



Pexip Infinity VMR Scheduling for Exchange

Deployment Guide

Software Version 32

Document Version 32.a

June 2023

]pexip[

Contents

Scheduling Pexip Infinity meetings using Microsoft Exchange	6
Supported Exchange deployments	6
Supported clients	6
Support for delegate access to calendars	6
Network architecture and firewalls	7
Using a load balancer in your Exchange deployment	7
Enabling VMR scheduling in personal VMRs	8
Overview	8
Prerequisites	8
Process flow - personal VMRs	8
User activates add-in	9
Initial user sign-in	10
Conferencing Node obtains VMRs	10
Add-in adds joining details to the meeting invitation	10
Next step	10
Configuring AD FS SSO for personal VMRs	11
How it works	11
Prerequisites	11
AD FS version	11
Internet accessibility and security	11
Certificates	12
Setting up an OAuth 2.0 Client on Windows Server	12
Creating a Native Application	12
Creating a Web API Resource	12
Configuring Claim Rules	13
Checking and enabling AD FS endpoints	13
Determining Federation Service Properties	14
Creating a Relying Party Trust	14
Configuring Claim Rules	14
Checking and enabling AD FS endpoints	15
Determining Federation Service Properties	15
Adding the OAuth 2.0 Client to AD FS	15
Next steps	16
Configuring Azure SSO for personal VMRs	17
How it works	17
Creating and configuring a new App Registration in Azure	17
Taking note of configuration	21
Next steps	22
Enabling VMR scheduling in single-use VMRs	23

Overview	23
Process flow - single-use VMRs	24
Add-in requests aliases	26
Management Node generates aliases and join instructions	26
Management Node creates VMRs	26
PXPS:- and TOK:- security tags	27
Using application impersonation	27
Recurring meetings	27
PINs and authentication	27
Next step	28
Configuring Exchange on-premises for scheduling	29
Prerequisites	29
Creating a service account	29
Configuring Application Impersonation on the service account	30
Creating an equipment resource	31
Configuring the equipment resource	32
Enabling authentication	33
NTLMv2 authentication	33
Basic authentication	33
Viewing the equipment resource's mailbox	34
Next steps	34
Configuring Office 365 for scheduling	35
Prerequisites	35
Creating a service account	35
Configuring Application Impersonation on the service account	36
Creating an equipment resource	37
Configuring the equipment resource	38
Enabling OAuth authentication	39
Viewing the equipment resource's mailbox	44
Next steps	44
Configuring Pexip Infinity for VMR Scheduling for Exchange	45
Prerequisites	45
Adding a VMR scheduling for Exchange integration to Pexip Infinity	45
Signing in to the service account if OAuth has been enabled	58
Saving and checking configuration	59
Formatting the email text	59
Working with jinja2 templates	60
Variables	60
Deleting and replacing VMR scheduling for Exchange integrations	61

Using multiple VMR scheduling for Exchange integrations	62
Different groups of users within the same Microsoft Exchange deployment	62
Different Microsoft Exchange deployments	62
Next step	62
Making the scheduling add-in available to users	63
Prerequisites	63
Downloading the add-in XML file	63
Testing the integration	67
Troubleshooting	67
Restricting the scheduling add-in to specific users	68
Prerequisites	68
Active Directory (AD) group	68
Exchange distribution group	69
Azure AD group	69
Verifying the add-in is available as expected	69
Changing the users for an existing add-in	70
Managing scheduled conferences	71
Scheduled conference VMRs	71
Viewing all single-use VMRs used for scheduled conferences	71
Editing the VMR for a scheduled conference	71
Viewing all upcoming scheduled meetings	72
Troubleshooting	72
Maintenance and recovery procedures for VMR Scheduling for Exchange	73
Running the scripts	73
Recovering meetings	73
Example	73
Deleting old mailbox items	74
Example	74
Locating the add-in	75
Outlook desktop client (new version)	75
Outlook desktop client	75
Office 365 (new version)	75
Office 365	75
On-prem OWA	76
Creating a new video meeting	77
Using a personal VMR	77
Using a single-use VMR	77

Changing an existing meeting into a video meeting	79
Editing or canceling an existing video meeting	80
Example joining instructions	81
Including images in the joining instructions	81
Example: dark background with images	81
Example: light background with images	84
Troubleshooting VMR Scheduling for Exchange	87

Scheduling Pexip Infinity meetings using Microsoft Exchange

Users can host their meeting in a [single-use VMR](#) that is created specifically for the meeting and only available for its duration, or they can host their meeting in their own [personal VMR](#). You can either let users decide which type of VMR to use for each meeting, or make just one type of VMR available in your deployment.

VMR Scheduling for Exchange is an optional [licensed feature](#) within the Pexip Infinity platform. When this feature has been enabled, you can create VMR scheduling for Exchange integrations to one or more Microsoft Exchange deployments.

In this topic:

- [Supported Exchange deployments](#)
- [Supported clients](#)
- [Support for delegate access to calendars](#)
- [Network architecture and firewalls](#)

Supported Exchange deployments

Pexip Infinity VMR Scheduling for Exchange is supported on the following Microsoft Exchange deployments:


- Office 365
- Exchange 2013 (with the latest updates)
- Exchange 2016 (with the latest updates)
- Exchange 2019 (with the latest updates)

Supported clients

The Pexip Infinity VMR Scheduling for Exchange add-in is supported on all Outlook clients that support the Microsoft Outlook add-in API. At the time of release, this includes the following clients:

- Outlook as part of Office 2013 and later on Windows
- Outlook as part of Office 2016 and later on Mac
- Outlook as part of Office 365 on Windows and Mac
- Outlook Web Application (OWA) when connected to any supported Microsoft Exchange deployment.

There are some minor usability issues when using Outlook add-ins under certain circumstances; see [Troubleshooting VMR Scheduling for Exchange](#) for more information.

 The Pexip Infinity VMR Scheduling for Exchange add-in is dependent on the Microsoft Outlook add-in API. Any changes to the API should be backwards-compatible, but may impact the functionality of the Pexip add-in.

Support for delegate access to calendars

An update to the Microsoft Outlook add-in API [enabled add-ins for users managing a calendar to which they have delegate access](#). Pexip Infinity version 24 and later supports this API update, enabling the use of the VMR Scheduling for Exchange add-in within delegate calendars. To enable this:

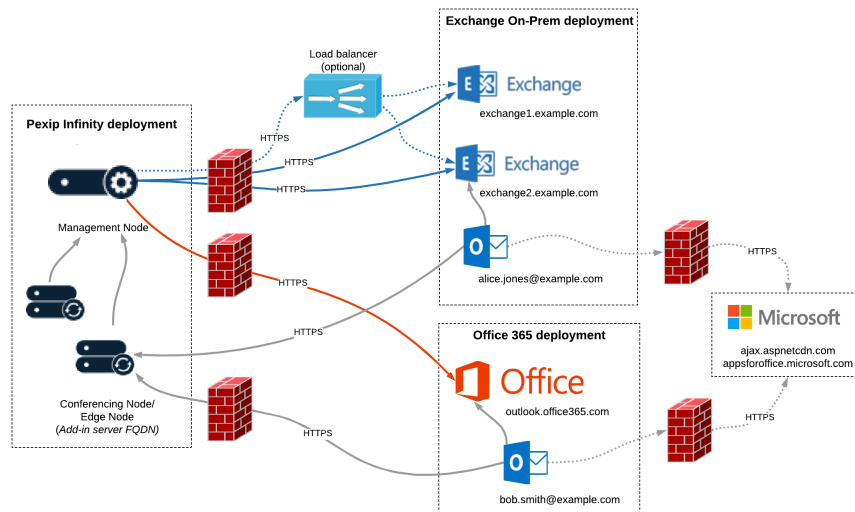
- Users must be using Office 365 and a version of Outlook that supports add-ins for delegates. At the time of writing, this only applies to Outlook on Windows or Mac as part of an Office 365 subscription. Outlook should be updated to version 1910 (build 12130.20272) or newer. For more information about which Outlook clients support which features, see [Microsoft's documentation](#).
- Delegate users must be set up in accordance with Microsoft's instructions for [granting delegate access](#).
- If you have upgraded Pexip Infinity from a version prior to v24, after upgrading you must download and re-upload the manifest file. For instructions on how to do this, see [Making the scheduling add-in available to users](#). Note that users will then need to restart Outlook, and may need to wait up to 24 hours for the add-in to be enabled.

Network architecture and firewalls

The diagram below summarizes the connectivity required between the components of the Pexip and Exchange/O365 deployments.

In this example, there are firewalls in place between the Pexip Infinity deployment and the Exchange and Office 365 deployments. Your own deployment may or may not have these, but in all cases you must ensure the following connections are permitted:

- from the Pexip Infinity Management Node to each Microsoft Exchange server: HTTPS, TCP port 443
 - from the Pexip Infinity Management Node to login.microsoftonline.com (if you are using OAuth)
 - from the Pexip Infinity Management Node to the [load balancer](#) (if you have one): HTTPS, TCP port 443
 - From the Pexip Infinity Conferencing Nodes to the [User OAuth token URI](#) (if [personal VMRs](#) are enabled)
 - from the Outlook clients to the hostname specified by the [Add-in server FQDN](#). This must be reachable either directly, or by using split DNS to resolve to a Transcoding Conferencing Node, Proxying Edge Node, or reverse proxy: HTTPS, TCP port 443
 - from the Outlook clients to <https://ajax.aspnetcdn.com> and <https://appsforoffice.microsoft.com>. These connections are required in order to use the JavaScript API for Office — for more information, see <https://docs.microsoft.com/en-us/office/dev/add-ins/reference/javascript-api-for-office>.
- i** It is possible to host these resources locally for deployments that are entirely offline. For more information, see [Advanced options](#).



Using a load balancer in your Exchange deployment

VMR scheduling for Exchange integrations support the use of load balancers in front of the Exchange servers.

In all deployments using load balancers, the FQDN of the load balancer must still be configured in the list of [Exchange domains](#), even if the [EWS URL](#) uses the address of the load balancer.

Enabling VMR scheduling in personal VMRs

This topic gives an overview of the process and prerequisites for using VMR Scheduling for Exchange with personal VMRs. This allows users who already have their own personal VMR in your deployment to schedule meetings in that VMR.

i You can also enable VMR Scheduling for Exchange with [single-use VMRs](#), either instead of, or in addition to, personal VMRs.

In this topic:

- [Overview](#)
- [Prerequisites](#)
- [Process flow - personal VMRs](#)
- [Next step](#)

See [Locating the add-in](#) for a guide for end users on how to use the add-in.

Overview

Enabling the use of personal VMRs within the VMR Scheduling for Exchange service involves the following steps:

1. Either [Configuring AD FS SSO for personal VMRs](#) or [Configuring Azure SSO for personal VMRs](#).
2. [Configuring Pexip Infinity](#), including [enabling personal VMRs](#) and creating the VMR Scheduling for Exchange add-in.
3. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

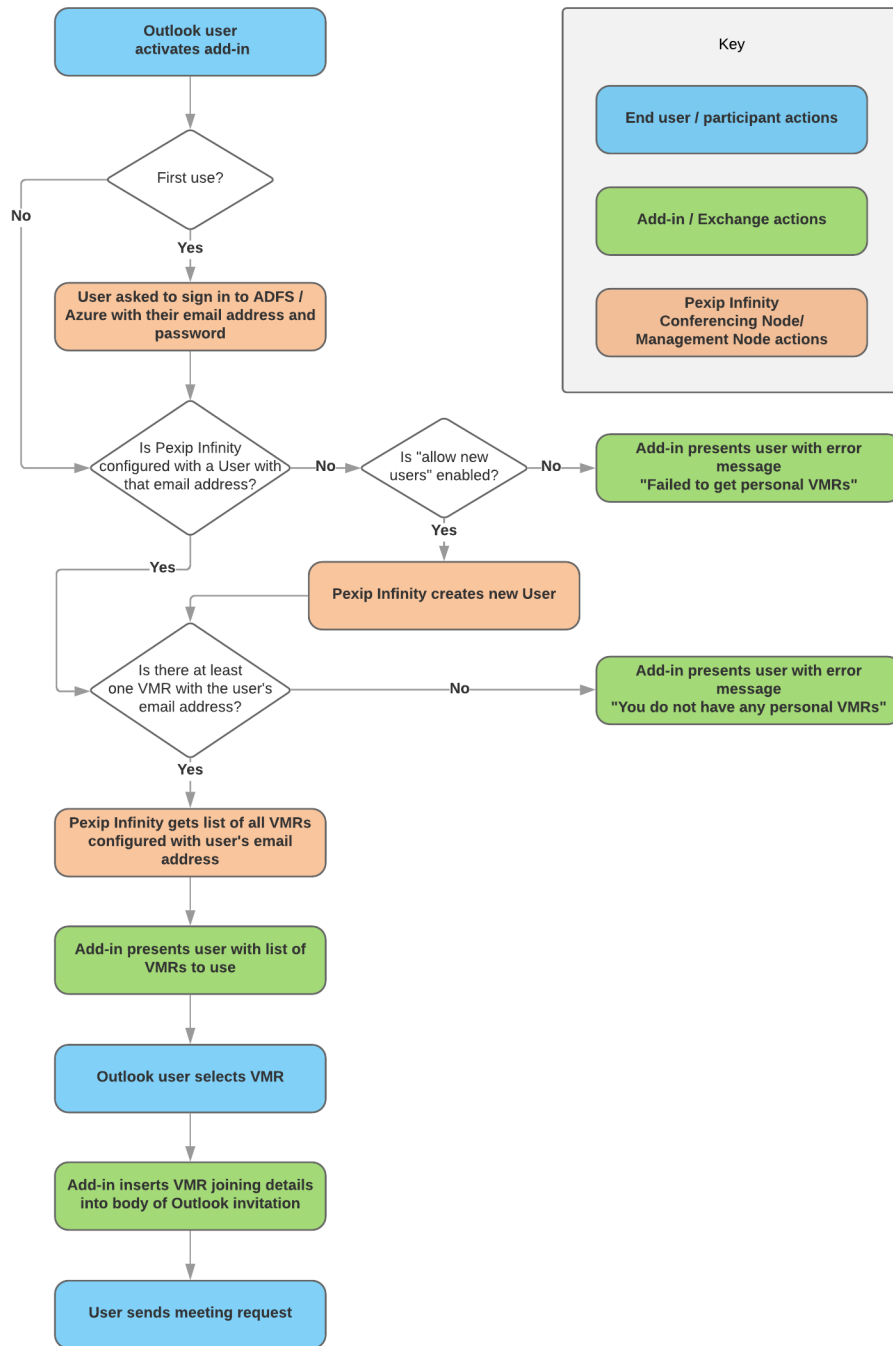
See [Locating the add-in](#) for a guide for end users on how to use the add-in.

Prerequisites

- You must be using either AD FS or Azure Single Sign-On (SSO) for Outlook end users.
- There must be a that has an **Email address** configured with the user's Single Sign-on (SSO) email address (or alternatively, you must configure this feature to [Allow new users](#), in which case the required record will be created by Pexip Infinity).
- You must ensure that for every user who will be scheduling meetings in their personal VMRs, your deployment includes at least one VMR that has an **Owner's email address** configured with the user's Single Sign-on (SSO) email address. If there is more than one VMR configured with the user's email address, the user will be presented with all the VMRs, and can choose which VMR to use for each particular meeting. Each one of these VMRs must also have at least one alias configured.

Process flow - personal VMRs

The diagram below outlines the process that is initiated when users activate the Pexip VMR Scheduling for Exchange add-in from their Outlook client and the **Personal VMR** option is used (either because this is the only option available to users, or because they have elected to use this option instead of a single-use VMR when both are available). This process is described in more detail in the paragraphs that follow.



User activates add-in

When a user activates the Pexip VMR Scheduling for Exchange add-in from within their Outlook client meeting request, the add-in sends a request to the reverse proxy or Conferencing Node identified by the **Add-in server FQDN** field. If a reverse proxy is used, it will forward the request on to an appropriate Conferencing Node. If personal VMRs have been enabled, the user will then be offered the option to sign in (if they have not already done so).

Initial user sign-in

If the user has not previously signed in, they will be presented with the sign in panel; if they have previously signed in, they will go straight to [Conferencing Node obtains VMRs](#). (Users' sign-in details will be remembered, so they should not need to sign in again unless their User record gets deleted from Pexip Infinity.)

The user must sign in with their SSO email address and password which has already been set up in your selected SSO provider. (For information on how to configure SSO, see [Configuring AD FS SSO for personal VMRs](#) or [Configuring Azure SSO for personal VMRs](#).)

The Conferencing Node then checks whether there is already a Pexip Infinity User configured (**Users & Devices > Users**) with the same email address.

- If the user already exists, the [Conferencing Node obtains VMRs](#).
- If the user does not already exist, but **Allow new users** (**System > VMR Scheduling For Exchange > Personal VMR Configuration > Allow New Users**) has been enabled, the Management Node will create a user with the SSO email address.
- If the user does not already exist and **Allow new users** has been disabled, the user will see the configured [Error getting personal VMRs message](#).

Conferencing Node obtains VMRs

The Conferencing Node then checks every configured VMR and returns a list of all VMRs with an **Owner's email address** that matches the user's SSO email address.

The list of VMRs is presented to the user, who then selects which VMR to use for that particular meeting.

Add-in adds joining details to the meeting invitation

The add-in then applies the **Personal VMR joining instructions template** to generate the joining instructions for the selected VMR, and inserts these into the invitation body. It also uses the **Personal VMR location template** to generate a location, and inserts that into the **Location** field of the meeting invitation.

The user then adds their own content to the meeting invitation and sends it in the usual way.

Next step

Depending on your SSO provider, either [Configuring AD FS SSO for personal VMRs](#) or [Configuring Azure SSO for personal VMRs](#).

Configuring AD FS SSO for personal VMRs

You can set up VMR Scheduling for Exchange to offer users the option to use their personal VMRs when scheduling meetings. This requires Single Sign-On (SSO).

This topic explains how to configure AD FS to enable SSO for VMR Scheduling for Exchange when using personal VMRs.

In this topic:

- [How it works](#)
- [Prerequisites](#)
- [Setting up an OAuth 2.0 Client on Windows Server](#)
- [Next steps](#)

How it works

The process of VMR Scheduling for Exchange users authenticating to Pexip Infinity via AD FS in order to obtain their personal VMRs works as follows:

1. When the Outlook add-in launches, it opens up a pop-up window for the user to sign in to AD FS using their AD credentials.
2. After the user has successfully signed in, they are redirected back to the Outlook add-in, which then requests an access token from AD FS.
3. The AD FS server returns the AD FS access token to the Outlook add-in. This token proves that the user has successfully authenticated with AD FS.
4. Pexip Infinity then updates its record for that user so that the user does not need to log in again when they next activate the add-in.

This process means that:

- users' SSO credentials are not stored by Pexip Infinity
- if you delete and recreate a user's record on Pexip Infinity (**Users & Devices > Users**), they will need to sign in to AD FS again.

Prerequisites

Before you integrate your AD FS deployment with Pexip Infinity, you must make sure your AD FS deployment satisfies the following requirements.

AD FS version

You must be using a version of Windows Server that supports OAuth 2.0 with AD FS, i.e. Windows Server 2012 R2 or later.

Internet accessibility and security

Your Federation Service must be accessible by:

- all Pexip Infinity Conferencing Nodes or, if you are using a [reverse proxy](#) for VMR Scheduling for Exchange, all Conferencing Nodes to which the reverse proxy points
- all users who need to sign into AD FS to authenticate with Pexip Infinity.

In practice this means your Federation Service must be accessible from the internet. This raises security concerns, but Microsoft provide documentation about the recommended deployment of AD FS:

- Top-level AD FS documentation can be found at <https://docs.microsoft.com/en-us/windows-server/identity/active-directory-federation-services>.
- Note the network layout recommendations made in the Microsoft documentation, for example <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/design/federation-server-farm-using-sql-server> where all AD FS servers are deployed inside the corporate network and are load-balanced.

- To make the Federation Service accessible from the internet, separate servers in the DMZ can be installed with the Web Application Proxy (WAP) role, which proxy requests to the internal AD FS servers from the internet.
- Your Federation Service Name, e.g. adfs.example.com, must be routable from both inside and outside your corporate network.
 - Inside your corporate network, it should resolve directly to your AD FS server (or the IP address used to load balance multiple AD FS servers).
 - Outside your corporate network, it should resolve to your WAP servers in the DMZ.

This requires the correct DNS configuration to be setup. Microsoft also provide documentation about this, for example <https://docs.microsoft.com/en-us/windows-server/identity/ad-fs/deployment/configure-name-resolution-for-a-federation-server-proxy-in-a-dns-zone-that-serves-only-the-perimeter-network>.

- Another very good source of information for creating a highly available AD FS deployment can be found in the series of blog posts at <https://blogs.technet.microsoft.com/platformspfe/2014/08/28/part-1-windows-server-2012-r2-ad-fs-federated-web-sso/>.

These posts refer to AD FS 3.0 on Windows Server 2012 R2, but they also apply to AD FS 4.0 on Windows Server 2016.

Certificates

Each AD FS server must be provided with a valid certificate which is trusted by your Pexip Infinity deployment. The subject of this certificate needs to match the Federation Service Name.

Setting up an OAuth 2.0 Client on Windows Server

To set up an OAuth 2.0 Client, use the appropriate set of instructions below for your version of AD FS and Windows Server.

- Windows Server 2016 and later
- AD FS 3.0 on Windows Server 2012 R2

Creating a Native Application

In this step you create a new application group with a new native application for the OAuth client — which is the Outlook add-in in this case.

1. Log on to a computer that can make configuration changes to your Federation Service. If your AD FS deployment uses Windows Internal Database (WID), this must be the Primary AD FS Server. If your AD FS deployment uses SQL Server then any AD FS server can make configuration changes.
2. From the top right of the Server Manager application window, select **Tools > AD FS Management**.
3. From the left panel, select **Application Groups** and then from the right panel select **Add Application Group**.
4. At the **Welcome** screen, enter a **Name** and **Description** for the application group. Then from the **Template** section, under **Standalone applications**, select **Native application**.
5. At the **Native Application** screen, enter a **Name** for the application. A new **Client Identifier** is randomly generated for you (this will be required later when configuring the [User OAuth client ID](#) on Pexip Infinity).

In the **Redirect URI** field, enter:

`https://<address>/api/client/v2/msexchange_schedulers/oauth_redirect`

where <address> is the [Add-in server FQDN](#) configured on Pexip Infinity, for example

`https://px01.vc.example.com/api/client/v2/msexchange_schedulers/oauth_redirect`

6. At the **Summary** screen, review the settings and select **Next**.

The new application group, along with the new native application, is created.

Creating a Web API Resource

In this step you create a Web API within your application group. The Web API acts as the resource that is accessed when users authenticate to Pexip Infinity using their AD credentials.

1. On the AD FS Management Tool, from the left-hand panel select **Application Groups** and from the middle panel select the application group you have just created. From the right-hand panel, select **Properties**.
2. At the bottom of the **Properties** window, select **Add application...**

3. At the **Welcome** screen, from the **Template** section, select **Web API**.
4. At the **Configure Web API** screen, enter a **Name** and an **Identifier** (which must be in URL format). You must use this URL as the **AD FS Resource Identifier** on Pexip Infinity when configuring a VMR scheduling for Exchange integration.
5. At the **Choose Access Control Policy** screen select an appropriate policy. The default is *Permit everyone*.
6. At the **Configure Application Permissions** screen, ensure the native application you [created above](#) appears in the list of **Client applications**. All the **Permitted scopes** should be deselected because VMR Scheduling for Exchange does not request any scopes.
7. At the **Summary** screen, review the entered settings then select **Next**.

The new Web API should now be created.


Configuring Claim Rules

In this step you configure an Issuance Transform Rule for the Web API. This rule specifies which claims should be sent to the Relying Party (i.e. which claims will be inside the OAuth token that is sent to Pexip Infinity).

Pexip Infinity requires certain claims to be present inside the token in order to establish the user's identity. These are claims that come from the user's Active Directory account.

1. Ensure there is an Attribute Store configured for Active Directory. To do this, from the AD FS Management Tool, in the left-hand panel expand **Service** and select **Attribute Stores**. Select the attribute store called Active Directory. Open its properties and ensure its **Attribute store type** is *Active Directory*.
If the Attribute Store is not present, add it by selecting **Add Attribute Store**. In the **Add An Attribute Store** window, enter a **Display name** of *Active Directory* and select an **Attribute store type** of *Active Directory*.
2. Add the Issuance Transform Rule on the Web API you just created. To do this, from the AD FS Management Tool, at the bottom of the left-hand panel select **Application Groups**. Select the Application Group you just created and open its Properties.
3. Select the [Web API you created earlier](#) and then select **Edit**.
4. Select the **Issuance Transform Rules** tab and then select **Add Rule**.
5. Select a **Claim rule template** of *Send Claims Using a Custom Rule* and then select **Next**.
6. Enter a **Claim rule name** and enter the following as the **Custom rule**.

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types = ("email", "first_name", "last_name", "display_name"), query =
";mail,givenName,sn,displayName;(0)", param = c.Value);
```

-  The above rule queries Active Directory for the attributes: **mail**, **givenName**, **sn** and **displayName**, and then maps them to the claims: **email**, **first_name**, **last_name** and **display_name** which will appear in the token payload that is returned when the user successfully logs in. The **email** claim is required by Pexip Infinity when verifying the token. If it is not present in the token, the user will fail to authenticate to Pexip Infinity.
7. Select **Finish**, and in the next window ensure you select **Apply**.

Checking and enabling AD FS endpoints

In this step you ensure that the appropriate AD FS endpoints have been enabled to support Pexip's requirements. In the context of AD FS, an endpoint is a URL that AD FS is configured to serve.

To find the details of these AD FS endpoints:

1. From the Server Manager application window, select **Tools > AD FS Management**.
2. From the AD FS Management Tool, in the left-hand panel expand **AD FS > Service > Endpoints**.
3. Locate and check the following endpoint:
 - an **OAuth** type endpoint with path **/adfs/oauth2/**
(this is used by users who sign in to AD FS)

Ensure that this endpoint is **Enabled**. If you are using a Web Application Proxy (WAP) you must also ensure they are **Proxy Enabled**.

Determining Federation Service Properties

To configure AD FS SSO for personal VMRs on the Pexip Infinity Management Node, you must first determine your **Federation Service Name** (this is the FQDN that clients use to access AD FS). The Federation Service Name will be used as the domain part of the [User OAuth authorization URI](#) and the [User OAuth token URI](#). To check this:

- From the AD FS Management Tool, from the left-hand panel select the top level **AD FS** folder, and then select **Edit Federation Service Properties**.

Creating a Relying Party Trust

In this step you create a Relying Party Trust, which acts as the resource that is accessed when users authenticate to Pexip Infinity using their AD credentials.

1. Log on to a computer that can make configuration changes to your Federation Service. If your AD FS deployment uses Windows Internal Database (WID), this must be the Primary AD FS Server. If your AD FS deployment uses SQL Server then any AD FS server can make configuration changes.
2. From the Server Manager application window, select **Tools > AD FS Management**.
3. From the left-hand panel, expand **AD FS > Trust Relationships > Relying Party Trusts**. Then from the right-hand panel select **Add Relying Party Trust....**
4. At the **Add Relying Party Trust Wizard** welcome screen, select **Start**.
5. At the **Select Data Source** screen, select **Enter data about the relying party manually** and select **Next**.
6. At the **Specify Display Name** screen, enter a **Display name** and **Note**, and select **Next**.
7. At the **Choose Profile** screen, select **AD FS profile** and select **Next**.
8. At the **Configure Certificate** screen, do not configure a certificate. Simply select **Next**.
9. At the **Configure URL** screen, do not enable support for either the WS-Federation Passive or the SAML 2.0 WebSO protocols. Simply select **Next**.
10. At the **Configure Identifiers** screen, enter a Relying Party Trust Identifier. This must be unique against all of your Relying Party Trusts, and must be in URL format.
You will need to enter this later when adding an [AD FS Resource Identifier](#) on Pexip Infinity when configuring a VMR scheduling for Exchange integration.
11. At the **Configure Multi-factor Authentication Now?** screen, optionally enable multi-factor authentication. Enabling multi-factor authentication will affect how your users sign in to AD FS.
12. At the **Choose Issuance Authorization Rules** screen, select **Permit all users to access this relying party**.
13. At the **Ready To Add Trust** screen, review the settings and then select **Next**.
14. At the **Finish** screen, verify that the relying party trust was added successfully. Choose to **Open the Edit Claim Rules dialog...** then select **Close**.

Configuring Claim Rules

In this step you configure an Issuance Transform Rule for the Relying Party. This rule specifies which claims should be sent to the Relying Party (i.e. which claims will be inside the OAuth token that is sent to Pexip Infinity).

Pexip Infinity requires certain claims to be present inside the token in order to establish the user's identity. These are claims that come from the user's Active Directory account.

1. Ensure there is an Attribute Store configured for Active Directory. To do this, in the AD FS Management Tool, from the left-hand panel expand **AD FS > Trust Relationships > Attribute Stores**. Look for the attribute store called **Active Directory**. Open its properties and ensure its **Attribute store type** is **Active Directory**.
If the Attribute Store is not present, add it by selecting **Add Attribute Store**. In the **Add An Attribute Store** window, enter a **Display name** of **Active Directory** and select an **Attribute store type** of **Active Directory**.
2. From the left-hand panel expand **AD FS > Trust Relationships > Relying Party Trusts**, select the Relying Party you just created, and from the right-hand panel select **Edit Claim Rules....**
3. Select the **Issuance Transform Rules** tab, then select **Add Rule....**
4. At the **Select Rule Template** screen, select a **Claim rule template** of **Send Claims Using a Custom Rule**.

- At the **Configure Rule** screen, enter a **Claim rule name**, and in the **Custom rule** section enter the following:

```
c:[Type ==
"http://schemas.microsoft.com/ws/2008/06/identity/claims/windowsaccountname", Issuer == "AD AUTHORITY"]
=> issue(store = "Active Directory", types = ("email", "first_name", "last_name", "display_name"), query =
";mail,givenName,sn,displayName;0)", param = c.Value);
```

- i** The above rule queries Active Directory for the attributes: **mail**, **givenName**, **sn** and **displayName**, and then maps them to the claims: **email**, **first_name**, **last_name** and **display_name** which will appear in the token payload that is returned when the user successfully logs in. The email claim is required by Pexip Infinity when verifying the token. If it is not present in the token, the user will fail to authenticate to Pexip Infinity.

- Select **Finish**.
- You are returned to the **Issuance Transform Rules** tab. Select **Apply**.

Checking and enabling AD FS endpoints

In this step you ensure that the appropriate AD FS endpoints have been enabled to support Pexip's requirements. In the context of AD FS, an endpoint is a URL that AD FS is configured to serve.

To find the details of these AD FS endpoints:

- From the Server Manager application window, select **Tools > AD FS Management**.
- From the AD FS Management Tool, in the left-hand panel expand **AD FS > Service > Endpoints**.
- Locate and check the following endpoint:

- an **OAuth** type endpoint with path **/adfs/oauth2/**
(this is used by users who sign in to AD FS)

Ensure that this endpoint is **Enabled**. If you are using a Web Application Proxy (WAP) you must also ensure they are **Proxy Enabled**.

Determining Federation Service Properties

To configure AD FS SSO for personal VMRs on the Pexip Infinity Management Node, you must first determine your **Federation Service Name** (this is the FQDN that clients use to access AD FS). The Federation Service Name will be used as the domain part of the [User OAuth authorization URI](#) and the [User OAuth token URI](#). To check this:

- From the AD FS Management Tool, from the left-hand panel select the top level **AD FS** folder, and then select **Edit Federation Service Properties**.

Adding the OAuth 2.0 Client to AD FS

In this final step you add the OAuth 2.0 client to AD FS. This is done using the `Add-AdfsClient` PowerShell command.

- i** A client ID is required to run this command. To obtain an appropriate client ID you can either:

- Use the client ID generated by Pexip Infinity when adding a VMR scheduling for Exchange integration. In this case you must now complete the configuration described in [Adding a VMR scheduling for Exchange integration to Pexip Infinity](#), take note of the [User OAuth client ID](#) that is generated, and then return to this step to complete the AD FS configuration.
- Generate your own version 4 UUID using a tool such as <https://www.uuidgenerator.net/>. In this case, you should use the generated UUID to complete the AD FS configuration in this step, and then enter that same UUID as the [User OAuth client ID](#) when [Adding a VMR scheduling for Exchange integration to Pexip Infinity](#).

After you have obtained a client ID, open PowerShell on your AD FS server, then run this command:

```
Add-AdfsClient -Name "<name>" -ClientId "<client id>" -RedirectUri "https://<address>/api/client/v2/msexchange_schedulers/oauth_redirect" -Description "<description>"
```

where

- <name>** is a name of your choice used to identify the AD FS client
- <client id>** is the [User OAuth client ID](#) obtained in either of the two ways described above
- <address>** is the [Add-in server FQDN](#) configured on Pexip Infinity (i.e. the FQDN of the reverse proxy or Conferencing Node that provides the add-in content)
- <description>** is an optional description.

For example:

```
Add-AdfsClient -Name "Pexip Scheduling" -ClientId "141c7f59-790b-46f7-add1-7490ee4b489e" -RedirectUri  
"https://tobyrrp.rd.pexip.com/api/client/v2/msexchange_schedulers/oauth_redirect" -Description "The OAuth Client for Pexip  
Scheduling personal VMRs"
```

To verify this worked, run `Get-AdfsClient` and make sure the client you just added is in the results.

Next steps

1. [Configuring Pexip Infinity](#) to integrate with your Microsoft Exchange deployment and create the VMR Scheduling for Exchange add-in.
2. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

Configuring Azure SSO for personal VMRs

You can set up VMR Scheduling for Exchange to offer users the option to use their personal VMRs when scheduling meetings. This requires Single Sign-On (SSO).

This topic explains how to configure Azure to enable SSO for VMR Scheduling for Exchange when using personal VMRs.

In this topic:

- [How it works](#)
- [Creating and configuring a new App Registration in Azure](#)
- [Taking note of configuration](#)
- [Next steps](#)

How it works

The process of VMR Scheduling for Exchange users authenticating to Pexip Infinity via Azure in order to obtain their personal VMRs works as follows:

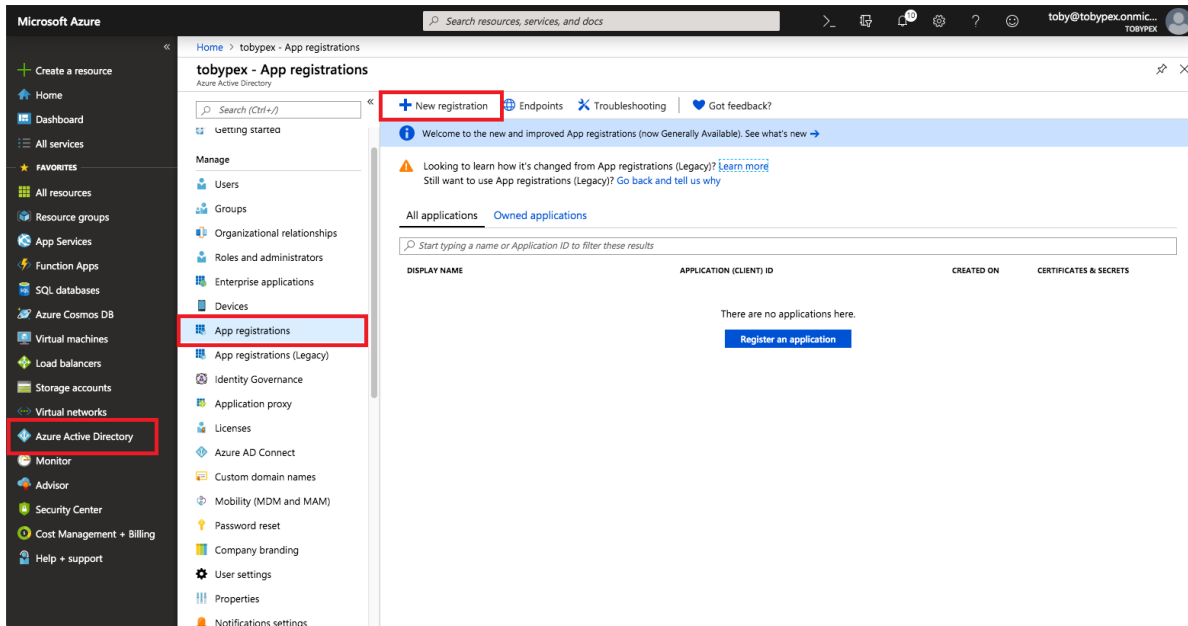
1. When the Outlook add-in launches, it opens up a pop-up window for the user to sign in to Azure using their AD credentials.
2. After the user has successfully signed in, they are redirected back to the Outlook add-in, which then requests an access token from Azure.
3. The Azure server returns the Azure access token to the Outlook add-in. This token proves that the user has successfully authenticated with Azure.
4. Pexip Infinity then updates its record for that user so that the user does not need to log in again when they next activate the add-in.

This process means that:

- users' SSO credentials are not stored by Pexip Infinity
- if you delete and recreate a user's record on Pexip Infinity (Users & Devices > Users), they will need to sign in to Azure again.

Creating and configuring a new App Registration in Azure

1. Log into the Azure portal at aad.portal.azure.com.
2. From the main panel on the left, select **Azure Active Directory**.
3. Select **App Registrations** and then **New registration**:



4. In the Register an application panel, enter the following options:
 - a. **Name:** this can be anything you wish. In our example we have used *Pexip Scheduling Personal VMRs*.
 - b. **Supported account types:** select *Accounts in this organizational directory only*.
Redirect URI: from the drop-down menu, select *Web*. The URI should be in the format:
https://<address>/api/client/v2/msexchange_schedulers/oauth_redirect
 where <address> is the Add-in server FQDN configured on Pexip Infinity, for example
https://px01.vc.example.com/api/client/v2/msexchange_schedulers/oauth_redirect
 In our example we have used **https://pexip.example.com/api/client/v2/msexchange_schedulers/oauth_redirect**
 - c. **The OAuth redirect URI** is the URI to which users will be returned after they have successfully signed in to their account. It must use the same domain as the Add-in server FQDN configured on Pexip Infinity in order for Azure to validate the sign-in request.

Microsoft Azure

Search resources, services, and docs (G+)

Home > Pexip >

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).

Pexip Scheduling Personal VMRs

Supported account types

Who can use this application or access this API?

☒ Accounts in this organizational directory only (Pexip only - Single tenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant)

☐ Accounts in any organizational directory (Any Azure AD directory - Multitenant) and personal Microsoft accounts (e.g. Skype, Xbox)

☐ Personal Microsoft accounts only

[Help me choose...](#)

Redirect URI (optional)

We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

Web

https://pexip.example.com/api/client/v2/msexchange_schedulers/o...

Register

5. Select **Register**.
You can now configure your application.
6. From the panel on the left, select **Certificates & secrets**.
7. Select **New client secret**.
8. Enter a **Description**, under **Expires** select a duration in accordance with your organization's security policies, and select **Add**:

Microsoft Azure

Search resources, services, and docs (G+)

Home > Pexip > Pexip Scheduling Per

Pexip Scheduling

Search (Ctrl+)

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Certificates & secrets

Token configuration

API permissions

Expose an API

Owners

Add a client secret

Description

Pexip Scheduling Personal VMRs

Expires

Recommended: 6 months

Recommended: 6 months

3 months

12 months

18 months

24 months

Custom

Add

Cancel

9. The new client secret will appear in the list at the bottom of the page. You must copy the **Value** now, before you navigate away from the page:

Microsoft Azure

Home > Pexip > Pexip Scheduling Personal VMRs

Pexip Scheduling Personal VMRs | Certificates & secrets

Search (Ctrl+/) Got feedback?

Overview Quickstart Integration assistant | Preview

Manage

- Branding
- Authentication
- Certificates & secrets**
- Token configuration
- API permissions
- Expose an API
- Owners
- Roles and administrators | Preview
- Manifest

Support + Troubleshooting

- Troubleshooting
- New support request

Certificates (0) **Client secrets (1)** Federated credentials (0)

A secret string that the application uses to prove its identity when requesting a token. Also can be referred to as application password.

Client secret values cannot be viewed, except for immediately after creation. Be sure to save the secret when created before leaving the page.

+ New client secret

Description	Expires	Value	Secret ID
Pexip Scheduling Personal VMRs	8/4/2022	WTf7Q~IB55_wq1ndRsPoNxUNo3_Au6p...	7ca788fd-e212-4530-bc90-e0369b593904

You must enter this as the **Azure OAuth client secret** when configuring the VMR scheduling for Exchange integration and [enabling personal VMRs](#)

10. The **User.Read** permission should have been added by default, with a type of **Delegated**. To confirm this, from the panel on the left, select **API permissions** and ensure the appropriate permission is present.

If it is not present, add it as follows:

- a. Select **Add a permission**.
- b. From the **Request API permissions** panel, select **Microsoft Graph**:

Request API permissions

Select an API

Microsoft APIs APIs my organization uses My APIs

Commonly used Microsoft APIs

Microsoft Graph

Take advantage of the tremendous amount of data in Office 365, Enterprise Mobility + Security, and Windows 10. Access Azure AD, Excel, Intune, Outlook/Exchange, OneDrive, OneNote, SharePoint, Planner, and more through a single endpoint.

Azure Batch

Schedule large-scale parallel and HPC applications in the cloud

Azure Data Catalog

Programmatic access to Data Catalog resources to register, annotate and

Azure DevOps

Integrate with Azure DevOps and Azure DevOps server

- c. From the **Request API permissions** page, select **Delegated permissions**, and from the list that appears, scroll down to the

User section and select **User.Read**. Then select **Add permissions**:

Request API permissions

< All APIs

✓ User (1)

<input type="checkbox"/>	User.Export.All ⓘ Export user's data	Yes
<input type="checkbox"/>	User.Invite.All ⓘ Invite guest users to the organization	Yes
<input type="checkbox"/>	User.ManageIdentities.All ⓘ Manage user identities	Yes
<input checked="" type="checkbox"/>	User.Read ⓘ Sign in and read user profile	-
<input type="checkbox"/>	User.Read.All ⓘ Read all users' full profiles	Yes
<input type="checkbox"/>	User.ReadBasic.All ⓘ Read all users' basic profiles	-
<input type="checkbox"/>	User.ReadWrite ⓘ Read and write access to user profile	-
<input type="checkbox"/>	User.ReadWrite.All ⓘ Read and write all users' full profiles	Yes

> WorkforceIntegration

Add permissions Discard

Taking note of configuration

When you [Configure the VMR scheduling for Exchange integration](#) and enable personal VMRs using Azure as your authentication provider, you'll need to provide the following information from Azure (in addition to the **Client Secret** which you have already noted):

- **Application (client) ID:** this was generated for you by Azure when you saved the App Registration:

Microsoft Azure

Home > Pexip > Pexip Scheduling Personal VMRs

Pexip Scheduling Personal VMRs

Search (Ctrl+/)

Overview

Quickstart

Integration assistant | Preview

Manage

Branding

Authentication

Got a second? We would love your feedback on Microsoft identity platform (previously Azure AD for developer). →

Essentials

Application (client) ID : e638adb0-0cd3-42e2-bddd-ea093e47bee4

Directory (tenant) ID : 368db7c4-0300-4304-b319-4680ad0c010d

Object ID : ce64a1ee-d173-4a32-bf38-fedb3b756ef7

Supported account types : My organization only

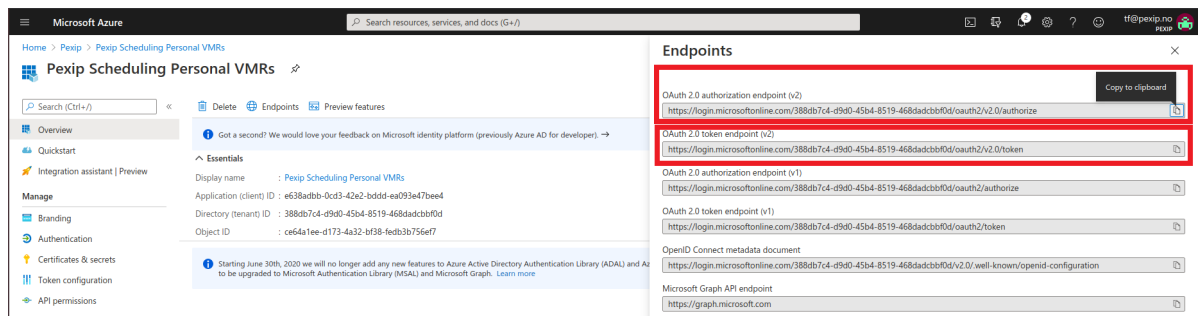
Redirect URIs : 1 web, 0 spa, 0 public client

Application ID URI : Add an Application ID URI

Managed application in I... : Pexip Scheduling Personal VMRs

i You can find this again in Azure under **Azure Active Directory > App Registrations**, under the **Application (client) ID** column. You will need to enter this as the **User OAuth client ID** when configuring the VMR scheduling for Exchange integration and [enabling personal VMRs](#).

- **OAuth 2.0 endpoints.** To find this information:
 - a. In the Azure Portal, select **Azure Active Directory > App registrations**, select the app you have just registered, and select the **Endpoints** tab:



- b. Copy the URL of the **OAuth 2.0 authorization endpoint (v2)**.

ⓘ Ensure that you use the URL for **... endpoint (v2)**, not **... endpoint (v1)**.

You will need to enter this as the **User OAuth authorization URI** when configuring the VMR scheduling for Exchange integration and [enabling personal VMRs](#).

- c. Copy the URL of the **OAuth 2.0 token endpoint (v2)**

ⓘ Ensure that you use the URL for **... endpoint (v2)**, not **... endpoint (v1)**.

You will need to enter this as the **User OAuth token URI** when configuring the VMR scheduling for Exchange integration and [enabling personal VMRs](#).

Next steps

1. [Configuring Pexip Infinity](#) to integrate with your Microsoft Exchange deployment and create the VMR Scheduling for Exchange add-in.
2. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

Enabling VMR scheduling in single-use VMRs

This topic gives an overview of the process and prerequisites for using VMR Scheduling for Exchange with single-use VMRs. These VMRs are created dynamically for a specific meeting, and are only available for the duration of that meeting (and any scheduled recurrences).


 You can also enable VMR Scheduling for Exchange with [personal VMRs](#), either instead of, or in addition to, single-use VMRs.

In this topic:

- [Overview](#)
- [Process flow - single-use VMRs](#)
- [PXPS:- and TOK:- security tags](#)
- [Using application impersonation](#)
- [Recurring meetings](#)
- [PINs and authentication](#)
- [Next step](#)

Overview

Enabling the use of single-use VMRs within your VMR Scheduling for Exchange service involves the following steps:

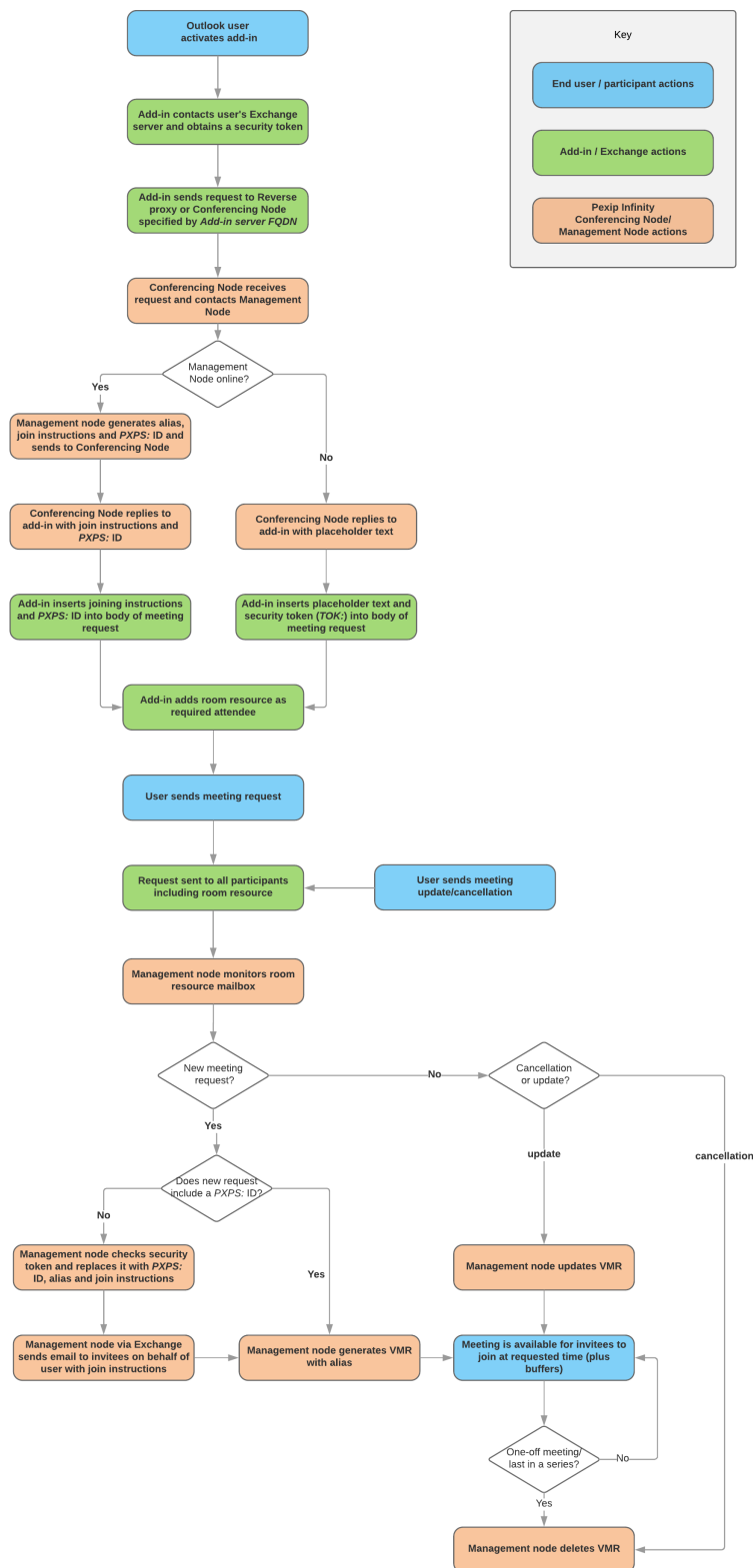
1. [Configuring Microsoft Exchange on-premises](#) or [Configuring Office 365](#) with a service account and equipment resource.
 -  This step is required if you wish to enable single-use VMRs. It is not required if you are **only** enabling personal VMRs in your deployment.
2. [Configuring Pexip Infinity](#), including [enabling single-use VMRs](#), providing the information required to connect to your Microsoft Exchange deployment, and generating the associated add-in.
3. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

See [Locating the add-in](#) for a guide for end users on how to use the add-in.

When VMR Scheduling for Exchange has been implemented, you will be able to view scheduled VMRs in the same way as existing VMRs. For more information, see [Managing scheduled conferences](#).

Process flow - single-use VMRs

The diagram below outlines the process that is initiated when users activate the Pexip VMR Scheduling for Exchange add-in from their Outlook client and select the **Single-use VMR** option; this process is described in more detail in the paragraphs that follow.



- i** The fields described in the following process are [configured on the Management Node](#) via **System > VMR Scheduling For Exchange Integrations**.

Add-in requests aliases

When a user activates the Pexip VMR Scheduling for Exchange add-in from within their Outlook client meeting request, the add-in sends a request to the reverse proxy or Conferencing Node identified by the **Add-in server FQDN** field. If a reverse proxy is used, it will forward the request on to an appropriate Conferencing Node. The Conferencing Node then forwards the request to the Management Node and asks for an alias for the VMR to be used for the meeting. If no Conferencing Node can be contacted at this stage, the user will get a message in the add-in pane of their client informing them that the add-in is not available.

Management Node generates aliases and join instructions

If the Management Node is online, it generates a unique number for the VMR and then uses this to create two aliases (one with a domain appended and one without), using the information in the following fields:

- [Scheduled alias prefix](#)
- [Scheduled alias suffix length](#)
- [Scheduled alias domain](#)

For example, if we have configured a **prefix** of *555*, a **suffix length** of *6* and a **domain** of *example.com*, the two aliases created for one particular VMR could be:

- 555123456
- 555123456@example.com

The Management Node also generates some joining instructions for the VMR, based on the VMR's alias and the **Joining instructions template** field. This information is sent back to the Conferencing Node which forwards it to the add-in as a response to the request. The add-in then inserts the join instructions into the top of the meeting request email. A unique security ID (in the format **PXPS:-<xxx>#**) is also obtained from the Management Node and inserted into the email; this text must not be edited or deleted.

If the Management Node cannot be contacted by the Conferencing Node, the Conferencing Node will respond to the add-in with the placeholder text from the **Placeholder instructions text** field. A multi-line security token in the format **TOK:-<xxx>#** (obtained directly from the Microsoft Exchange server by the add-in) is also inserted into the email; again, this text must not be edited or deleted.

The add-in will also add the [equipment resource](#) as a required attendee. This equipment resource must be included in all subsequent requests relating to this meeting.

Management Node creates VMRs

When the user sends the meeting request, a message is sent to the equipment resource's mailbox. The Management Node monitors this mailbox using the [service account](#). For each new meeting request received, the Management Node generates a VMR with the required aliases (one numeric, the other numeric with domain). For recurring meetings, the same alias is used for all instances of the meeting. For meeting updates and cancellations, the Management Node will update the associated VMR accordingly.

The VMR will be created as soon as the Management Node receives the meeting request, but meeting participants will not be able to use the VMR until they are within the period of time configured by the **Join before buffer** and **Join after buffer**. Participants who have successfully joined the VMR can continue to use it until the last participant has left; the conference will not be terminated automatically by the scheduling service, although it may be [automatically terminated](#) for other reasons.

If the Management Node has been offline, when it comes online it connects to the equipment resource's mailbox and reads the requests. At this point it creates and updates VMRs. For meetings that were not assigned a **PXPS:-** ID, the Management Node will generate an alias and create the VMR. It will then replace the **Placeholder instructions text** and security token (**TOK:-<xxx>#**) in the original meeting request with a **PXPS:-** ID, along with details of the aliases and the joining instructions. The Management Node will then use the service account to send the updated request to all attendees on behalf of the meeting organizer (the request will show in the organizer's sent items folder). This updated request will also be sent to the equipment resource's mailbox.

PXPS:- and TOK:- security tags

To ensure that the VMR Scheduling for Exchange service processes only those meeting requests created using the add-in, and in order to track each meeting request, each request contains a security tag in the format of either **TOK:-** or **PXPS:-**.

When the add-in is activated, it obtains a **TOK:-** security tag from the user's Microsoft Exchange server. This **TOK:-** is then passed to the Management Node when it is asked to allocate an alias for the VMR. If the **TOK:-** is valid, the Management Node will generate the alias and return a **PXPS:-** ID to the Conferencing Node. The **PXPS:-** ID is passed back to the add-in and inserted into the body of the meeting request.

In normal circumstances, end users will not see the **TOK:-** tag because the request to generate a VMR alias will be actioned immediately by the Management Node. However, if the Management Node is offline at the time the request is sent, and therefore a VMR alias is not generated immediately, the **TOK:-** will be inserted into the body of the meeting request. When the Management Node comes back online, it will process the requests; for any with a valid **TOK:-** it will generate a VMR alias and **PXPS:-** ID and send an updated meeting request that includes these.

Note that the **TOK:-** is only valid for a limited amount of time. If the Management Node processes the request after the **TOK:-** expires, it will be considered invalid. In such cases, the meeting organizer must create a new meeting request using the add-in.

Using application impersonation

The use of Exchange impersonation is common in business applications that work with mail, when a single account needs to access many accounts.

The service account used by VMR Scheduling for Exchange uses impersonation as follows:

- To **access the mailbox of the equipment resource** used for VMR Scheduling for Exchange. This impersonation is required in order for the VMR Scheduling for Exchange feature to work.
- To **send emails on behalf of all VMR Scheduling for Exchange users**. This impersonation is only required in the two scenarios described below. If the service account is not permitted to impersonate users, the users will still be able to schedule and update meetings as usual, but the following scenarios will not be supported in your deployment:
 - If an invitation was sent when the Management Node was offline. In this case, when the Management Node comes back online it will generate a new alias and joining instructions for the meeting. It will then update the meeting invitation using impersonation, so that it appears as though the meeting organizer is sending out the updated joining instructions to all the attendees.
 - When the [scheduling recovery tool](#) is run after the Management Node has been restored from a backup. The recovery tool queries the room resource mailbox and finds all meetings that have previously been accepted, and checks whether they are in the scheduling service's database. If not, the Management Node will generate a new alias and new joining instructions for that meeting. This meeting update is sent using impersonation so that it appears as though the meeting organizer is sending out the updated joining instructions to all the attendees.

The following information from Microsoft provides further background on the use of impersonation in Exchange:

- <https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/impersonation-and-ews-in-exchange> for guidelines on when to use impersonation in your Exchange service applications.
- <https://blogs.msdn.microsoft.com/exchangedev/2009/06/15/exchange-impersonation-vs-delegate-access/> for information on the differences between impersonation and delegate access.


Recurring meetings

For recurring meetings in single-use VMRs, the VMR Scheduling for Exchange service creates a single VMR which exists until after the last meeting in the series has taken place. However, participants will only be able to join this VMR during any of the scheduled meeting times.

PINs and authentication

By default, single-use VMRs are created without PINs, meaning participants do not need to enter a PIN and all participants join with Host privileges.

You can optionally require that all participants must [authenticate with an Identity Provider](#) in order to join a single-use VMR; this is configured on a per-VMR scheduling for Exchange integration basis, using the [Identity Provider group](#) and [Other participants](#) settings.

-  When enabled for single-use VMRs, the requirement for participant authentication applies to all meetings scheduled using the add-in associated with that VMR scheduling for Exchange integration. To allow users to choose between scheduling authenticated and unauthenticated meetings, create two integrations and associated add-ins, one with authentication enabled and one without.


In addition, after an individual single-use VMR has been created, you can [edit the configuration for that VMR](#) to add Host PINs and Guest PINs, and/or require participant authentication.

Next step

- [Configuring Microsoft Exchange on-premises](#) or [Configuring Office 365](#) with a service account and equipment resource.

Configuring Exchange on-premises for scheduling

To enable users to schedule meetings in single-use VMRs in an Exchange on-premises environment, you must first configure Exchange on-premises appropriately. The steps are as follows, described in more detail in the sections that follow:

1. [Creating a service account](#). The Pexip Infinity VMR Scheduling for Exchange feature uses a unique service account to log into Exchange.
 -  This should be a different service account to any used for One-Touch Join, because the configuration will be different.
2. [Configuring Application Impersonation on the service account](#). This allows the service account to impersonate users on Exchange.
3. [Create an equipment resource](#). This resource will be added as an attendee to all meetings scheduled using the Pexip add-in.
4. [Configure the equipment resource](#).
5. [Enable the authentication method](#) used for the service account — either NTLMv2 or basic authentication.

PowerShell commands are provided for all steps; parameters to be replaced with your own relevant information are shown in the format **<your info here>**.

Prerequisites



Before you start, ensure you have access to your Exchange Admin Center (EAC) web interface, and access to Exchange Management PowerShell.

Creating a service account

In this step, you create the service account to be used by VMR Scheduling for Exchange.

The VMR Scheduling for Exchange feature uses a service account to log into Exchange. You can use an existing service account (the same service account can be used by more than one VMR scheduling for Exchange integration), or create a new account.

You need to provide the authentication credentials of this service account when configuring Pexip Infinity to integrate with a Microsoft Exchange deployment.

-  A single service account can be used by more than one VMR scheduling for Exchange integration.
-  Changes to the service account may take some time to take effect, depending on the cache lifetime configured on the Microsoft Exchange server.

You can create a new service account using either EAC or PowerShell, as follows:

EAC	PowerShell
<ol style="list-style-type: none"> Log in to your Exchange Admin Center as an administrator and go to recipients > mailboxes. Add a new mailbox for the service account by selecting the + icon and then User mailbox. Complete the fields as appropriate. Uncheck the Require password change on next login box. <p>new user mailbox</p> <p>Alias: pexip</p> <p><input type="radio"/> Existing user</p> <p><input type="radio"/> New user</p> <p>First name: Pexip</p> <p>Initials: </p> <p>Last name: Exchange Service</p> <p>*Display name: Pexip Exchange Service</p> <p>*Name: Pexip Exchange Service</p> <p>Organizational unit: browse...</p> <p>*User login name: pexip @ rd.pexip.com</p> <p>*New password: *****</p> <p>*Confirm password: *****</p> <p><input type="checkbox"/> Require password change on next login</p> <p>More options...</p> <p>save cancel</p>	<p>i The first command lets the administrator type in a password for the service account as a secure string. This password variable is then used in the second command to create a mailbox for the service account. The third command ensures the password of the service account will not expire.</p> <pre>\$password = Read-Host "Enter password" -AsSecureString New-Mailbox -Name "<Account Name>" -UserPrincipalName "<UPN>" -Password \$password -Alias "<Account Alias>" -FirstName "<Account First Name>" -LastName "<Account Last Name>" -DisplayName "<Account Name>" Set-ADUser -Identity "<UPN>" -PasswordNeverExpires \$true</pre> <p>For example:</p> <pre>New-Mailbox -Name "Service Account" -UserPrincipalName pexip@example.com -Password \$password -Alias pexip -FirstName Service -LastName Account -DisplayName "Service Account" Set-ADUser -Identity pexip@example.com -PasswordNeverExpires \$true</pre>
<ol style="list-style-type: none"> Select Save. 	

Configuring Application Impersonation on the service account

In this step you configure the service account with a Role of Application Impersonation, which allows the service account to impersonate users on Exchange.

The service account must be configured with a Role of **Application Impersonation**. This allows the service account to impersonate all users who will be using VMR Scheduling for Exchange, and to impersonate the equipment resource that is to be used for the scheduling service. For more information, see [Using application impersonation](#).

The VMR Scheduling for Exchange service impersonates users when sending email updates containing joining instructions (in cases where these instructions could not be added at the time of scheduling). This makes it appear to the recipients that the joining instructions were sent from the meeting organizer, instead of the service account.

To check if your service account has Application Impersonation already configured, use the PowerShell command:

```
Get-ManagementRoleAssignment -RoleAssignee "<email_of_service_account>" -Role ApplicationImpersonation | Format-List
```

Below is an example of the output of the command when the service account already has Application Impersonation configured:

```
[PS] C:\Windows\system32>Get-ManagementRoleAssignment -RoleAssignee pexip@rd.pexip.com -Role ApplicationImpersonation |
Format-List

RunspaceId           : 439dc5ca-7895-4341-ad2e-8182741cd596
DataObject           : PexipSchedulingService
User                 : rd.pexip.com/Users/Pexip Exchange Service
AssignmentMethod      : Direct
Identity             : PexipSchedulingService
EffectiveUserName     : Pexip Exchange Service
AssignmentChain       :
RoleAssigneeType     : User
RoleAssignee         : rd.pexip.com/Users/Pexip Exchange Service
Role                 : ApplicationImpersonation
RoleAssignmentDelegationType : Regular
CustomRecipientWriteScope :
CustomConfigWriteScope :
RecipientReadScope   : Organization
ConfigReadScope      : None
RecipientWriteScope   : Organization
ConfigWriteScope     : None
Enabled              : True
RoleAssigneeName     : Pexip Exchange Service
IsValid              : True
ExchangeVersion      : 0.11 (14.0.550.0)
Name                 : PexipSchedulingService
DistinguishedName     : CN=PexipSchedulingService,CN=Role Assignments,CN=RBAC,CN=Pexip Dev,CN=Microsoft
Exchange,CN=Services,CN=Configuration,DC=rd,DC=pexip,DC=com
Guid                 : 4bf0f9ac-74cf-4056-94c1-1403cc3ba630
ObjectCategory       : rd.pexip.com/Configuration/Schemas/ms-Exch-Role-Assignment
ObjectClass           : <top, msExchRoleAssignment>
WhenChanged          : 11/05/2017 14:51:17
WhenCreated           : 11/05/2017 14:51:17
WhenChangedUTC        : 11/05/2017 13:51:17
WhenCreatedUTC        : 11/05/2017 13:51:17
OrganizationId        :
OriginatingServer     : tobyad.rd.pexip.com
ObjectState           : Unchanged

[PS] C:\Windows\system32>_
```

If the service account does not have Application Impersonation configured, then the above command will not return anything at all. If this is the case, enable Application Impersonation as follows:

```
New-ManagementRoleAssignment -name:"<role_name>" -Role:ApplicationImpersonation -User:"<email_of_service_account>"
```

For example:

```
New-ManagementRoleAssignment -name:PexipSchedulingService -Role:ApplicationImpersonation -User:pexip@exchange.example.com
```

This will enable the service account to impersonate all users in the organization.

For more information on these commands, see Microsoft help:

- Configuring Application Impersonation: <https://msdn.microsoft.com/en-us/library/office/dn722376%28v=exchg.150%29.aspx>
- Get-ManagementRoleAssignment command: [https://technet.microsoft.com/en-us/library/dd351024\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd351024(v=exchg.150).aspx)
- New-ManagementRoleAssignment command: [https://technet.microsoft.com/en-us/library/dd335193\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335193(v=exchg.150).aspx)
- Set-ManagementRoleAssignment command (used if you need to edit the role assignment): [https://technet.microsoft.com/en-us/library/dd335173\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335173(v=exchg.150).aspx)

Creating an equipment resource

In this step you create an equipment resource to be used by VMR Scheduling for Exchange. This resource is added as an attendee to all meetings scheduled using the Pexip add-in. The scheduling service monitors the equipment resource's mailbox, processes all meeting requests sent to it, and schedules the meetings as appropriate.

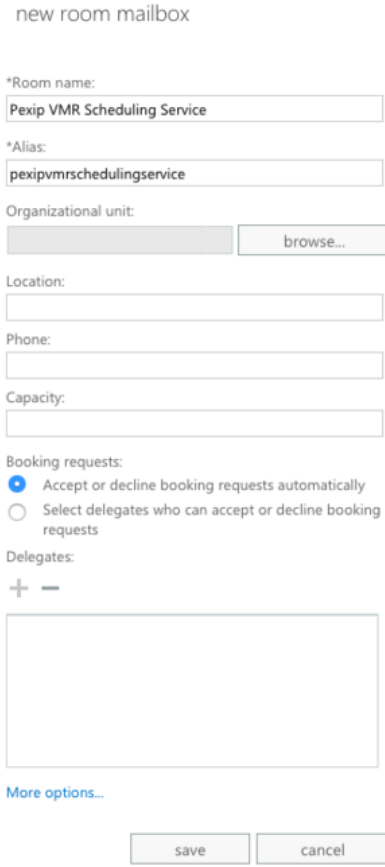
- i** An equipment resource can only be used by a single VMR scheduling for Exchange integration. If you have separate test and development environments, you must use a different resource for each.

The equipment resource will be added as a resource attendee to all VMR Scheduling for Exchange meetings. Users will see replies from this resource when it accepts or rejects a meeting request.

Each equipment resource can be used by only one VMR scheduling for Exchange integration.

- i** Previously we recommended using a room resource, but this may cause issues if users are using the Room Finder tool. For this reason, we now recommend using an equipment resource.

You can create an equipment resource using either EAC or PowerShell, as follows:

EAC	PowerShell
<ol style="list-style-type: none"> 1. Log in to your Exchange Admin Center. 2. Go to recipients > resources. 3. Select the + icon and then Equipment mailbox 4. Give the equipment resource a name and alias. <p>The equipment name will appear as the location of any meeting requests, and as a recipient.</p>  <ol style="list-style-type: none"> 5. Select Save. 	<p>This command creates an equipment resource with the specified Name, Alias and Display Name. Name and Display Name should be the same, and will appear as the location of any meeting requests, and as a recipient. The Alias (also known as the mail nickname) will be used as the email address.</p> <pre>New-Mailbox -Equipment -Name "<Equipment Name>" -Alias "<Equipment Alias>" -DisplayName "<Equipment Name>"</pre> <p>For example:</p> <pre>New-Mailbox -Equipment -Name "Pexip Meeting" -Alias pexipmeeting -DisplayName "Pexip Meeting"</pre>

Configuring the equipment resource

In this step you disable automatic processing for the equipment resource, so that the processing can be done by the scheduling service. You must also configure it to permit conflicts, because meetings may be scheduled at the same time by different users.

This configuration is done using the following PowerShell command:

```
Set-CalendarProcessing -Identity "<email_of_equipment_resource>" -AutomateProcessing None -AllowConflicts $true -BookingWindowInDays 1080 -MaximumDurationInMinutes 0 -AllowRecurringMeetings $true -EnforceSchedulingHorizon $false -ScheduleOnlyDuringWorkHours $false -ConflictPercentageAllowed 100 -MaximumConflictInstances 2147483647
```

To verify that the above command has configured everything correctly, use the PowerShell command:

```
Get-CalendarProcessing -Identity "<email_of_equipment_resource>" | Format-List
```

The output should look something like this:


```
[PS] C:\Windows\system32>Get-CalendarProcessing -Identity pexipvmrschedulingservice@rd.pexip.com | Format-List

RunspaceId           : 439dc5ce-7895-4341-ad2e-8182741cd596
AutomateProcessing    : None
AllowConflicts        : True
BookingWindowInDays   : 1000
MaximumDurationInMinutes : 0
AllowRecurringMeetings : True
EnforceSchedulingHorizon : False
ScheduleOnlyDuringWorkHours : False
ConflictPercentageAllowed : 100
MaximumConflictInstances : 2147483647
ForwardRequestsToDelegates : True
DeleteAttachments     : True
DeleteComments        : True
RemovePrivateProperty : True
DeleteSubject         : True
AddOrganizerToSubject : True
DeleteNonCalendarItems : True
TentativePendingApproval : True
EnableResponseDetails : True
OrganizerInfo         : True
ResourceDelegates     : {}
RequestOutOfPolicy     : {}
AllRequestOutOfPolicy : False
BookInPolicy          : {}
AllBookInPolicy       : True
RequestInPolicy        : {}
AllRequestInPolicy     : False
AddAdditionalResponse  : False
AdditionalResponse     : 
RemoveOldMeetingMessages : True
AddNewRequestsTentatively : True
ProcessExternalMeetingMessages : False
RemoveForwardedMeetingNotifications : False
MailboxOwnerId        : rd.pexip.com/Users/Pexip VMR Scheduling Service
Identity              : rd.pexip.com/Users/Pexip VMR Scheduling Service
IsValid               : True
ObjectState           : Changed

[PS] C:\Windows\system32>_
```

For more information on these commands, see Microsoft help:

- Set-CalendarProcessing command: [https://technet.microsoft.com/en-us/library/dd335046\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd335046(v=exchg.160).aspx)
- Get-CalendarProcessing command: [https://technet.microsoft.com/en-us/library/dd298137\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd298137(v=exchg.160).aspx)

Enabling authentication

In this step you enable your Exchange on-premises deployment to support your chosen authentication method for the service account. VMR Scheduling for Exchange uses basic authentication by default, but you can [elect to use NTLMv2 authentication](#) instead.

For both forms of authentication, Pexip Infinity stores the credentials in encrypted form and all authentication is carried out over a secure TLS channel.

NTLMv2 authentication

In most on-premises Exchange deployments, NTLMv2 authentication is enabled by default. To confirm that it has been enabled in your environment:

1. Open Server Manager and select the server on which Exchange is installed.
2. From the top right options select Tools > Local Security Policy.
3. On the tree on the left, expand Local Policies then select Security Options.
4. Scroll down to Network security: Restrict NTLM: Incoming NTLM traffic.
5. Ensure this is either left to the default value of *Not Defined*, or set to *Allow All*.

Basic authentication

If you are using basic authentication with on-prem Exchange you need to ensure it is enabled for Exchange Web Services (EWS).

You can do this using **either** Windows Service Manager or PowerShell, as follows:

Windows Service Manager	PowerShell
<ol style="list-style-type: none">1. Go to the Windows server on which Exchange is installed and open the Service Manager.2. Select the server on which Exchange is installed, and right-click to select Computer Management.3. From the panel on the left, select Services and Applications > Internet Information Services (IIS) Manager.4. Expand the options and select Sites > Default Web Site > EWS.5. Select the Authentication button in the main pane.6. Find Basic Authentication in the list and ensure it is <i>Enabled</i>. (If not, right-click and select <i>Enable</i>.)7. Select Save.	<p>This command enables basic authentication for EWS on a specific server:</p> <pre>Set-WebServicesVirtualDirectory -Identity "<server>\EWS (Default Web Site)" -BasicAuthentication \$true</pre> <p>For example, if your server name is PEXCHANGE then:</p> <pre>Set-WebServicesVirtualDirectory -Identity "PEXCHANGE\EWS (Default Web Site)" -BasicAuthentication \$true</pre>

Viewing the equipment resource's mailbox


There may be occasions, such as when troubleshooting, that you want to view the equipment resource's mailbox or calendar. To do this, you first need to assign full access to the equipment resource's mailbox to a delegate account, and then view the mailbox or calendar using the delegate account. (The delegate account could be the service account, or it could be, for example, an administrator's account.)

Next steps

1. [Configuring Pexip Infinity](#) to integrate with your Microsoft Exchange deployment and create the VMR Scheduling for Exchange add-in.
2. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

Configuring Office 365 for scheduling

To enable users to schedule meetings in single-use VMRs in an Office 365 environment, you must first configure Office 365 appropriately. The steps are as follows, described in more detail in the sections that follow:

1. [Creating a service account](#). The Pexip Infinity VMR Scheduling for Exchange feature uses a unique service account to log into Exchange.
 -  This should be a different service account to any used for One-Touch Join, because the configuration will be different.
2. [Configuring Application Impersonation on the service account](#). This allows the service account to impersonate users on Exchange.
3. [Create an equipment resource](#). This resource will be added as an attendee to all meetings scheduled using the Pexip add-in.
4. [Configure the equipment resource](#).
5. [Enable OAuth authentication](#) for the service account.

PowerShell commands are provided for all steps; parameters to be replaced with your own relevant information are shown in the format **<your info here>**.

Prerequisites

Before you start, ensure you can access your Office 365 Admin Center: <https://portal.office.com/adminportal/home#/homepage>.

You will also need to have a remote PowerShell session to your Exchange server. See these Microsoft articles about connecting to [Exchange online](#) and [Microsoft 365](#) with PowerShell for more information.

Note that for Office 365, the service account must have a mailbox license and appropriate licenses to allow it to connect to Exchange and use EWS.




Creating a service account

In this step, you create the service account to be used by VMR Scheduling for Exchange.

The VMR Scheduling for Exchange feature uses a service account to log into Exchange. You can use an existing service account (the same service account can be used by more than one VMR scheduling for Exchange integration), or create a new account.

You need to provide the authentication credentials of this service account when configuring Pexip Infinity to integrate with a Microsoft Exchange deployment.

After creating the service account, you must ensure that it is assigned an appropriate Exchange license, such as Office 365 Enterprise E1, Office 365 Business Basic (formerly Essentials) or one of the Exchange Online plans.

-  A single service account can be used by more than one VMR scheduling for Exchange integration.
-  Changes to the service account may take some time to take effect, depending on the cache lifetime configured on the Microsoft Exchange server.
-  If the service account is subject to a password rotation policy or uses multi-factor authentication (MFA), then each time the password changes or the MFA is refreshed, you must [sign in to the service account again](#) via the Pexip Infinity Administrator interface.

You can create a new service account using either the Office 365 admin portal or PowerShell, as follows:

O365

1. Go to portal.office.com and log in as the administrator.
2. Go to the admin portal by selecting the Admin tile (this takes you to <https://portal.office.com/adminportal/home#/homepage>).
3. From the Users section, select **Add** a user and complete the necessary fields:
 - a. In the Password section:
 - Select **Let me create the password**.
 - Uncheck **Make this user change their password when they first sign in**.
 - b. In the Product licenses section, assign an appropriate product license from the available list.

4. Select **Add** to create the user.

PowerShell

You must run Powershell as administrator.

Establishing a remote connection

To use PowerShell for Office 365 you first need to connect remotely. These commands install the required PowerShell modules (if they are not already installed) and then connects to Exchange Online:

```
#If not installed, install Exchange Online Module
Install-Module ExchangeOnlineManagement

#If not installed, install Azure AD Module
Install-Module -Name AzureAD

#Connect to Exchange Online and AzureAD, works also with a MFA
enabled account
Connect-ExchangeOnline
```

Creating the service account

The first command lets the administrator type in a password for the service account as a secure string. This password variable is then used in the second command to create a mailbox for the service account. The remaining commands log you into Azure AD and then set the password of the service account to never expire.

```
#Capture password for service account
$password = Read-Host "Enter password" -AsSecureString

# Create service account and mailbox
New-Mailbox -Name "<Account Name>" -MicrosoftOnlineServicesID
"<UPN>" -Password $password -Alias "<Account Alias>" -FirstName
"<Account First Name>" -LastName "<Account Last Name>" -DisplayName
"<Account Name>"

#Connect to AzureAD
Connect-AzureAD

#Set password policy
Set-AzureADUser -ObjectId "<UPN>" -PasswordPolicies
DisablePasswordExpiration
```

Example New-Mailbox command:

```
New-Mailbox -Name "Service Account" -MicrosoftOnlineServicesID
pexip@example.com -Password $password -Alias pexip -FirstName
Service -LastName Account -DisplayName "Service Account"
```

Example Set-AzureADUser command:

```
Set-AzureADUser -ObjectId pexip@example.com -PasswordPolicies
DisablePasswordExpiration
```

Assigning a license to the service account

You must now assign an appropriate license to the service account.

See <https://docs.microsoft.com/en-us/powershell/azure/active-directory/enabling-licenses-sample> for information on how to do this.

Configuring Application Impersonation on the service account

In this step you configure the service account with a Role of Application Impersonation, which allows the service account to impersonate users on Exchange.

The service account must be configured with a **Role of Application Impersonation**. This allows the service account to impersonate all users who will be using VMR Scheduling for Exchange, and to impersonate the equipment resource that is to be used for the scheduling service. For more information, see [Using application impersonation](#).

The VMR Scheduling for Exchange service impersonates users when sending email updates containing joining instructions (in cases where these instructions could not be added at the time of scheduling). This makes it appear to the recipients that the joining instructions were sent from the meeting organizer, instead of the service account.

To check if your service account has Application Impersonation already configured, use the PowerShell command:

```
Get-ManagementRoleAssignment -RoleAssignee "<email_of_service_account>" -Role ApplicationImpersonation | Format-List
```

Below is an example of the output of the command when the service account already has Application Impersonation configured:

```
PS C:\WINDOWS\system32> Get-ManagementRoleAssignment -RoleAssignee pexip@pexip1.onmicrosoft.com -Role ApplicationImpersonation | Format-List

RunspaceId           : bb53f66c-015d-414a-a11f-057381dd8398
DataObject            : PexipSchedulingService
User                  : pexip
AssignmentMethod       : Direct
Identity              : PexipSchedulingService
EffectiveUserName      : pexip
AssignmentChain        :
RoleAssigneeType       : User
RoleAssignee           : pexip
Role                   : ApplicationImpersonation
RoleAssignmentDelegationType : Regular
CustomRecipientWriteScope :
CustomConfigWriteScope :
RecipientReadScope     : Organization
ConfigReadScope        : None
RecipientWriteScope     : Organization
ConfigWriteScope        : None
Enabled                : True
RoleAssigneeName       : pexip
IsValid                : True
ExchangeVersion        : 0.11 (14.0.550.0)
Name                   : PexipSchedulingService
DistinguishedName       : CN=PexipSchedulingService,CN=Role Assignments,CN=RBAC,CN=Configuration,CN=pexip1.onmicro
                        : soft.com,CN=ConfigurationUnits,DC=GBRP123A001,DC=PROD,DC=OUTLOOK,DC=COM
Guid                   : 08ae2550-f870-4f6f-9cb2-fb9e5309cd50
ObjectCategory         : GBRP123A001.PROD.OUTLOOK.COM/Configuration/Schema/ms-Exch-Role-Assignment
ObjectClass             : {top, msExchRoleAssignment}
WhenChanged            : 14/08/2017 12:15:32
WhenCreated            : 14/08/2017 12:15:32
WhenChangedUTC         : 14/08/2017 11:15:32
WhenCreatedUTC         : 14/08/2017 11:15:32
OrganizationId         : GBRP123A001.PROD.OUTLOOK.COM/Microsoft Exchange Hosted
                        : Organizations/pexip1.onmicrosoft.com -
                        : GBRP123A001.PROD.OUTLOOK.COM/ConfigurationUnits/pexip1.onmicrosoft.com/Configuration
Id                      : PexipSchedulingService
OriginatingServer       : LOXP123A001DC01.GBRP123A001.PROD.OUTLOOK.COM
ObjectState            : Unchanged

PS C:\WINDOWS\system32>
```

If the service account does not have Application Impersonation configured, then the above command will not return anything at all. If this is the case, enable Application Impersonation as follows:

```
New-ManagementRoleAssignment -name "<role_name>" -Role:ApplicationImpersonation -User:"<email_of_service_account>"
```

For example:

```
New-ManagementRoleAssignment -name:PexipSchedulingService -Role:ApplicationImpersonation -User:pexip@exchange.example.com
```

This will enable the service account to impersonate all users in the organization.

For more information on these commands, see Microsoft help:

- Configuring Application Impersonation: <https://msdn.microsoft.com/en-us/library/office/dn722376%28v=exchg.150%29.aspx>
- Get-ManagementRoleAssignment command: [https://technet.microsoft.com/en-us/library/dd351024\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd351024(v=exchg.150).aspx)
- New-ManagementRoleAssignment command: [https://technet.microsoft.com/en-us/library/dd335193\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335193(v=exchg.150).aspx)
- Set-ManagementRoleAssignment command (used if you need to edit the role assignment): [https://technet.microsoft.com/en-us/library/dd335173\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/dd335173(v=exchg.150).aspx)

Creating an equipment resource

In this step you create an equipment resource to be used by VMR Scheduling for Exchange. This resource is added as an attendee to all meetings scheduled using the Pexip add-in. The scheduling service monitors the equipment resource's mailbox, processes all meeting

requests sent to it, and schedules the meetings as appropriate.

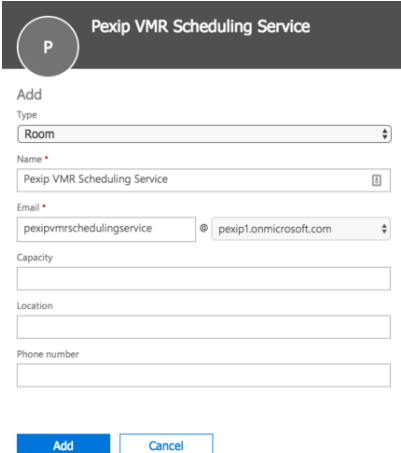
- i** An equipment resource can only be used by a single VMR scheduling for Exchange integration. If you have separate test and development environments, you must use a different resource for each.

The equipment resource will be added as a resource attendee to all VMR Scheduling for Exchange meetings. Users will see replies from this resource when it accepts or rejects a meeting request.

Each equipment resource can be used by only one VMR scheduling for Exchange integration.

- i** Previously we recommended using a room resource, but this may cause issues if users are using the Room Finder tool. For this reason, we now recommend using an equipment resource.

You can create an equipment resource using either the Office 365 admin portal or PowerShell, as follows:

O365	PowerShell
<p>To create the equipment resource via the Office 365 admin portal:</p> <ol style="list-style-type: none"> Go to portal.office.com and log in as the administrator. From the left-hand menu, select Resources > Rooms & Equipment and then Add. Select a Type of <i>Equipment</i>. Assign an appropriate Name and Email address and select Add. The equipment name will appear as the location of any meeting requests, and as a recipient. 	<p>This command creates an equipment resource with the specified Name, Alias and Display Name. Name and Display Name should be the same, and will appear as the location of any meeting requests, and as a recipient. The Alias (also known as the mail nickname) will be used as the email address.</p> <pre>New-Mailbox -Equipment -Name "<Equipment Name>" -Alias "<Equipment Alias>" -DisplayName "<Equipment Name>"</pre> <p>For example:</p> <pre>New-Mailbox -Equipment -Name "Pexip Meeting" -Alias pexipmeeting -DisplayName "Pexip Meeting"</pre>

The equipment resource should now appear in the list of resources.

Configuring the equipment resource

In this step you disable automatic processing for the equipment resource, so that the processing can be done by the scheduling service. You must also configure it to permit conflicts, because meetings may be scheduled at the same time by different users.

This configuration is done using the following PowerShell command:

```
Set-CalendarProcessing -Identity "<email_of_equipment_resource>" -AutomateProcessing None -AllowConflicts $true -BookingWindowInDays 1080 -MaximumDurationInMinutes 0 -AllowRecurringMeetings $true -EnforceSchedulingHorizon $false -ScheduleOnlyDuringWorkHours $false -ConflictPercentageAllowed 100 -MaximumConflictInstances 2147483647
```

To verify that the above command has configured everything correctly, use the PowerShell command:

```
Get-CalendarProcessing -Identity "<email_of_equipment_resource>" | Format-List
```

The output should look something like this:

```

PS C:\WINDOWS\system32> Get-CalendarProcessing -Identity pexipvmrschedulingservice@pexip1.onmicrosoft.com | Format-List

RunspaceId                : bb53f66c-015d-414a-a11f-057381dd8398
AutomateProcessing         : None
AllowConflicts             : True
BookingWindowInDays        : 1080
MaximumDurationInMinutes   : 0
AllowRecurringMeetings     : True
EnforceSchedulingHorizon   : False
ScheduleOnlyDuringWorkHours : False
ConflictPercentageAllowed   : 100
MaximumConflictInstances    : 2147483647
ForwardRequestsToDelegates : True
DeleteAttachments          : True
DeleteComments             : True
RemovePrivateProperty      : True
DeleteSubject              : True
AddOrganizerToSubject      : True
DeleteNonCalendarItems     : True
TentativePendingApproval   : True
EnableResponseDetails      : True
OrganizerInfo              : True
ResourceDelegates          : {}
RequestOutOfPolicy         : {}
AllRequestOutOfPolicy      : False
BookInPolicy               : {}
AllBookInPolicy            : True
RequestInPolicy            : {}
AllRequestInPolicy         : False
AddAdditionalResponse       : False
AdditionalResponse         :
RemoveOldMeetingMessages   : True
AddNewRequestsTentatively  : True
ProcessExternalMeetingMessages : False
RemoveForwardedMeetingNotifications : False
MailboxOwnerId             : Pexip VMR Scheduling Service
Identity                   : Pexip VMR Scheduling Service
IsValid                    : True
ObjectState                 : Changed

PS C:\WINDOWS\system32>

```

For more information on these commands, see Microsoft help:

- Set-CalendarProcessing command: [https://technet.microsoft.com/en-us/library/dd335046\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd335046(v=exchg.160).aspx)
- Get-CalendarProcessing command: [https://technet.microsoft.com/en-us/library/dd298137\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/dd298137(v=exchg.160).aspx)

Enabling OAuth authentication

In this step you enable OAuth authentication for the service account.

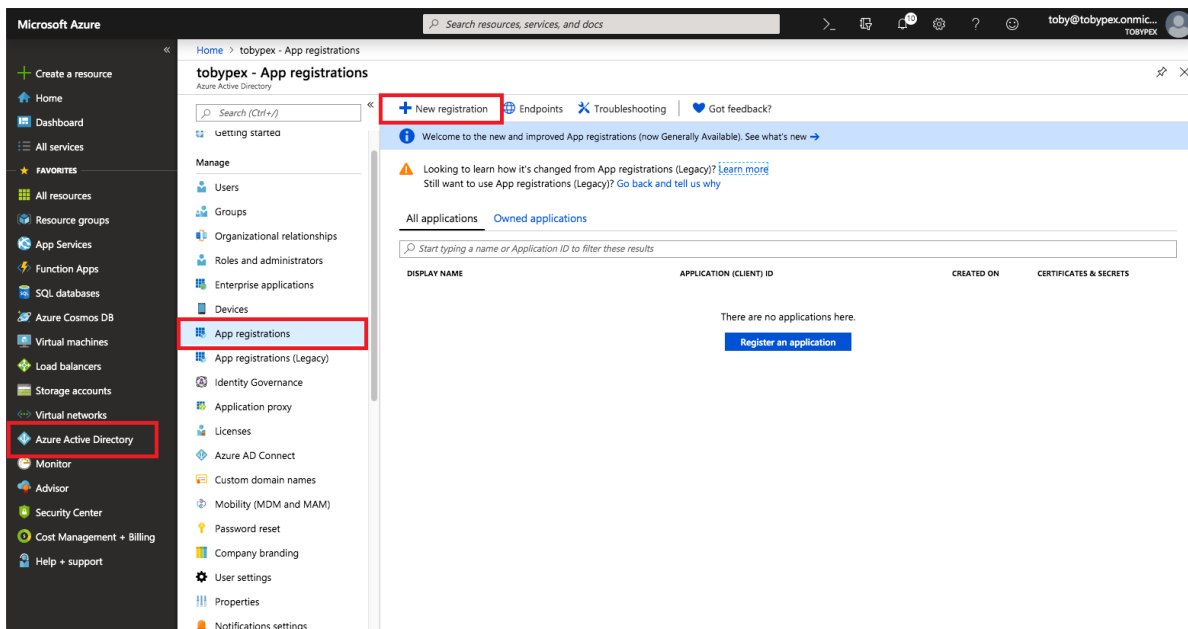
VMR Scheduling for Exchange uses a service account to log in to Exchange.

As of October 2022, Microsoft will stop supporting and fully decommission basic authentication for EWS to access Exchange Online (for more information, see [Microsoft's announcement](#)). We therefore strongly recommend that for Office 365, all new deployments authenticate the service account using OAuth 2.0, and all existing deployments are updated to enable this option as soon as possible.

To use OAuth for the service account, you must create an app registration in Azure and then use the settings from this app registration when enabling and configuring the OAuth options within the VMR scheduling for Exchange integration.

Create a new App Registration in Azure

1. Log into the Azure portal at aad.portal.azure.com.
2. From the main panel on the left, select **Azure Active Directory**.
3. Select **App Registrations** and then **New registration**:



4. In the Register an application panel, enter the following options:
 - a. **Name:** this can be anything you wish. In our example we have used *Pexip Scheduling App*.
 - b. **Supported account types:** select *Accounts in this organizational directory only*.
 - c. **Redirect URI:** from the drop-down menu, select *Public client/native (mobile and desktop)*. The URI must use the IP address or FQDN of the Management Node, in the format
https://<Management Node Address>/admin/platform/msexchangeconnector/oauth_redirect/
 In our example we have used **https://infinity.example.com/admin/platform/msexchangeconnector/oauth_redirect/**
 You will need to enter this as the **OAuth redirect URI** when configuring a VMR scheduling for Exchange integration.

i The **OAuth redirect URI** is the page on the Administrator interface to which the Pexip Infinity administrator will be returned after they have successfully **signed in to the service account**. Because it is a page on the Management Node, this URI is internal to your deployment and only needs to be accessible from the administrator's web browser; you do not need to make it externally accessible. This URI must be the same on Azure and Pexip Infinity in order for Azure to validate the sign-in request.

Home > [tobypex - App registrations](#) > Register an application

Register an application

*** Name**
The user-facing display name for this application (this can be changed later).
 ✓

Supported account types
Who can use this application or access this API?
☒ Accounts in this organizational directory only (tobypex)
☐ Accounts in any organizational directory
☐ Accounts in any organizational directory and personal Microsoft accounts (e.g. Skype, Xbox, Outlook.com)
[Help me choose...](#)

Redirect URI (optional)
We'll return the authentication response to this URI after successfully authenticating the user. Providing this now is optional and it can be changed later, but a value is required for most authentication scenarios.

✓

By proceeding, you agree to the [Microsoft Platform Policies](#) [\[?\]](#)

Register

5. Select **Register**.
A new panel will open where you can configure your application.
6. From the panel on the left, select **API permissions**.
7. Select **Add a permission**.
8. From the **Request API permissions** panel, select **APIs my organization uses**, search for **Office 365 Exchange Online** and select it:

Request API permissions



Select an API

Microsoft APIs

APIs my organization uses

My APIs

Apps in your directory that expose APIs are shown below

<input type="text" value="office"/>	
Name	Application (client) ID
Office 365 Exchange Online	00000002-0000-0ff1-ce00-000000000000
Office 365 Information Protection	2f3f02c9-5679-4a5c-a605-0de55b07d135
Office 365 Management APIs	c5393580-f805-4401-95e8-94b7a6ef2fc2
Office 365 Search Service	66a88757-258c-4c72-893c-3e8bed4d6899
Office 365 SharePoint Online	00000003-0000-0ff1-ce00-000000000000
Office Agent Service	5225545c-3ebd-400f-b668-c8d78550d776
Office Delve	94c63fef-13a3-47bc-8074-75af8c65887a
Office Hive	166f1b03-5b19-416f-a94b-1d7aa2d247dc
Office Personal Assistant at Work Service	28ec9756-deaf-48b2-84d5-a623b99af263
Office Scripts Service	62fd1447-0ef3-4ab7-a956-7dd05232ecc1
Office Shredding Service	b97b6bd4-a49f-4a0c-af18-af507d1da76c
Office365 Zoom	0d38933a-0bbd-41ca-9ebd-28c4b5ba7cb7
OfficeServicesManager	9e4a5442-a5c9-4f6f-b03f-5b9fcaaf24b1

9. Select **Delegated permissions**, and from the **Select permissions** list, expand **EWS** and select **Access mailboxes** as the signed-in user via **Exchange Web Services**, and then select **Add permissions**:

Request API permissions



[← All APIs](#)



Office 365 Exchange Online

<https://outlook-tdf-2.office.com/>

What type of permissions does your application require?

Delegated permissions

Your application needs to access the API as the signed-in user.

Application permissions

Your application runs as a background service or daemon without a signed-in user.

Select permissions

[expand all](#)

Permission	Admin consent required
> Calendars	
> Contacts	
> EAS	
<div> <div> <div>✓</div> <div>EWS (1)</div> </div> <div> <div><input checked="" type="checkbox"/></div> <div> EWS.AccessAsUser.All ⓘ Access mailboxes as the signed-in user via Exchange Web Services </div> </div> </div>	
> Exchange	

Add permissions

Discard

Taking note of configuration

When you [Configure the VMR scheduling for Exchange integration](#) and enable OAuth authentication for the service account, you'll need to provide the following information from Azure:

- **Application (client) ID:** this was generated for you by Azure when you saved the App Registration:

Home > Pexip - App registrations > Toby Pexip Dev Scheduling

Toby Pexip Dev Scheduling

Overview

Quickstart

Manage

Branding

Authentication

Certificates & secrets

API permissions

Delete

Endpoints

Display name

Toby Pexip Dev Scheduling

Application (client) ID

95ba451d-1811-4104-81c8-b49e3174cbad

Directory (tenant) ID

388db7c4-d9d0-45b4-8519-468dadcbbf0d

Object ID

88774a26-6a84-4a54-a859-269c6e89733d

Supported account types

My organization only

Redirect URIs

0 web, 1 public client

Managed application in local directory

Toby Pexip Dev Scheduling

- You can find this again in Azure under **Azure Active Directory > App Registrations**, under the **Application (client) ID** column. You will need to enter this as the **OAuth client ID** when configuring the VMR scheduling for Exchange integration.

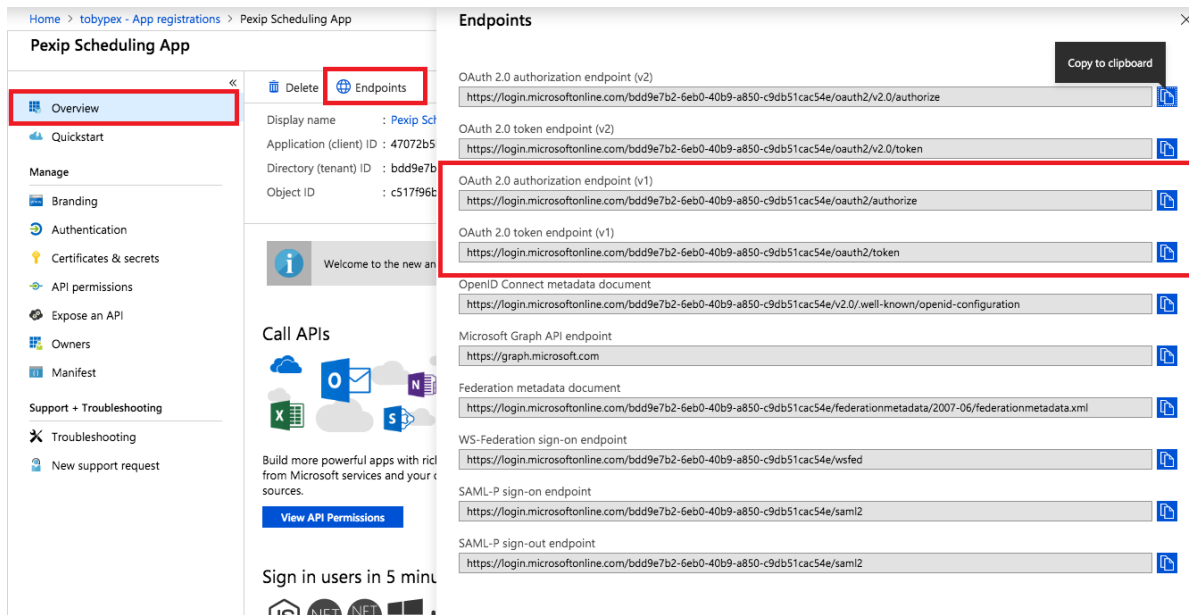
- **Redirect URI:** this is the URI you entered when creating the App Registration.

- i** You can find this again in Azure under **Azure Active Directory > App Registrations**, clicking on the app registration, and then clicking **Redirect URIs**.

You will need to enter this as the **OAuth redirect URI** when configuring the VMR scheduling for Exchange integration.

You will also need to know the OAuth Endpoints to use. To find this information:

1. In the Azure Portal, select **Overview > Endpoints**.
2. Copy the URL of the **OAuth 2.0 authorization endpoint (v1)**.
 - i** Ensure that you use the URL for **... endpoint (v1)**, not **... endpoint (v2)**.You will need to enter this as the **OAuth authorization endpoint** when configuring the VMR scheduling for Exchange integration.
3. Copy the URL of the **OAuth 2.0 token endpoint (v1)**
 - i** Ensure that you use the URL for **... endpoint (v1)**, not **... endpoint (v2)**.You will need to enter this as the **OAuth token endpoint** when configuring the VMR scheduling for Exchange integration.



Viewing the equipment resource's mailbox

There may be occasions, such as when troubleshooting, that you want to view the equipment resource's mailbox or calendar. To do this, you first need to assign full access to the equipment resource's mailbox to a delegate account, and then view the mailbox or calendar using the delegate account. (The delegate account could be the service account, or it could be, for example, an administrator's account.)

Next steps

1. [Configuring Pexip Infinity](#) to integrate with your Microsoft Exchange deployment and create the VMR Scheduling for Exchange add-in.
2. [Making the add-in available to users](#) within your Microsoft Exchange deployment.

Configuring Pexip Infinity for VMR Scheduling for Exchange

Users can host their meeting in a [single-use VMR](#) that is created specifically for the meeting and only available for its duration, or they can host their meeting in their own [personal VMR](#). You can either let users decide which type of VMR to use for each meeting, or make just one type of VMR available in your deployment.

Prerequisites

- If you wish to enable single-use VMRs in your VMR Scheduling for Exchange deployment, you must first complete the steps in either [Configuring Exchange on-premises for scheduling](#) (for Exchange on-premises environments), or [Configuring Office 365 for scheduling](#) (for Office 365 environments).
- If you wish to enable personal VMRs in your VMR Scheduling for Exchange deployment, you must first complete the steps in either [Configuring AD FS SSO for personal VMRs](#) or [Configuring Azure SSO for personal VMRs](#).

Adding a VMR scheduling for Exchange integration to Pexip Infinity






A VMR scheduling for Exchange integration defines a specific connection between your Pexip Infinity deployment and a Microsoft Exchange deployment. In some cases a single Pexip Infinity deployment will require [more than one VMR scheduling for Exchange integration](#).


Adding a new VMR scheduling for Exchange integration involves the following steps:

- deciding whether VMRs used by the VMR Scheduling for Exchange service will be the users' personal VMR(s), single-use (dynamic) VMRs, or both
- (for single-use VMRs) adding details of your Microsoft Exchange deployment and accounts, defining how the single-use VMRs will be configured, and configuring the template to be used for joining instructions
- (for personal VMRs) adding details of your authentication provider (ADFS or Azure), and defining how the join instructions and meeting location will be generated from the existing personal VMR details
- configuring the wording to be used by the add-in.

From the Pexip Infinity Management Node go to **System > VMR Scheduling For Exchange** and complete the following fields:


Option	Description	Notes
Name	The name used to refer to this VMR scheduling for Exchange integration.	
Description	An optional description of this VMR scheduling for Exchange integration.	
Enable single-use VMRs	Enable this option to allow Outlook users to schedule meetings in single-use (randomly generated) VMRs.	
Enable personal VMRs	Enable this option to allow Outlook users to schedule meetings in their personal VMRs.	
Exchange server information (available and required when single-use VMRs are enabled)		
EWS URL	The URL used to connect to Exchange Web Services (EWS) on the Microsoft Exchange server. <ul style="list-style-type: none"> • For Office 365 deployments this will be https://outlook.office365.com/EWS/Exchange.asmx • For Exchange on-prem this will usually be <a href="https://<exchange_server>/EWS/Exchange.asmx">https://<exchange_server>/EWS/Exchange.asmx <ul style="list-style-type: none"> ◦ If you have multiple Exchange servers in your deployment, this can be the URL of EWS on any one of the servers. ◦ If you are using a load balancer, this can use the FQDN of the load balancer within the URL (e.g. <a href="https://<load_balancer>/EWS/Exchange.asmx">https://<load_balancer>/EWS/Exchange.asmx). 	

Option	Description	Notes
Service account username †	<p>The username of the service account to be used by this VMR scheduling for Exchange integration.</p> <p>This is the username you assigned when Creating a service account for Exchange on-premises or Creating a service account for O365.</p> <ul style="list-style-type: none"> For Office365 deployments, the format is usually <code>name@domain</code>. If you are using NTLMv2, this must be in the format <code>name@domain</code>. For other on-premises deployments, the format may be either <code>domain\name</code> or <code>name@domain</code>, depending on your domain. <p> A single service account can be used by more than one VMR scheduling for Exchange integration.</p>	
Enable OAuth **	<p>Enable this option to authenticate the service account using OAuth 2.0. This option is only supported for Exchange in Office 365. Leave this option disabled to continue using basic authentication. If you select this option, you must sign in to the service account after completing and saving your configuration.</p> <p> As of October 2022, Microsoft will stop supporting and fully decommission basic authentication for EWS to access Exchange Online (for more information, see Microsoft's announcement). We therefore strongly recommend that for Office 365, all new deployments authenticate the service account using OAuth 2.0, and all existing deployments are updated to enable this option as soon as possible.</p>	
Enable NTLM authentication	<p>Enable this option to authenticate the service account using NTLMv2. This option is only supported for Exchange on-premises. Leave this option disabled to continue using basic authentication.</p>	
OAuth client ID †	<p>(Available if OAuth for the service account has been enabled)</p> <p>Enter the Application (client) ID that was generated for you by Azure when you saved the App Registration (see Taking note of configuration).</p>	
OAuth redirect URI	<p>(Available if OAuth for the service account has been enabled)</p> <p>Enter the Redirect URI that you used when Enabling OAuth authentication for Office 365.</p> <p>This must be in the format <code>https://<Management Node Address>/admin/platform/msexchangeconnector/oauth_redirect/</code>.</p> <p> The OAuth redirect URI is the page on the Administrator interface to which the Pexip Infinity administrator will be returned after they have successfully signed in to the service account. Because it is a page on the Management Node, this URI is internal to your deployment and only needs to be accessible from the administrator's web browser; you do not need to make it externally accessible. This URI must be the same on Azure and Pexip Infinity in order for Azure to validate the sign-in request.</p>	
OAuth authorization endpoint	<p>(Available if OAuth for the service account has been enabled)</p> <p>Enter the URL of the OAuth 2.0 authorization endpoint (v1) (see Taking note of configuration).</p> <p> Ensure that you use the URL for ... endpoint (v1), not ... endpoint (v2).</p>	
OAuth token endpoint †	<p>(Available if OAuth for the service account has been enabled)</p> <p>URL of the OAuth 2.0 token endpoint (v1) (see Taking note of configuration).</p> <p> Ensure that you use the URL for ... endpoint (v1), not ... endpoint (v2).</p>	

Option	Description	Notes
Service account password	<p>(Available if OAuth for the service account has not been enabled)</p> <p>The password of the service account to be used by this VMR scheduling for Exchange integration.</p> <p>This is the password you assigned when Creating a service account.</p>	
Mailbox name	<p>The name of the equipment resource that is to be used by this VMR scheduling for Exchange integration.</p> <p>This is the name you assigned when Creating an equipment resource in Exchange on-premises or Creating an equipment resource in O365.</p> <p> An equipment mailbox must only be used by a single VMR scheduling for Exchange integration.</p>	
Mailbox email address	<p>The email address of the equipment resource that is to be used by this VMR scheduling for Exchange integration.</p> <p>This is the email address you assigned when Creating an equipment resource in Exchange on-premises or Creating an equipment resource in O365.</p>	
Single-use VMR configuration (available and required when single-use VMRs are enabled)		
Conference name template	<p>A jinja2 template that is used to generate the name of scheduled conferences. The name is used by the Management Node to identify the conference, and may also appear to conference participants (depending on the endpoint being used).</p> <p>Note that conference names must be unique, so a random number may be appended if the name that is generated is already in use by another service (Virtual Meeting Room, Virtual Auditorium, Virtual Reception, scheduled conference, Media Playback Service, or Test Call Service).</p> <p>Default: <code>{{subject}} {{organizer_name}}</code></p>	<p>Accepted variables:</p> <ul style="list-style-type: none"> • subject • organizer_email • organizer_name • alias • numeric_alias
Conference description template	<p>A jinja2 template that is used to generate the description of scheduled conferences.</p> <p>Default: <i>Scheduled Conference booked by {{organizer_email}}</i></p>	<p>Accepted variables:</p> <ul style="list-style-type: none"> • subject • organizer_email • organizer_name • alias • numeric_alias
Conference subject template	<p>A jinja2 template that is used to generate the subject field of scheduled conferences. This will be shown on the Management Node when viewing information about the conference, and by default will use the subject line of the meeting invitation so the default should be deleted or amended if you do not want administrators to be able to view the meeting subject.</p> <p>Default: <code>{{subject}}</code></p>	<p>Accepted variables:</p> <ul style="list-style-type: none"> • subject • organizer_email • organizer_name • alias • numeric_alias
Scheduled alias prefix	<p>The prefix to use when generating aliases for scheduled conferences.</p> <p>Note: this must be between 1 and 8 characters long.</p>	

Option	Description	Notes
Scheduled alias suffix length	<p>The length of the random number suffix part of aliases generated for scheduled conferences.</p> <p>This must be a number between 6 and 15.</p> <p>Default: 6.</p>	
Scheduled alias domain	The domain to use when generating aliases for scheduled conferences.	
Identity Provider group	<p>The set of Identity Providers used to authenticate participants attempting to join scheduled conferences. If this is blank, participants will not be required to authenticate.</p> <p>For more information, see About participant authentication.</p>	
Other participants	<p>(Available when an Identity Provider Group has been selected)</p> <p>Determines whether participants joining a SSO-protected service from devices other than the Connect web app (for example SIP or H.323 endpoints) are allowed to dial in to the service.</p> <ul style="list-style-type: none"> Disallow all: these devices may not join the service. Allow if trusted: these devices may join the service if they are locally registered. They must still enter a Host PIN or Guest PIN if either is required. <p>Default: Disallow all</p>	
Join before buffer	<p>The number of minutes before the meeting's scheduled start time that participants will be able to join the VMR.</p> <p>Range: 0 to 180.</p> <p>Default: 30.</p>	
Join after buffer	<p>The number of minutes after the meeting's scheduled end time that participants will be able to join the VMR.</p> <p>Range: 0 to 180.</p> <p>Default: 60.</p>	
Scheduled conference theme	<p>The theme used by all conferences scheduled using the add-in. For more information, see Customizing images and voice prompts using themes.</p> <p>Default: <use Default theme> (the global default theme is used).</p>	
Personal VMR configuration (available and required when personal VMRs are enabled)		
Allow new users	<p>Enable this option to allow users who do not have an existing Pexip Infinity User record (Users & Devices > Users) to access the Outlook add-in. When these users sign in, Pexip Infinity will create a new user record for them.</p> <p>Disable this option to allow only those users with an existing User record to access the Outlook add-in.</p>	
Authentication provider	The method by which users will sign into the Outlook add-in.	

Option	Description	Notes
User OAuth authorization URI	<p>The authorization URI of the OAuth application used to authenticate users when signing in to the Outlook add-in.</p> <p>Azure</p> <p>This will be in the format <a href="https://login.microsoftonline.com/<UUID>/oauth2/v2.0/authorize">https://login.microsoftonline.com/<UUID>/oauth2/v2.0/authorize</p> <ul style="list-style-type: none"> To find this in Azure, see Taking note of configuration. <p>AD FS</p> <p>This will be in the format <a href="https://<Federation Service Name>/adfs/oauth2/authorize">https://<Federation Service Name>/adfs/oauth2/authorize</p> <ul style="list-style-type: none"> To find this in AD FS with Windows Server 2016 or later, see Determining Federation Service Properties To find this in AD FS with Windows Server 2012, see Determining Federation Service Properties 	
User OAuth token URI	<p>The token URI of the OAuth application used to authenticate users when signing in to the Outlook add-in.</p> <p>Azure</p> <p>This will be in the format <a href="https://login.microsoftonline.com/<UUID>/oauth2/v2.0/token">https://login.microsoftonline.com/<UUID>/oauth2/v2.0/token</p> <ul style="list-style-type: none"> To find this in Azure, see Taking note of configuration. <p>AD FS</p> <p>This will be in the format <a href="https://<Federation Service Name>/adfs/oauth2/token">https://<Federation Service Name>/adfs/oauth2/token</p> <ul style="list-style-type: none"> To find this in AD FS with Windows Server 2016 or later, see Determining Federation Service Properties To find this in AD FS with Windows Server 2012, see Determining Federation Service Properties 	
User OAuth client ID	<p>The client ID of the OAuth application used to authenticate users when signing in to the Outlook add-in.</p> <ul style="list-style-type: none"> To find this in Azure, see Taking note of configuration. To find this in AD FS with Windows Server 2016 or later, see Creating a Native Application For AD FS with Windows Server 2012, you can either use the default client ID shown here, or enter the one you generated earlier. For more information, see Adding the OAuth 2.0 Client to AD FS. 	
AD FS Resource Identifier	<p>(Applies when an Auth Provider of AD FS has been selected)</p> <p>The URL which identifies the OAuth 2.0 resource in AD FS.</p> <ul style="list-style-type: none"> For AD FS with Windows Server 2016 or later, this should be the identifier you gave when Creating a Web API Resource. For AD FS with Windows Server 2012, this should be the identifier you gave when Creating a Relying Party Trust. 	
Azure OAuth client secret	<p>(Applies when an Auth Provider of Azure has been selected)</p> <p>The client secret of the OAuth application used to authenticate users when signing in to the Outlook add-in.</p> <p>For more information, see Creating and configuring a new App Registration in Azure.</p>	

Option	Description	Notes
Personal VMR joining instructions template	<p>A jinja2 template that is used to generate the joining instructions that are added by VMR Scheduling for Exchange to the body of the meeting request when a personal VMR is being used.</p> <p> For more details on constructing the URLs used for joining from a web browser, see Creating preconfigured links to launch conferences via s.</p> <p>Default:</p> <pre>{% if domain_aliases %} {% set alias = domain_aliases[0] %} {% elif other_aliases %} {% set alias = other_aliases[0] %} {% else %} {% set alias = numeric_aliases[0] %} {% endif %} {% if (not allow_guests) and pin %} {% set meeting_pin = pin %} {% elif allow_guests and guest_pin %} {% set meeting_pin = guest_pin %} {% else %} {% set meeting_pin = "" %} {% endif %}
 <div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> Please join my Pexip Virtual Meeting Room in one of the following ways:

 From a VC endpoint or a Skype/Lync client:
 {{alias}}

 From a web browser:
 https://{{addin_server_domain}}/webapp/#/?conference={{alias}}

 From a Pexip Infinity Connect client:
 pexip://{{alias}}

 {% if numeric_aliases %} From a telephone:
 [Your number], then {{numeric_aliases[0]}} #


 {% endif %} {% if meeting_pin %} Please join using the PIN {{meeting_pin}}

 {% endif %} </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> aliases domain_aliases numeric_aliases other_aliases addin_server_domain name description service_type pin allow_guests guest_pin

Option	Description	Notes
Personal VMR location template	<p>A jinja2 template that is used to generate the text that will be inserted into the Location field of the meeting request when a personal VMR is being used. The output of this should be a single line of text.</p> <p>Default:</p> <pre>{% if domain_aliases %} {% set alias = domain_aliases[0] %} {% elif other_aliases %} {% set alias = other_aliases[0] %} {% else %} {% set alias = numeric_aliases[0] %} {% endif %} https://{{addin_server_domain}}/webapp/#/?conference={{alias}}</pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> • aliases • domain_aliases • numeric_aliases • other_aliases • addin_server_domain • name • description • service_type • pin • allow_guests • guest_pin
Personal VMR name template	<p>A jinja2 template that is used to generate the name of the personal VMR, as it appears on the button offered to users when selecting which VMR to use. By default, this uses the Name configured for the user's personal VMR.</p> <p>We recommend that the output is a single line.</p> <p>Default:</p> <pre>{{name}}</pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> • aliases • domain_aliases • numeric_aliases • other_aliases • addin_server_domain • name • description • service_type • pin • allow_guests • guest_pin

Option	Description	Notes
Personal VMR description template	<p>A jinja2 template that is used to generate the text that will appear when hovering over the button offered to users when selecting which VMR to use. By default this uses the Description configured for the user's personal VMR.</p> <p>Default:</p> <pre>{{description}}</pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> aliases domain_aliases numeric_aliases other_aliases addin_server_domain name description service_type pin allow_guests guest_pin
Add-in configuration		
Add-in server FQDN *	<p>The FQDN of the reverse proxy or Conferencing Node (which can be either a Proxying Edge Node or Transcoding Conferencing Node) that provides the add-in content. This reverse proxy or Conferencing Node must:</p> <ul style="list-style-type: none"> be reachable by all Outlook clients, whether they are located on an internal network or on the public internet have installed a valid, trusted certificate; in particular, there must be a server certificate with a subject name that matches the FQDN, and which is signed by a trusted root CA. <p>Pexip's Reverse Proxy and TURN Server v3 and later supports the VMR Scheduling for Exchange feature; we recommend v5 for additional security.</p> <p>If you do not have a reverse proxy in your deployment, you can choose any Conferencing Node that meets the above criteria.</p>	
Add-in provider name *	<p>The name of the organization which provides the add-in.</p> <p>Default: <i>Pexip</i>.</p>	
Add-in display name *	<p>The display name of the add-in.</p> <p>Default: <i>Pexip Scheduling Service</i>.</p>	
Add-in description *	<p>The description of the add-in. Maximum length: 250 characters.</p> <p>Default: <i>Turns meetings into Pexip meetings</i>.</p>	
Add-in group label *	<p>The name of the group in which to place the add-in button on desktop clients.</p> <p>Default: <i>Pexip Meeting</i>.</p>	
Add-in button label *	<p>The label for the add-in button on desktop clients.</p> <p>Default: <i>Create a Pexip Meeting</i>.</p>	
Add-in supertip title *	<p>The title of the supertip help text for the add-in button on desktop clients.</p> <p>Default: <i>Makes this a Pexip Meeting</i>.</p>	

Option	Description	Notes
Add-in supertip text *	The text of the supertip for the add-in button on desktop clients. Default: <i>Turns this meeting into an audio or video conference hosted in a Pexip VMR. The meeting is not scheduled until you select Send.</i>	
Add-in pane title	The title of the add-in on the side pane. Default: <i>Add a VMR.</i>	
Add-in pane description	The description of the add-in on the side pane. Default: <i>This assigns a Virtual Meeting Room for your meeting.</i>	
Add-in pane single-use VMR button label	The label of the button on the side pane. Default: <i>Add a Single-use VMR.</i>	
Add-in pane success heading	The message that appears on the side pane when an alias has been obtained successfully from the Management Node. Default: <i>Success.</i>	
Already video meeting heading	The heading that appears on the side pane when the add-in is activated after an alias has already been obtained for the meeting. Default: <i>VMR already assigned.</i>	
Unable to add joining instructions heading	The heading that appears on the side pane when the Management Node cannot be contacted to obtain an alias. Default: <i>Cannot assign a VMR right now.</i>	
General error heading	The heading that appears on the side pane when an error occurs trying to add the joining instructions. Default: <i>Error.</i>	
Success message	The message that appears on the side pane when an alias has been obtained successfully from the Management Node. Default: <i>This meeting is now set up to be hosted as an audio or video conference in a Virtual Meeting Room. Please note this conference is not scheduled until you select Send.</i>	
Already video meeting message	The message that appears on the side pane when the add-in is activated after an alias has already been obtained for the meeting. Default: <i>It looks like this meeting has already been set up to be hosted in a Virtual Meeting Room. If this is a new meeting, select Send to schedule the conference.</i>	
Unable to add joining instructions message	The message that appears on the side pane when the Management Node cannot be contacted to obtain an alias. Maximum length: 250 characters. Default: <i>Sorry, we are unable to assign a Virtual Meeting Room at this time. Select Send to schedule the meeting, and all attendees will be sent joining instructions later.</i>	
Error inserting single-use VMR message	The message that appears on the side pane when an error occurs trying to add the joining instructions of a single-use VMR. Default: <i>There was a problem adding the joining instructions. Please try again.</i>	
Add-in pane personal VMR button label	The label of the button on the side pane used to add a personal VMR. Default: <i>Add a Personal VMR</i>	

Option	Description	Notes
Add-in pane sign in button label	The label of the button on the side pane requesting users to sign in to obtain the list of their personal VMRs. Default: <i>Sign In</i>	
Select personal VMR message	The message that appears on the side pane requesting users to select a personal VMR to use for the meeting. Default: <i>Select the VMR you want to add to the meeting</i>	
No personal VMR message	The message that appears on the side pane when the user has no personal VMRs. Default: <i>You do not have any personal VMRs</i>	
Error getting personal VMRs message	The message that appears on the side pane when an error occurs trying to obtain a list of the user's personal VMRs. Default: <i>There was a problem getting your personal VMRs. Please try again.</i>	
Error signing in message	The message that appears on the side pane when an error occurs trying to sign the user in. Default: <i>There was a problem signing you in. Please try again.</i>	
Error inserting personal VMR meeting message	The message that appears on the side pane when an error occurs trying to add the personal VMR details to the meeting. Default: <i>There was a problem adding the joining instructions. Please try again.</i>	
Add-in image icon	Select the image file to use as the add-in icon. Images must be in PNG file format and 80 x 80 pixels in size. Note that Outlook clients may cache the add-in icon, so it may be some time after uploading a new icon that it appears to end users. You can resolve this by deleting the cache .  Default:	

Single-use VMR email text (available and required when single-use VMRs are enabled; for more information, see [Formatting the email text](#))

Option	Description	Notes
Single-use VMR joining instructions template	<p>A jinja2 template that is used to generate the joining instructions that are added by VMR Scheduling for Exchange to the body of the meeting request when a single-use VMR is being used.</p> <p>Note that the <code>{{alias_uuid}}</code> variable, which inserts the PXPS: token, must be included.</p> <p>For examples of templates that use images and other formatting, see Example joining instructions.</p> <p>For more details on constructing the URLs used for joining from a web browser, see Creating preconfigured links to launch conferences via s.</p> <p>Default:</p> <pre>
 <div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> Please join my Pexip Virtual Meeting Room in one of the following ways:

 From a VC endpoint or a Skype/Lync client:
 {{alias}}


 From a web browser:
 https://{{addin_server_domain}}/webapp/#/?conference={{alias}}

 From a Pexip Infinity Connect client:
 pexip://{{alias}}

 From a telephone:
 [Your number], then {{numeric_alias}} #

 {{alias_uuid}}
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> alias addin_server_domain numeric_alias alias_uuid
Placeholder instructions text	<p>The text that is added by VMR Scheduling for Exchange to email messages when the actual joining instructions cannot be obtained.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting will be hosted in a Virtual Meeting Room. Joining instructions will be
 sent to you soon in a separate email.
 </div></pre>	
Accept new single meeting template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has successfully scheduled a new single meeting.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting has been successfully scheduled using the aliases: {{alias}} and {{numeric_alias}}.
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> start_time end_time alias numeric_alias
Accept edited single meeting template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has successfully scheduled an edited single meeting.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting has been successfully rescheduled using the aliases: {{alias}} and {{numeric_alias}}.
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> start_time end_time alias numeric_alias

Option	Description	Notes
Accept new recurring meeting template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has successfully scheduled a new recurring meeting.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This recurring meeting series has been successfully scheduled.
 All meetings in this series will use the aliases: {{alias}} and {{numeric_alias}}.
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> start_time end_time alias numeric_alias
Accept edited occurrence template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has successfully scheduled an edited occurrence in a recurring series.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting occurrence in a recurring series has been successfully rescheduled using the aliases: {{alias}} and {{numeric_alias}}.
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> start_time end_time alias numeric_alias
Accept edited recurring meeting template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has successfully scheduled an edited recurring meeting.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This recurring meeting series has been successfully rescheduled.
 All meetings in this series will use the aliases: {{alias}} and {{numeric_alias}}.
 </div></pre>	<p>Accepted variables:</p> <ul style="list-style-type: none"> start_time end_time alias numeric_alias
Reject invalid alias ID text	<p>The text that is sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a meeting because the alias ID in the meeting email is invalid.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting request does not contain currently valid scheduling data, and therefore cannot be processed.
 Please use the add-in to create a new meeting request, without editing any of the content that is inserted by the add-in.
 If this issue continues, please contact your system administrator.
 </div></pre>	
Reject alias conflict template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a meeting because the alias conflicts with an existing alias.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> We are unable to schedule this meeting because the alias: {{alias}} is already
 in use by another Pexip Virtual Meeting Room. Please try creating a new meeting.
 </div></pre>	<p>Accepted variable:</p> <ul style="list-style-type: none"> alias
Reject alias deleted text	<p>The text that is sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a meeting because the alias for this meeting has been deleted.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> We are unable to schedule this meeting because its alias has been deleted.
 Please try creating a new meeting.
 </div></pre>	

Option	Description	Notes
Reject recurring series in past text	<p>The text that is sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a recurring meeting because all instances occurred in the past.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This recurring series cannot be scheduled because all
 occurrences happen in the past.
 </div></pre>	
Reject single meeting in past text	<p>The text that is sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a meeting because it occurred in the past.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> This meeting cannot be scheduled because it occurs in the past.
 </div></pre>	
Reject general error template	<p>A jinja2 template that is used to produce the message sent to meeting organizers when VMR Scheduling for Exchange has failed to schedule a meeting because a general error has occurred. The <code>{{correlation_id}}</code> variable is a UUID which can be used to find more information from the administrator log.</p> <p>Default:</p> <pre><div style="font-size:11.0pt; color:#000000; font-family:Calibri,Arial,Helvetica,sans-serif;"> We are unable to schedule this meeting. Please try creating a new meeting.
 If this issue continues, please forward this message to your system administrator, including the following ID:
 CorrelationID="{{correlation_id}}".
 </div></pre>	<p>Accepted variable:</p> <ul style="list-style-type: none"> <code>correlation_id</code>
Advanced options		
Disable web proxy	Select this option to bypass the web proxy (where configured for the Management Node) for outbound requests sent from this VMR scheduling for Exchange integration.	
Enable add-in debug logs	Enable this option to view debug logs within the add-in side pane in the desktop and web Outlook client. Only do this as a temporary measure if you are experiencing issues deploying the add-in. Note that these logs will appear for all users of this add-in.	
Use custom add-in sources	<p>Enable this option to override the default locations from which the add-in JavaScript and CSS are served. This option is intended for use in deployments that are fully offline (where Outlook users will not have internet access) and therefore these resources must be available locally.</p> <p>If you enable this option, you must host these files on your own internal server, and enter the URLs for each in the relevant fields below.</p> <p> We recommend contacting your Pexip authorized support representative before enabling this option.</p>	
Office.js URL	<p>(Available if Use custom add-in sources has been enabled)</p> <p>The URL used to download the Office.js JavaScript library.</p>	
Microsoft Fabric CSS URL	<p>(Available if Use custom add-in sources has been enabled)</p> <p>The URL used to download the Microsoft Fabric CSS.</p>	
Microsoft Fabric Components CSS URL	<p>(Available if Use custom add-in sources has been enabled)</p> <p>The URL used to download the Microsoft Fabric Components CSS.</p>	

Option	Description	Notes
Additional add-in script sources	<p>(Available if Use custom add-in sources has been enabled)</p> <p>Optionally specify additional URLs from which to download JavaScript script files.</p> <p>These URLs will be used in preference to any other URLs specified elsewhere for the same resource. In particular, we recommend that you specify here the URL for MicrosoftAjax.js.</p> <p>Each URL must be entered on a separate line.</p>	
Exchange Metadata Domains and URLs		
Domain or URL	<p>(Required for single-use VMRs and personal VMRs)</p> <p>An FQDN or URL which can be used to access a page containing the Exchange Metadata for your Exchange deployment. This page provides the public key of the Microsoft Exchange Server Auth Certificate used by the add-in to verify user identities.</p> <p>If a FQDN is supplied, the default URL path https://<FQDN>/autodiscover/metadata/json/1 will be used.</p> <p>This URL must be reachable by the management node.</p> <p>If you have a hybrid Exchange and Office 365 deployment, you must include outlook.office365.com in the list of domains as well as the domain of one of your Exchange on-premises servers.</p> <p>If your Exchange deployment uses more than one domain or URL (for example, if you have an on-premises Microsoft Exchange deployment with more than one Microsoft Exchange server, or your Exchange server has more than one FQDN), and they use separate signing certificates, you must include all the FQDNs of all the Exchange servers in your deployment. To do this, select Add another Exchange Metadata Domain or URL and add the FQDN of each.</p>	
<p>* If you change this setting, you must re-generate and re-install the add-in XML file.</p> <p>** If you select this option you must sign in to the service account after completing and saving the configuration.</p> <p>† If you change this configuration when OAuth is enabled you must also sign in to the service account again.</p>		

Signing in to the service account if OAuth has been enabled

If you have enabled OAuth for the first time, you must sign in to the service account after saving the configuration of the VMR scheduling for Exchange integration.

You may also need to re-sign in to the service account if:

- the service account password has changed
- the service account uses multi-factor authentication (MFA) and the MFA is refreshed
- you disable and then subsequently re-enable OAuth
- you update any of the following configuration for the VMR scheduling for Exchange integration:
 - Service account username
 - OAuth client ID
 - OAuth token endpoint
- the Management Node has been offline for more than 90 days.

To sign in to the service account:

- Ensure you have signed out of **all** Microsoft accounts on your device, including the Microsoft Azure portal.
- From the Management Node, go to **System > VMR Scheduling For Exchange** and select the VMR scheduling for Exchange integration. At the bottom of the **Change VMR Exchange Integration** page, select **Sign in to service account**. You will be taken to the **Sign in to service account** page.:

]pexip[Infinity Conferencing Platform

Status ▾ History & Logs ▾ System ▾ Platform ▾ Call Control ▾ Services ▾ Users & Devices ▾ **One-Touch Join ▾** Utilities ▾

Sign in to service account

Please open the link below. It will take you to a Microsoft sign-in page where you must sign in as the service account with username **test**.

Warning: If you are already signed into a Microsoft account, you may not be prompted to enter a username. Please make sure you are not signed in to a Microsoft account before opening the link.

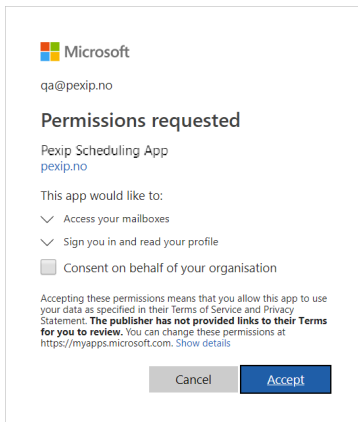
Sign-in link

Sign in

https://infinity.example.com/admin/platform/otj/oauth_redirect/?state=2e546d1d-cb4f-46d1-b6c6-f7caf1d97f44&redirect_uri=

3. Copy the **Sign in** link and paste it into a new browser tab.
4. Sign in as the service account.

You are asked to permit the scheduling application registration to sign in as the service account:



- i** If there is an option to **Consent on behalf of your organization**, do not select this — consent only needs to be given to the service account.

5. Select **Accept**.
You are returned to the Management Node.
6. You may be asked to sign in to the Management Node again. If so, you must sign in to the Management Node (using your Management Node credentials) to complete the process of signing in to the service account.

When complete, you are returned to the **Sign in to service account** page and see the message **Successfully signed in**.

Saving and checking configuration

When you have finished, select **Save**. You will be taken back to the main **VMR Scheduling For Exchange Integration** page. The Pexip Infinity platform will attempt to contact the Microsoft Exchange deployment, and if there are any issues, it will raise an alarm on the Management Node.

Formatting the email text

All the templates and text specified in the **Email text** section can be entered as HTML. This allows you to customize the text (for example, the font, size, and color). When using HTML, you must ensure all HTML tags are closed properly, otherwise you may affect the format of any existing text in the email body.


The add-in pane headings and text can also be formatted using HTML, although some formatting may be overridden by the base HTML. We recommend that you check that any formatting applied to add-ins appears as expected in all clients used in your environment.

Working with jinja2 templates

VMR Scheduling for Exchange uses a subset of the jinja2 templating language (<https://jinja.palletsprojects.com/en/2.10.x/templates/>) to create the text used in emails.

Variables

The following variables can be used when creating the jinja2 templates used for VMR Scheduling for Exchange. Note that not all variables can be used in all templates; see the descriptions of each template in [Single-use VMR configuration](#), [Personal VMR configuration](#) and [Single-use VMR email text](#) for a list of which variables can be used in each template.

Variable	Description
Valid for Single-use VMRs	
{{addin_server_domain}} *	Inserts the FQDN configured in the Add-in server FQDN field. This FQDN is used by Connect apps as part of the address to use when connecting to the meeting. For more information, see Creating preconfigured links to launch conferences via Infinity Connect .
{{alias}}	Inserts the full alias that was generated for the VMR that will be used for this meeting. This is in the format: <prefix><random_number>@domain.
{{alias_uuid}} *	Inserts the PXPS:- ID. For more information, see PXPS:- and TOK:- security tags .  The Single-use VMR joining instructions template must contain this variable.
{{correlation_id}}	Used in the Reject general error template only Inserts a UUID which can be used to find more information about the error from the administrator log .
{{end_time}} **	Inserts the end time of the meeting, as per the meeting request. (This time does not include the Join after buffer .) Note that this will use the format hh:mm on DD/MM/YYYY, e.g. 15:30 on 31/07/2017; this format cannot be changed.
{{numeric_alias}}	Inserts the numeric part of the alias that was generated for the VMR that will be used for this meeting. This is in the format: <prefix><random_number>.
{{organizer_email}} †	Inserts the email address of the meeting organizer.
{{organizer_name}} †	Inserts the name of the meeting organizer, as it appears in the meeting invitation.
{{start_time}} **	Inserts the start time of the meeting, as per the meeting request. (This time does not include the Join before buffer .) Note that this will use the format hh:mm on DD/MM/YYYY, e.g. 15:30 on 31/07/2017; this format cannot be changed.
{{subject}} †	Inserts the subject line of the meeting invitation sent by the meeting organizer. Note that this information will be visible to anyone with access to the Management Node, so do not use this variable if privacy is an issue.
Valid for Personal VMRs	
{{addin_server_domain}}	Inserts the FQDN configured in the Add-in server FQDN field. This FQDN is used by Connect apps as part of the address to use when connecting to the meeting. For more information, see Creating preconfigured links to launch conferences via Infinity Connect .

Variable	Description
{{aliases}}	Provides access to a jinja2 list object which contains all aliases that have been configured for the personal VMR. You can then access any particular alias by using a list index. See the Personal VMR joining instructions template for example usage.
{{allow_guests}}	Returns <code>true</code> or <code>false</code> , which can then be used in an <code>if</code> statement. See the Personal VMR joining instructions template for example usage.
{{description}}	Inserts the configured Description of the personal VMR.
{{domain_aliases}}	Provides access to a jinja2 list object which contains all aliases configured for this personal VMR that include the <code>@</code> character followed by a domain. You can then access any one of these aliases by using a list index. See the Personal VMR joining instructions template for example usage.
{{guest_pin}}	Inserts the configured Guest PIN of the personal VMR.
{{name}}	Inserts the configured Name of the personal VMR.
{{numeric_aliases}}	Provides access to a jinja2 list object which contains all aliases configured for this personal VMR that include only digits. You can then access any one of these aliases by using a list index. See the Personal VMR joining instructions template for example usage.
{{other_aliases}}	Provides access to a jinja2 list object which contains all aliases configured for this personal VMR that do not include either the <code>@</code> character followed by a domain, or only digits. You can then access any one of these aliases by using a list index. See the Personal VMR joining instructions template for example usage.
{{owners_email}}	Inserts the configured Owner's email address of the personal VMR.
{{pin}}	Inserts the configured Host PIN of the personal VMR.
{{service_type}}	Inserts a string to indicate whether the personal VMR is a "conference" (Virtual Meeting Room), "lecture" (Virtual Auditorium), or "two_stage_dialing" (Virtual Reception).
* Can only be used in joining instructions.	
** Can only be used in acceptance messages.	
† Can only be used in the name, description or subject fields of the VMR to be created for this meeting.	

Deleting and replacing VMR scheduling for Exchange integrations

If you delete an existing VMR scheduling for Exchange integration and replace it with another, you must also [re-generate and re-install the add-in XML file](#), even if the configuration of the new VMR scheduling for Exchange integration is identical to that of the old one.

Using multiple VMR scheduling for Exchange integrations

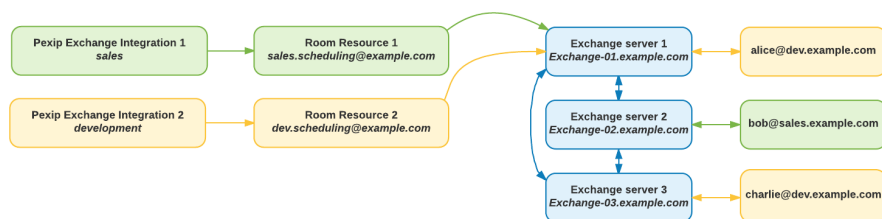
Different groups of users within the same Microsoft Exchange deployment

You can provide different groups of users within your Microsoft Exchange deployment with different options when using the VMR Scheduling for Exchange feature. For example, you may wish to vary the [prefix](#) used as part of the VMR alias, or use different text for the [joining instructions](#). To do this, create multiple VMR scheduling for Exchange integrations that connect to the same Exchange environment. (Note however that each VMR scheduling for Exchange integration must have a separate [equipment resource](#).)

Each VMR scheduling for Exchange integration that you create will have an associated add-in which you can then [make available to specific users](#) by using Exchange PowerShell commands.

The diagram below shows a single Pexip Infinity deployment with two VMR scheduling for Exchange integrations to the same Microsoft Exchange deployment. Each VMR scheduling for Exchange integration uses the same [EWS URL](#) and is configured with the [FQDNs of all the Exchange servers](#) in the Exchange deployment.

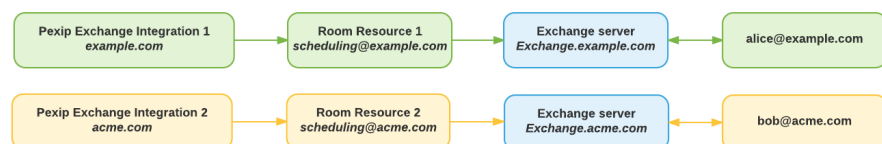
The first connection provides an add-in for sales staff; the second provides an add-in for development staff. Both add-ins are uploaded to Microsoft Exchange, but each user will only see the add-in relevant to their group.



Different Microsoft Exchange deployments

If you are a service provider, you can configure one or more VMR scheduling for Exchange integrations for each of your customers.

The diagram below shows a single Pexip Infinity deployment with two VMR scheduling for Exchange integrations to two different Microsoft Exchange deployments. The first connection provides an add-in for everyone at Example Corp; the second provides an add-in everyone at Acme Corp.



Next step

- [Making the add-in available to users](#) within your Exchange deployment.

Making the scheduling add-in available to users

This topic explains how to make the Pexip VMR Scheduling for Exchange add-in available to Outlook users from their desktop and Web App clients. This involves uploading an XML manifest file to your Microsoft Exchange deployment. There are two ways to do this:

- For Office 365 users, our recommended method is to use [Centralized Deployment](#). Using this method allows you to deploy the add-in either to all users, or to selected groups of users; when group members are added or removed, the add-in is added or removed accordingly.
- You can also [upload the file via Exchange Admin Center \(EAC\)](#). Using this method allows you to deploy the same add-in to all users in your Exchange deployment. It is possible to restrict the add-in to a particular group of users using PowerShell, but this is a manual process that must be re-run every time group members are added or removed, and is limited to groups of 1,000 or fewer. For more information, see [Restricting the scheduling add-in to specific users](#).

Prerequisites

Before you start you must have completed steps described in [Configuring Pexip Infinity for VMR Scheduling for Exchange](#).

Downloading the add-in XML file

The add-in XML manifest file contains all the add-in configuration and is generated by the Pexip Infinity Management Node based on the information you provided when [Configuring Pexip Infinity for VMR Scheduling for Exchange](#).

To download the file:

1. From the Management Node, go to **System > VMR Scheduling For Exchange**.
2. Select the VMR scheduling for Exchange integration you have configured.
3. From the bottom of the page, select **Download Exchange add-in manifest**.

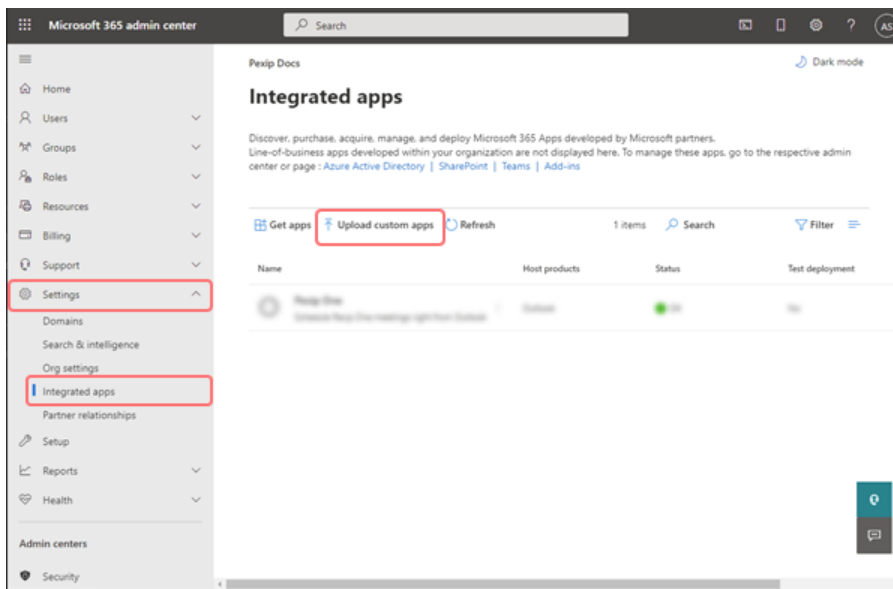
You must now upload the add-in XML manifest file to your Microsoft Exchange deployment.

Uploading the add-in XML file to Office 365 using Centralized Deployment

Centralized Deployment is Microsoft's recommended way for an Office 365 admin to deploy Office add-ins, provided that the organization meets all requirements for using Centralized Deployment. For information about these requirements, see <https://docs.microsoft.com/en-gb/office365/admin/manage/centralized-deployment-of-add-ins?view=o365-worldwide>.

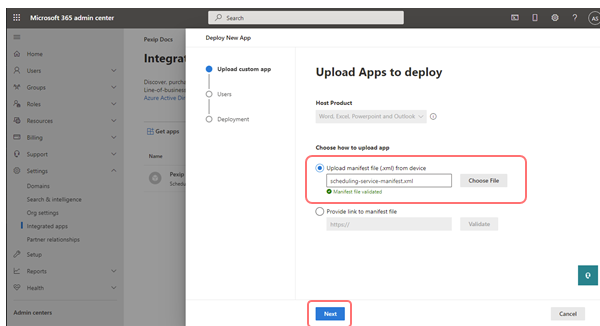
There are a different ways to upload an add-in XML manifest file using Centralized Deployment. The instructions below are one way; if you do not see the same options when logged in to the Microsoft Office 365 admin center then see <https://docs.microsoft.com/en-us/microsoft-365/admin/manage/manage-deployment-of-add-ins> for alternatives.

1. Log in to the Microsoft Office 365 admin center at <https://admin.microsoft.com>.
2. From the left-hand panel, select **Settings > Integrated apps**.
3. At the top of the **Integrated apps** page, select **Upload custom apps**:

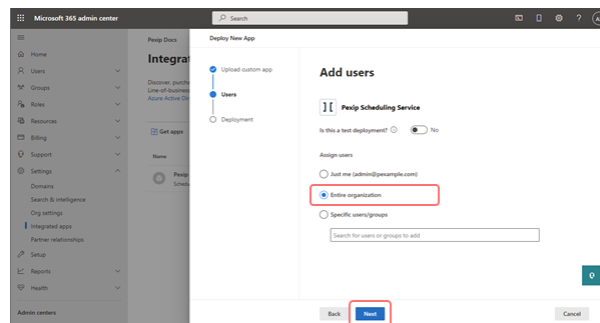


- From the **Upload Apps to deploy** page, under **Choose how to upload app**, select **Upload manifest file (.xml)** from device and select the file.

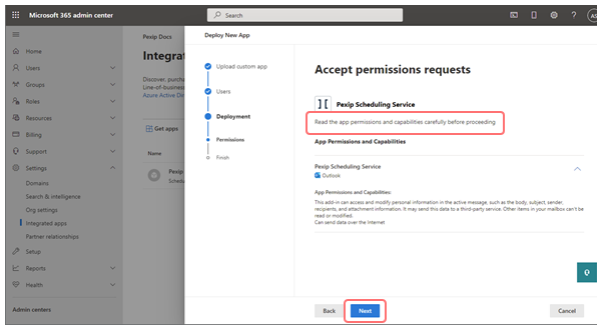
When it has been successfully uploaded you'll see a **Manifest file validated** notification. Select **Next**:



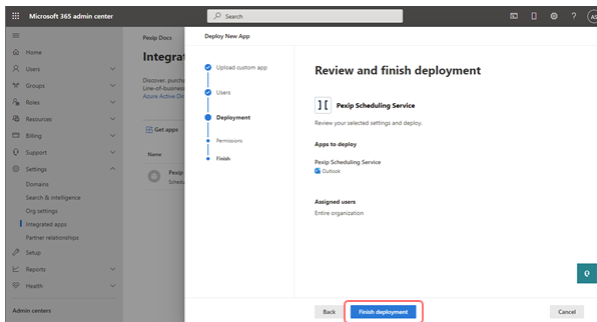
- From the **Add users** page, specify whether you want to give access to your **Entire organization**, or to **Specific users/groups**. Select **Next**:



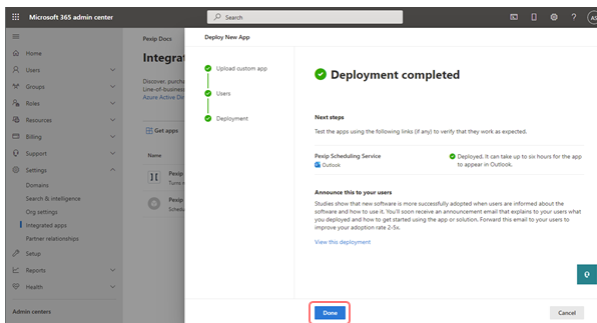
- From the **Accept permissions requests** page, review the permissions and select **Next**:



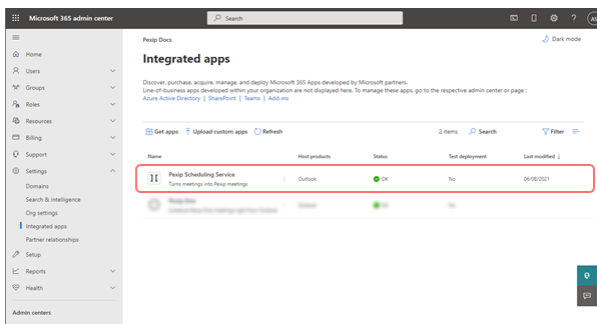
7. From the Review and finish deployment page, select Finish deployment:



8. After a short delay you see the Deployment completed page. Select Done:



9. You are returned to the Integrated apps page, which now lists the add-in:



It can take up to 24 hours for the add-in icon to appear to all Outlook users, and users might need to relaunch Office.

When the add-in appears, users will be able to click on it to quickly [schedule meetings in Pexip Infinity VMRs](#).

Uploading the add-in XML file to Microsoft Exchange

To upload the add-in XML manifest file to your Microsoft Exchange deployment:

1. Log in to the Exchange Admin Center (EAC) and select **organization > apps** (for Exchange 2013) or **organization > add-ins** (for Exchange 2016).
2. Select the add icon (+) and then **Add from file**.
3. Browse to the manifest XML file and then select **Next**.
The **Pexip Scheduling Service** add-in will appear in the list.
4. Double click the Pexip add-in to edit it.
5. Select **Make this add-in available to users in your organization**.
6. Select either **Optionally, enabled by default** or **Mandatory, always enabled**.

Pexip Scheduling Service

☒ **Make this add-in available to users in your organization**

Specify user defaults:

☐ Optional, enabled by default

☐ Optional, disabled by default

☒ **Mandatory, always enabled. Users can't disable this add-in.**

Save

Cancel

7. Select **Save**.

Enterprise Office 365

Administrator ?

Exchange admin center

recipients
permissions
compliance management
organization
protection
mail flow
mobile
public folders
unified messaging
servers
hybrid
tools

sharing add-ins address lists

Add-ins let your users do and see more without leaving their mailbox. The following list shows add-ins that have been installed for the organization. [Find more add-ins for Outlook at the Office Store...](#)

NAME	PROVIDER	USER DEFAULT	PROVIDED TO
Action Items	Microsoft	Enabled	Everyone
Bing Maps	Microsoft	Enabled	Everyone
My Templates	Microsoft	Enabled	Everyone
Pexip Scheduling Service	Pexip	Mandatory	Everyone
Suggested Meetings	Microsoft	Enabled	Everyone
Unsubscribe	Microsoft	Enabled	Everyone

11

Pexip Scheduling Service
Version: 1.1.4878.51093
Created by: Pexip

Turns meetings into Pexip meetings

Permissions: Read write item
When the user clicks this add-in, the add-in will be able to access and modify personal information in the active message, such as the subject, sender, recipients, content in the message body, and attachments. The add-in may send this data to a third-party service. Other items in the user's mailbox won't be read or modified.

1 selected of 6 total

Now, when users access Outlook, the Pexip VMR Scheduling for Exchange add-in will be available for them to use to schedule meetings in Pexip Infinity VMRs. The add-in will be available to all Outlook users in your deployment unless you choose to [restrict it to certain users](#).

Testing the integration

You can test that the add-in is working as expected by logging in to an Outlook client and creating a test meeting, and then joining that meeting using the links that were generated. Note that you should ensure that the test meeting is scheduled to start within the [buffer time](#), otherwise it won't be available to join immediately.

Troubleshooting

If you are having issues installing the add-in, see [Troubleshooting VMR Scheduling for Exchange](#).

Restricting the scheduling add-in to specific users

This topic explains how to use Windows PowerShell to enable the VMR Scheduling for Exchange scheduling add-in for all users from a specific group (rather than all users in your deployment). You should only use this method if you cannot [deploy the add-in using Centralized Deployment](#).

Note that:

- These instructions extract a list of users in a particular group, and then make the add-in available to each of those users. If the members of a group change, you will need to [use the Set-App command](#) to make the add-in available to the updated list of users.
- Using Windows PowerShell to enable the scheduling add-in for specific users is limited to a maximum size of 1000 users. This means the commands below will only work if the AD group contains 1000 users or fewer.

Prerequisites

Before you start you must have completed the following steps:

1. [Configuring Pexip Infinity for VMR Scheduling for Exchange](#)
2. [Downloading the add-in XML file](#)

Exchange 2013 on-prem

If you have an Exchange 2013 on-premises deployment, you can enable the scheduling add-in for users from either a specific [Active Directory \(AD\) group](#) or a specific [Exchange distribution group](#). For full information on the add-in PowerShell commands for Exchange 2013 used in these examples, see the following Microsoft documentation:

- Get-App: [https://technet.microsoft.com/en-us/library/jj218673\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj218673(v=exchg.150).aspx)
- New-App: [https://technet.microsoft.com/en-us/library/jj218722\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj218722(v=exchg.150).aspx)
- Set-App: [https://technet.microsoft.com/en-us/library/jj218630\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj218630(v=exchg.150).aspx)
- Managing user access to add-ins for Outlook: [https://technet.microsoft.com/en-us/library/jj943757\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/jj943757(v=exchg.150).aspx)

Active Directory (AD) group

To restrict the add-in to all members of an AD group (for example, a distribution group or a security group) that has been created on your AD server:

1. Get all the users in the group, and then get each user's UPN:

```
$users = Get-AdGroupMember -Identity "<Group Name>" | % { Get-AdUser $_.SamAccountName | select UserPrincipalName }
```

2. Put each UPN in an array:

```
$user_list = @()
for ($i=0; $i -lt $users.length; $i++) {
    $user_list += $users[$i].UserPrincipalName
}
```

3. Read the scheduling add-in manifest from file:

```
$Data=Get-Content -Path "<Scheduling Manifest File Path>" -Encoding Byte -ReadCount 0
```

4. Execute the `New-App` command:

```
New-App -OrganizationApp -FileData $Data -ProvidedTo SpecificUsers -UserList $user_list -DefaultStateForUser Enabled
```

Exchange distribution group

To restrict the add-in to all members of a specific Exchange distribution group:

1. Get all the users in the distribution group:

```
$user_list = Get-DistributionGroupMember "<Group Name>"
```

2. Read the scheduling add-in manifest from file:

```
$Data=Get-Content -Path "<Scheduling Manifest File Path>" -Encoding Byte -ReadCount 0
```

3. Execute the `New-App` command:

```
New-App -OrganizationApp -FileData $Data -ProvidedTo SpecificUsers -UserList $user_list -DefaultStateForUser Enabled
```

Office 365 with Azure AD

For full information on the add-in PowerShell commands for Office 365 used in these examples, see the following Microsoft documentation:

- Get-App: [https://technet.microsoft.com/en-us/library/jj218673\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj218673(v=exchg.160).aspx)
- New-App: [https://technet.microsoft.com/en-us/library/jj218722\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj218722(v=exchg.160).aspx)
- Set-App: [https://technet.microsoft.com/en-us/library/jj218630\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj218630(v=exchg.160).aspx)
- Managing user access to add-ins for Outlook: [https://technet.microsoft.com/en-us/library/jj943757\(v=exchg.160\).aspx](https://technet.microsoft.com/en-us/library/jj943757(v=exchg.160).aspx)

Azure AD group

To restrict the add-in to all members of an Azure AD group:

1. Set up a PowerShell session with access to both Azure and Exchange. To do this, follow the instructions at <https://technet.microsoft.com/en-gb/library/dn568015.aspx>.

2. Get a list of your Groups and their corresponding IDs:

```
Get-MsolGroup | Format-Table -Auto ObjectID,DisplayName
```

Example output:

ObjectID	DisplayName
977e8519-c71e-4670-bc7b-2aef408189da	Pexip List
145f2550-82ef-419d-830b-ca018a21cea4	Pexip Group

3. Get the users from the targeted group:

```
$users = Get-MsolGroupMember -GroupObjectID "<ObjectID>"
```

4. Get each user's email address and put in an array:

```
$user_list = @()
for ($i=0; $i -lt $users.length; $i++) {
    $user_list += $users[$i].EmailAddress
}
```

5. Read the scheduling add-in manifest from file:

```
$Data=Get-Content -Path "<Scheduling Manifest File Path>" -Encoding Byte -ReadCount 0
```

6. Execute the `New-App` command:

```
New-App -OrganizationApp -FileData $Data -ProvidedTo SpecificUsers -UserList $user_list -DefaultStateForUser Enabled
```

Verifying the add-in is available as expected

After you have enabled the add-in for a group, you should confirm it is provided to the users you expect. To do this:

1. Get the App ID of the add-in you want to check:

```
Get-App -OrganizationApp | Format-Table -Auto DisplayName,AppId
```

Example output:

DisplayName	AppId
Pexip Scheduling Service	79623c8b-9daf-42a0-b051-b130b8c3aef4
Bing Maps	7a774f0c-7a6f-11e0-85ad-07fb4824019b
My Templates	a216ceed-7791-4635-a752-5a4ac0a5eb93
Suggested Meetings	bc13b9d0-5ba2-446a-956b-c583bdc94d5e

```
Unsubscribe      d39dee0e-fdc3-4015-af8d-94d4d49294b3
Action Items     f60b8ac7-c3e3-4e42-8dad-e4e1fea59ff7
```

2. Execute the `Get-App` command:

```
Get-app -OrganizationApp -Identity "<AppId>" | Format-List DisplayName,AppId,Enabled,Default*,ProvidedTo,UserList
```

Example output:

```
DisplayName      : Pexip Scheduling Service
AppId            : 79623c8b-9daf-42a0-b051-b130b8c3aef4
Enabled         : True
DefaultStateForUser : Enabled
ProvidedTo       : SpecificUsers
UserList         : {rd.pexip.com/Users/Administrator, rd.pexip.com/Users/Toby Finch, rd.pexip.com/Users/Ben Hockley,
rd.pexip.com/Users/Bob Test, rd.pexip.com/Users/Alice Test}
```

Changing the users for an existing add-in

You can edit the set of users to which an existing add-in is available. You may wish to do this if, for example, users have been added or removed from the group, or the add-in was added using EAC and you now wish to restrict it to a particular set of users.

1. Get the App ID of the add-in:

```
Get-App -OrganizationApp | Format-Table -Auto DisplayName,AppId
```

Example output:

```

DisplayName      AppId
-----
Pexip Scheduling Service 79623c8b-9daf-42a0-b051-b130b8c3aef4
Bing Maps        7a774f0c-7a6f-11e0-85ad-07fb4824019b
My Templates     a216ceed-7791-4635-a752-5a4ac0a5eb93
Suggested Meetings bc13b9d0-5ba2-446a-956b-c583bdc94d5e
Unsubscribe      d39dee0e-fdc3-4015-af8d-94d4d49294b3
Action Items     f60b8ac7-c3e3-4e42-8dad-e4e1fea59ff7
```

2. Get a list of users using the method appropriate for your version of Exchange:

- [Exchange 2013 AD group](#)
- [Exchange 2013 distribution group](#)
- [O365 Azure AD group](#)

3. Execute the `Set-App` command:

```
Set-App -OrganizationApp -Identity "<AppId>" -ProvidedTo SpecificUsers -UserList $user_list
```

For example:

```
Set-App -OrganizationApp -Identity "79623c8b-9daf-42a0-b051-b130b8c3aef4" -ProvidedTo SpecificUsers -UserList $user_list
```

Managing scheduled conferences

This topic describes how to view and modify any scheduled single-use conference VMRs that have been created by the VMR Scheduling for Exchange service.


Scheduled conference VMRs

When a user creates a scheduled single-use conference using the VMR Scheduling for Exchange feature, a unique Virtual Meeting Room is created for that conference. This VMR is just like any other VMR, except it was created by the VMR Scheduling for Exchange service rather than by an administrator. For this reason, on the Pexip Infinity Administrator interface, scheduled single-use conferences have a **Service type** of VMR, and a **VMR origin** of VMR Scheduling for Exchange: followed by the [name of the VMR scheduling for Exchange integration](#) being used.

Viewing all single-use VMRs used for scheduled conferences

All single-use VMRs that have been created using the VMR Scheduling for Exchange feature are listed on the **Scheduled Conferences** page (**Services > Scheduled Conferences**).


Depending on when VMR Scheduling for Exchange has last synced with the Microsoft Exchange server, this may include meetings with a start time of up to 24 hours in the past.

-  Meetings that have been scheduled in personal VMRs using the VMR Scheduling for Exchange feature will not appear here, because they take place in existing, permanent VMRs.


Editing the VMR for a scheduled conference


To view or edit information about a particular single-use scheduled conference's Virtual Meeting Room, select it from the list.

Note that any changes made to a recurring conference's VMR will apply to all instances of that meeting, since the same VMR is used for all of them.

-  You can add additional aliases to a scheduled conference's VMR but you should not change either of the aliases that were assigned by VMR Scheduling for Exchange.

When editing scheduled conference VMRs, all of the standard VMR settings may be modified. However, the options that specifically have scheduling-related content are:

Option	Description
Name	<p>The name used to refer to this Virtual Meeting Room.</p> <p>By default this will be the subject line of the meeting invitation followed by the organizer's name, but you can change the default by editing the content of the Conference name template field.</p> <ul style="list-style-type: none"> If you can access this VMR via a Virtual Reception then the VMR Name entered here is shown to conference participants as they are transferred into the VMR (it is overlaid onto the <code>virtual_reception_connecting</code> splash screen of the theme associated with the Virtual Reception that is transferring the call).
Description	<p>A description of the Virtual Meeting Room.</p> <p>By default this will say <i>Scheduled Conference booked by</i> followed by the organizer's email address, but you can change the default by editing the content of the Conference description template field.</p>

Option	Description
Owner's email address	<p>The email address of the owner of the VMR.</p> <p>For scheduled conferences, this will be the email address of the person who sent the meeting request.</p>
Scheduling details	
Start time*	<p>This read-only field shows the time at which the scheduled conference will be available for participants to join. This will be the scheduled start time offset by the time specified by the Join before buffer.</p> <p>For recurring meetings, this shows the start time of the current recurrence. Depending on when VMR Scheduling for Exchange has last synced with the Microsoft Exchange server, this could be up to 24 hours in the past or up to 48 hours into the future.</p>
End time*	<p>This read-only field shows the time at which the scheduled conference will no longer be available for participants to join. This will be the scheduled end time plus the time specified by the Join after buffer.</p> <p>For recurring meetings, this shows the end time of the current recurrence. Depending on when VMR Scheduling for Exchange has last synced with the Microsoft Exchange server, this could be up to 24 hours in the past or up to 48 hours into the future.</p>
Next recurrence*	<p>(For recurring meetings only)</p> <p>If the next recurrence is due within the next two days, this read-only field shows the time at which that conference will be available for participants to join. This will be the scheduled start time offset by the time specified by the Join before buffer.</p>
Subject	<p>This read-only field shows the content generated by the Conference subject template field. By default, this is the subject line of the meeting invitation sent by the meeting organizer.</p> <p>Note that if a user updates the meeting subject and re-sends the invitation, the updated subject will not be reflected in the VMR configuration unless the user has also updated the meeting's start or end time.</p>
<p>* For recurring meetings, information is available up to 48 hours in the future. If there are no instances of the recurring meeting scheduled within this time, these fields will show There are no further scheduled recurrences of this conference in the next two days.</p>	
Advanced options	
VMR origin	<p>This read-only field shows the name of the service used to create this VMR. This will be VMR Scheduling for Exchange: followed by the name of the VMR scheduling for Exchange integration being used.</p>
Aliases	
<p> Two aliases are automatically generated for all VMRs created by the VMR Scheduling for Exchange service (for more information, see Scheduling Pexip Infinity meetings using Microsoft Exchange). You must not delete either of these aliases, but you can add additional aliases.</p>	

Viewing all upcoming scheduled meetings

To view all instances of meetings in single-use VMRs that have been scheduled using the VMR Scheduling for Exchange service, log into Microsoft Exchange and view the calendar for the equipment resource. To do this, you first need to assign full access to the equipment resource's mailbox to a delegate account, and then view the mailbox or calendar using the delegate account. (The delegate account could be the service account, or it could be, for example, an administrator's account.)

Troubleshooting

For help with troubleshooting VMR Scheduling for Exchange issues, see [Troubleshooting VMR Scheduling for Exchange](#).

Maintenance and recovery procedures for VMR Scheduling for Exchange

The VMR Scheduling for Exchange feature includes two scripts that can be run from the Management Node to allow you to [restore meetings](#) and to [delete old calendar and mail items](#) from the equipment resource's mailbox.

Running the scripts

To run the scripts, you must log into the Management Node over SSH. To allow this, SSH access must be enabled (**Platform > Global Settings > Connectivity > Enable SSH** and **Platform > Management Node > Enable SSH**).

Log in as **admin**, using the password that was set during initial installation.

Recovering meetings

The scheduling recovery script allows you to reinstate meetings that may have been lost after Pexip Infinity was reinstalled or [restored from a backup](#).

This tool finds **Accepted** scheduled meetings in the Exchange equipment resource's mailbox and checks whether the corresponding VMR exists on the Management Node. If not, it creates the VMR. In doing so it will assign new aliases to the reinstated VMR (since the Management Node will have no record of the previous alias), so it will therefore also send out updated joining instructions to attendees.

To run this script, enter:

```
/usr/bin/schedulingrecovery
```

using the following arguments:

Argument	Description
--config	<p>The file path of the <code>scheduling_config.json</code> file. Unless this has been changed on the advice of your Pexip authorized support representative, it will be the default so does not need to be specified.</p> <p>Default: <code>/etc/pexip/scheduling/scheduling_config.json</code></p>
--exchange-connector-id	<p>The ID of the VMR scheduling for Exchange integration you want to be processed.</p> <p>To process all VMR scheduling for Exchange integrations in the database, do not include this argument.</p> <p>(To find the ID of a particular VMR scheduling for Exchange integration, go to System > VMR Scheduling For Exchange IntegrationS and select the VMR scheduling for Exchange integration. The ID will be the number that appears between the slashes at the end of the URL.)</p>
--time-limit	<p>The date and time after which meetings must start in order to be saved back to Pexip. You must use the format <code>YYYY-MM-DDTHH:MM:SS</code> in UTC.</p> <p>If you do not specify a time then the current time is used, meaning that only meetings happening in the future will be recovered.</p>
--update-message	<p>The message inserted at the top of the email update sent to attendees, which will be followed by the text in the Single-use VMR joining instructions template. This argument supports HTML.</p> <p>Default: "This meeting has updated joining instructions."</p>

Example

To restore all meetings starting after noon on 1 May 2017, enter:

```
/usr/bin/schedulingrecovery --time-limit 2017-05-01T12:00:00
```

Deleting old mailbox items

The scheduling room maintenance script deletes old inbox and calendar items from the equipment resource's mailbox. This may be useful if mailbox space needs to be freed up.

To run this script, enter:

```
/usr/bin/schedulingmaintenance
```

using the following arguments:

Argument	Description
--config	<p>The file path of the <code>scheduling_config.json</code> file. Unless this has been changed on the advice of your Pexip authorized support representative, it will be the default so does not need to be specified.</p> <p>Default: <code>/etc/pexip/scheduling/scheduling_config.json</code></p>
--exchange-connector-id	<p>The ID of the VMR scheduling for Exchange integration you want to be processed.</p> <p>To process all VMR scheduling for Exchange integrations in the database, leave this blank.</p> <p>(To find the ID of a particular VMR scheduling for Exchange integration, go to System > VMR Scheduling For Exchange IntegrationS and select the VMR scheduling for Exchange integration. The ID will be the number that appears between the slashes at the end of the URL.)</p>
--inbox-time-limit	<p>The date and time by which inbox items must have been received, in order to be deleted. You must use the format <code>YYYY-MM-DDTHH:MM:SS</code> in UTC.</p> <p>If you do not specify a time then the current time is used, meaning that all inbox items will be deleted.</p>
--calendar-time-limit	<p>The date and time by which calendar items must finish, in order to be deleted. You must use the format <code>YYYY-MM-DDTHH:MM:SS</code> in UTC.</p> <p>Recurring meeting items are finished only when the last instance in the series has finished.</p> <p>If you do not specify a time then the current time is used, meaning that all calendar items that have already finished will be deleted.</p>

Example

To delete all emails received before noon on 1 May 2017, and all meeting items that finished by this date, enter:

```
/usr/bin/schedulingmaintenance --inbox-time-limit 2017-05-01T12:00:00 --calendar-time-limit 2017-05-01T12:00:00
```

You can use the Pexip VMR Scheduling for Exchange add-in in Outlook to turn any of your new or existing meetings into a meeting that can be held over video or audio in a Virtual Meeting Room (VMR).

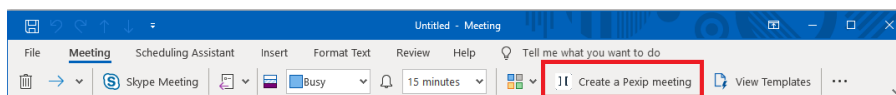
All meetings created in this way will be assigned their own unique VMR which will be created specifically for that meeting. The VMR will have a unique alias, and information about how participants can join the meeting from a variety of video and audio clients will be inserted automatically into the meeting request.

Locating the add-in

The location of the add-in will depend on the Outlook client that you are using - some examples are given below. These examples use the default Pexip names and icons for the add-in, but these may be different in your deployment.

Outlook desktop client (new version)

When creating a new meeting request, select the **Create a Pexip meeting** button in the toolbar:



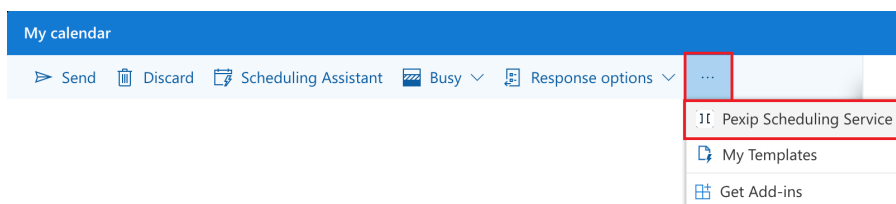
Outlook desktop client

When creating a new meeting request, select the **Create a Pexip meeting** button in the toolbar:



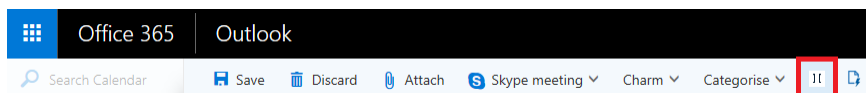
Office 365 (new version)

When creating a new meeting request, select the **More** button in the toolbar and then **Pexip Scheduling Service**:



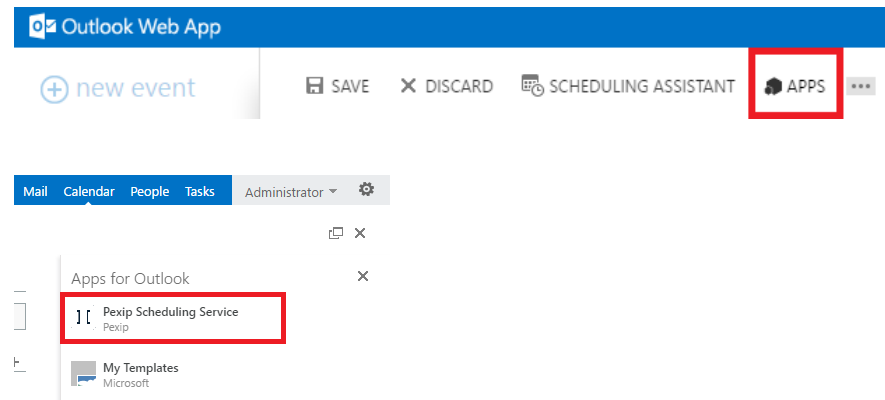
Office 365

When creating a new meeting request, select the **PEXIP Scheduling Service** button in the toolbar:



On-prem OWA

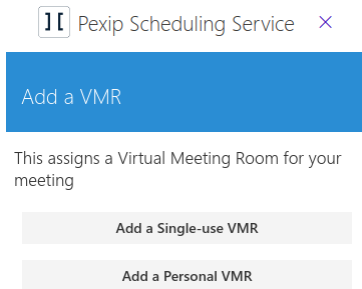
When creating a new meeting request, select the **APPS** button in the toolbar to open the **Apps For Outlook** panel, and then select **Pexip Scheduling Service**:



Creating a new video meeting

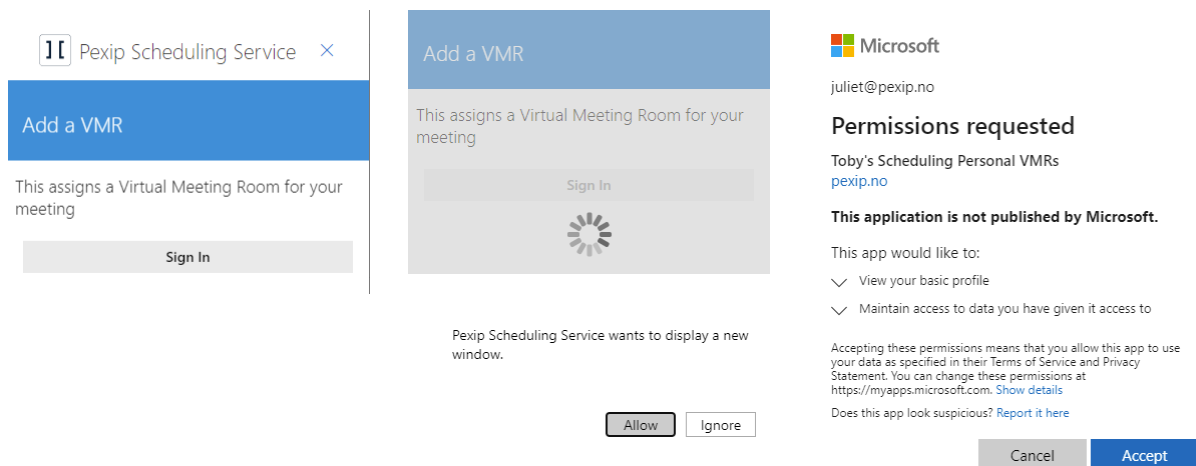
To create a new meeting to be held over video:

1. From your Outlook client, create a new meeting request in your usual way, adding the date, time, rooms and participants as required.
2. Select the [Pexip Scheduling Service add-in](#).
3. If offered a choice, select whether you want to hold the meeting in a **Personal VMR** or a **Single-use VMR**:



Using a personal VMR

The first time you use a personal VMR, you will be asked to sign in using your SSO username and password. You may need to grant the requested permissions:



After you have signed in for the first time, whenever you select a personal VMR (or if that is the only option available to you), details of how to join it will be inserted at the top of the meeting request. Simply add any further information to the meeting request and select **Send**.

If you wish to reschedule or cancel the meeting, you can do this in the usual way by editing the invitation and re-sending it.

Using a single-use VMR

If you have selected a single-use VMR (or if that is the only option available to you), note that the scheduling service uses a special equipment resource (the name of which will depend on your deployment), which will be added to the attendee list, and details of how to join the meeting will be inserted at the top of the meeting request (above any existing text you have already added).

- i** Do not delete the scheduling service equipment resource as an attendee, or edit any of the details in the joining instructions, particularly the text between **PXPS:-** or **TOK:-** and **#**.

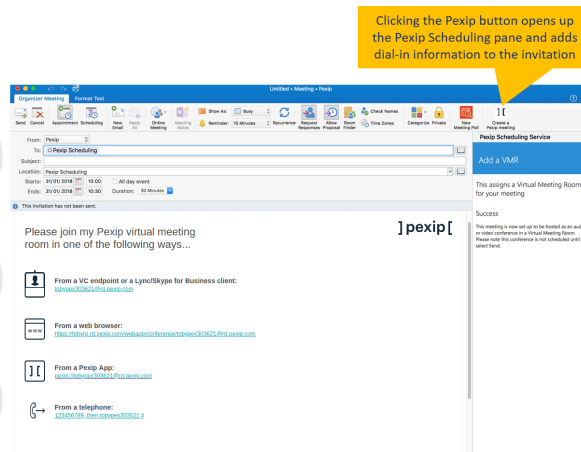
Simply add any further information to the meeting request and select **Send**.

You will soon receive an email from the scheduling service equipment resource accepting the meeting.

You and all other participants will be able to join the VMR at any time between the scheduled start and end times of the meeting. For recurring meetings, you will join the same VMR each time, but it will not be available for use outside of any of the scheduled meeting times.

On the rare occasion that the system is unable to assign a VMR at the point at which you select the **Pexip Scheduling Service** add-in button, the text inserted into the meeting request will state that joining details will be sent in a subsequent email. You should send this request to all attendees as usual. When the system is then able to assign a VMR, a meeting update will be sent on your behalf to all attendees which will include the joining instructions. You will know when this email has been sent because you will receive an updated acceptance email from the scheduling service equipment resource.

- 1 Select the Pexip icon in Outlook to schedule a meeting. Add attendees to invitation as you would for a regular meeting.
- 2 Attendees will receive a meeting invitation containing dial-in information. The dial-in details are for a unique VMR created specifically for that meeting.
- 3 Join the scheduled VMR using any client – H.323, SIP, Skype for Business, Pexip – by dialling in. After the meeting has ended, the unique VMR will be deleted.




Changing an existing meeting into a video meeting

If you want to turn a meeting you have already scheduled into a video meeting hosted in a VMR:

1. From your Outlook client, open the meeting request.

2. [Select the Pexip Scheduling Service add-in.](#)

The scheduling service equipment resource will be added to the attendee list, and details of how to join the meeting will be inserted at the top of the meeting request (above any existing information).

-  Do not delete the scheduling service equipment resource as an attendee, or edit any of the details in the joining instructions, particularly the text between **PXPS:-** or **TOK:-** and #.

3. Make any further changes to the meeting and select **Send**.

The updated meeting request will be sent to all attendees.

You will soon receive an acceptance email from the equipment resource to confirm that the meeting has been successfully scheduled as a video meeting.

Editing or canceling an existing video meeting

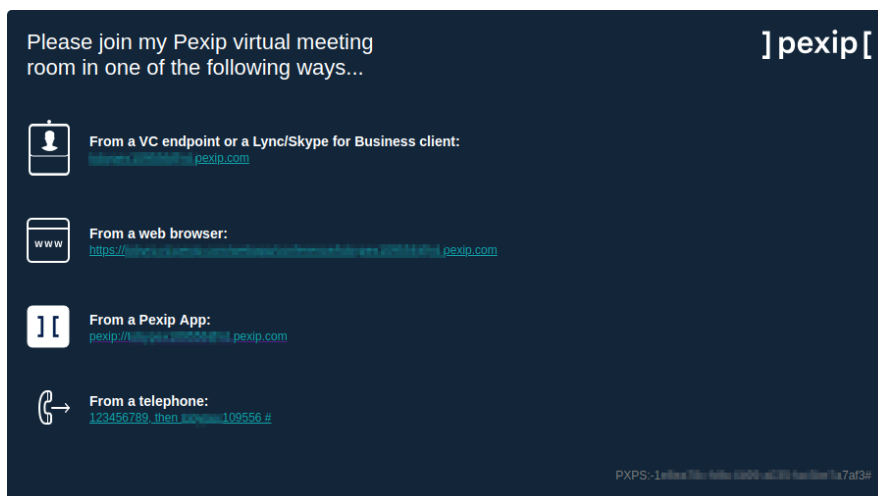
If you want to change the details of an existing video meeting, such as changing its date or time, adding or removing participants, or canceling it completely, you can do this as you would any other Outlook meeting. However, in all cases you must not remove from the attendee list the equipment resource (the name of which will depend on your system's configuration).

If you want to change your video meeting back into a normal meeting, you must cancel the meeting and then re-create it without activating the Pexip add-in.

The `{{alias_uid}}` variable, which inserts the **PXPS:** token, must always be included in the joining instructions.

The images used in these examples are available in the **v22_scheduling.zip** file at <https://dl.pexip.com/resources/icons/>.

Example: dark background with images



To generate the joining instructions shown above, use the following HTML. You must substitute the following:

- **[your link]** with the FQDN of the server on which the images are stored, followed by the directory path to their location
- all **.png** image file names with the names of the images you have uploaded
- **[your number]** with the telephone number used by audio participants.
 - ❗ This can be a direct dial number, or, if the telephone number directs callers to a Virtual Reception, you can include commas (,) after the direct dial number, followed by the conference ID. This will mean that users of devices that support DTMF can click on the link and their device will automatically enter the conference ID after calling into the g Virtual Reception.

```
<br>
<style>
    .pexip-cell {
        padding: 20px;
    }
    .main-title {
        font-size: 22px;
        color: #ffffff;
    }
    .pexip-heading {
```

```

        font-weight: bold;
        font-size: 14px;
        color: #ffffff;
    }
    .pexip-info {
        font-size: 12px;
        color: #02a8ae;
    }
    a:link {
        color: #02a8ae;
    }
    .pexip-pxps {
        font-size: 12px;
        color: #808080;
    }
    .left-column {
        padding: 20px;
        text-align: right;
    }
    .center-column {
        width: 100%;
        padding: 20px 20px 20px 0px;
    }
}
</style>
<table style="width: 100%; border-collapse: collapse; background: #0a2136; border-radius: 5px; font-family: IBM Plex Sans, Calibri, sans-serif, serif;">
    <tbody>
        <tr>
            <td colspan="2" class="pexip-cell" style="vertical-align: top;">
                <p>
                    <span class="main-title">
                        Please join my Pexip virtual meeting<br>
                        room in one of the following ways...
                    </span>
                </p>
            </td>
            <td class="pexip-cell" style="text-align: right; vertical-align: top;">
                
            </td>
        </tr>
        <tr>
            <td class="left-column">
                
            </td>
            <td class="center-column">
                <p>
                    <span class="pexip-heading">
                        From a VC endpoint or a Lync/Skype for Business client:
                    </span>
                    <br>
                    <a href="sip:{{alias}}">
                        <span class="pexip-info">
                            {{alias}}
                        </span>
                    </a>
                </p>
            </td>
        </tr>
        <tr>
            <td class="left-column">
                
            </td>
            <td class="center-column">
                <p>
                    <span class="pexip-heading">
                        From a web browser:
                    </span>
                    <br>
                    <a href="https://{{addin_server_domain}}/webapp/#/conference={{alias}}">
                        <span class="pexip-info">
                            https://{{addin_server_domain}}/webapp/#/conference={{alias}}
                        </span>
                    </a>
                </p>
            </td>
        </tr>
    </tbody>
</table>

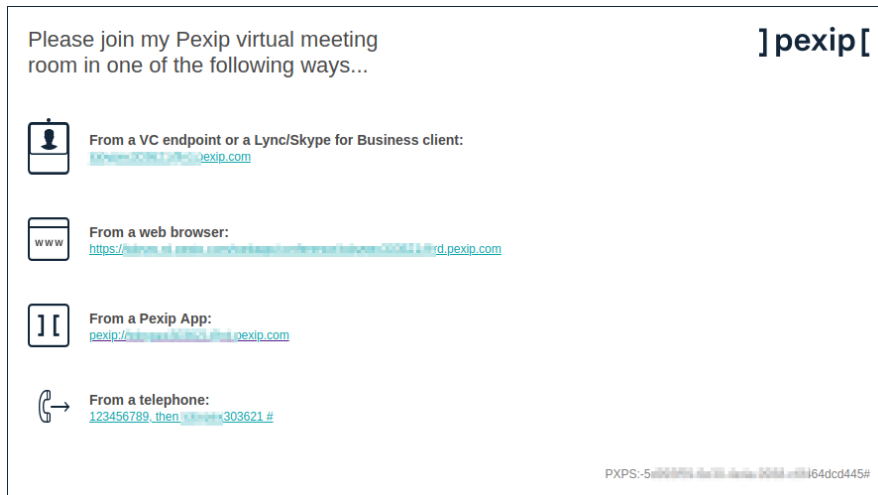
```

```

        </td>
        <td class="pexip-cell"/>
    </tr>
    <tr>
        <td class="left-column">
            
        </td>
        <td class="center-column">
            <p>
                <span class="pexip-heading">
                    From a Pexip App:
                </span>
                <br>
                <a href="pexip://{{alias}}">
                    <span class="pexip-info">
                        pexip://{{alias}}
                    </span>
                </a>
            </p>
        </td>
        <td class="pexip-cell"/>
    </tr>
    <tr>
        <td class="left-column">
            
        </td>
        <td class="center-column">
            <p>
                <span class="pexip-heading">
                    From a telephone:
                </span>
                <br>
                <a href="tel:[your number]">
                    <span class="pexip-info">
                        [your number], then {{ numeric_alias|pex_regex_replace('(\d{3})(\d{2})(\d{3})', '\1 \2 \3') }} #
                    </span>
                </a>
            </p>
        </td>
        <td class="pexip-cell"/>
    </tr>
    <tr>
        <td class="left-column"/>
        <td colspan="2" class="pexip-cell" style="text-align: right;">
            <p>
                <span class="pexip-pxps">
                    {{alias_uuid}}
                </span>
            </p>
        </td>
    </tr>
</tbody>
</table>

```

Example: light background with images



To generate the joining instructions shown above, use the following HTML. You must substitute the following:

- **[your link]** with the FQDN of the server on which the images are stored, followed by the directory path to their location
- all **.png** image file names with the names of the images you have uploaded
- **[your number]** with the telephone number used by audio participants.
 - ❗ This can be a direct dial number, or, if the telephone number directs callers to a Virtual Reception, you can include commas (,) after the direct dial number, followed by the conference ID. This will mean that users of devices that support DTMF can click on the link and their device will automatically enter the conference ID after calling into the g Virtual Reception.

```
<br>
<style>
  .pexip-cell {
    padding: 20px;
  }
  .main-title {
    font-size: 22px;
    color: #4a4a4a;
  }
  .pexip-heading {
    font-weight: bold;
    font-size: 14px;
    color: #4a4a4a;
  }
  .pexip-info {
    font-size: 12px;
    color: #02a8ae;
  }
  a:link {
    color: #02a8ae;
  }
  .pexip-pxps {
    font-size: 12px;
    color: #808080;
  }
  .left-column {
    padding: 20px;
    text-align: right;
  }
  .center-column {
    width: 100%;
    padding: 20px 20px 20px 0px;
  }
</style>
<table style="width: 100%; border-collapse: collapse; border: 1px solid #0a2136; font-family: IBM Plex Sans, Calibri, sans-serif, serif;">
  <tbody>
```

```

<tr>
  <td colspan="2" class="pexip-cell" style="vertical-align: top;">
    <p>
      <span class="main-title">
        Please join my Pexip virtual meeting<br>
        room in one of the following ways...
      </span>
    </p>
  </td>
  <td class="pexip-cell" style="text-align: right; vertical-align: top;">
    
  </td>
</tr>
<tr>
  <td class="left-column">
    
  </td>
  <td class="center-column">
    <p>
      <span class="pexip-heading">
        From a VC endpoint or a Lync/Skype for Business client:
      </span>
      <br>
      <a href="sip:{{alias}}">
        <span class="pexip-info">
          {{alias}}
        </span>
      </a>
    </p>
  </td>
  <td class="pexip-cell"/>
</tr>
<tr>
  <td class="left-column">
    
  </td>
  <td class="center-column">
    <p>
      <span class="pexip-heading">
        From a web browser:
      </span>
      <br>
      <a href="https://{{addin_server_domain}}/webapp/#/conference={{alias}}">
        <span class="pexip-info">
          https://{{addin_server_domain}}/webapp/#/conference={{alias}}
        </span>
      </a>
    </p>
  </td>
  <td class="pexip-cell"/>
</tr>
<tr>
  <td class="left-column">
    
  </td>
  <td class="center-column">
    <p>
      <span class="pexip-heading">
        From a Pexip App:
      </span>
      <br>
      <a href="pexip://{{alias}}">
        <span class="pexip-info">
          pexip://{{alias}}
        </span>
      </a>
    </p>
  </td>
  <td class="pexip-cell"/>
</tr>
<tr>
  <td class="left-column">
    
  </td>
  <td class="center-column">

```

```
<p>
  <span class="pexip-heading">
    From a telephone:
  </span>
  <br>
  <a href="tel:[your number]">
    <span class="pexip-info">
      [your number], then {{ numeric_alias|pex_regex_replace('(\d{3})(\d{2})(\d{3})', '\1 \2 \3') }} #
    </span>
  </a>
</p>
</td>
<td class="pexip-cell"/>
</tr>
<tr>
  <td class="left-column"/>
  <td colspan="2" class="pexip-cell" style="text-align: right;">
    <p>
      <span class="pexip-pxps">
        {{alias_uuid}}
      </span>
    </p>
  </td>
</tr>
</tbody>
</table>
```

Troubleshooting VMR Scheduling for Exchange

This section provides guidance on the troubleshooting of issues with the VMR Scheduling for Exchange feature.

For guidance on the troubleshooting of general issues, see [Troubleshooting the Pexip Infinity platform](#).


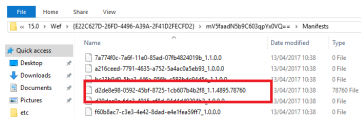
- i** When troubleshooting VMR Scheduling for Exchange issues via the Administrator log and the Support log, search for `User="schedulingsservice"`. This is an internal system user responsible for all configuration changes relating to the scheduling service (such as creating and deleting scheduled VMRs).

Symptom	Possible cause	Resolution
General issues		
Users are able to use the add-in to generate meeting aliases, but when they send the meeting request they get an email response from the equipment resource with the message configured in the Reject invalid alias ID text field. By default this will begin with <i>This meeting request does not contain valid data, and cannot be processed</i> .	The VMR Scheduling for Exchange feature has been enabled on more than one Management Node and both have VMR scheduling for Exchange integrations that are configured with the same equipment resource. This may occur if you have separate test and development environments, each with their own Management Node; you will be prevented from using the same equipment resource for different VMR scheduling for Exchange integrations on the same Management Node.	Ensure that each equipment resource is being used by no more than one VMR scheduling for Exchange integration and no more than one Management Node.
	A user has changed, removed, or added an invalid meeting ID before the meeting has been accepted by the equipment resource. This ID appears in the format <code>PXPS:-<xxx>#</code> or <code>TOK:-<xxx>#</code> .	Remind users that they should not edit or delete this text, and use the add-in to generate it.
	A user has added the equipment resource as an attendee, but without activating the add-in.	Remind users that they must always use the add-in to schedule meetings.
	The Management Node was offline and did not come back online before the security token expired (usually around 8 hours).	Create a new meeting request.
	A user has tried to reschedule a meeting that occurred in the past, but the meeting no longer exists in the database because the scheduling service regularly deletes expired meetings.	Users should create new meetings rather than attempt to reschedule meetings that have occurred in the past.
There is a long delay between a meeting being scheduled and a response being received from the meeting resource.	In deployments where the VMR Scheduling for Exchange feature is receiving consistently high levels of usage (i.e. more than 30 meeting requests per minute), the processing of emails by the equipment resource may be delayed.	The workaround is to: <ol style="list-style-type: none"> 1. Split users into several smaller groups. 2. Create an individual Exchange Integration (with a different equipment resource mailbox) for each group of users. 3. For each Exchange Integration, deploy the add-in manifest file to that specific group of users only.
Users are able to use the add-in to generate meeting aliases, but when they send the meeting request no response is received from the equipment resource.	The scheduling license has expired.	Renew the scheduling license or delete the add-in from the Microsoft Exchange server.
	The equipment resource has been deleted from the meeting request.	Remind users that they must not delete the equipment resource as an attendee.

Symptom	Possible cause	Resolution
When a user attempts to activate the add-in, they get message stating that there was an Invalid Token or Token error.	The FQDN in the security token does not match the FQDN of any of the configured Microsoft Exchange servers. This occurs when not all Microsoft Exchange server FQDNs have been configured under Exchange Metadata Domains and URLs .	Ensure that the FQDN of all Microsoft Exchange servers in your deployment are listed under Exchange Metadata Domains and URLs . This is required even if you are using just one Microsoft Exchange server.
Outlook for Mac users who activate the add-in before they have added any participants to the invitation get the configured Error inserting single-use VMR message . By default this is <i>There was a problem adding the joining instructions. Please try again</i> .	This is a known Microsoft issue and has been resolved in Outlook for Mac version 16.27 (19062615).	As a workaround, until users have upgraded their clients to Outlook for Mac version 16.27 (19062615) and later, users should add at least one participant to the meeting invitation before they activate the add-in.
Users get the configured Error inserting single-use VMR message . By default this is <i>There was a problem adding the joining instructions. Please try again</i> along with <i>The token is not valid until <time> and/or The token is not valid after <time></i> .	(Mac users) There is a known issue with Outlook for Mac where time does not synchronize properly after a user's laptop has been "asleep" for a period of time. The security token has expired, or is not yet valid.	Restart the Outlook for Mac client. <ul style="list-style-type: none">Restart the Outlook client.Check that both the Management Node and the Exchange server are synchronizing their time with an NTP server, and that both systems are showing the same time.
Users who attempt to connect to a VMR get the message "Cannot connect to <alias>. Check this address and try again" or "Invalid conference <alias>".	The VMR was created using the VMR Scheduling for Exchange feature but the user is attempting to connect to it outside of the allowed time (which is the scheduled meeting time plus the configured Join before buffer and Join after buffer).	Remind users that VMRs created using the VMR Scheduling for Exchange feature are only available for use during the scheduled meeting time.
The equipment resource has accepted the meeting but the scheduled conference is not listed on the Management Node (Services > Scheduled Conferences).	The equipment resource has automatically accepted the meeting invitation. This is the default behavior for an equipment resource, but in order for VMR Scheduling for Exchange to process meeting invitations, automatic processing must be disabled.	Disable automatic processing for the equipment resource - see Configuring Exchange on-premises for scheduling .
When Microsoft's OWA is used to connect to an Office 365 account and an add-in is activated, the absence of a horizontal scroll bar in the add-in panel may mean that not all text is visible.	This is a known Microsoft issue.	To view all text, VMR Scheduling for Exchange users should either widen the window or pop-out the meeting request.
Users who attempt to join a scheduled meeting by clicking the link under "From a Pexip App" from within the meeting invite get a Microsoft Outlook Security Notice warning that "This location may be unsafe".	Links to meetings that are to be opened using the Connect desktop app begin with <code>pexip:</code> . However, Outlook does not recognize the <code>pexip:</code> protocol, so it will bring up a warning when a user attempts to open such links.	It is possible to modify the registry to disable warnings for specific protocols. Consult Microsoft support documentation for the appropriate way to do this for your version of Outlook.

Symptom	Possible cause	Resolution
Add-in issues		
The add-in button appears but is grayed out.	Outlook is not connected to the Exchange Server or is running in Offline or Cached mode.	Ensure that Outlook is connected to the Exchange server and is able to send and receive email.
	(Desktop client users) The user is attempting to use the add-in in a calendar to which they have delegate access.	Enable delegate access - for information, see Support for delegate access to calendars Alternatively, users can use the OWA client.
The add-in icon has been changed but the old icon is still showing in Outlook clients, even after deleting the Outlook profile.	The image icons are being cached on the client device.	<ol style="list-style-type: none"> 1. Close the Outlook client. 2. Delete the "Wef" folder which stores the add-in manifests, from the following location: For Windows users: <code>..\Users\<user>\AppData\Local\Microsoft\Office\16.0\Wef</code> For Mac users: <code>../Users/<user>/Library/Containers/com.microsoft.Outlook/Data/Library/Application Support/Microsoft/Office/16.0/Wef</code> 3. Clear the cache in Internet Explorer, ensuring you delete temporary internet files and website files.
The add-in appears for OWA users, but not for desktop client users	Desktop client users' registry settings may be preventing the download and display of the add-in.	<p>Ensure that the users' registry settings include the following settings for <code>downloadcontentdisabled</code> and <code>controllerconnectedservicesenabled</code> (for more information, see Microsoft's documentation):</p> <pre>Windows Registry Editor Version 5.00 [HKEY_CURRENT_USER\Software\Policies\Microsoft\office\16.0\common\privacy] "downloadcontentdisabled"=dword:00000001 "controllerconnectedservicesenabled"=dword:00000001</pre>

Symptom	Possible cause	Resolution
The add-in button does not appear, does not show the correct image and/or there is an error loading the add-in.	<p>The Conferencing Node or reverse proxy specified by the Add-in server FQDN does not have a valid, trusted certificate.</p> <p>To check this, enter the FQDN in a web browser. If the certificate is not valid, a message to that effect will appear.</p>	Ensure that the Conferencing Node or reverse proxy has a trusted, valid certificate.
	<p>The user's device cannot connect to the Conferencing Node or reverse proxy specified by the Add-in server FQDN.</p> <p>To check this, from a web browser on the same device, attempt to connect to:</p> <p><code>https://<Add-in server FQDN>/api/client/v2/msexchange_schedulers/<connector_id>/images/addin_icon_80.png</code></p> <p>where <connector_id> is the ID of the VMR scheduling for Exchange integration on the Management Node. To find the ID, select the VMR scheduling for Exchange integration; the ID is the number that appears between the slashes at the end of the URL. For example, if the URL is</p> <p><code>https://testmgr.example.com/admin/platform/msexchangeconnector/1/</code></p> <p>the ID is 1.</p>	Resolve the connection issue between the user's device and the Conferencing Node or reverse proxy.

Symptom	Possible cause	Resolution
	<p>The add-in XML manifest file being used by the Outlook client is out of date. This may occur if an Administrator has changed the server FQDN or has re-added a VMR scheduling for Exchange integration without then downloading a new XML file and uploading it to Microsoft Exchange.</p>	<p>Ensure that after making any changes to the configuration of a VMR scheduling for Exchange integration on the Management Node, you download a new add-in XML manifest file and then upload the file to Microsoft Exchange.</p>
	<p>(Desktop client users)</p> <p>The add-in XML manifest file has not been received by the Outlook client from the Microsoft Exchange server. To confirm that it has been received:</p> <ol style="list-style-type: none"> From the Exchange admin center, select the Pexip add-in and note the version number:  <ol style="list-style-type: none"> On the user's device, go to the folder for the Outlook manifest files e.g. <code>..\AppData\Local\Microsoft\Office\16.0\Wef\{uuid}\random_string\Manifests\</code> and check whether there is a file that ends with the same number: 	<p>Resolve the connection issue between the Outlook client and the Microsoft Exchange server.</p>
	<p>The add-in was specified as <i>Optional...</i>, and the user has disabled it. To check this for Office 365 users:</p> <ol style="list-style-type: none"> Log into OWA as the user, and then select Settings. Search for Manage Integrations. Select My Add-ins to view the Add-ins page. The Pexip Scheduling Service should be listed here, and shown as On. 	<ul style="list-style-type: none"> Re-enable the add-in. Specify the add-in as Mandatory.
	<p>(Desktop client users)</p> <p>The Outlook email account being used was added manually (rather than via the auto account setup option).</p>	<p>Delete the Outlook email profile and re-add it automatically. Note that DNS must be set up properly to allow the auto-discovery service to work.</p>
	<p>(Desktop client users)</p> <p>The "apps for Office" button has not been enabled.</p>	<p>Ensure that the "apps for Office" button is enabled.</p> <p>Refer to Microsoft's Outlook add-in troubleshooting guide.</p>
	<p>(Desktop client users)</p> <p>The version of Outlook being used is out of date.</p>	<p>Update Outlook to use the latest available version.</p> <p>From Outlook 2016 this can be done via File > Office Account > Office Updates.</p>

Symptom	Possible cause	Resolution
The pop-up window that opens to allow users to authenticate when using personal VMRs does not automatically close after the user has signed in, and instead appears blank.	(OWA users connecting to Exchange 2016 or 2019) This is a known issue with OWA (for more information, see https://github.com/OfficeDev/office-js/issues/1286).	Users can manually close the blank pop-up window and click the sign-in button again. They will not be asked to sign-in again (if they signed in successfully the first time); instead, they will be presented with a list of VMRs to select from, as expected.
OWA users in on-premises Exchange deployments are presented with a message saying that the add-in has been disabled.	Following a recent update to Exchange on-premises, when activating add-ins OWA users are now required to agree that they trust the hosted domain (for more information, see https://github.com/OfficeDev/office-js/issues/1441).	Ensure that your on-premises Exchange servers are updated to the latest Cumulative Update (CU) and run Windows update.
	Other issues not listed above.	Refer to Microsoft's Outlook add-in troubleshooting guide .