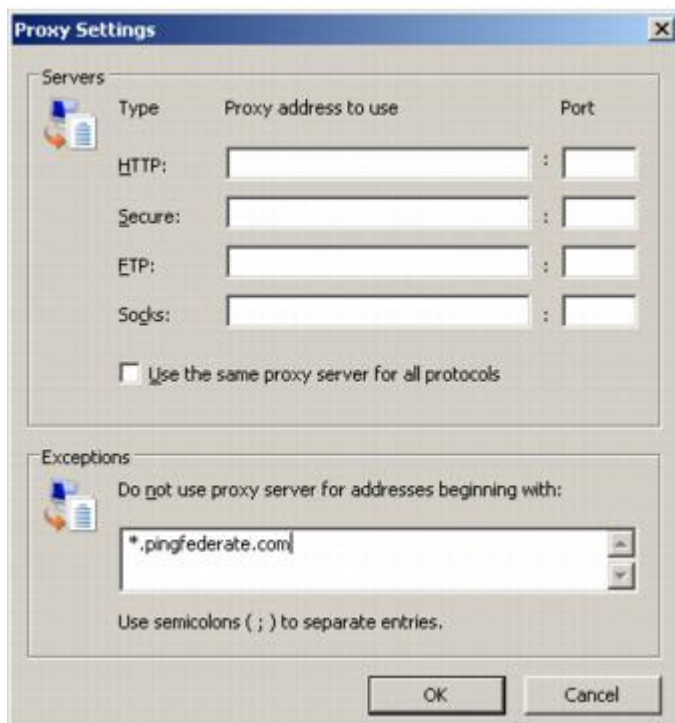
a. Click the **Connections** tab in the Internet Options dialog.



b. Click **LAN settings**.



c. In the LAN Settings dialog, ensure **Use a proxy server for your LAN** is selected 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 browser

Steps

1. Enter `about:config` into the address bar.
2. On the configuration-settings 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)

Internet Explorer 9.0 or higher

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

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

i 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 23).

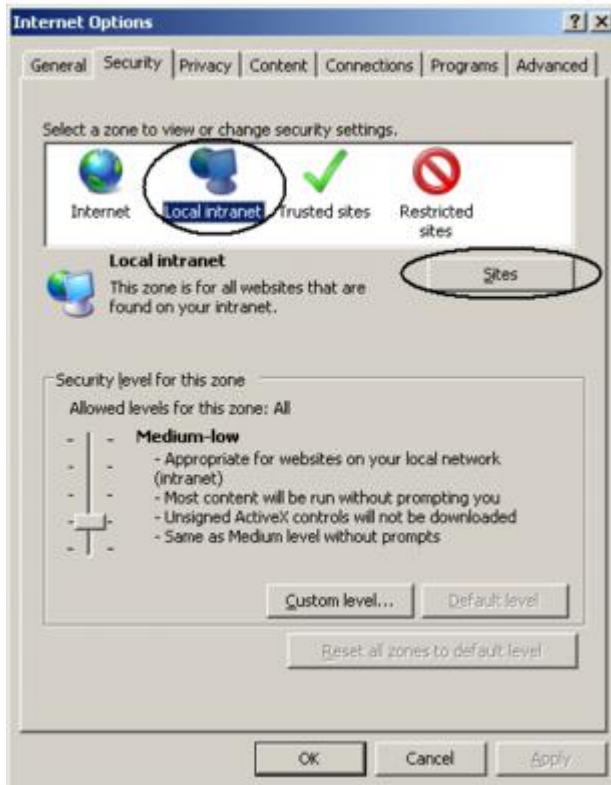
Configure IE for PingFederate

About this task

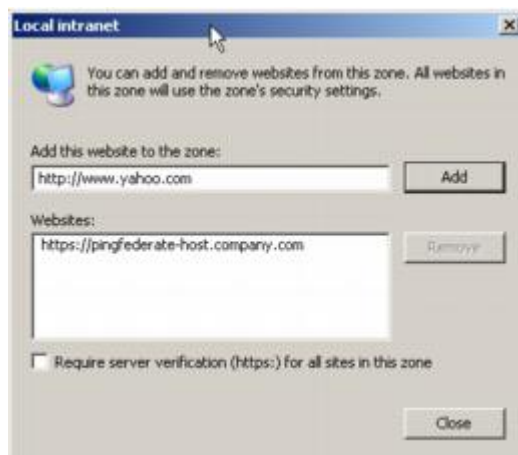
Steps

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**.

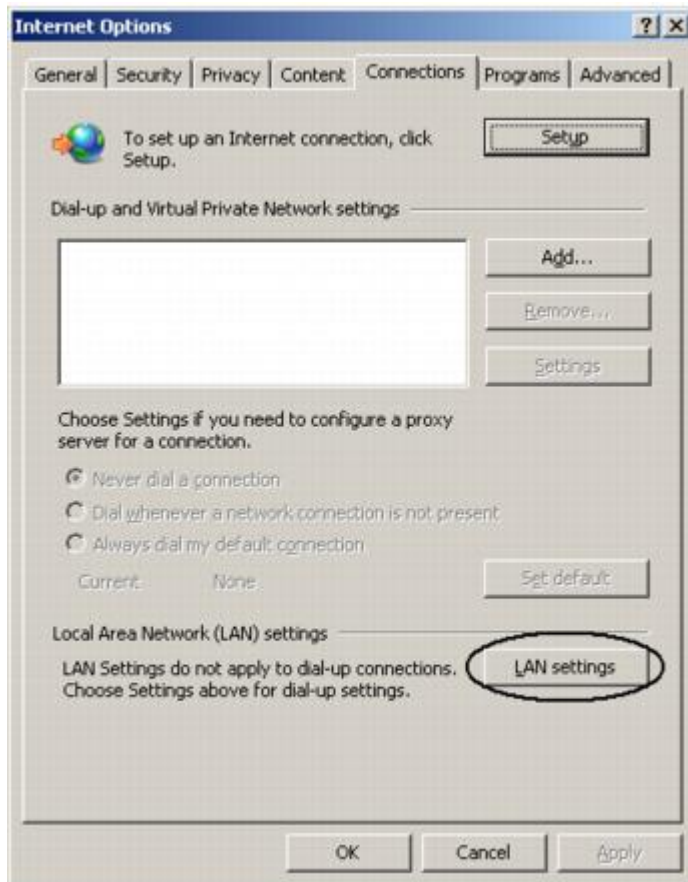


- c. Enter <pf-idp.domain.name> and click **Add**.
- d. Click **Close** and then click **OK** to close the dialog boxes.

2. Verify proxy settings.

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

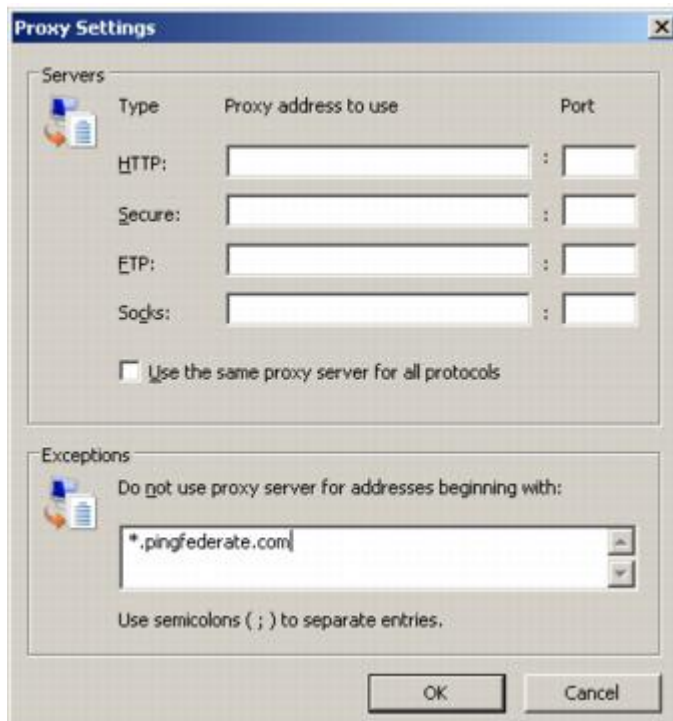
a. Click the **Connections** tab in the Internet Options dialog.



b. Click **LAN settings**.



c. In the LAN Settings dialog, ensure **Use a proxy server for your LAN** is selected 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.

Configure IE for PingFederate

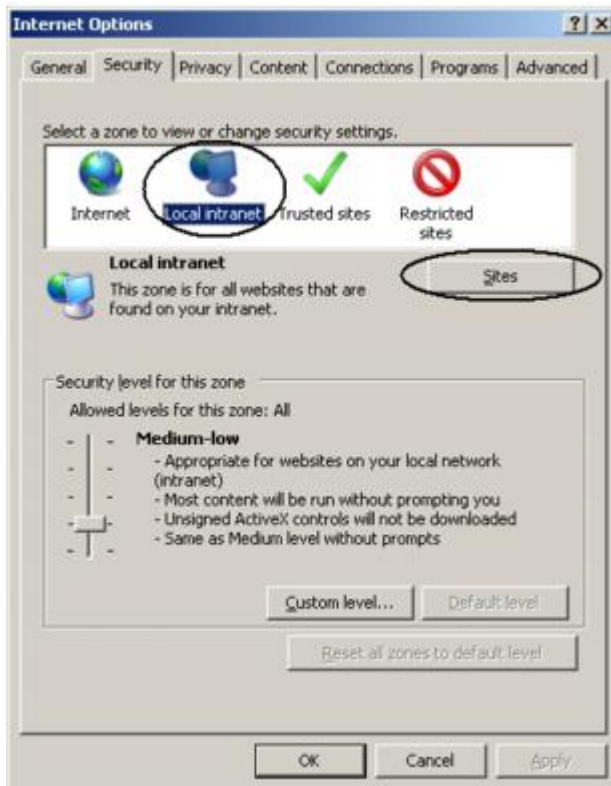
About this task

Steps

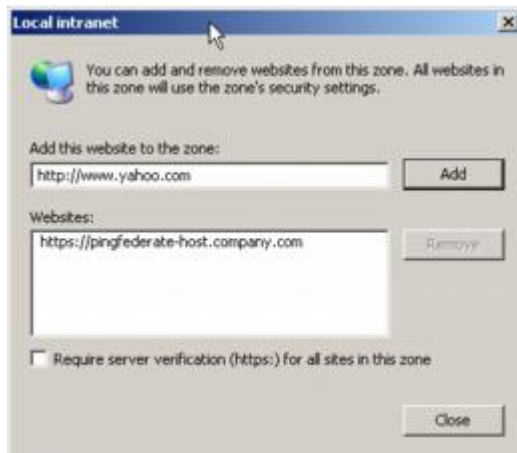
1. Under the Security tab for the Local intranet, add to the list of accessible Web sites the fully qualified domain name that is part of the PingFederate URL used to start SSO (<pf-idp.domain.name>).

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.



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

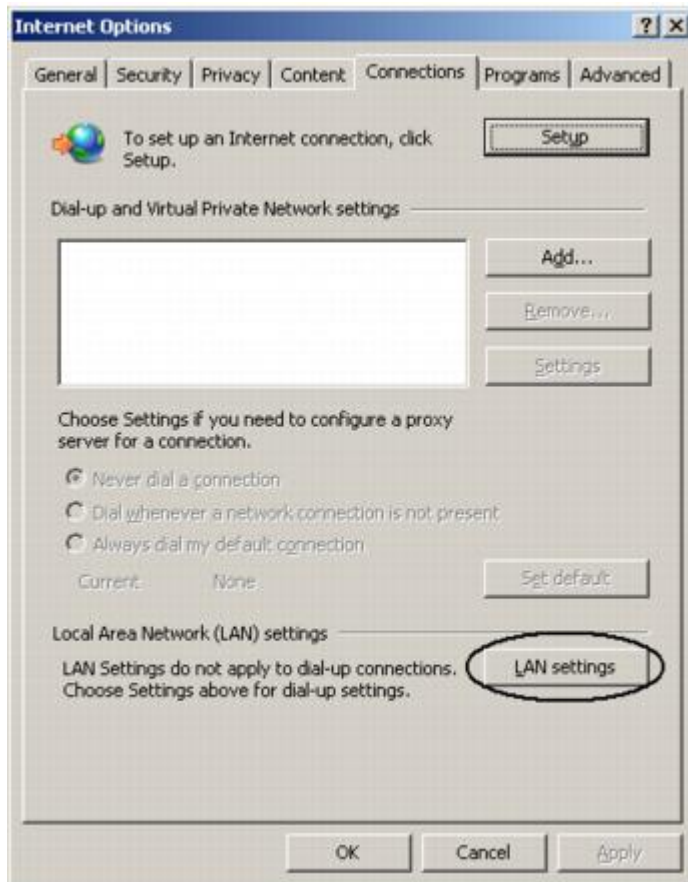


- Enter `<pf-idp.domain.name>` and click **Add**.
- Click **Close** and then click **OK** to close the dialog boxes.

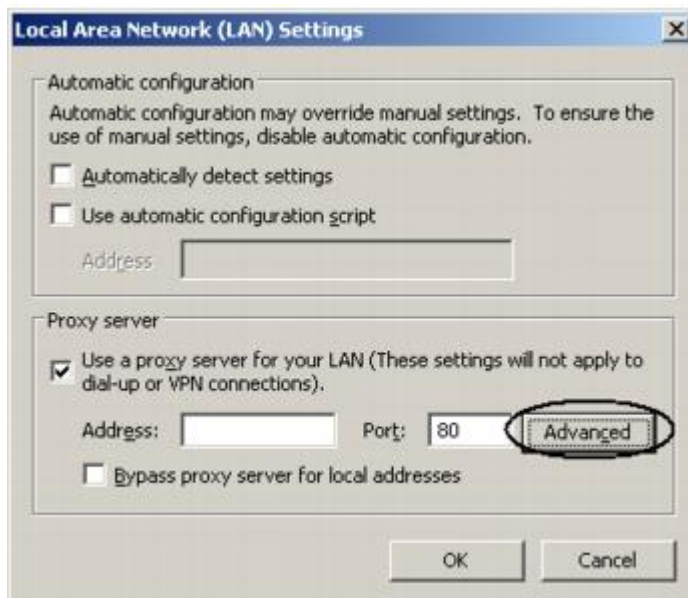
2. Verify proxy settings.

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

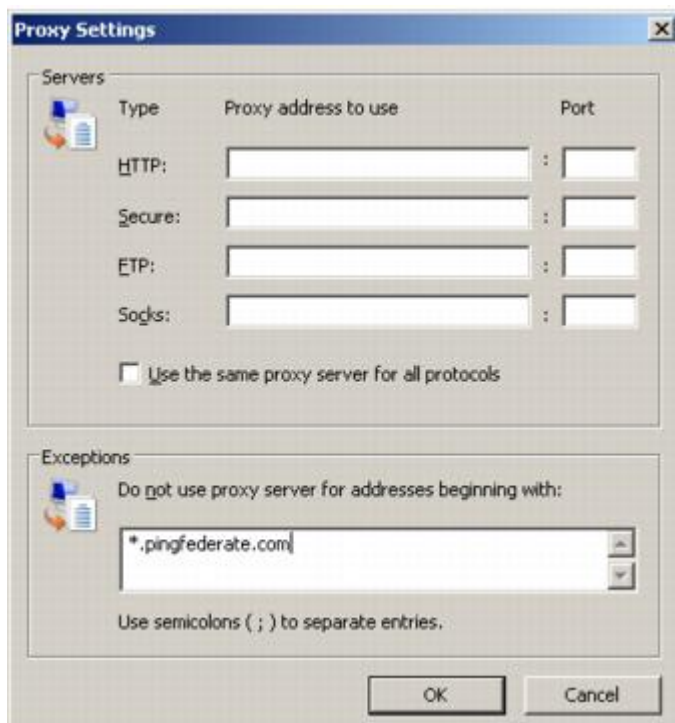
a. Click the **Connections** tab in the Internet Options dialog.



b. Click **LAN settings**.



c. In the LAN Settings dialog, ensure **Use a proxy server for your LAN** is selected 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 browser

Steps

1. Enter `about:config` into the address bar.
2. On the configuration-settings 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.

Problem	Possible Solution
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 Server Clustering Guide). This restriction is due to NTLM design; however, the same is true for Kerberos authentication.

Problem	Possible Solution
SSO fails with a “FULL HEAD” warning in the server log.	<p>Increase the <code>headerBufferSize</code> in the Jetty configuration file <code>jboss-service.xml</code>, located in the directory:</p> <pre data-bbox="617 289 1398 352"><pf_install>/pingfederate/server/default /deploy/jetty.sar/META-INF</pre> <p>For PingFederate version 6.9 and higher, the file is called <code>jetty-service.xml</code>, located in the directory:</p> <pre data-bbox="617 447 1398 478"><pf_install>/pingfederate/server</pre>
Kerberos authentication is not working—always fails over to NTLM.	<p>Ensure the SPN for the Adapter service account is unique (see Integrating Kerberos authentication on page 7).</p> <p>If the SPN is okay, ensure end-user browser settings are correct (see Configure user browsers on page 11 and Checking default IE browser settings on page 23).</p> <p>There can be a variety of other reasons for Kerberos issues. You can find additional information at the Ping Identity Support Center.</p>
The error "Failed to locate authority for name:" appears in <code>server.log</code> .	<p>Try setting the DNS Server field in the adapter configuration.</p>
The exception "account used is a Computer Account" appears in <code>server.log</code> .	<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 Integrating NTLM authentication 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>
The exception "Failed to retrieve property: domain.netbios.name" appears in <code>server.log</code> .	<p>This error indicates that DNS servers for the domain are not specified where PingFederate is deployed outside of the domain (see step 7).</p>
The error "jespa.security.SecurityProviderException: NetrLogonSamLogon return authenticator check failed" appears in <code>server.log</code> .	<p>The error indicates that the node index is not defined. In a clustered environment, this causes nodes to share the NTLM credential when accessing the domain controller—which may cause runtime issues (see Configure the adapter in PingFederate on page 8).</p>
Upgrading to PingFederate 6.8 or higher from a version that includes configured IWA adapters	<p>Be sure to delete any existing IWA adapter instances prior to installing the IWA Adapter 3.x (see Install or upgrade the integration kit on page 5).</p>

Checking default IE browser settings

About this task

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 [Configure user browsers](#) on page 11). If those settings are correct, ensure IE default settings for IWA support have not been changed, as described in the following steps:

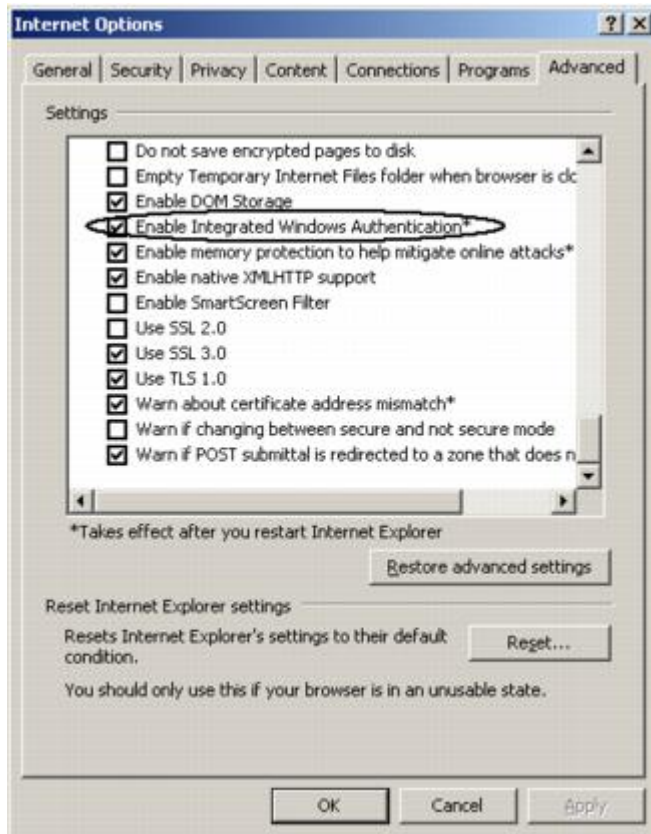
Steps

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 the 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**.

Release notes

Changelog

IWA Integration Kit 3.2.1 – February 2018 (Current Release)

- Updated license for NTLM library (Jespa v1.2.3)

IWA Integration Kit 3.2 – December 2017

- Updated to the latest version of the NTLM library (Jespa v1.2.3)
- Bug fixes

IWA Integration Kit 3.1.1 – January 2016

- Maintenance update to support latest PingFederate release

IWA Integration Kit 3.1 – June 2013

- Removed support for Microsoft Windows 2003 Server
- Added support for Microsoft Windows 2012 Server
- Added support for multiple browsers and platforms (see Qualification Statement for further details).
- Added support for Jespa 1.1.19 Java software library
- Added support for IdpAuthenticationAdapterV2 Interface

- Integrated Jespa logs into PingFederate server log file (as a result, the iwa-ntlm.log file was removed)
- Added 15 character limit (GUI validation) to the NTLM Username field

IWA Integration Kit 3.0 – April 2012

- Centralized the management of AD domains/Kerberos realms within the PingFederate IdP server rather than inside the adapter configuration
- Added options to enable either Kerberos or NTLM authentication, or both
- Removed the ability to specify network ranges and XFF header support—the CIDR adapter selector should be used to perform these functions
- Added support for multiple IWA adapter instances—as a result, the `IWADomain/RequestedAuthnCtx` parameters used to specify domains in the previous version are no longer necessary
- Limited the number of domains that can be mapped to an adapter instance to one
- Added support for an error template (included with the Integration Kit) with Kerberos only authentication

IWA Integration Kit 2.6 – January 2012

- Added support to use XFF header within incoming requests when PingFederate is deployed behind proxies or load balancers
- Bug Fix – Issues with SSO using iOS 5 with Safari
- Bug Fix – Intermittent failure when performing NTLM SSO in a clustered PingFederate environment
- Bug Fix – Issues with SSO when IP addresses are used in browser configuration and/or in the startSSO URL

IWA Integration Kit 2.5 – July 2011

- Added an option to specify Active Directory Sites & Services (ADSS) sites in adapter configuration
- Audit logging now records SSO failures
- Bug Fix – Issues when Safari is used to SSO

IWA Integration Kit 2.4 – July 2010

- Added full NTLM functionality and support for security policies exhibited by Windows clients and servers
- Added support for Kerberos failover to NTLM authentication when the user is external to the domain

IWA Integration Kit 2.3 – April 2010

- Qualified on Java SE 6 update 19 (J2SE 1.6.0_19) which corrected interoperability issues with Microsoft extended protection (channel binding)
- Added support for SP-Initiated SSO from multiple forests without a trust relationship
- Bug Fix – When NTLM is not allowed, the IWA Adapter no longer challenges for NTLM

IWA Integration Kit 2.2 – December 2008

- Added ability to specify Kerberos only for IWA authentication
- Allowed the Domain Controller to be optionally specified rather than resolved through DNS
- Added support for JDK 1.6
- Bug Fix – Adapter supports NTLM in a PingFederate cluster fronted with a load balancer using keep-alive connections

IWA Integration Kit 2.1 – July 2008

- Improved Kerberos/NTLM fallback authentication
- Improved NTLM support for trusted domains
- Improved logging and exception handling
- Simplified adapter configuration
- Added support for Microsoft Vista Internet Explorer 7

IWA Integration Kit 2.0 – February 2008

- Merged NTLM and IWA Integration Kits
- Added multi-domain support
- Simplified installation
- Added support for Domain Controller failover
- Added ability to force TCP when communicating with the Domain Controller (default is UDP)
- Bug Fix - Adapter now works when PingFederate is running as a service
- Bug Fix (NTLM) - Outside domain login failure now limited to three attempts

IWA Integration Kit 1.0 - June 2006

- Initial release

Known issues and limitations

Known Issues

- See [IWA Kerberos authentication may fail when user belongs to many AD groups](#) in the Ping Identity Knowledge Base.
- The Service Account Name for the IWA Adapters is not restricted to a 15 character limit. Added checks for 15 character limit for NTLM Username field.
- When using Internet Explorer to perform SSO with “Both” Kerberos and NTLM and Kerberos fails, the browser may not fallback to NTLM properly, if the client machine lost connection to the domain.

Known Limitations

- When running PingFederate in a cluster, NTLM authentication does not work unless the load balancer supports keep-alive connections, because successive requests in the NTLM handshake must go to the same node in a cluster. This restriction is due to NTLM design. For details, see Authentication in WinHTTP in the Microsoft documentation.
- IWA authentication does not work over HTTP proxy connections. NTLM Challenge/Response authentication requires implicit end-to-end state and does not work when PingFederate is running through a reverse HTTP proxy server or a non-transparent proxy load balancer. See <http://www.microsoft.com/technet/prodtechnol/WindowsServer2003/Library/IIS/523ae943-5e6a-4200-9103-9808baa00157.msp?mfr=true>) in the Microsoft documentation.
- Internet Explorer limits the number of login attempts to three regardless of what is configured in the adapter setup.
- When authenticating outside of the domain using NTLM, the user is prompted to enter credentials. These credentials must specify which domain to authenticate against, i.e. <DOMAIN>\<USERNAME> rather than <USERNAME>.
- If PingFederate is running on the same machine as the domain controller, Kerberos is not used.
- In rare cases, Kerberos tokens sent by the user-agent are larger than PingFederate’s jetty container to properly parse. This manifests itself in an IO exception in PingFederate’s server log with the statement: `java.io.IOException: FULL head`. This can be fixed by disabling the “Privilege Attribute Certificate” that the KDC attaches to Kerberos tickets.
- Connections from IPv6 clients are not supported.
- Chrome is not supported on macOS.

Download manifest

The distribution .zip archive for the IWA Integration Kit contains the following:

- `ReadMeFirst.pdf` – contains links to this online documentation
- `/legal` – contains this document:
 - `legal.pdf` – copyright and license information

- /dist – contains libraries needed to run the adapter:
 - pf-iwa-authn-adapter-3.2.1.jar – the IWA Adapter JAR file
 - kerberos.only.error.template.html – User-facing HTML template