

PingFederate®

Integration Note

SSO to Microsoft Office 365™



PingFederate Integration Note
SSO to Microsoft Office 365

© 2015 Ping Identity Corporation. All rights reserved.

About Integration Notes

PingFederate software developers, specialty teams, and third parties periodically submit supplemental documentation to give our customers insight into configuration, deployment, integration, or use cases that are not specifically covered by the core product documentation.

Acknowledgements

This document was written by Travis Spencer (travis.spencer@twobotechnologies.com) and Peter Motykowski (pmotykowski@pingidentity.com).

Disclaimer

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

Note that Ping Identity may not provide support for any sample configurations provided in this document. The variability inherent among security environments prevents full testing and support for all possible platform configurations. If you need special assistance or would like to inquire about implementation or support programs, please contact Ping Identity Support (www.pingidentity.com/support).

Document Lifetime

Ping Identity may occasionally update PingFederate online documentation between releases of the related software. Consequently, if this PDF was not downloaded recently, it may not contain the most up-to-date information. Please refer to the online documentation at documentation.pingidentity.com for the most current information.

From the Web site, you may also download and refresh this PDF if it has been updated, as indicated by a change in this date: **February 17, 2015**.

Contact Information

Ping Identity Corporation
1001 17th Street, Suite 100
Denver, CO 80202
U.S.A.

Phone: 877.898.2905 (+1 303.468.2882 outside North America)

Fax: 303.468.2909

E-mail: info@pingidentity.com

Web Site: www.pingidentity.com

SSO to Office 365 Introduction

Cloud computing provides organizations with cost-effective alternatives to traditional software solutions. The Microsoft Office™ suite, which organizations have been using for years, is no exception. With the cloud-based version of these tools, organizations have the opportunity to acquire Office on a per-use model backed by a Service-Level Agreement (SLA) and including financially-guaranteed uptime and scalability. By paying as you go, workers are able to securely manage documents over the Web from anywhere, using any device.

The adoption of cloud computing presents problems for organizations that want to maintain control over user accounts. This need can be satisfied using Web single sign-on (SSO), which the enterprise edition of Office 365™ supports. For organizations that have complex heterogeneous environments, federation to Office 365 can pose certain challenges (for example, integration with non-Microsoft identity management solutions) that can be quickly overcome by using PingFederate. For organizations that already have a federated SSO infrastructure built around PingFederate, reusing it for integration with Office 365 makes even more sense.

Rolling out Office 365 requires careful preparation and planning. This document provides a high-level overview of the steps required to do so successfully in conjunction with PingFederate.

Prerequisites

The following steps (described in more detail below) enable you to use PingFederate and Office 365:

- Sign up for an Office 365 account.
- Set up Active Directory (AD) and enable directory synchronization.
- Create a federated domain in Office 365 and prove ownership of it.
- Install and configure PingFederate 6.10 or higher. If you need to support multiple subdomain accounts in Office 365, install PingFederate 7.2 (or higher).

Note: If you need to support *active* clients, such as native desktop applications, for use with Office 365, ensure that PingFederate is installed with a license that enables the WS-Trust Security Token Service (STS).

- Replace the default self-signed SSL server certificate included with PingFederate with one that is signed by a public Certificate Authority (CA). This enables Office 365 to establish a trusted SSL session with PingFederate. For instructions on how to do this, refer to the [SSL Server Certificates](#) section of the PingFederate [Administrator's Manual](#).

By performing these steps (described in more detail below), organizations can use PingFederate and Office 365 together to:

- Access online services included in Office 365 without having to remember an additional username and password.
- Authenticate email access on mobile devices with usernames and passwords that are stored centrally in AD.
- Revoke access to email and secure content by simply disabling an account in AD.

- Reuse existing PingFederate infrastructure used to address complex Web SSO requirements.

Preparing Office 365 for Use with PingFederate

The following sections cover steps needed relating to Office 365.

Sign up for Office 365

Microsoft offers various Office 365 plans for different types of organizational needs. Not all of them support Web SSO, but all enterprise plans support federation (see the [Office 365 Web site](#) for more information on [signing up for Office 365](#)).

Set up Active Directory and Directory Synchronization

When you configure Office 365 to use federation, all user accounts are stored in AD and are pushed to the cloud. While PingFederate has no restriction on how users are authenticated, synchronization is provided by the Microsoft Online Services (MSOL) Directory Synchronization Tool, which requires AD. This one-way synchronization tool can be downloaded from the administration portal and is similar in functionality to other synchronization products from Microsoft; however, it is specifically designed to work with Office 365. It requires a host connected to AD and that is not a domain controller. For more specific information about system requirements, installation instructions, and configuration, see the [Office 365 online help](#). For more information on setting up AD for use with federated access to Office 365, refer to the [online guides](#) found in the online help.

Create a Federated Domain

After signing up for Office 365, the only domain associated with your account is the `onmicrosoft.com` subdomain chosen during registration (for example, `contoso.onmicrosoft.com`). To allow users to SSO to Office 365, add another domain specifically for Web SSO using PowerShell:

1. Authenticate to Office 365 using the **Connect-MsolService** PowerShell cmdlet.¹

Enter the same credentials that you use when authenticating to the Microsoft Online Services portal.

2. Execute the command:

```
New-MsolDomain -Name <name> -Authentication Federated
```

3. Execute the command:

```
Get-MsolDomainVerificationDns -DomainName <name>
```

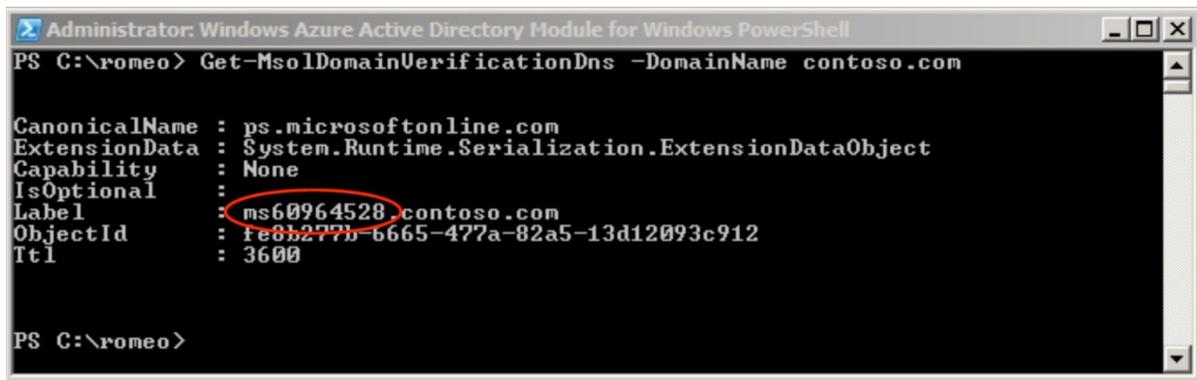
¹ This and the other cmdlets described in this document can be loaded by launching PowerShell using the **Microsoft Online Services Module for Windows PowerShell** desktop and **Start** menu shortcuts.

- To prove that you control the domain, use the output of the **Get-MsolDomainVerificationDNS** command to create a TXT record on the DNS server of the domain used in the previous step, see the examples below.

Note: This server must be accessible over the Internet so that Microsoft servers can resolve and access them.

The DNS record name should match the Domain Name and the DNS record value should be MS=<ms portion of the Label>.

Example from the **Get-MsolDomainVerificationDNS** Command:



```

Administrator: Windows Azure Active Directory Module for Windows PowerShell
PS C:\romeo> Get-MsolDomainVerificationDns -DomainName contoso.com

CanonicalName : ps.microsoftonline.com
ExtensionData : System.Runtime.Serialization.ExtensionDataObject
Capability     : None
IsOptional    :
Label         : ms60964528.contoso.com
ObjectId      : fe0b277b-b665-477a-82a5-13d12093c912
Ttl           : 3600

PS C:\romeo>

```

Note: Creating a DNS record value can vary between different DNS host providers. For more information about adding your domain to Office 365, see Microsoft's instructions at <http://office.microsoft.com/en-ca/office365-suite-help/add-your-domain-to-office-365-HA102818660.aspx>.

Example Values for Creating a Text Record:

Record Type (choose one)	Alias or Hostname	Destination or Points to Address	TTL
TXT	@ or jkdoctest.com	MS=ms60016396	1 Hour
MX	@ or jkdoctest.com	Ms60016396.msv1.invalid.outlook.com	1 Hour

- Prove your control of the domain by running the command **Confirm-MsolDomain** shown in the sample PowerShell script below.

Note: The `IssuerURI` parameter should be unique so that Office 365 can identify your Identity Provider.

When you execute this, you need to provide the URLs for PingFederate, the public portion of its signing certificate, and some other inputs. To export the signing certificate from PingFederate, refer to the [Digital Signing and Decryption Keys and Certificates](#) section of the

PingFederate [Administrator's Manual](#). When you finish, remove the BEGIN CERTIFICATE header, END CERTIFICATE footer, and any endlines either manually or automatically using a PowerShell script similar to the sample shown below.

```
PS> $certFile = "C:\temp\pf-signing.crt"

PS> $cert = [IO.File]::ReadAllText($certFile)

PS> $cert = $cert.replace("-----BEGIN CERTIFICATE-----", "")

PS> $cert = $cert.replace("-----END CERTIFICATE-----", "")

PS> $cert = $cert.replace("`r", "")

PS> $cert = $cert.replace("`n", "")

PS> $domainName = "<Federated Domain Name>"

PS> $hostName = "<Hostname>.$domainName"

PS> $port = 9031

PS> $pingfederate = "https://{hostName}:$port"

PS> $brandName = "<Federated Domain Alias>"

PS> $issuer = "<SAML 20 Entity ID>"

PS> $spId = "urn:federation:MicrosoftOnline"

PS> $activeLogOn = "$pingfederate/idp/sts.wst"

PS> $logOff = "$pingfederate/idp/prp.wsf"

PS> $metaData = "$pingfederate/pf/sts_mex.ping?partnerSpId=$spId"

PS> $passiveLogOnPF="$pingfederate/idp/prp.wsf"

PS> Confirm-MsolDomain -DomainName "$domainName" -ActiveLogOnUri "$activeLogOn" -
FederationBrandName "$brandName" -IssuerUri "$issuer" -LogOffUri "$logOff" -
MetadataExchangeUri "$metaData" -PassiveLogOnUri "$passiveLogOnPF" -
SigningCertificate "$cert"
```

For more information about the **Confirm-MsolDomain** command, see <https://msdn.microsoft.com/en-us/library/azure/dn194117.aspx>.

Tip: If you have multiple subdomain accounts in Office 365, you can connect to them in one SP connection using multiple virtual server IDs in PingFederate 7.2 (or higher).

For example, both the marketing and the engineering departments of contoso.com have their own departmental subdomains, marketing.contoso.com and engineering.contoso.com. They are both registered in Office 365 under the parent domain, contoso.com. Their `IssuerUri` values are marketing.contoso.com and engineering.contoso.com, respectively.

In PingFederate 7.2 (or higher), you can connect to both subdomain accounts in one SP connection by including marketing.contoso.com and engineering.contoso.com as the virtual server IDs (described in detail later in [Creating a Connection to Office 365](#) on page 13).

When you run the `Confirm-MsolDomain` PowerShell command for an Office 365 subdomain account, you must include the base64url-encoded value of the virtual server ID presenting

that subdomain in the paths for the `ActiveLogOnUri`, `LogoffUri`, `PassiveLogOnUri`, and `MetadataExchangeUri` parameters.

To specify a virtual server ID in the path:

- a. Construct a JSON object containing a key-value pair of the virtual server ID in the format of

`{"vsid": "<VirtualServerIdValue>"}`. For example:

```
{"vsid": "Engineering"}
```

- b. Base64url-encode the JSON object. For example:

```
eyJ2c2lkIjoiRW5naW5lZXJpbmcfQ
```

- c. Insert the base64url-encoded value between `/idp` or `/pf` and the rest of the respective endpoint for `ActiveLogOnUri`, `LogoffUri`, `PassiveLogOnUri`, and `MetadataExchangeUri`. For examples:

```
$pingfederate/idp/eyJ2c2lkIjoiRW5naW5lZXJpbmcfQ/sts.wst
```

```
$pingfederate/idp/eyJ2c2lkIjoiRW5naW5lZXJpbmcfQ/prp.wsf
```

```
$pingfederate/pf/eyJ2c2lkIjoiRW5naW5lZXJpbmcfQ/sts_mex.ping  
?PartnerSpId=urn:federation:MicrosoftOnline
```

where `$pingfederate` is the Base URL of your PingFederate installation.

- d. Repeat these steps for each Office 365 subdomain accounts.

For more information about base64url, see [RFC4648](https://tools.ietf.org/html/rfc4648) (tools.ietf.org/html/rfc4648).

6. To verify that the domain settings are up to date and in effect, run the command:

```
Get-MsolDomainFederationSettings -DomainName <name>
```

7. To change domain settings after the domain is created and verified, run the following command with extra arguments for the settings you want to change:

```
Set-MsolDomainFederationSettings -DomainName <name>
```

See the Office 365 documentation for more information on [adding a domain to Office 365](#).

Installing and Configuring PingFederate

Using PingFederate for SSO to Office 365 makes it a key component of your daily operations. When you use PingFederate in this way, it is important that your deployment be highly available. For information on installation and high availability, refer to the [Installation](#) section of the PingFederate [Getting Started Guide](#) and the PingFederate [Server Clustering Guide](#). After you install PingFederate, configure it for use with Office 365 by creating an IdP Adapter and a WS-Federation connection at minimum.

PingFederate System Setup

Omit Line Breaks in Digital Signatures

Configure PingFederate to omit line breaks in digital signatures by using one of the following procedures.

Note: This change is global, for all cases in which PingFederate may write encoded signatures to XML or log files.

On Windows (running PingFederate from the command line):

1. Open `<pf_install>/pingfederate/bin/run.bat` in a text editor.
2. Locate the variable `PF_JAVA_OPTS`
3. Add `-Dorg.apache.xml.security.ignoreLineBreaks=true` as a variable value.

On Windows (running PingFederate as a service):

1. Open `<pf_install>/pingfederate/sbin/wrapper/PingFederateService.conf` in a text editor.

Example:

```
wrapper.java.additional.9=-Dorg.apache.xml.security.ignoreLineBreaks=true
```

2. Locate the heading:

```
# Java Additional Parameters
```

3. Add `-Dorg.apache.xml.security.ignoreLineBreaks=true` as a variable value below the heading.

On Linux/Unix (running PingFederate from the command line or as a service):

1. Open `<pf_install>/pingfederate/bin/run.sh` in a text editor.
2. Locate an instance where the environment variable `JAVA_OPTS` is set.
3. Add `-Dorg.apache.xml.security.ignoreLineBreaks=true` as a variable value.

Installing the Username Token Translator

To install the Username Token Translator:

1. Download the Username Token Translator from the [Downloads](#) page at pingidentity.com.
2. Extract the `pf-username-token-translator-1.1.jar` from the `dist` directory in the ZIP file to:

```
<pf-install>/pingfederate/server/default/deploy
```

Note: For PingFederate 7.2 or higher, Username Token Processor is part of the product and does not require a separate download or installation.

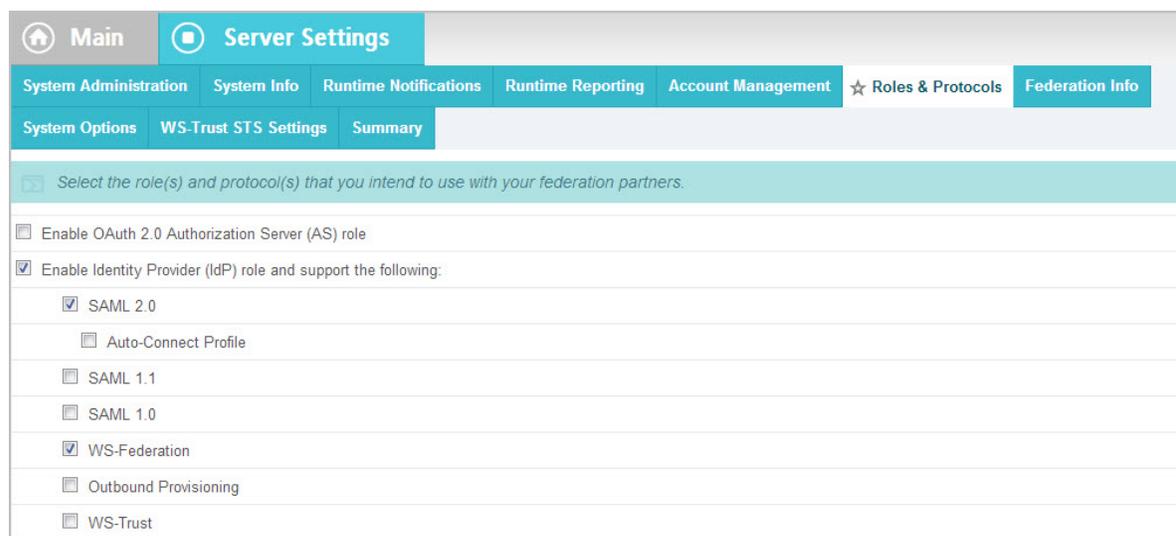
Restart PingFederate

Restart PingFederate and launch the administrative console to perform the remainder of the setup.

Enable Server Protocols

In the PingFederate administrative console, make sure that the necessary protocols are enabled by clicking **Server Settings** and then **Roles & Protocols**. Ensure that **WS-Federation** is selected at a minimum under the IdP role. Select **WS-Trust** if you need to support active clients.

Note: The WS-Trust STS is licensed separately. This protocol selection is available only if an STS-enabled license is installed.



Replacing the Default SSL Certificates

When PingFederate is installed, the included SSL certificate is self-signed. Left as is, email and some other Office 365 applications do not work because Microsoft's WS-Trust clients are not able to establish an SSL connection with PingFederate. To ensure proper functionality, be sure to replace the default SSL certificate with one that is signed by a

public Certificate Authority (CA). For instructions on how to do this, refer to the [SSL Server Certificates](#) section of the PingFederate [Administrator's Manual](#).

Configuring an LDAP Connection

If you have not yet already done so, create a connection from PingFederate to your LDAP data store, see [Managing Data Stores](#) in the System Settings chapter of the PingFederate [Administrator's Manual](#) for instructions on configuring an LDAP connection.

Note: Ensure the `objectGUID` attribute is set to binary. It must be a binary attribute to create a connection to Office 365, see [Creating a Connection to Office 365](#) on page 13.

Tip: If you need to support multiple Office 365 subdomain accounts via one SP connection in PingFederate 7.2 (or higher), create additional LDAP data store connections to LDAP servers of the subdomains.

Creating a Password Credential Validator

After configuring an LDAP connection, the next step is to create an LDAP Password Credential Validator, see [Validating Password Credentials](#) in the Security Management chapter of the PingFederate [Administrator's Manual](#) for instructions on configuring an LDAP connection.

Tip: If you need to support multiple Office 365 subdomain accounts via one SP connection in PingFederate 7.2 (or higher), create additional LDAP password credential validators against your LDAP data store connections (see the previous section, [Configuring an LDAP Connection](#)).

Creating an IdP Adapter

PingFederate supports a wide selection of integration kits that plug into the PingFederate server enabling it to interface with various identity management systems. After authentication, PingFederate can look up more attributes in various data stores to collect additional information that is placed in the SAML token passed to Office 365.

Regardless of which integration kit is used or the source of the attributes, two things need to be provided to Office 365:

User Principal Name (UPN) – Format as an email address and the domain name *must* match the domain name registered with Office 365. For example, if the domain `contoso.com` is created using the `New-MSolDomain` PowerShell command, then the UPN attribute value in the SAML assertion for all users must be their username followed by `@contoso.com`.

Note: The UPN of the user in AD can be different from what is placed in the SAML assertion created by PingFederate.

ObjectId - The Office 365 Directory Synchronization Tool (described below) copies this Id to the cloud when it creates shadow accounts. The ObjectId, which uniquely represents the user in AD, is an immutable identifier used to associate local and remote identities. The AD attribute is a binary value, so must be base-64 encoded in order to be transmitted in a SAML token.

Note: The expected value can be determined by examining the **ImmutableId** attribute output by the **Get-MSolUser** PowerShell command after synchronization is set up.

PingFederate packages an HTML Form adapter that renders a simple HTML form in which users can enter their username and password. This credential can be checked against AD using the previously configured Password Credential Validator. Follow these steps to set up this adapter in PingFederate:

1. From the Main Menu of the PingFederate administrative console under My IdP Configuration, click **Adapters**.
2. On the Manage IdP Adapter Instances screen, click **Create New Instance**.
3. On the Type screen, specify an Instance Name and Instance Id (for example, HtmlFormIdpAdapter1) and select **HTML Form IdP Adapter** as the Type.
4. On the IdP Adapter screen, click the **Add a new row to 'Credential Validators'** link near the upper-right of the screen.
5. From the Password Credential Validator Instance drop-down list, select the validator ID you previously configured, click **Update**, and then click **Next**.
6. On the Adapter Attributes screen, select the username checkbox under Pseudonym and click **Next**.
7. On the Summary screen, click **Done**, and then **Save** to complete the HTML Form IdP Adapter configuration.

Tip: If you need to support multiple Office 365 subdomain accounts via one SP connection in PingFederate 7.2 (or higher), repeat steps 1 through 7 to create additional HTML Form adapters against your LDAP password credential validators (see the previous section, [Creating a Password Credential Validator](#)).

Configuring a Username Token Processor Instance

To allow email clients, mobile phones, and other active clients that use Office 365 to authenticate, users must provide the username and password of their AD domain account. For this credential to be verified, Office 365 relays them to PingFederate using the WS-Trust protocol. For the username and password to be validated, a username token processor is set up to bind to the domain controller (see [Create a Federated Domain](#) on page 4). Whenever requests are sent to PingFederate, they include a UsernameToken element that PingFederate passes along for authentication.

Note: This configuration is *not required* for browser-only implementations (passive WS-Federation).

Tip: With PingFederate 6.11 (or higher), you can also configure the Kerberos token processor to allow the STS to accept and validate Kerberos tokens and to enable SSO for clients that support Kerberos authentication. See [User Kerberos Token Processor User Guide](#) for detailed configuration instructions.

To configure the Token Processor for PingFederate:

1. From the Main Menu, select **Token Processors** from the Application Integration Settings section under IdP Configuration.



If the Token Processors menu item is not present under Application Integration Settings, be sure that WS-Trust is enabled in the Roles and Protocols section of the Server Settings screen (see the [Enable Server Protocols](#) section).

2. Click **Create New Instance**.
3. On the Type screen, enter an Instance Name (for example, Username Token Processor), Instance Id (for example, UsernameTokenProcessor1), and select **Username Token Processor 1.1** from the Type drop-down list.

Note: For PingFederate 7.2 (or higher), select **Username Token Processor** from the Type drop-down list and follow the steps in the [Configuring a Username Token Processor Instance](#) section of the PingFederate [Administrator's Manual](#). When finished, skip to step 8.

Click **Next**.

 A screenshot of the 'Create Token Processor Instance' configuration screen. The 'Type' tab is selected. The form contains the following fields:

- Instance Name:** UsernameTokenProcessor *
- Instance Id:** UsernameTokenProcessor *
- Type:** Username Token Processor 1.1 (dropdown menu) * [Visit PingIdentity.com for additional types](#)

 A teal banner at the top of the form area contains the instruction: 'Enter a Token Processor Instance Name and Id, and select the Token Processor Type. The selection is limited to the processors currently installed on your server.'

4. On the Instance Configuration screen, select **LDAP bind** as the Processing Scheme and click **Show Advanced Fields**.
5. From the LDAP Datastore drop-down list, select the data store you created previously.
6. In the Search Base text box, enter the location in the LDAP directory server from which to begin searching (for example, CN=Users,DC=contoso,DC=com).

7. In the Search Filter text box, enter a search filter to find a specific user (for example, `userPrincipalName=${username}`).
8. Click **Next** on both the Instance Configuration (or Extended Contract for the Username Token Processor bundled with PingFederate 7.2 or higher) and Token Attributes screens.
9. Click **Done** on the Summary screen and then click **Save** on the Manage Token Processors screen.

Tip: If you need to support multiple Office 365 subdomain accounts via one SP connection in PingFederate 7.2 (or higher), repeat steps 1 through 9 to create additional token processors against your LDAP password credential validators (see [Creating a Password Credential Validator](#) on page 10).

Creating a Connection to Office 365

Setting up SSO in PingFederate is done on a connection-by-connection basis. When you create a connection for Office 365, use the following properties:

- The protocol must include **WS-Federation** at minimum for browser-based SSO. Add **WS-Trust** for active clients such as native desktop applications.
- The Partner's Realm (i.e., Connection ID) must be **urn:federation:MicrosoftOnline**.
- Claims required by Office 365:

`http://schemas.microsoft.com/LiveID/Federation/2008/05/ImmutableID`

`http://schemas.xmlsoap.org/claims/UPN`

- The name identifier type is **UPN**.
- The Office 365 endpoint where WS-Federation messages must be sent is:

`https://login.microsoftonline.com/login.srf`

- The signing algorithm must be **SHA-1**.

To create a connection, follow these steps:

1. From PingFederate's Main Menu, under SP Connection click **Create New**.
2. Click **Next**.
3. Select the **Browser SSO Profiles** checkbox and select **WS-Federation** as the Protocol.

If you do not see **WS-Federation** in the list, ensure it has been enabled in the server settings for roles and protocols, see [Choosing Roles and Protocols](#) in the System Settings chapter of the PingFederate [Administrator's Manual](#).

If you are configuring the connection for active federation, select the **WS-Trust STS** checkbox and **SAML 1.1** as the Default Token Type.

4. Click **Next** and then again on the Connection Options screen.
5. On the General Info screen, enter the following and then click **Next**:

Partner's Realm (Connection ID) – **urn:federation:MicrosoftOnline**

Connection Name – **Office 365**

Virtual Server ID – Enter the domain name as the issuer entity ID to be used with Office 365 (for example, `contoso.com`). This domain name should match the issuer entity ID as specified in the PowerShell script used in the [Create a Federated Domain](#) section (Step 5) above. If no value is entered here, the server-wide default is used. Either the Virtual Server ID or the server-wide default must be set. For more information on setting the server-wide default, see [Specifying Federation Information](#).

Note: To support multiple Office 365 subdomain accounts via one SP connection in PingFederate 7.2 (or higher), add a virtual server ID for each subdomain; the virtual server ID value should match the issuer entity ID (`IssuerUri`) of the respective subdomain account in Office 365.

6. Click **Configure Browser SSO**, click **Next** on the Assertion Lifetime screen, and click **Configure Assertion Creation**.
7. On the Identity Mapping screen, select **User Principal Name** and click **Next**.
8. Add two attributes to Extend the Contract and then click **Next**:
 - Enter **ImmutableID** and select `http://schemas.microsoft.com/LiveID/Federation/2008/05` as the Attribute Name Format.
 - Enter **UPN** and select `http://schemas.xmlsoap.org/claims` as the Attribute Name Format.

An Attribute Contract is a set of user attributes that this server will send in the assertion.

EXTEND THE CONTRACT	ATTRIBUTE NAME FORMAT	ACTION
SAML_SUBJECT		
ImmutableID	<code>http://schemas.microsoft.com/LiveID/Federation/2008/05</code>	Edit / Delete
UPN	<code>http://schemas.xmlsoap.org/claims</code>	Edit / Delete

9. On the IdP Adapter Mapping screen, click **Map New Adapter Instance**, select the HTML Form adapter (see [Creating an IdP Adapter](#) on page 10) as the Adapter Instance and click **Next**.
10. On the Virtual Server IDs screen (visible only if you added multiple virtual server IDs on the General Info screen in step 5 to support multiple Office 365 subdomain accounts), select the Restrict Virtual Server IDs checkbox, choose the virtual server ID representing the subdomain this IdP adapter is meant for, and click **Next**. This restricts resources to the right

subdomain. For more information, see [Restricting an IdP Adapter to certain Virtual Server IDs](#) in the PingFederate [Administrator's Manual](#).

Important: If you have only one IdP adapter for users across subdomains, consider using an OGNL expression on the Issuance Criteria screen to protect against unauthorized access in step 19. Leave the Restrict Virtual Server IDs checkbox unchecked and click **Next**.

11. On the Assertion Mapping screen, select the first option to retrieve additional attributes from multiple data stores using one mapping and click **Next**.
12. On the Attribute Sources & User Lookup screen, click **Add Attribute Source**.
13. On the Data Store screen, enter a value for Attribute Source Description (for example, AD), select the previously created data store from the Active Data Store drop-down list, and click **Next**.
14. On the LDAP Directory Search screen, enter the following:
 - Base DN – Specify the base DN of the container holding user entries from which additional attributes should be retrieved (for example, CN=Users,DC=contoso,DC=com).
 - Root Object Class – Select **<Show All Attributes>**.
 - Attribute – Select **objectGUID** and click **Add Attribute**. Select **userPrincipalName** as another attribute and click **Add Attribute**. Click **Next**.
15. On the LDAP Binary Attribute Encoding Types screen, select **Base64** as the Attribute Encoding Type for the objectGUID attribute (if it isn't already selected) and click **Next**.
16. On the LDAP Filter screen, specify the value you want to search by in the Filter field (for example, sAMAccountName=\${username}, userPrincipalName=\${username}@contoso.com, etc.) and click **Next**.

Note: The value of \${username} in this context is the value entered on the login page that PingFederate presents to the user for passive (browser-based) SSO.

17. Click **Done** and **Next**.
18. On the Attribute Contract Fulfillment screen, enter the following values and click **Next**.

Adapter contract	Source	Value
ImmutableID	LDAP	objectGUID
SAML_SUBJECT	LDAP	userPrincipalName
UPN	LDAP	userPrincipalName

19. On the Issuance Criteria screen, if you have only one IdP adapter for users across subdomains, consider using an OGNL expression to verify the virtual server ID in conjunction with other conditions, such as group membership information, to protect against unauthorized access (see [Issuance Criteria and Multiple Virtual Server IDs](#) in the [Administrator's Manual](#) for a sample OGNL expression); otherwise, click **Next**.
20. On the Summary screen, click **Done**.
21. If you have multiple IdP adapters for different subdomains, repeat steps 9 through 19 to add them one at a time; otherwise, click **Next**, followed by **Done** and **Next**.
22. On the Protocol Settings screen, click **Configure Protocol Settings** and enter `https://login.microsoftonline.com/login.srf` as the Endpoint URL and click **Next**.
23. Click **Done** and **Next**, and then **Done** and **Next**.

Note: If you are not using active federation, then you do not need to configure WS-Trust STS settings: skip ahead to step 46. If the task bar is showing **WS-Trust STS**, return the Connection Type screen and clear the WS-Trust checkbox. Then go to the Credentials screen.

24. On the WS-Trust STS screen, click **Configure WS-Trust STS**.
25. On the Protocol Settings screen, enter `urn:federation:MicrosoftOnline` as the Partner Service Identifier and click **Add**.

Enter the URL that was passed as the `ActiveLogOnUri` to the `Set-MsolDomainFederationSettings` PowerShell cmdlet, minus the URI scheme (for example, `contoso.com:9031/idp/sts.wst`) and click **Add**.

Note: Though it might seem odd to add the identifier of the PingFederate server to the list of acceptable *partner* identifiers, both it and the URN are necessary for successful interoperability.

26. Click **Next** and on the Token Lifetime screen, click **Next**.
27. On the Token Creation screen, click **Configure Token Creation**.
28. On the Attribute Contract screen, add the same two attributes to Extend the Contract and then click **Next**:

- Enter **ImmutableID** and select `http://schemas.microsoft.com/LiveID/Federation/2008/05` as the Attribute Name Format.
- Enter **UPN** and select `http://schemas.xmlsoap.org/claims` as the Attribute Name Format.

29. On the Request Contract screen, click **Next**.

30. On the IdP Token Processor Mapping screen, click **Map New Token Processor Instance**.

31. On the Token Processor Instance screen, select the Username token processor previously created for the Token Processor Instance and click **Next**.

32. On the Virtual Server IDs screen (visible only if you added multiple virtual server IDs on the General Info screen in step 5 to support multiple Office 365 subdomain accounts), select the Restrict Virtual Server IDs checkbox, choose the virtual server ID representing the subdomain this token processor is meant for, and click **Next**. This restricts resources to the right subdomain. For more information, see [Restricting a Token Processor to certain Virtual Server IDs](#) in the PingFederate [Administrator's Manual](#).

Important: If you have only one token processor for users across subdomains, consider using an OGNL expression on the Issuance Criteria screen to protect against unauthorized access in step 41.

33. On the Attribute Retrieval screen, select the option to retrieve additional attributes from data stores and click **Next**.

34. On the Attribute Sources & User Lookup screen, click **Add Attribute Source**.

35. On the Data Store screen, define the following fields and then click **Next**:

Attribute Source Id – Enter a value that uniquely identifies the data source for the mapping (for example, AttributeSource1).

Attribute Source Description – Enter a description (for example, AD).

Active Data Store – Select the previously created data store.

36. On the LDAP Directory Search screen:

Base DN – Enter the base DN of the container holding user entries that will authenticate to Office 365 using an active client (for example, CN=Users,DC=contoso,DC=com).

Root Object Class – Select **<Show All Attributes>**.

Attribute – Select **objectGUID** and click **Add Attribute**. Select **userPrincipalName** as another Attribute and click **Add Attribute**. Click **Next**.

37. On the LDAP Binary Attribute Encoding Types screen, select **Base64** as the Attribute Encoding Type for the objectGUID attribute (if it isn't already selected) and click **Next**.

38. On the LDAP Filter screen, specify a Filter that can be used to find the user that is being authenticated (for example, `userPrincipalName=${username}` or `userPrincipalName=${principal}` for Kerberos).

Note: The username sent is always a UPN.

39. Click **Next**, **Done**, and then **Next**.
40. On the Attribute Contract Fulfillment screen, enter the following values, click **Next** and then **Next** again.

Adapter contract	Source	Value
ImmutableID	LDAP	objectGUID
SAML_SUBJECT	LDAP	userPrincipalName
UPN	LDAP	userPrincipalName

41. On the Issuance Criteria screen, if you have only one token processor for users across subdomains, consider using an OGNL expression to verify the virtual server ID in conjunction with other conditions, such as group membership information, to protect against unauthorized access (see [Issuance Criteria and Multiple Virtual Server IDs](#) in the [Administrator's Manual](#) for a sample OGNL expression); otherwise, click **Next**.
42. On the Summary screen, click **Done**.
43. If you have multiple token processors for different subdomains, repeat steps 27 through 42 to add them one at a time.
44. If you are configuring a Kerberos token processor, repeat steps 27 through 42 to map a Kerberos token processor instance.

Note: For PingFederate 6.10 to 7.1.4, when mapping a token processor to the WS-Trust connection, only one Username Token Processor and one Kerberos Token Processor can be mapped to the connection. Mapping two token processors of the same type causes unwanted server behavior. For PingFederate 7.2 or higher, multiple Username Token Processors are allowed; however, they must not share the same allowed virtual server ID value selected on the Virtual Server IDs screen in step 32. The same rule applies to Kerberos Token Processors as well.

45. Click **Next** until you reach the Credentials screen.
46. On the Credentials screen, click **Configure Credentials**.
47. Select the certificate you exported and uploaded to Office 365 when you executed the `Confirm-MsolDomain` PowerShell command. Select **RSA SHA1** from the Signing Algorithm drop-down list and click **Next**.
48. Click **Done** and **Next**.

49. On the Activation & Summary screen, select the **Active** option at the top of the screen and click **Save**.
50. Finally, on the **SP Connections** screen click **Save**.

Testing the Setup

To test browser-based access to Office 365 applications such as the team portal, do the following:

1. Open a browser window and navigate to <https://portal.microsoftonline.com>.
2. In the **User ID** field, specify the address of a user that has been synchronized.
3. Click the **Sign in at <your federated domain brand name>** link.
4. When presented with a login form, enter the credentials of the user and click **Submit**.

Your browser should be redirected to the Office 365 team portal, and you should be logged in. If you receive an error stating that the user does not have a license to use Office 365, first log in as an administrator and [allocate that user a license](#); you may also need to grant the user rights if you are testing SharePoint Online. After making these changes, retest.

To test access to the federated instance of Office 365 using Microsoft Outlook or some other client that supports POP3 or IMAP4, follow the [instructions specific to the application you are using](#). To find the server settings you need to configure the client in Office 365, consult the [documentation](#) on the Microsoft Outlook Web App site.

After you find the correct POP/IMAP server settings and configure your client, try to send and receive email. This should trigger a prompt for a password. This password relays back to PingFederate via WS-Trust, so monitor its log files for activity. If you do not see any, and receive an error in your email program about the password not being valid, the SSL certificate that PingFederate is using is probably self-signed. Check that this SSL certificate is signed by a CA that Microsoft trusts and then retest.

Performance Considerations

Testing performed in-house has shown that an Outlook client (default configuration) will, on average, make between 9 and 12 requests to the PingFederate STS endpoint per hour. Moreover, the first time an editor is opened, a request is made to the PingFederate STS endpoint.

To help size your deployment we have documented performance results for the Username and Kerberos Token Processors in the Performance Capacity Planning Guide available from the Ping Identity [Customer Portal](#).

Troubleshooting

The following provides useful links when troubleshooting sign-in issues with Microsoft Lync.

[How to Troubleshoot Sign-in Issues in Lync Online](#) – Describes how to troubleshoot sign-in issues with Microsoft Lync and Office 365.

[Troubleshooting Lync Online Sign-in Errors](#) – Describes how to troubleshoot sign-in issues with Microsoft Lync. This is similar to the article above, but details how to clear the credential cache that can occur on some operating systems.

[Fix Lync Client-Side Issues](#) – Describes how Microsoft Lync can cache its connection endpoints and how to resolve the issue.

[Troubleshoot Lync for Mac Issues in Lync Online for Office 365](#) – Describes how to troubleshoot common issues between Lync for Mac and Office 365.