Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

Tele2 Växel

Exchange calendar integration – deployment information

TELE2
FÖRETAG

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

Innehåll

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

For whom is this document

This document is aimed at personnel administrating the Calendar integration service in the company and personnel responsible for the Microsoft Exchange Server or Office 365 solution.

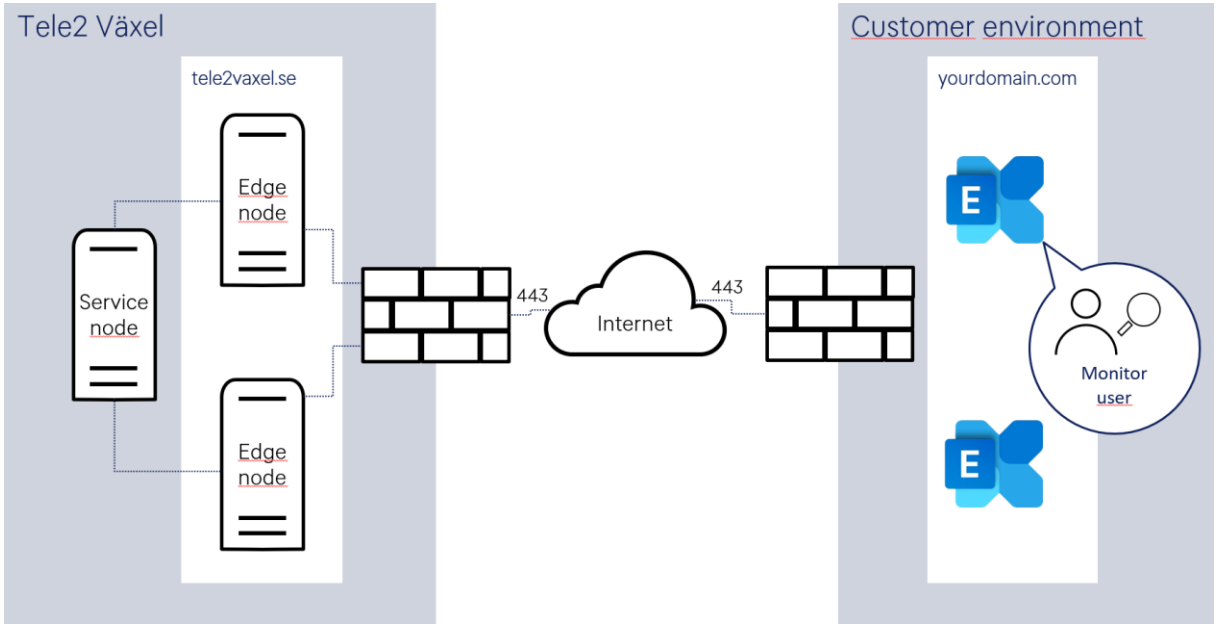
We assume that you already understand how users and service configuration works within the Calendar integration solution, as well as configuration in Microsoft Exchange or Office 365, and have administration rights on the Microsoft Exchange Server or in Office 365.

The intention of this document is to provide setup instructions and configuration guidance to enable the presence synchronization service. This document does not cover all possible situations, ways of setting the service up or possible complications, but aims to give initiated professionals an introduction in setting up the Microsoft Exchange Server for interaction with the Tele2 Växel Calendar integration service.

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

1. How the integration works

Communication with Microsoft Exchange Server / Office 365 occurs through Exchange Web Services over the edge nodes in Tele2 Växel. The edge node will establish connections with the specified Microsoft Exchange Server environment over encrypted HTTPS connections using standard port 443. Therefore, the enterprise firewall must be configured to allow inbound connections from any of the edge nodes in Tele2s edge node cluster towards all necessary exchange servers within the enterprise.



It is recommended that the firewall resolves the inbound connection source IP-address against the tele2vaxel.se domain. This is because the connections will originate from different edge nodes, from different IP-addresses from time to time.

In larger Microsoft Exchange Server installations, auto-discover may be used to eliminate the question of which server a user's calendar is currently hosted on. Tele2 Växel will then send an auto-discover request to autodiscover.yourdomain.com. If this shall be used, this address must be specified in the public DNS of the organization.

Once the Microsoft Exchange Server connector and synchronization policy service are configured in the Customer's organization in Tele2 Växel, it will start to fetch upcoming user calendar events at regular intervals.

The connector uses the credentials (username and password) of a monitor user in Exchange / Office 365, the monitor user is authorized access to the calendars of the users.

The integration uses information from synchronized calendar events to create *future presence* events in Tele2 Växel using a presence synchronization mapping; therefore, the monitor user must be authorized to get information from certain fields from all relevant calendars and users. It is for example possible to

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

only give authorization to Availability, but that reduces the users' available options to control the experience.
As the calendar information will be stored in Tele2s servers, a granular policy limiting the access to calendar subjects for individuals with particularly sensitive events can generally be recommended. It is also recommended to authorize the monitor user access only to users that shall use the calendar integration – and not the entire company, for example by basing the authorization on users belonging to a DistributionGroup.

The following information can be used:

• Subject - The subject text of the calendar event.
Used to set different presence states and other settings based on expressions in the subject text, such as setting Lunch presence for events containing "lunch" or to exclude events containing a specific expression (standard "##")

• Privacy - Information if the event is marked as private or public.
As standard, the synchronization is set to exclude private events.

• Location - The text in the location field for the event.

• Availability - The availability information for the event such as Free, Tentative, Busy, Out of Office

When the calendar event starts, the user presence is changed according to the synchronization policies. In the case a user has multiple parallel calendar events the event with the nearest end time will be used for matching.

Once the end-time for the calendar event has passed, the presence will be reset to the state it had before the automatic presence change. If a user manually changes a presence state that has been set automatically during an ongoing calendar event, this state will remain and not be automatically changed at the end-time of the event.

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

1.1 Presence synchronization policy

Default settings for the synchronization of calendar events to presence are the following, prioritized in descending order as below. The policy is set up by Tele2 during implementation:

Type	Matching on	Activity	Role
Subject	*semester*	Semester	No change
Subject	*sjuk*	Sjuk	No change
Subject	*vab*	VAB	No change
Subject	*möte*	Möte	No change
Subject	*lunch*	Lunch	No change
Subject	*upptagen*	Upptagen	No change
Subject	*frånvarande*	Frånvarande, Gått för dagen or Inte på kontoret	No change
Availability	Out of office	Frånvarande, Gått för dagen or Inte på kontoret	No change
Availability	Busy	Möte	No change

1.1.1 Exclusions

The following attributes will exclude the event from the mapping:

Availability	Tentative
Private	X
Availability	Free
Subject	*##*

The mapping can be adjusted by an organization administrator, see the Tele2 Växel administrator's manual for more information.

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

2. Firewall settings and security

To establish the required communication with the Calendar integration Solution, it is recommended that the EWS (Exchange Web Services) is published on port 443 externally and not blocked by firewalls or other obstructions.

However, the firewall may be configured to only allow access to EWS from IP-addresses within Tele2 Växel. For the latest information, please see the Tele2 Växel Firewall settings document at:

http://www.tele2.se/globalassets/foretagssektionen/pdf/vaxel/tele2-vaxel-firewall-settings.pdf

The calendar integration may be set up using Basic Authentication or NTLM for Exchange Server (on-premise) and using OAuth 2.0 for Office 365.

The presence synchronization is one way. Calendar event details are read from the Exchange service, but Tele2 Växel will never update calendar events in Exchange based on any presence changes in Tele2 Växel.

Tele2 Växel will only fetch calendar events from users that have the calendar integration license activated.

In large organizations where a shared Exchange environment is used for calendar integration for multiple Tele2 Växel organizations, it is recommended to setup separate monitor users with granular access to only the relevant users for each organization.

Please find additional security recommendations in section **Error! Reference source not found.**. **Error! Reference source not found.**

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

3. Setting up the Exchange synchronization

Different localizations of Microsoft Exchange Server will have translated terms. For example, "Calendar" is called "Kalender" in Swedish and "Calendrier" in French. These differences in terminology must be considered when performing the following steps.

3.1 Microsoft Exchange Server 2010, 2013, 2016 and 2019

To configure the calendar synchronization in Exchange, go through the following steps:

1. Verify that you have a public DNS record pointing to the exchange server from public Internet, for example by resolving **yourdomain.com**.
   - ❑ Done
2. Verify that the enterprise firewall is configured to allow inbound HTTPS connections, using TCP port 443 from all edge nodes, resolved from **tele2vaxel.se**, to all exchange servers deployed for the relevant users in the organization.
   - ❑ Done
3. Access Windows PowerShell in the exchange server and prepare a password string to be used to create a monitor user with the password <your Password>. This command creates a secure string that will be used later in the script. Password length can be maximum 64 characters. First, setup the password securely with the command:
   ```
   $Password = "your Password" | ConvertTo-SecureString -AsPlainText –Force
   ```
   - ❑ Done
4. Run the command below to setup the user <Monitor>, using the password string created in step 3. This command creates a new user and enables a mailbox. Username length can be maximum 64 characters. The command to enable an existing user would be Enable-Mailbox:
   ```
   New-Mailbox -Name "Monitor" -Alias "Monitor" -OrganizationalUnit
   domain/Users'-UserPrincipalName monitor@yourdomain.com
   -SamAccountName "monitor" -FirstName "yourFirstName" -LastName "Monitor"
   -Password $Password -ResetPasswordOnNextLogon $false
   -Database "yourStorageGroup\yourDatabase"
   ```
   - ❑ Done
5. Get the mailbox of your monitor-user:
   ```
   $User = Get-Mailbox Monitor
   ```
   - ❑ Done
6. Create a variable with the mailboxes to be administered by using:
   ```
   $Mailboxes = Get-Mailbox -ResultSize Unlimited
   ```
   - ❑ Done

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

7. Set rights on every mailbox in the variable by using the following. Please keep in mind that the Calendar folder will be named differently in translated editions of Microsoft Exchange Server:
```
$Mailboxes | ForEach-Object { Add-MailboxFolderPermission -identity $_:\Calendar -User $User.identity -AccessRights Reviewer }
```
   ❑ Done

3.2 Office 365

Make sure that you have Administrator access rights before attempting to set up Microsoft Exchange Server access rights.

To configure the calendar synchronization for Microsoft Exchange Server in Office 365, you need to use the Windows PowerShell on your local computer to create a remote session:

1. Start Windows PowerShell, run as administrator.
   ❑ Done

2. Make sure that the Execution policy is set to Remote Signed, use the following:
```
Get-ExecutionPolicy
Set-ExecutionPolicy RemoteSigned
```
   ❑ Done

3. Create a credential object with Administrator rights credentials in Office 365. Use the following:
```
$UserCredential = Get-Credential
```
   ❑ Done

4. Create a session to Office 365 by connecting to https://outlook.office365.com/powershell-liveid/ with the previously mentioned credentials. Use the following:
```
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential $UserCredential -Authentication Basic –AllowRedirection
```
   ❑ Done

5. Import the session into your present Windows PowerShell-session, by using the following:
```
Import-PSSession $Session
```
   ❑ Done

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

3.2.1 Setting up Office 365 monitor user

Calendar rights of the monitor user must be configured on a per-user basis. A script will be created to iterate through all users and avoid a lot of tedious and repetitive rights management. The example below assumes that the monitor user is called "Monitor":

1. Get the mailbox of your monitor-user:
   ```
   $User = Get-Mailbox Monitor
   ```
2. Create a variable with the mailboxes to be administered by using:
   ```
   $Mailboxes = Get-Mailbox -ResultSize Unlimited
   ```
3. Set rights on every mailbox in the variable by using:
   ```
   $Mailboxes | ForEach-Object { Add-MailboxFolderPermission -identity
   $_:\Calendar -User $User.identity -AccessRights Reviewer }
   ```
   Please keep in mind that the the Calendar folder will be named differently in translated editions of Microsoft Exchange Server

3.2.2 Configure OAuth2 Authentication

Make sure that you have Administrator access rights and can access the Azure Active Directory admin center.

To configure the calendar synchronization to use OAuth2-based authentication, you need to give permission to the exchange synchronization application for it to be able to read the users' calendars:

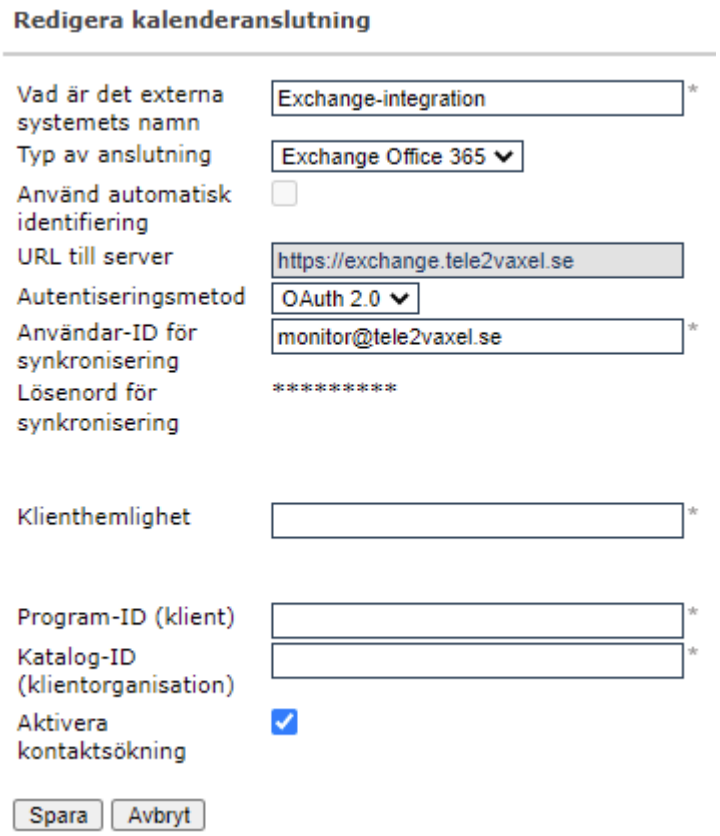
1. Sign in to https://aad.portal.azure.com/
2. Go to the **Azure Active Directory**.
3. Navigate to **App registrations**.
4. Choose **New registration** and name the new application, for example, *Exchange calendar synchronization* and then select **Register**.
5. Note the **Application (client) ID** and the **Directory (tenant) ID**.
6. Navigate to **Certificates & Secrets**.
7. Choose **New client secret** and name the secret, for example, *Exchange calendar synchronization secret* and select expires **Never**.
8. Copy the generated secret to a safe place. The secret together with the Application (client) ID and Directory (tenant) ID will need to be entered in the Calendar Connector setting page when configuring the connector. Share with Tele2 if Tele2 is involved in the implementation process.
9. Navigate to **API permissions**.
10. Choose **Add a permission** and then select **Microsoft Graph**.
11. Select **Application permissions** and then choose **Calendars.Read**.
12. Select **Grant admin consent for** *{your company}*.
13. Follow the instruction in the new window.
14. Wait for **Status** in the **Configured Permissions** window to turn green.

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

3.3 Configure Contacts Search for Microsoft Exchange in Office365 using OAuth2 Authentication

Follow the steps as described in **3.2.2 Configure OAuth2 Authentication** and select **Contacts.Read** in **Application permissions** as part of step 11.

Enter the authentication information in the Calendar connector in Tele2 Växel under Organization – Calendar connectors / Organisation – Kalenderanslutningar.



a. Set Authentication method / Autentiseringsmetod to OAuth 2.0
b. Enter Client secret (Klienthemlighet)
c. Enter Application (client) ID / Program ID (klient
d. Enter Directory (tenant) ID / Katalog-ID (klientorganisation)

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

4. Testing and troubleshooting

4.1 Create a test event

Create a calendar event that matches the presence synchronization policy.

The future presence view in the Softphone, web interface and mobile app reads the calendar events in real time when viewed. It can be used to verify that the integration is working.

The synchronization engine that changes presence automatically is synchronizing at regular intervals. This means that an event can be visible in the future presence view, but if it is created too close before the start time, the user's presence might not be changed when expected.

An easy way to check that Microsoft Exchange Server EWS (Exchange Web Service) is configured correctly is to use the E-mail AutoConfiguration tool in Outlook. It will attempt to establish a connection and log the results.

4.2 Test your connectivity

At https://testconnectivity.microsoft.com/ under *Microsoft Exchange Web Services Connectivity Tests* in the Exchange Server or Office365 tabs you can perform the *Synchronization, Notification, Availability, and Automatic Replies* test using the monitor user credentials.

4.3 Troubleshooting

If events are not synchronized, validate the following:

- The Firewall is properly configured allowing inbound TLS connections on port 443.
- The public DNS is properly configured.
- The monitor user is properly set up and granted access to the calendars to be synchronized.
- The IIS settings for "Basic authentication" is set to "Enabled" if Basic authentication is to be used.

The default location for the Exchange logs is:

```
EventViewer\Application and <ExchangeInstallDir>\Logging
```

IIS logging is in:

```
%SystemDrive%\inetpub\logs\LogFiles
```

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

5. Script example

Here is an example of a PowerShell script that can be scheduled via Task Scheduler, that automates the rights management for new Exchange users.

The code example requires the users to be members of an Exchange group, for which the monitor user is authorized with read access to the calendars. Customizations to fit local prerequisites are needed.

```
### Create a log file
$LogPath=Get-Date -UFormat "%Y-%m-%d-%H%M-%S"
$Path="D:\PSscripts\T2VaxelCalInt\Logs\"+$Logpath+"\"
New-Item -Path $Path -ItemType directory
start-transcript -Path $Path"scriptlog.txt"

Set-ExecutionPolicy remotesigned -Confirm:$false

### Login to O365
#Retrieve stored credentials for a system account with Global admin rights
to manage your tenant
$Uname = cat ("D:\PSScripts\o365-systemaccountUser.txt")
$pwd = cat ("D:\PSScripts\o365-systemaccountPass.txt") | ConvertTo-
SecureString
$LoginCred = New-Object -TypeName System.Management.Automation.PSCredential
-ArgumentList $Uname,$pwd
$Session = New-PSSession -ConfigurationName Microsoft.Exchange -
ConnectionUri https://outlook.office365.com/powershell-liveid/ -Credential
$LoginCred -Authentication Basic -AllowRedirection
import-pssession $Session

### Input generator
# All users that will be using Tele2 Växel should be member of the group
listed below.
$Users=Get-DistributionGroupMember -Identity "T2VaxelO365CalendarAccess"
Foreach ($User in $Users){
$CalFoldername=Get-MailboxFolderStatistics $User.Name| Where-Object
{$_.FolderType -eq "Calendar"} | Select -ExpandProperty name
Add-MailboxFolderPermission -Identity ${User}:\$CalFoldername -User [enter
the account name of the monitor user for the  Tele2 Växel calendar
integration here] -AccessRights Reviewer
}

### stop logging
Write-host "stop logging`n"
```

Tele2 Sverige AB
Box 62
164 94 Kista
Telefon 90 444
tele2.se

```
### Logoff from O365
Write-host "logging off`n"

Remove-PSSession $Session
```