



# Configuring Calendar and Contact Integration

- [Configuring Calendar and Contact Integration](#), on page 1

## Configuring Calendar and Contact Integration

### Overview

You can configure calendar and contact integration on Unity Connection with Exchange or Office 365 servers. For more information on calendar and contact integration, see the [Calendar and Contact Integration, page 1-11](#) section.

### Configuring Calendar and Contact Integration with Exchange or Office 365 Servers

1. Review the system requirements to ensure that all the requirements for Exchange 2019, Exchange 2016 and Office 365 are met. For more information see the sections “[Requirements for Accessing Calendar Information for Meetings](#)” and “[Requirements for Accessing Exchange Contact Information](#)” of *System Requirements for Cisco Unity Connection, Release 15* at [https://www.cisco.com/c/en/us/td/docs/voice\\_ip\\_comm/connection/15/requirements/b\\_15cucsysreqs.html](https://www.cisco.com/c/en/us/td/docs/voice_ip_comm/connection/15/requirements/b_15cucsysreqs.html).
2. Configure the Exchange server with which Unity Connection is integrated for calendar and contact integration. See the following sections:
  - [Configuring Office 365, Exchange 2019, Exchange 2016 for Calendar and Contact Integration](#)
  - [Configuring Unity Connection for Calendar and Contact Integration](#)
3. Configure Unity Connection for calendar and contact integration. See the [Configuring Unity Connection for Calendar and Contact Integration](#).
4. (When enabling *Personal Call Transfer Rules* only) Verify that the users or templates are assigned to a class of service that enables them to use the personal call transfer rules feature.
5. Configure the Unity Connection users for calendar and contact integration. See the [Configuring Unity Connection Users for Calendar and Contact Integration](#).
6. Test the calendar integration. See the [Testing Calendar Integration with Exchange or Office 365 Servers](#).

## Configuring Office 365, Exchange 2019, Exchange 2016 for Calendar and Contact Integration

Do the following tasks to configure Exchange 2019, Exchange 2016 for the calendar and contact integration:

1. Confirm that **Client Access role** has been enabled on Exchange 2019 and Exchange 2016 server.
2. Do the [Configuring Exchange 2019, Exchange 2016 for Calendar and Contact Integration](#).
3. (Optional) If you are using SSL for secure access to the Exchange server, follow the steps mentioned in the section [Configuring Secure Access to Exchange Server](#).




---

**Note** If you have already configured secure IMAP with SSL on Exchange server and enabled the certificate for both IMAP and IIS, then follow the section [Configuring Exchange 2019, Exchange 2016 for Calendar and Contact Integration](#).

---

### Configuring Exchange 2019, Exchange 2016 for Calendar and Contact Integration

---

- Step 1** On the Exchange server, open the **Internet Services (IIS) Manager** application.
- Step 2** Go to Internet Information Services > <Exchange server name> > Web Sites > Default Web Site.
- Step 3** Right-click Exchange and select **Properties**.
- Step 4** In the **Exchange Properties** dialog box, select the **Virtual Directory** tab.
- Step 5** From the **Content For This Resource Should Come From** menu, select **A Directory Located On This Computer**.
- Step 6** Confirm the Local Path is set to \\.\BackOfficeStorage\<your-domain.com>\MBX.
- Step 7** Select the **Read** check box.
- Step 8** Select the **Directory Security** tab.
- Step 9** From the **Authentication and Access Control** menu, select **Edit**.
- Step 10** In the **Authenticated Access section of the Authentication Methods** dialog box, check the check boxes for one or more of the following options:
- Integrated Windows authentication (sometimes referred to as NTLM)
  - Basic Authentication
  - Digest Authentication for Windows Domain Servers
- Step 11** Select **OK**.
- Step 12** In the **Exchange Properties** dialog box, select **OK**.
- Step 13** Go to **Internet Information Services > <server name > > Web Service Extensions**.
- Step 14** In the right-hand pane, select **WebDav** and confirm that the status is “Allowed.” If the status is not “Allowed”, click **Allow**.
- Step 15** On the Exchange server, open the **Exchange Management Console**.
- Step 16** Go to **Server Configuration > Mailbox**.
- Step 17** Do the following for each mailbox that you want to configure for the calendar and contact integration:
- a) In the upper middle pane, select the mailbox name.
  - b) In the lower middle pane, select the **WebDav** tab.

- c) Right-click **Exchange (Default Web Site)** and select **Properties**.
- d) In the **Exchange (Default Web Site) Properties** dialog box, select the **Authentication** tab.
- e) Select **Use One or More Standard Authentication Methods** and select the same authentication method(s) that you configured in [Step 10](#).

- Step 18** Click **OK**.
- Step 19** Open the **Exchange Management Shell**.
- Step 20** In the **Exchange Management Shell**, enter the following command:
- ```
iisbreset /noforce
```
- Step 21** Press **Enter**.

---

### Configuring Secure Access to Exchange Server

- Step 1** On the Exchange Server, open the **Exchange Management Shell** application.
- Step 2** Enter the following command, where *<Exchange server>* is the IP address or fully qualified domain name of the Exchange server and *<friendly name>* is the friendly name that you selected for the Exchange server:
- **new-exchangecertificate -generaterequest -domainname <Exchange server> -friendlyname <friendly name> -path c:\csr.txt**
- Caution** The domain name for the Exchange server must be the IP address or the fully qualified domain name (recommended) so that the Unity Connection server can successfully ping the Exchange server. Otherwise, the calendar and contact integration may not function correctly.
- Step 3** Press **Enter**.
- A Certificate Signing Request (CSR) file with the name Csr.txt is created in the root directory.
- Step 4** Send the CSR file to a Certification Authority (CA), which generates and sends back a new certificate.
- Note** You must have a copy of the CA public root certificate or public root certificate chain. This certificate is needed for configuring Unity Connection to trust the Exchange server.
- Step 5** Save the new certificate in a location that is accessible to the Exchange server on which you want to import the certificate.
- Step 6** On the Exchange Server, open the **Exchange Management Shell** application.
- Step 7** Enter the following command, where *<path>* is the full path of the new certificate that you received from the CA:
- ```
import-exchangecertificate -path <path>
```
- Step 8** Press **Enter**.
- Step 9** Enter the following command:
- ```
dir cert:\localmachine\my | fl
```
- Step 10** Press **Enter**.
- Step 11** Highlight the “thumbprint” property and press **Ctrl-C** to copy it to the clipboard.
- Step 12** If Unity Connection is configured to use IMAP to access both email and calendar data from Exchange server, enter the following command, where *<thumbprint>* is the “thumbprint” that you copied in [Step 11](#):
- ```
enable-exchangecertificate -thumbprint <thumbprint> -services "IIS,IMAP"
```

If Unity Connection is not configured to use IMAP but configured to use calendar data from Exchange server, enter the following command, where <thumbprint> is the “thumbprint” that you copied in [Step 11](#):

```
enable-exchangecertificate -thumbprint <thumbprint> -services "IIS"
```

- Step 13** Press **Enter**.
- Step 14** If you want data transmitted as clear text, skip the remaining steps in this procedure and continue with the [Configuring Unity Connection for Calendar and Contact Integration](#). Otherwise, open the **IIS Manager** application.
- Step 15** Go to **IIS** > <server name> > **Web Sites** > **Default Web Site**.
- Step 16** Right-click **Default Web Site** and select **Properties**.
- Step 17** In the **Properties** dialog box, select the **Directory Security** tab.
- Step 18** From the **Secure Communications** menu, select **Edit**.
- Step 19** Check the **Require Secure Channel** check box.
- Step 20** Select **OK**.
- Step 21** In the **Properties** dialog box, select **OK**.

---

## Configuring Unity Connection for Calendar and Contact Integration

- Step 1** In Cisco Unity Connection Administration, expand **Unified Messaging** and select **Unified Messaging Services**. You can modify an existing unified messaging service or create a new service using **Add New**.
  - Step 2** On the New Unified Messaging Service page, in the **Type** list, select **Exchange/BPOS-D** and check the **Enabled** check box to enable the unified messaging service.
  - Step 3** Enter the details of the required fields and select **Save**. (For information on each field, see [Help > This Page](#)).
- Note** Make sure to check the **Access Exchange Calendars and Contacts** check box under **Service Capabilities** menu.
- Step 4** Select **Test** and a message appears indicating whether the configuration has been successfully verified. If the verification fails, follow the above configuration steps to ensure that they have been properly implemented.

---

## Configuring Unity Connection Users for Calendar and Contact Integration

After configuring the Unity Connection server for calendar and contact integration, you can configure the applicable users.



- Note** There must be a user account in Active Directory for each Unity Connection user configured for unified messaging. Also, there must be a corresponding mailbox for each user account in Exchange 2019, Exchange 2016 that communicates with the Unity Connection server.

- 
- Step 1** In Cisco Unity Connection Administration, expand **Users** and select **Users**. Select an applicable user.
  - Step 2** On the Edit User Basics page, in the **Edit** menu, select **Unified Messaging Accounts**.
  - Step 3** On the Unified Messaging Accounts page, select **Add New**.

**Note** Make sure that a unified messaging service is configured before creating unified messaging accounts.

- Step 4** On the New Unified Messaging Accounts page, select the following details:
- In **Unified Messaging Service** drop-down, select the unified messaging service created in the section [Configuring Unity Connection for Calendar and Contact Integration](#).
  - From the **Account Information** menu, in the **Use This Email Address** field, enter the Exchange email address in Active Directory for the user.
- Step 5** In the **Service Capabilities** menu, check the **Access Exchange Calendar and Contacts** check box and select **Save**.
- Step 6** Check the calendar and contact configuration for the user, selecting **Test**. The **Task Execution Results** window appears with the test results. If any part of the test fails, verify the configuration for Exchange 2019, Exchange 2016, Active Directory, Unity Connection, and the user.
- Step 7** Repeat [Step 2](#) through [Step 6](#) for all remaining users.
- 

## Testing Calendar Integration with Exchange or Office 365 Servers

---

- Step 1** Sign in to Outlook.
- Step 2** On the **Go** menu, select **Calendar**.
- Step 3** On the **File** menu, select **New > Meeting Request**.
- Step 4** Enter values in the required fields to schedule a new meeting for the current time, and invite a user who has an account on Unity Connection. Select **Send**.
- Step 5** Sign in to the Unity Connection mailbox of the user that you invited to the Outlook meeting:
- If the user account is configured for speech access, say **Play Meetings**.
  - If the user account is not configured for speech access, press **6**, and then follow the prompts to list meetings.

Unity Connection reads the information about the Exchange 2019, 2016 meetings.

---

