for Microsoft

Quick Install Manual
OnTime® for Microsoft version 6.4.x

Revision 10

IntraVision

OnTime® for Microsoft

This Quick Install guide is the fast track to install OnTime for Microsoft.

Additional information is available in the *OnTime for MS – Installation & Configuration Guide.*

Table of Contents

About OnTime® for Microsoft

This ‘quick install guide’ describes the fewest possible steps to make the OnTime Group Calendar available for web and mobile users.

Preparing the new OnTime installation

Server requirements

The OnTime installation is supported on
- Windows Server 2019/2022/2025 with Microsoft SQL Server® 2019/2022/2025 Express

OnTime must be installed running as a Windows administrator.

For small and middle-size installations of OnTime, You may use Microsoft SQL Server® 2019/2022/2025 Express which is free.

It is recommended using the full Microsoft SQL Server if your OnTime installation has more than 2.000 users.

Processor

- Intel-compatible processor with a minimum speed of 2 GHz or a faster processor

RAM

- Minimum of 8 GB Ram dedicated to the OnTime solution
- If you are running OnTime on a Hyper V configuration, then you need to configure it to use static memory for the SQL Server to perform properly.

Hard Disk Space

- Minimum of 20 GB hard drive dedicated to the OnTime solution

Typical 500 users install

- Intel-compatible processor with a minimum speed of 2 GHz or a faster processor
- Minimum of 8 GB Ram dedicated to the OnTime solution
- Minimum of 20 GB hard drive dedicated to the OnTime solution

Ports for the OnTime server

The ports 80 and 9080 are required open for HTTP data.
The ports 443 and 9443 are required open for HTTPS data.
The port 8080 is required for the admin client, http is only supported for localhost.
The port 8443 is required for the admin client, https is supported remotely

Ports for Microsoft 365

If OnTime configuration for Microsoft 365, check ports outwards through the firewall (port 443) from the OnTime server:
https://login.microsoftonline.com
https://graph.microsoft.com
https://portal.azure.com

Prerequisites

AD domain

The OnTime server can be part of your user AD domain to ensure your OnTime users web authentication (SSO) without providing their AD password.
An OnTime server installed in a Windows ‘Workgroup’ is supported. IIt is expected the Workgroup server to be dedicated to OnTime because this will be more secure. The name of the workgroup must be descriptive. Workgroup names like 'Workgroup' or 'Workgroup01' will not be accepted.

SQL 2019/2022/2025 Express or an existing MS SQL Server must be available.

The SQL Server Express may be downloaded from Microsoft. It is free.
Limitations: Microsoft SQL Server Express supports 1 physical processor, 1 GB memory, 10 GB storage.

Create an Impersonation User in MS Exchange/Microsoft 365

a. Mailbox user (minimum type 1 if in Microsoft 365).
b. Assign the user to the “ApplicationImpersonation Role”.

License key

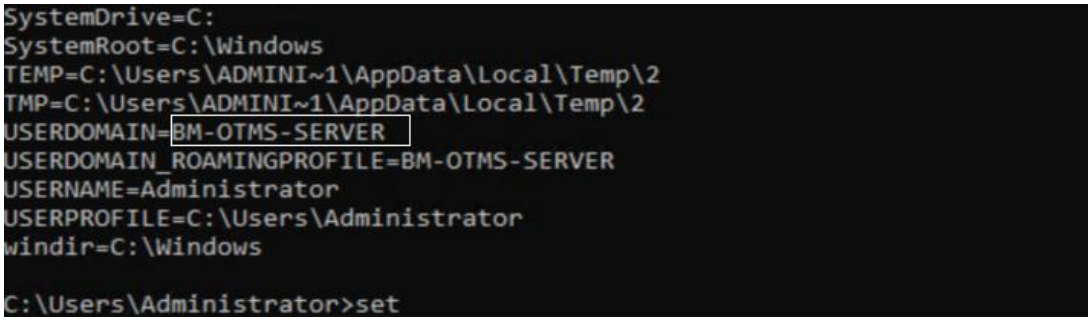
- OnTime requires a license key with the required number of users enabled to run.
- These keys are delivered directly by IntraVision or an OnTime Partner.
- A list of OnTime Partners is available at www.ontimesuite.com.

For obtaining a license key, provide the following info:

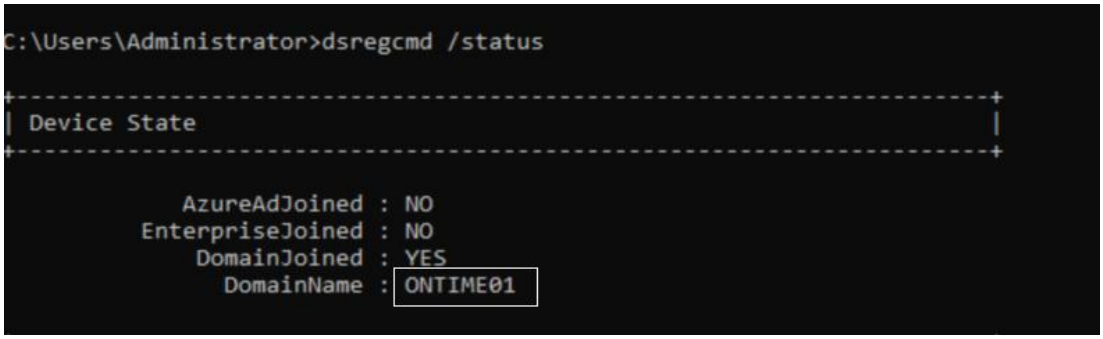
- your Company name
- total number of users, including rooms and equipment
- a. OnTime server in an AD domain,

  check your OnTime server's environment by logging in as a domain user.

  In a Command prompt > set (Enter) – to see your **'USERDOMAIN'** to see your device name



  In a Command prompt > **dsregcmd /status** (Enter) – to see your domain name



  b. OnTime server in a workgroup, check your Workgroup name.

  Enter 'net config workstation' in a Command prompt to see your 'Workstation domain' (Workgroup name).

- If you are running a trial installation, a time-limited, fully functional key should have been provided for you when you downloaded the OnTime software from www.ontimesuite.com.

OnTime Installation

Quick installation

Quick installation requires:

- SQL Server being installed on the same machine as the OnTime distribution

- Integrated Security is used, instead of SQL Server Security

- Port number for SQL Server is 1433

If you want to change anything of the above, you should do the manual setup of the database.

An MS SQL Server 2019 Express with scripts for a silent install may be downloaded from this download link:
SQL Server 2019 Express

An MS SQL Server 2022 Express with scripts for a silent install may be downloaded from this download link:
SQL Server 2022 Express

An MS SQL Server 2025 Express with scripts for a silent install may be downloaded from this download link:
SQL Server 2025 Express

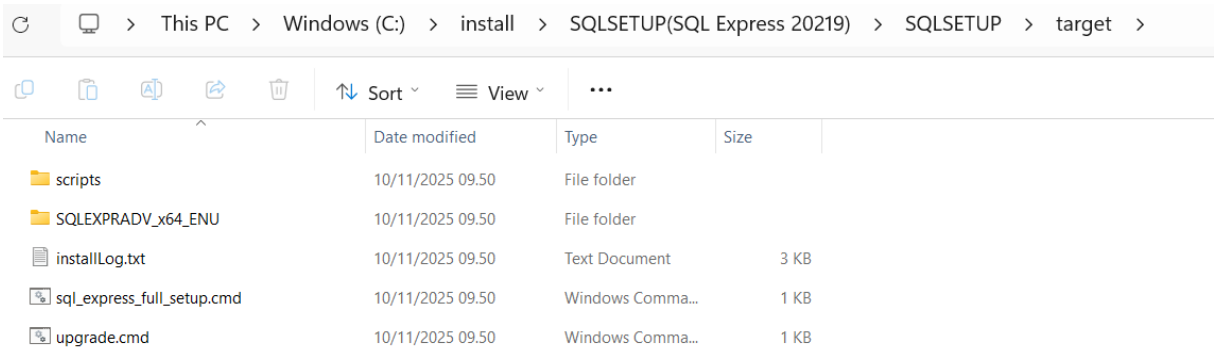
Note: SQL Server 2025 Express is supported only with **OnTime 6.4.2 or later**. Earlier versions of OnTime do not support SQL Server 2025 Express.

The tool to inspect the databases in the Microsoft 'SQL Server Management Studio' (SSMS). Currently, a link to download the tool from Microsoft:
https://docs.microsoft.com/en-us/sql/ssms/download-sql-server-management-studio-ssms

It is the default installation with a local SQL Server, installed at C:\Program Files\Microsoft SQL Server

Installing the SQL Server Express

Extract the file downloaded from SQL Server 2019 Express



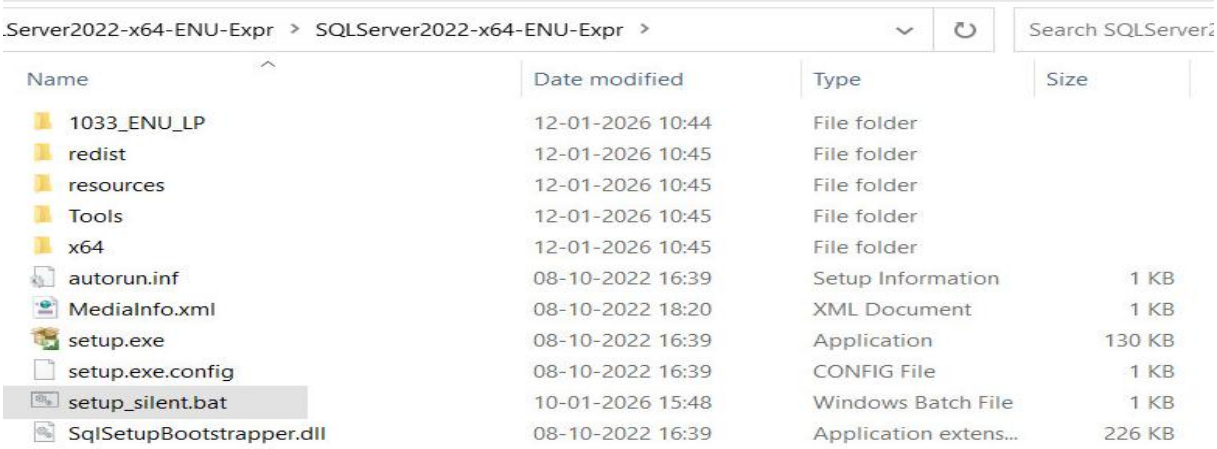
To install the SQL server, start a Command Prompt in administrator mode in the OnTime (silent) folder.

Run the command:
sql_express_full_setup.cmd

This command will silently install the SQL server.
A log file, 'installLog.txt' from the installation is created in the folder.

Result:
The SQL Server is installed in the default path, C:\Program Files\Microsoft SQL Server.
It is installed with 'Windows Authentication', 'Integrated Security' is used
- and TCP/IP is enabled and listening on port 1433

Extract the file downloaded from [SQL Server 2022 Express]

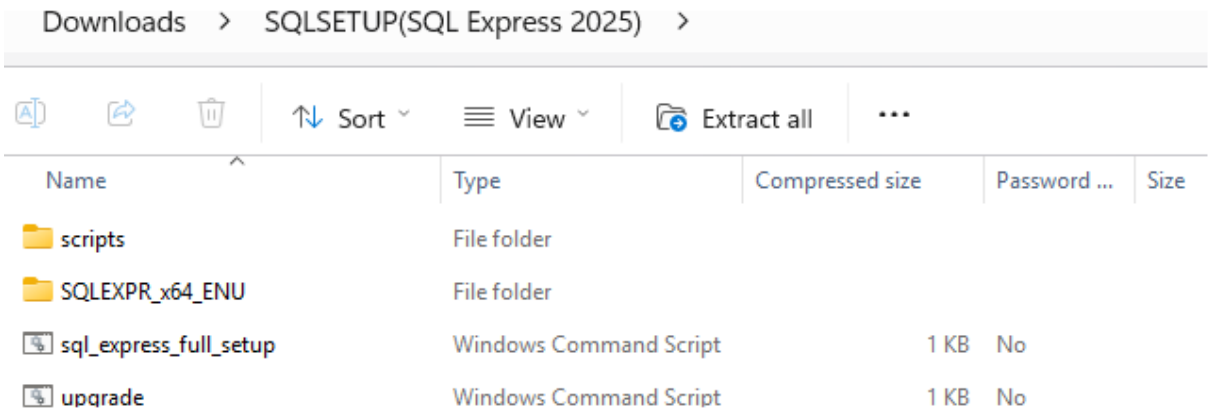


To install the SQL server, start a Command Prompt in administrator mode in the OnTime (silent) folder.

Run the command:
setup_silent.bat

This command will silently install the SQL server.
A log file, during installation is created in the folder: 'C:\Program Files\Microsoft SQL Server\160\Setup Bootstrap\Log'

Extract the file downloaded from [SQL Server 2025 Express]



To install the SQL server, start a Command Prompt in administrator mode in the OnTime (silent) folder.

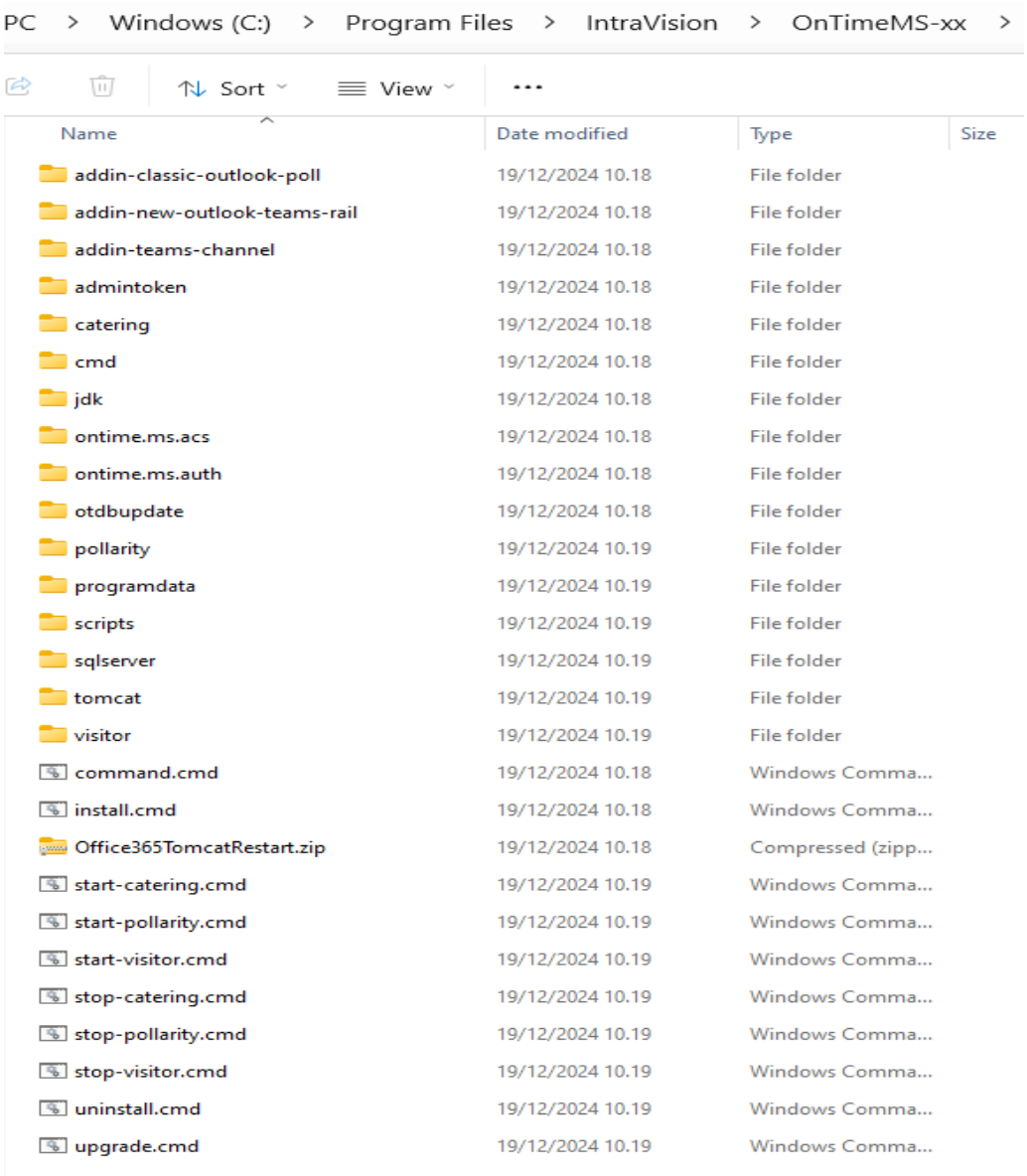
Run the command:
sql_express_full_setup.cmd

This command will silently install the SQL server.
A log file, during installation is created in the folder: 'C:\Program Files\Microsoft SQL Server\170\Setup Bootstrap\Log'

Result:
The SQL Server is installed in the default path, C:\Program Files\Microsoft SQL Server.
It is installed with 'Windows Authentication', 'Integrated Security' is used
- and TCP/IP is enabled and listening on port 1433

Install OnTime

Extract the downloaded OnTime package to a temporary location and then move the folder “OnTimeMS-x.x” to the recommended path: C:\Program Files\IntraVision\



Right-click ‘install.cmd’ and choose ‘Run as Administrator’

This command will do the following things:

1. You are asked to enter a new password for the OnTime admin
2. It will create a database, ‘ontimems’, for OnTime use in the local SQL Server
3. It will configure the user NT AUTHORITY\USER as a user in the ontimems database with the api_role
4. It will install a Windows service ‘OnTimeMS Auth’ that offers Windows domain logon authentication for web users, SSO – Single Sign On
5. It will install the Tomcat web server used for OnTime
6. Create a database for Pollarity
7. **Note:** Pollarity has an optional License.
8. Create a database for Catering
9. **Note:** Catering has an optional License.
10. Create a database for Visitor
11. **Note:** Visitor has an optional License.

OnTime Configuration

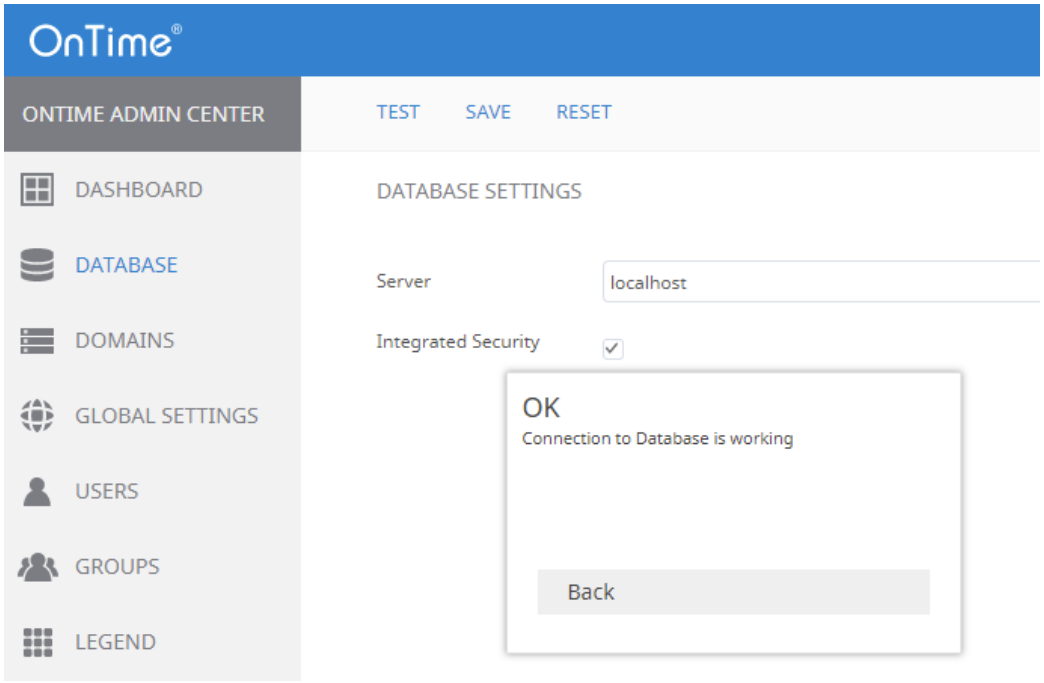
From a browser - Open the administration URL – for example:
https://ontime.example.com:8443/ontimegcms/admin
Note: Insert your relevant URL instead of 'ontime.example.com'.

In the initial OnTime setup phase you may run administration without certificates locally at the OnTime server with http and port 8080 for the apache Tomcat.
http://127.0.0.1:8080/ontimegcms/admin

Administrator:	admin	(beware of casing, no capitals)
Password:	*******	(the password from your installation phase)

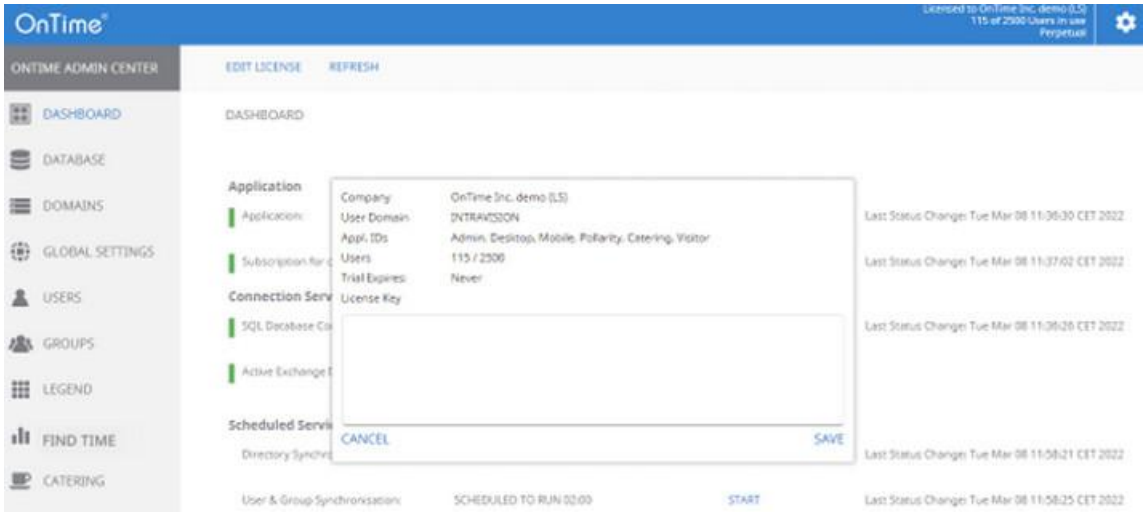
Database

In the web admin interface, “OnTime Admin Centre”, click “Database”.
Click “Test” in the upper menu line to test the database connection.
Upon the response “OK Connection to Database is working” click “Back”.
Click Save.



License key

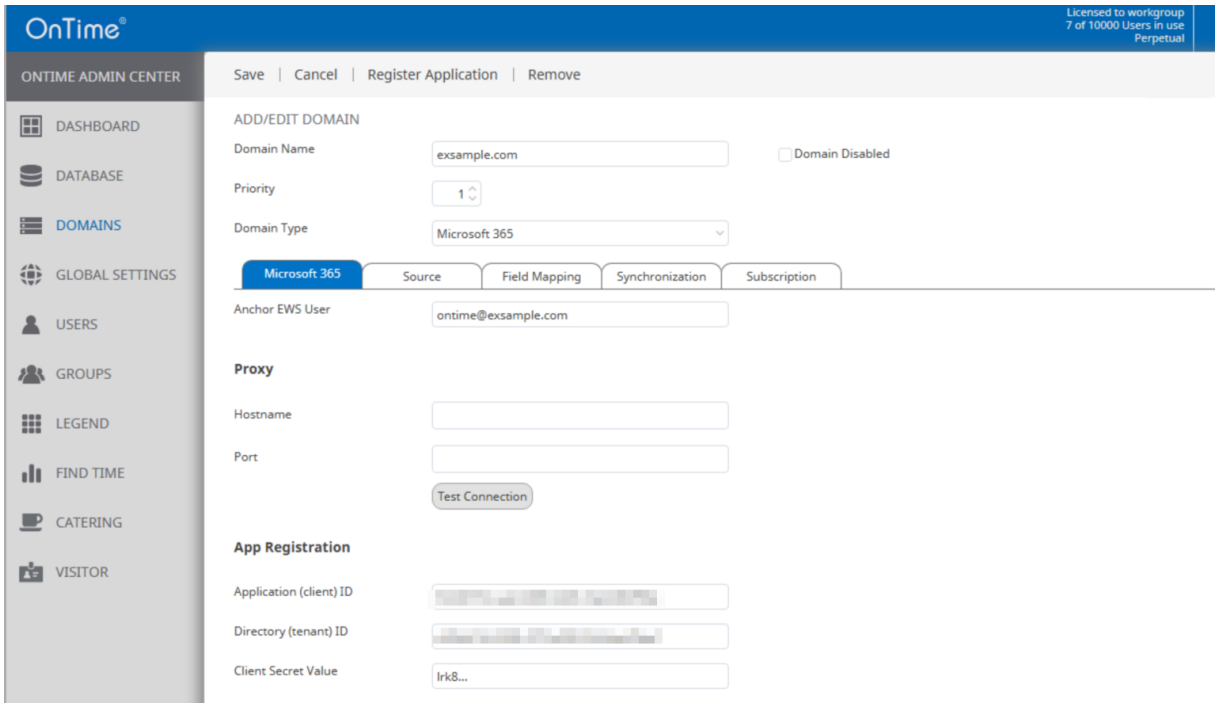
Click ‘Dashboard’
– Enter your license key by clicking ‘License’ in the upper right corner of the dashboard. Click ‘Save’



In the Dashboard click 'stop/start' the application.
Note: When you see the Connection/Database Service “Running” (green), press ‘F5’ to refresh the whole web page from the new database.

Domain settings

Click ‘Domains/Create New’ to configure your Exchange environment.



Domain name is a text field for naming your domain setup.

Priority - is for prioritising the users in OnTime. Priority ‘1’ is the highest priority.

Domain Type – 'Microsoft 365'.

Microsoft 365 configuration, Authentication

Authentication Type: Modern Method (OAuth – Client Credentials).

Anchor EWS User - is a user required only for technical purposes.
EWS API fails when a user is not provided for a call. And if some calls have an explicit user - such as list of appointments, others don't - such as getting a server timezone list. To have at least some user in the call, so that EWS does not fail we introduced an anchor user, which is simply a valid user and has no special abilities, apart from making EWS API succeed on the user-less calls.

Normally this username is written as an email address (UPN name

The three values, for Application (client) ID, Directory (tenant) ID, Client Secret Value - are obtained from Microsoft Portal, look below.

Missing parameters in 'Microsoft Entra ID' will be listed.

Register OnTime in ‘Microsoft Entra ID’

The following permissions are required for OnTime functionality to work with Microsoft Entra ID. The following table describes the required API permissions and their purpose.

Permissions For OnTime Core Application			
API Permission	**Access**	**Requirement**	**Description**
Application.Read.All	Read-only	Mandatory	Let OnTime confirm that the correct permissions have been granted and show this on the administration screen. It does not allow OnTime to change anything.
Calendars.ReadWrite	Read & write	Mandatory	The core of OnTime: show calendars, and create, update, move and delete meetings on user and resource (room) calendars, plus receive calendar change notifications. Write access is required because OnTime books and edits meetings on the user's behalf.
MailboxSettings.ReadWrite	Read & write	Mandatory	Read and set a user's automatic replies (out-of-office). Write access is required so OnTime can turn out-of-office on or off when the user asks.
Group.Read.All	Read-only	Optional	Preparing upcoming feature. Reading the group visibility flags.
GroupMember.Read.All	Read-only	Mandatory	Allows the app to read memberships and basic group properties for all groups without a signed-in user and allows the app to read Teams group memberships and members
Place.Read.All	Read-only	Mandatory	List meeting rooms and workspaces so they can be found and booked.
User.Read.All	Read-only	Mandatory	Look up directory details for users (name, email address, manager) so OnTime can

			display people and build its directory.
People.Read.All	Read-only	Mandatory	Search a user's relevant people (such as frequent contacts and colleagues) so OnTime can suggest matches when they look for someone to invite to a meeting.
Mail.Send	Send	Optional	Allows OnTime to send notification emails on a user's mailbox on behalf of the user. It is required if you use any OnTime feature that sends email — including the Mail Auth, Pollarity, Catering and Visitor modules (their invitations and notifications), ShareMyTime links, and OnTime's own system messages (e.g. licence and app-secret-expiry alerts). It can be omitted only if none of these features are used.
EWS.AccessAsUser.All	Auth	Optional	Delegated permissions are used for OAuth authentication functionality. Note: Required only if OnTime uses Forms-Based Authentication, even with the full Microsoft Graph method.
full_access_as_app	Read	Optional	OnTime uses it to connect to Exchange mailboxes over EWS with its own application identity (app-only), for calendar access and mailbox change notifications. It is not needed if OnTime runs in Graph-only mode or against on-premises Exchange.
Contacts.Read	Read	Optional	It allows OnTime to read users' Outlook contacts stored in Exchange Online through Microsoft Graph. When enabled, OnTime uses a user's personal contacts as an additional source for attendee searches and contact information.
Channel.ReadBasic.All	Read	Optional	It allows OnTime to retrieve Microsoft Teams channel members. This permission supports Microsoft Teams channel integration.

Steps to Register the OnTime Application in Microsoft Entra ID:

a) Login to https://portal.azure.com

b) Select View ‘Manage Microsoft Entra ID’

c) Click ‘App registrations.

d) Click ‘New registration’.

e) Enter a ‘Name’ for the application.
Choose ‘Accounts in this organizational directory only - Single tenant’.
Populate ‘Redirect URL’ (optional), https://example.com:8443/ontimegcms/code.html

f) Select a Platform ‘Web’
Click ‘Register’.

g) On next page (Overview) Copy the values [Application (client) ID] and [Directory (tenant) ID] into a text editor e.g. Notepad.

h) Click “Add a certificate or secret”.

i) Click ‘+ New client secret’

j) Add a description, such as ‘OnTime Client Secret’

k) Choose expiration. Click Add

l) Copy the value of the secret ID into the text editor.

m) Click ‘Authentication’ tab. Tick ‘Access Tokens’. Click ‘Save’.

n) Copy the three values from ‘Microsoft Entra ID’ in the text editor into the page ‘OnTime Admin Centre’ –
‘Domains Add/Edit Domain/Authentication’.

o) Click ‘API permissions’ tab. Click ‘Add a permission’.

p) Click ‘Microsoft Graph’

q) Click ‘Application permissions’

r) The following 'API permissions' must be checked, type a few letters in the Search field and tick the following permissions:

Application.Read.All, EWS.AccessAsUser.All (Optional), Calendars.ReadWrite, MailboxSettings.Read, Group.Read.All (Optional), GroupMember.Read.All, Place.Read.All, User.Read.All, People.Read.All, Mail.Send (Optional), Full-access_as_app (Optional), Channel.ReadBasic.All (optional), Contacts.Read (Optional)

You may remove 'User.Read', if already selected.

Note: 'EWS.AccessAsUser.All' permission is required only if OnTime uses form-based authentication. Delegated permissions are used for OAuth authentication functionality even with the full Microsoft Graph method.

s) Click 'Add a permission'.

t) Click 'Microsoft Graph'

u) Click 'Delegated permissions'

v) Search for EWS, tick:
EWS.AccessAsUser.All

w) Click 'Add a permission'

x) Click 'APIs my organization uses'

y) In the field for search, enter 'Office'

z) Click 'Microsoft 365 Exchange Online

aa) Click 'Application permissions'

bb) Tick 'full-access_as_app'

cc) Click 'Add permissions'

dd) Click "Grant admin consent for *Your Company*".
Click 'Yes' to answer the question 'Do you want to grant consent ...'

ee) If it is a configuration update of 'Microsoft Entra ID' for your OnTime server – remember to stop/start the OnTime application.

Microsoft Exchange Online Subscriptions Methods

Overview

OnTime Group Calendar uses subscriptions to receive notifications when calendar data changes in Microsoft Exchange Online. This allows OnTime to react quickly when users create, modify, or delete calendar events without continuously polling every mailbox for changes.

Historically, OnTime has used EWS Streaming Subscriptions for this purpose. Microsoft is retiring Exchange Web Services (EWS) in Exchange Online, which means that EWS-based streaming subscriptions must be replaced by subscriptions based on Microsoft Graph Change Notifications.

From OnTime 6.4.x, three subscription models are available:

1. **Legacy EWS Streaming Subscription**
2. **Microsoft Graph Subscription – Integrated OnTime Server**
3. **Microsoft Graph Subscription – External Subscription Hub**

The first model is the legacy architecture. Models 2 and 3 both use Microsoft Graph and remove the subscription mechanism's dependency on EWS.

> **Note:** EWS Streaming Subscriptions can continue to be used with Exchange Server on-premises. The EWS retirement discussed here concerns Microsoft Exchange Online.

1. Legacy EWS Streaming Subscription

Architecture

The original OnTime subscription model is based on Exchange Web Services (EWS) Streaming Subscriptions.

In this architecture, the OnTime server establishes streaming subscription connections directly to Exchange Online. Exchange keeps these connections open and uses them to notify OnTime when calendar events change.

The subscription functionality is handled as part of the OnTime server itself.

Communication flow

Exchange Online → EWS Streaming Subscription → OnTime Server

The OnTime server:

- creates and maintains EWS streaming subscriptions;
- maintains the connections to Exchange;
- receives notifications through the streaming connections;
- processes notifications and updates the OnTime calendar data

Advantages

The primary advantage is simplicity for existing installations:

- No separate subscription service is required.
- No inbound Internet endpoint is required for Microsoft Graph notifications.
- Existing OnTime installations may already be configured for this model.
- It continues to be applicable to Exchange Server on-premises.

Limitations

The model depends entirely on EWS Streaming Subscriptions.

Because Microsoft is retiring EWS for Exchange Online, this architecture should be considered a legacy configuration for Microsoft 365 environments. Once EWS is no longer available in Exchange Online, the EWS-based subscription mechanism will no longer function.

New Exchange Online installations should therefore use one of the Microsoft Graph-based subscription models described below.

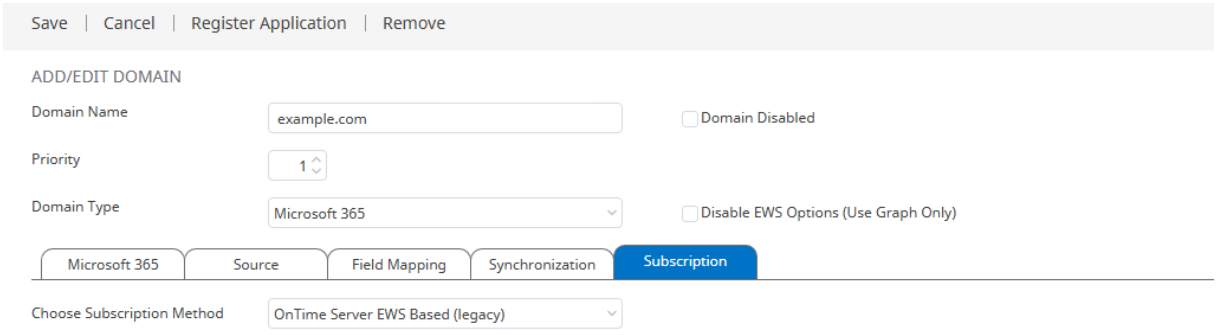
Selecting the Legacy Subscription Method

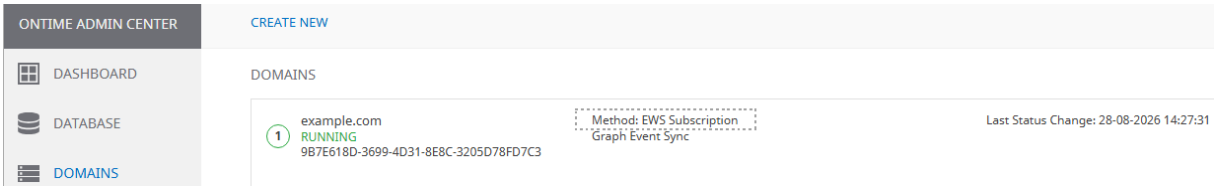
In the OnTime Admin Centre:

`Domains → Subscription → Choose Subscription Method`

Using EWS Based (Legacy) event subscription:

From the drop-down list, 'Choose Subscription Method' select 'OnTime Server EWS Based (Legacy)'.
Click 'Save'. Then, in the OnTime Dashboard, stop and restart the OnTime application. (see the example below)



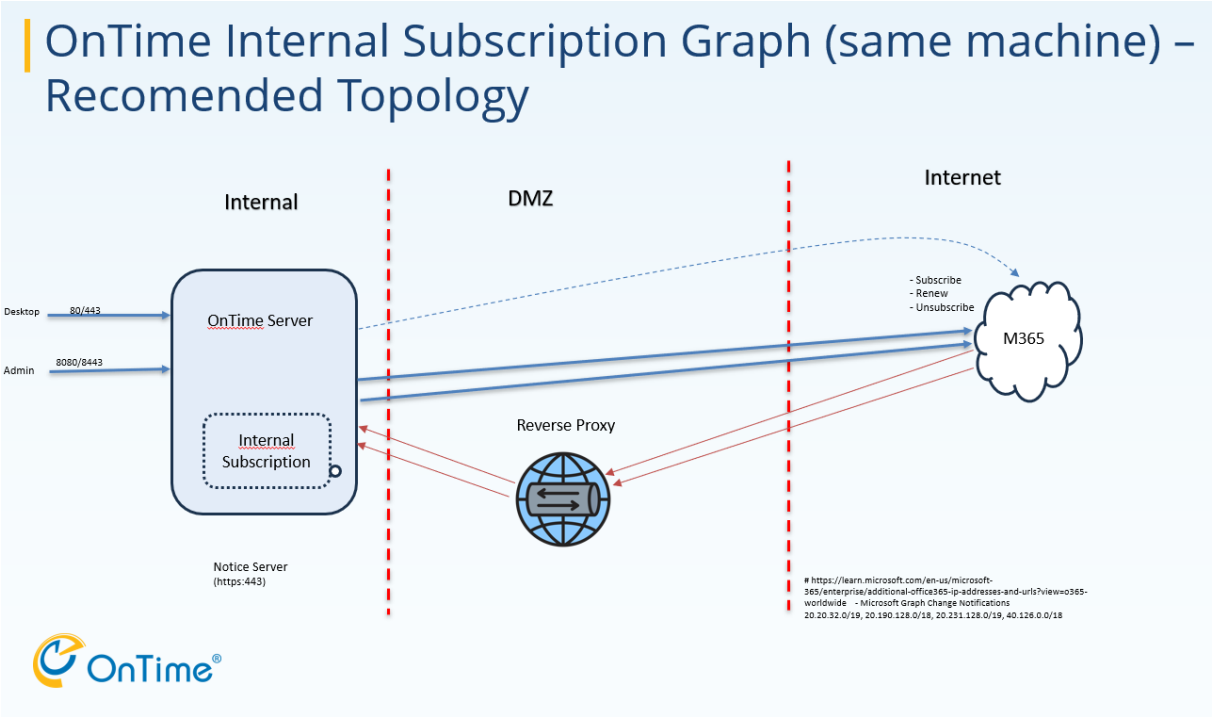


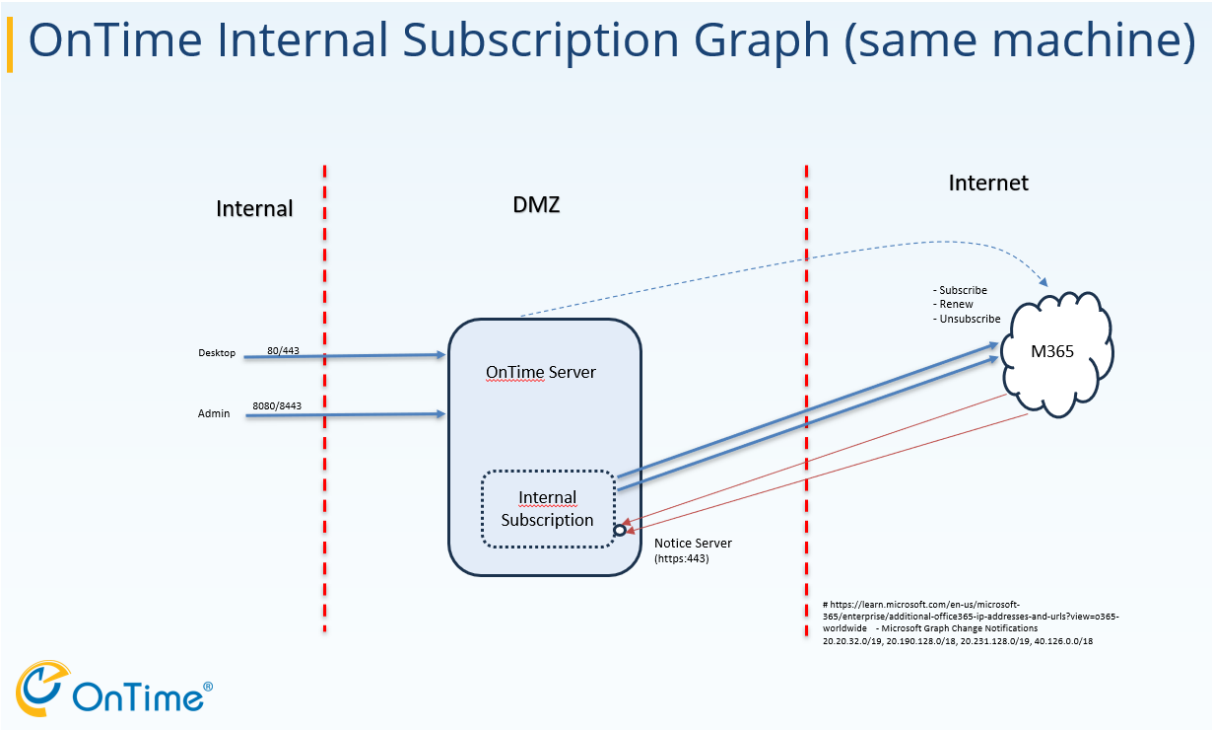
2. Microsoft Graph Subscription – Integrated OnTime Server

Architecture

The second model replaces EWS Streaming Subscriptions with Microsoft Graph change notifications while keeping the subscription functionality integrated with the OnTime server.

In this architecture, subscription handling is performed by OnTime running on its Tomcat application server.





Communication flow

```
Microsoft Graph → HTTPS Change Notification → OnTime Server / Tomcat
```

OnTime creates subscriptions through Microsoft Graph. Microsoft 365 subsequently sends change notifications to a publicly reachable HTTPS endpoint on the OnTime server.

This removes EWS from the subscription mechanism while avoiding the need for an additional Subscription Hub server.

Network Requirements

Unlike EWS Streaming Subscriptions, Microsoft Graph change notifications require Microsoft 365 to initiate an HTTPS connection to the notification endpoint.

The OnTime server therefore requires:

- outbound HTTPS connectivity to Microsoft Graph;
- inbound HTTPS connectivity from Microsoft 365 to the configured Notice URL;
- reliable DNS resolution;
- a valid HTTPS certificate and configuration.

The Notice URL is the externally reachable HTTPS URL of the OnTime server, for example:

```
https://ontime.example.com:443
```

A reverse proxy can optionally be placed between the Internet and the OnTime server.

Typical topology

```
Microsoft 365 / Microsoft Graph → HTTPS → Firewall / Reverse Proxy → OnTime Server / Tomcat
```

Advantages

- No EWS dependency for subscription handling.
- No additional Subscription Hub server is required.
- Subscription management remains part of the standard OnTime installation.
- Administration remains concentrated on the OnTime server.
- Suitable for environments where exposing the OnTime notification endpoint through a firewall or reverse proxy is acceptable.

Considerations

The OnTime server must be reachable from Microsoft 365 for Graph Change Notifications.

Consequently, organisations must provide an inbound HTTPS route from Microsoft 365 to the OnTime server, either directly or through infrastructure such as a reverse proxy.

Subscription processing also remains part of the main OnTime server workload. For larger environments, separating subscription processing from the main OnTime server may therefore be preferable.

Selecting the Integrated Graph Based Subscription Method

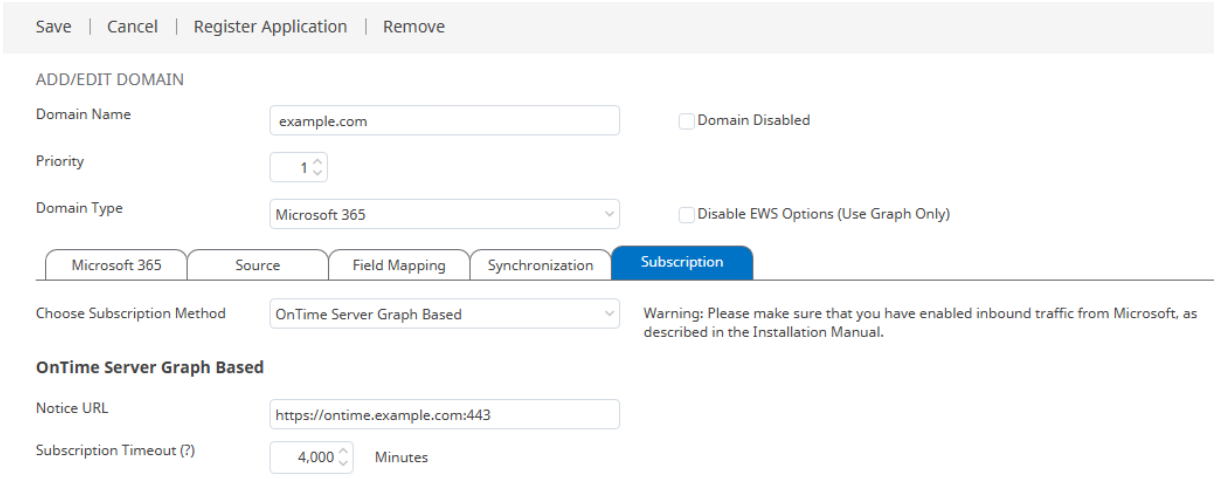
In the OnTime Admin Centre:

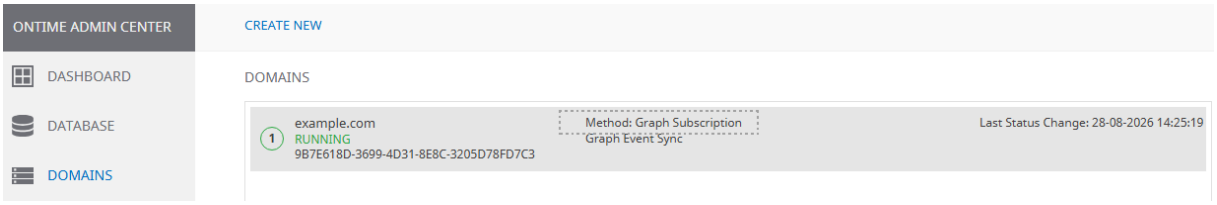
`Domains → Subscription → Choose Subscription Method`

Using Integrated Graph-Based event subscription

From the 'Choose Subscription Method' drop-down list, select **'**OnTime Server Graph Based'.
In the **'**Notice URL' field, enter the full externally reachable HTTPS URL of OnTime server including the port number.

Click 'Save'. Then, in the OnTime Dashboard, stop and restart the OnTime application. (see the example below)





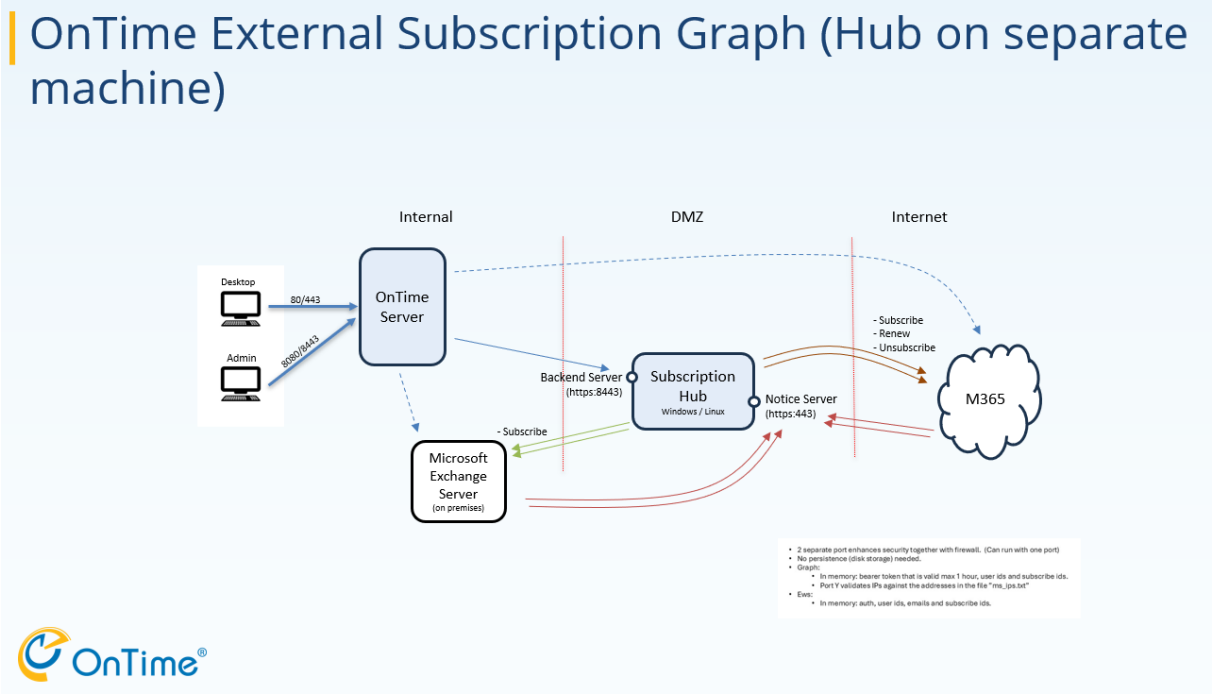
3. Microsoft Graph Subscription – External Subscription Hub

Architecture

The third model also uses Microsoft Graph change notifications but separates subscription management from the main OnTime server.

The subscription functionality runs as a dedicated Node.js-based Subscription Hub (otSubHub).

Instead of sending notifications directly to the OnTime server, Microsoft Graph sends them to the Subscription Hub. The Subscription Hub then communicates with the internal OnTime server.



Communication flow

```
Microsoft 365 / Microsoft Graph ⇔ Subscription Hub ⇔ OnTime Server
```

This separation is the major architectural difference between methods 2 and 3.

In the recommended topology, the OnTime server is located on the internal network, the Subscription Hub is in the DMZ, and Microsoft 365 is accessed through the Internet.

Microsoft Graph communicates with the Subscription Hub's Notice Server, while the OnTime backend communicates with the Subscription Hub through its Backend Server interface.

Selecting the External Subscription Hub Graph-Based Method

In the OnTime Admin Centre:

`Domains → Subscription → Choose Subscription Method`

Using External Subscription Hub Graph-Based event subscription

From the drop-down list, ‘Choose Subscription Method’, select ‘External Subscription Hub Graph-Based’.

Subscription Hub URL: Enter the HTTPS URL of the Subscription Hub endpoint.

Secret Subscription Hub Application Key: Enter the secret application key used to authenticate the OnTime server with the Subscription Hub.

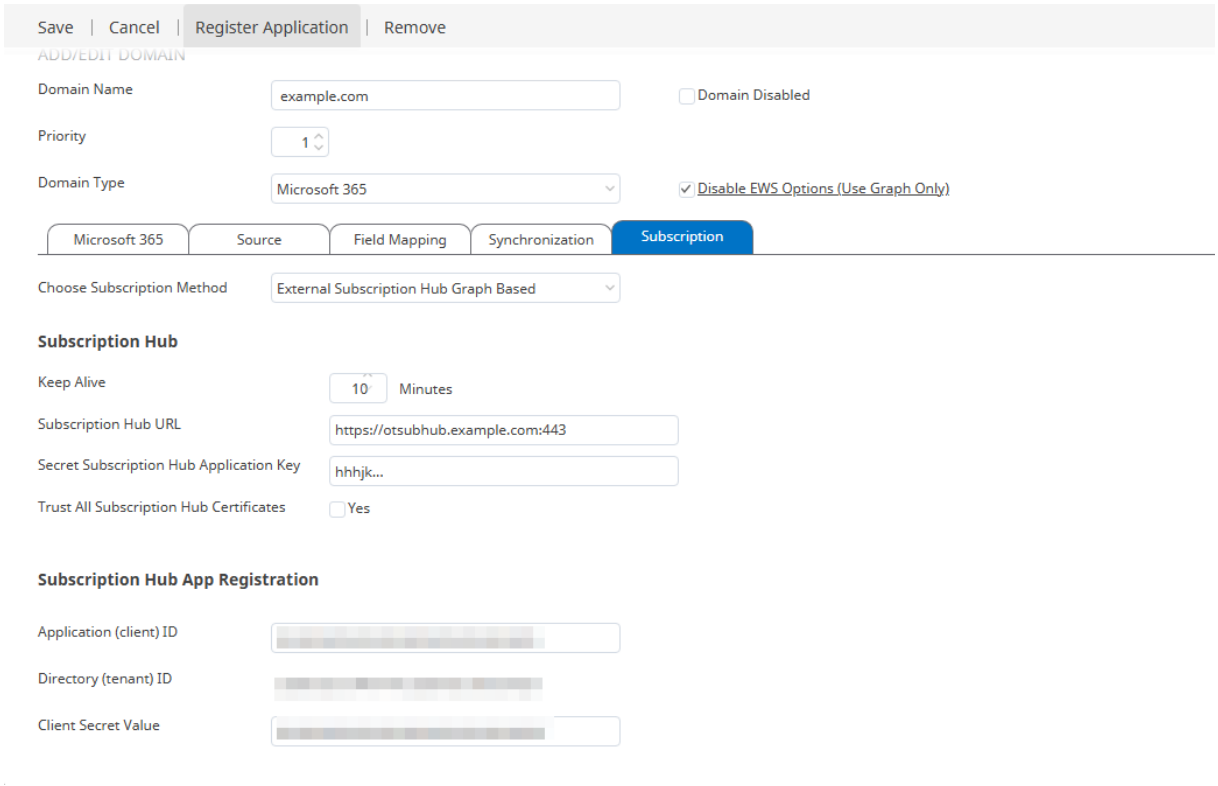
Trust All Subscription Hub Certificates: When selected, OnTime accepts all certificates presented by the Subscription Hub. This option should only be enabled when required, for example when using a self-signed or privately issued certificate.

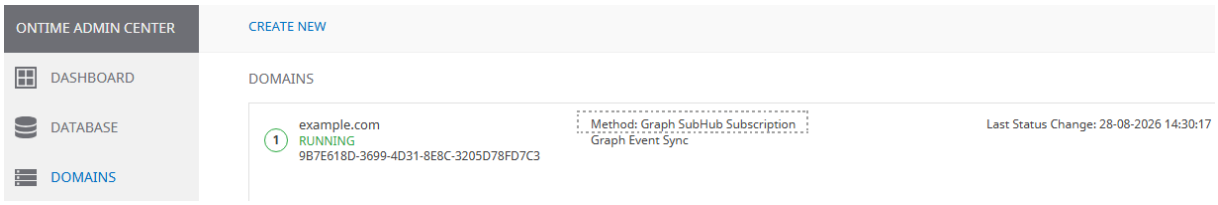
Application (client) ID: Enter the Application (client) ID of the Microsoft Entra ID app registration. (go to)

Directory (tenant) ID: Enter the Directory (tenant) ID of the Microsoft Entra ID tenant where the application is registered.

Client Secret Value: Enter the client secret value created for the Microsoft Entra ID application registration.

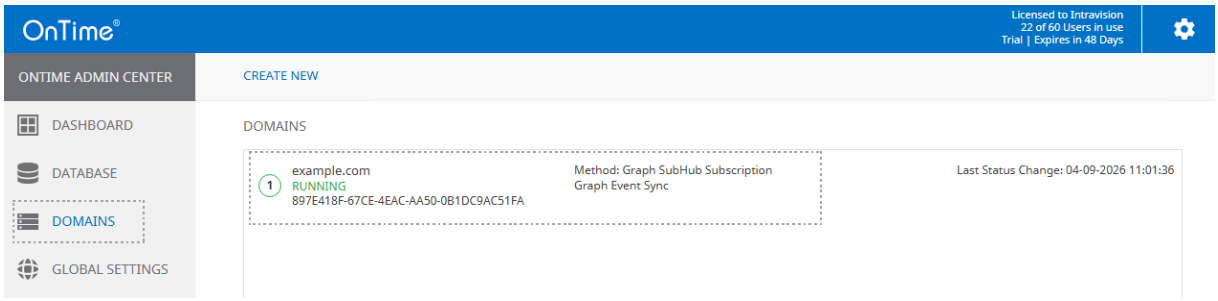
Click ‘Save’. Then, in the OnTime Dashboard, stop and restart the OnTime application. (see the example below)


Save | Cancel | Register Application | Remove
ADD/EDIT DOMAIN
Domain Name
example.com
Domain Disabled
Priority
1
Domain Type
Microsoft 365
Disable EWS Options (Use Graph Only)
Microsoft 365
Source
Field Mapping
Synchronization
Subscription
Choose Subscription Method
External Subscription Hub Graph Based
Subscription Hub
Keep Alive
10
Minutes
Subscription Hub URL
https://otsubhub.example.com:443
Secret Subscription Hub Application Key
hhhjk...
Trust All Subscription Hub Certificates
Yes
Subscription Hub App Registration
Application (client) ID
Directory (tenant) ID
Client Secret Value


ONTIME ADMIN CENTER
CREATE NEW
DASHBOARD
DATABASE
DOMAINS
DOMAINS
example.com
RUNNING
9B7E618D-3699-4D31-8E8C-3205D78FD7C3
Method: Graph SubHub Subscription
Graph Event Sync
Last Status Change: 28-08-2026 14:30:17

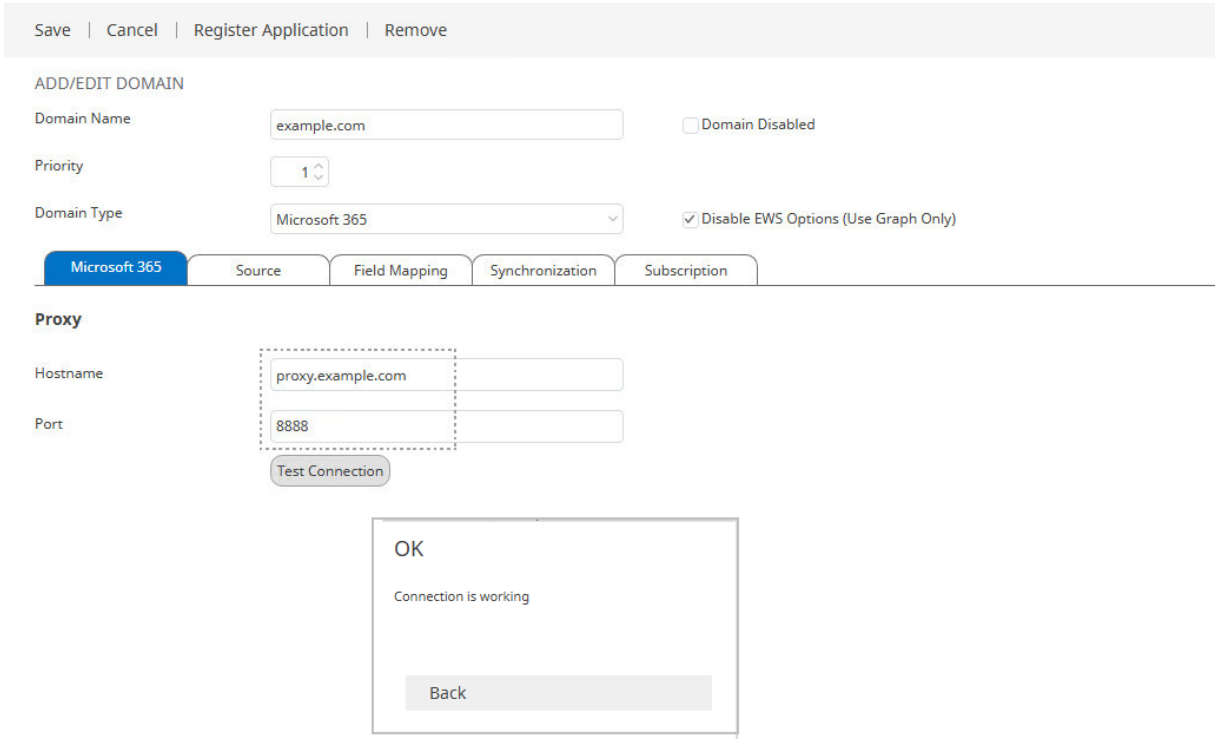
How to Configure Subscription hub using a Proxy

In OnTime Admin, select “DOMAINS” from the left-side panel, then select your domain. (see example below)



Proxy Configuration: Specify the proxy server hostname and port that OnTime should use for outbound connections to Microsoft 365. Use Test Connection to verify the proxy configuration.

Hostname: Enter the name or IP address of the proxy server.
Port: Enter the network port used by the proxy server.
Test Connection: Tests whether OnTime can connect through the specified proxy. (see below as example)



Disabling EWS Completely

Moving the subscription mechanism to Microsoft Graph does not by itself necessarily mean that every other OnTime function has been switched from EWS to Graph.

OnTime therefore provides the option:

```
Disable EWS Options (Use Graph Only)
```

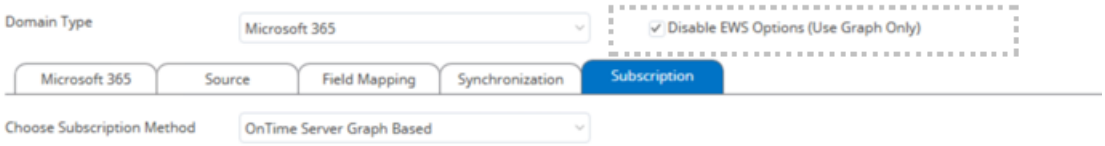
When enabled, OnTime switches its applicable configurations to Microsoft Graph only. EWS can subsequently be disabled at the Microsoft 365 tenant level.

This distinction is important:

- Subscription Method - controls how OnTime receives calendar change Notifications.
- Disable EWS Options (Use Graph Only) - determines whether OnTime as a whole is configured to avoid EWS connections where Graph functionality is available.

If you want to disable all connections to EWS, select the “Disable EWS Options (Use Graph Only)” checkbox. Click **“Save.”** Then, in the OnTime Dashboard, stop and restart the application.

This will switch all configurations to use only Microsoft Graph, and EWS can then be disabled at the tenant level.(see the example below)



Register Subscription Hub in “Microsoft Entra ID”

The following permissions are required for Subscription Hub functionality to work with Microsoft Entra ID. The following permissions are required.

Calendars.Read, User.Read

a) Login to https://portal.azure.com

b) Select View ‘Manage Microsoft Entra ID’

c) Click ‘App Registrations’

d) Click ‘New registration’

e) Enter a ‘Name’ for the application.
Choose ‘Accounts in this organizational directory only - Single tenant’.
Populate ‘Redirect URL’, insert https://example.com:8443/ontimegcms/code.html - this field cannot be empty
Select a Platform ‘Web’
Click ‘Register’.

f) On next page (Overview) Copy the values [Application (client) ID] into a text editor e.g. Notepad.

g) Click ‘Add a certificate or secret’ for Subscription Hub

h) Click ‘+ New client secret’ for Subscription Hub

i) Add a description, such as ‘Subscription Hub for OnTime Client Secret’

j) Choose expiration. Click Add

k) Click ‘API permissions’ tab. Click ‘Add a permission’.

l) Click ‘Microsoft Graph’

m) Click ‘Application permissions’

n) The following ‘API permissions must be checked, type a few letters in the Search field and tick the following permissions:
Calendars.Read (application), User.Read (delegated)

o) Click ‘Add a permission’

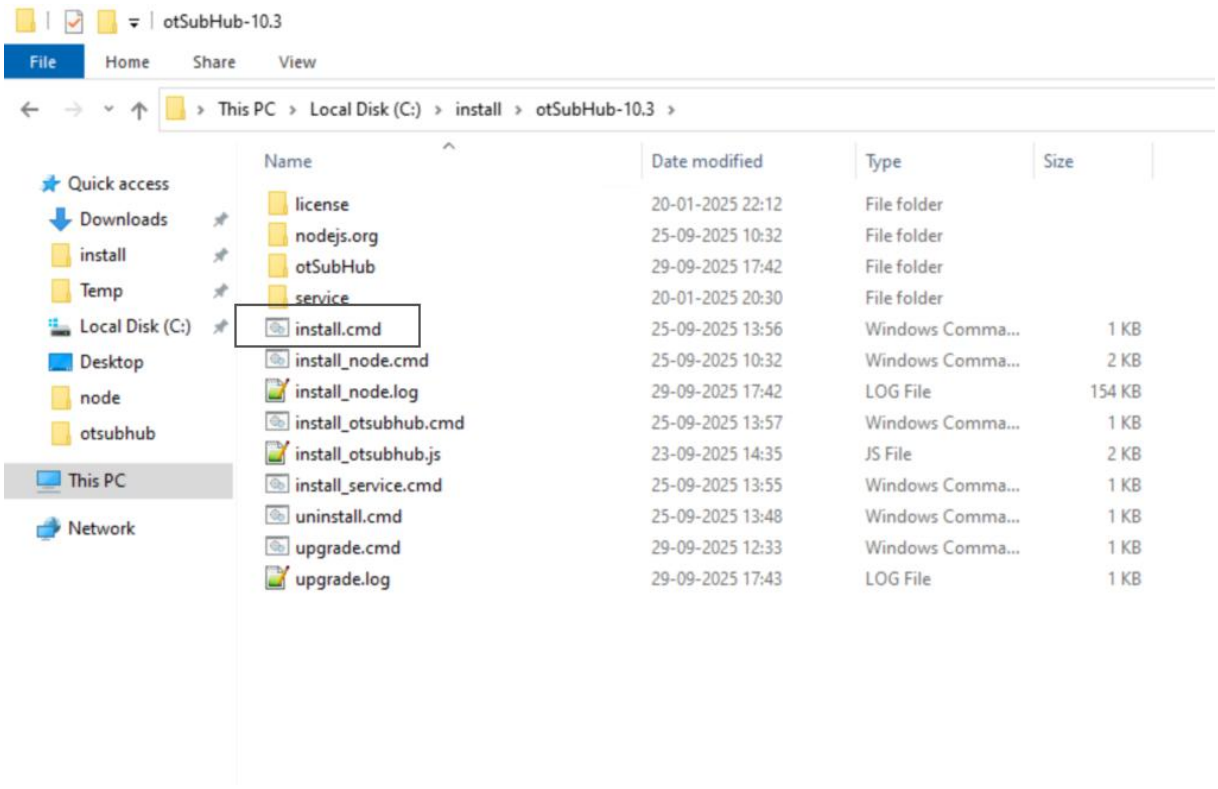
p) Click "Grant admin consent for *Your Company*"
Click ‘Yes’ to answer the question ‘Do you want to grant consent ...’

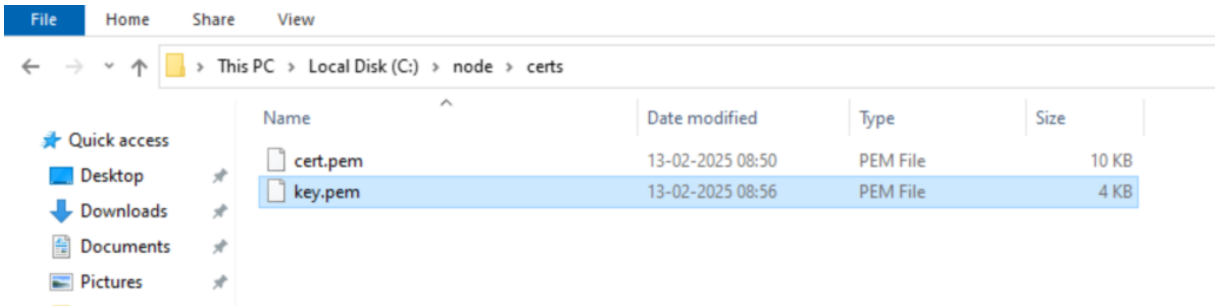
Subscription Hub “otSubHub” Installation and Configuration Steps

1. **Unzip the installation file**
   Unzip the file ‘otSubHub-10.x.zip’ from the OnTime server into a temporary folder on the Subscription Hub server. (Required when installing the Subscription Hub on a separate machine). If you are using the same machine for both OnTime and Subscription Hub, You may simply unzip package locally on that machine. (For both options, see example below)
2. **Run the installer**
   Go to the folder where you extracted the files and run install.cmd as Administrator. (see example below)
   The Subscription Hub service will be installed in the folder ‘c:\node\otsubhub’.
3. **Add SSL certificates**
   Create a folder named ‘certs’ (under C:\node) and copy the PEM certificate files used by your domain into the folder ‘c:\node\certs’. (see example page 169)
4. **Edit the configuration file**
   Open the configuration file ‘otSubHub.json’ located in ‘C:\node\otsubhub’.
5. **Set the certificate paths**
   In the configuration file ‘otSubHub.json’ update the paths for the certificate files ‘key.pem’ and ‘cert.pem’. (see example below)
6. **Set the service URL**
   In the ‘URL’ field of the configuration file ‘otSubHub.json’ enter the full HTTPS domain name where the service will run. (see example below)
7. **Save and restart the service**
   Save your changes and ‘restart the Subscription Hub service’ on the server. (see example below)

Additional Notes:

- If the protocol for the ‘backendServer’ is set to https, it will automatically use the ‘key’ and ‘cert’ from the ‘noticeServer’, unless you set them differently.
- Both services can also run on the same port if required.
- Log files for the Subscription Hub service are stored in the folder. ‘C:\node\otsubhub’.

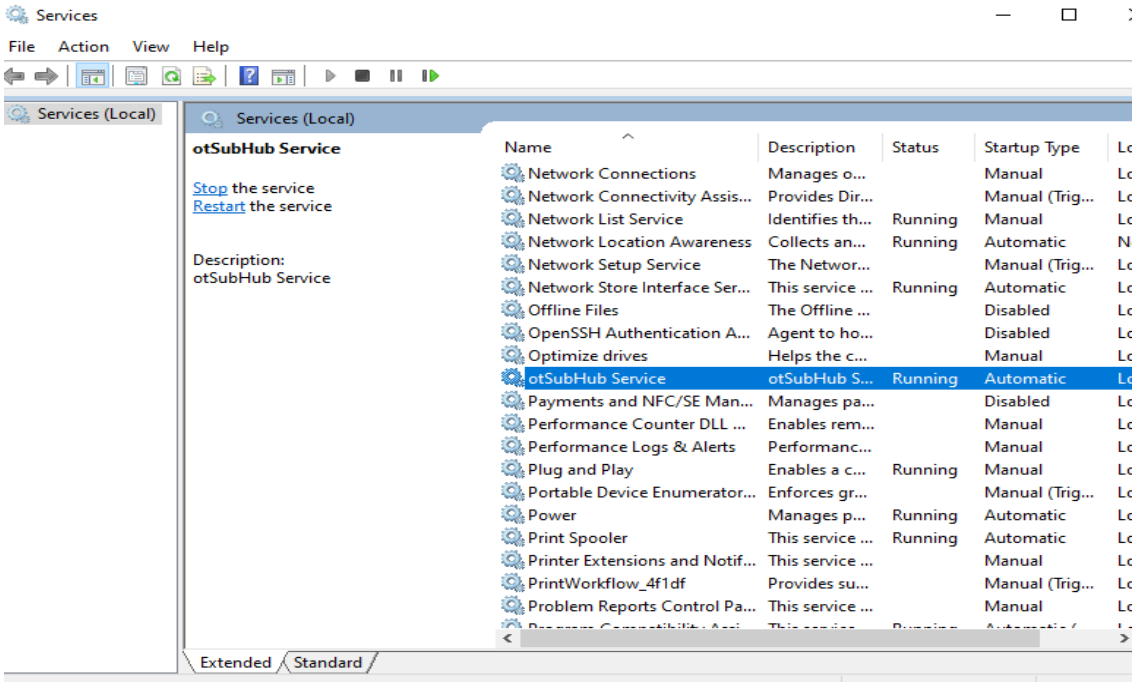

otSubHub-10.3
File
Home
Share
View
This PC › Local Disk (C:) › install › otSubHub-10.3 ›
Quick access
Downloads
install
Temp
Local Disk (C:)
Desktop
node
otsubhub
This PC
Network
Name
Date modified
Type
Size
license 20-01-2025 22:12 File folder
nodejs.org 25-09-2025 10:32 File folder
otSubHub 29-09-2025 17:42 File folder
service 20-01-2025 20:30 File folder
install.cmd 25-09-2025 13:56 Windows Comma... 1 KB
install_node.cmd 25-09-2025 10:32 Windows Comma... 2 KB
install_node.log 29-09-2025 17:42 LOG File 154 KB
install_otsubhub.cmd 25-09-2025 13:57 Windows Comma... 1 KB
install_otsubhub.js 23-09-2025 14:35 JS File 2 KB
install_service.cmd 25-09-2025 13:55 Windows Comma... 1 KB
uninstall.cmd 25-09-2025 13:48 Windows Comma... 1 KB
upgrade.cmd 29-09-2025 12:33 Windows Comma... 1 KB
upgrade.log 29-09-2025 17:43 LOG File 1 KB


File
Home
Share
View
This PC › Local Disk (C:) › node › certs
Quick access
Desktop
Downloads
Documents
Pictures
Name
Date modified
Type
Size
cert.pem 13-02-2025 08:50 PEM File 10 KB
key.pem 13-02-2025 08:56 PEM File 4 KB

Example of the ‘otSubHub.json’ file is shown below:

```
{
        "noticeServer": {
                "protocol": "https",
                "port": 443,
                "key": "c:/node/certs/key.pem",
                "cert": "c:/node/certs/cert.pem",
                "payload": {
                        'URL': "https://otsubhub.example.com",
                        "clientState": " 05vy+WNM2JurnOc/HuEFg+tsVco= "
                }
        },
        "backendServer": {
                "protocol": "http",
                "port": 8443,
                "secretKey": " kH7KoGfI42Wqp5f/flKrCBJnB2I "
        },
        "graph": {
                "expiration_min": 60,
                "subscribe_threads": 3,
                "renew_threads": 3,
                "unsubscribe_threads": 5
        },
        "ews": {
                "subscribe_threads": 5
        }
}
```

You may now find ‘otSubHub’ listed under Windows Services, as shown below:



Since the Subscription Hub server only requires HTTPS access from the internet, we recommend applying an IP filter in the firewall. See Microsoft Graph Change Notifications for more details.

https://learn.microsoft.com/en-us/microsoft-365/enterprise/additional-office365-ip-addresses-and-urls?view=o365-worldwide

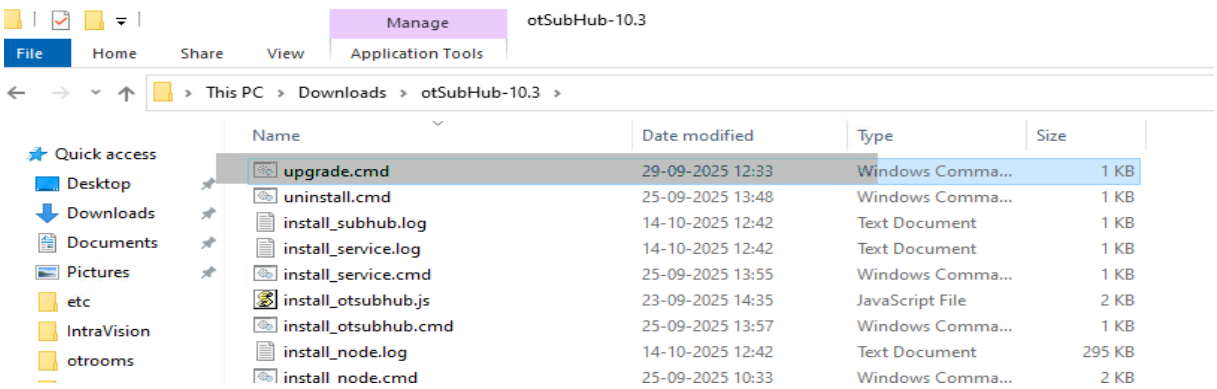
See the section *Microsoft Graph Change Notifications* for more information

Note: 'clientstat' is a unique value defined in the *otSubHub.json* file during installation of the *otSubHub* service. It represents the 'clientState' property included in each change notification (max length: 128 characters) and allows the client to verify the notification's authenticity by matching it with the subscribed 'clientState' value.

Note: The 'secretKey' is a unique value generated in the *otSubHub.json* file during *otSubHub* installation. It is sent from the backend server (OnTime) to the Subscription server, defining the 'secretKey' property exchanged between them.

Upgrading Subscription Hub (otSubHub)

1. Unzip the file 'otSubHub-10.x.zip' from the OnTime server into a temporary folder on the Subscription Hub server. (This is needed if you are installing the Subscription Hub on a separate machine). If you are using the same machine for both OnTime and Subscription Hub, You may simply unzip the file locally on that machine.
2. Go to the folder where you extracted the files and run **upgrade.cmd** as an administrator. The Subscription Hub will be upgraded under existing 'C:\node\otsubhub' (see example below)
3. Finally, make sure that 'otSubHub' service listed under Windows Services after the upgrade assignment.



Configuring the Subscription Hub in OnTime Admin

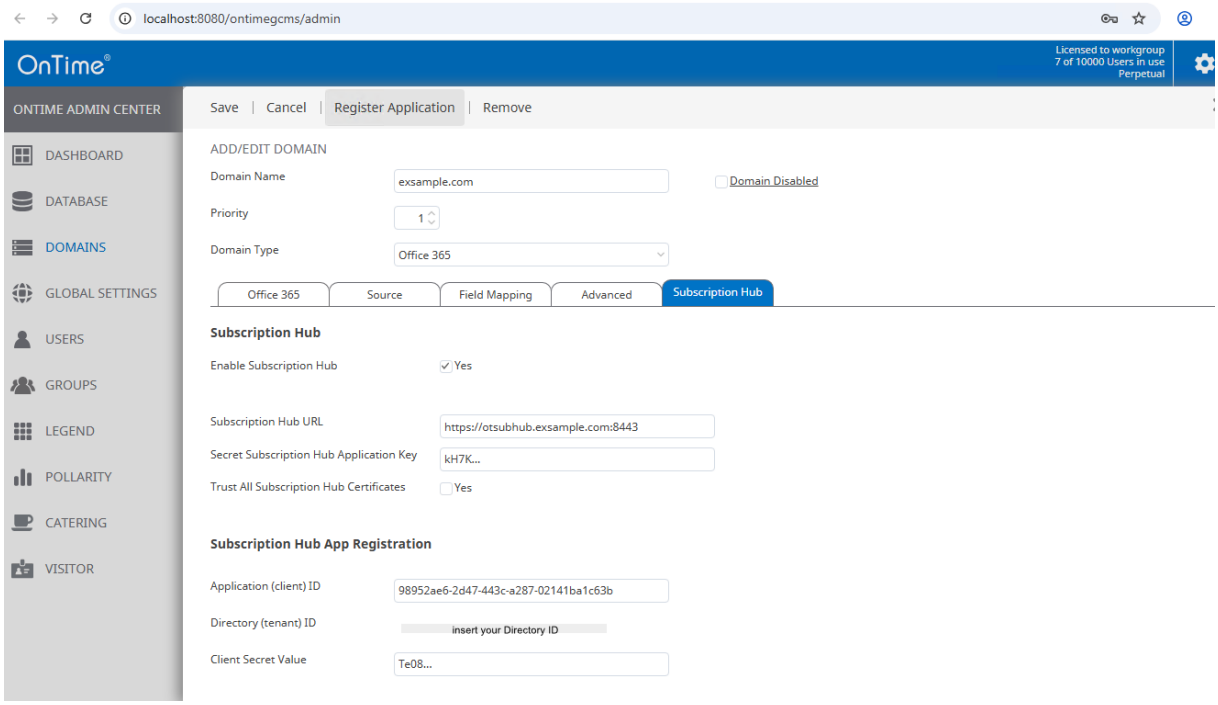
1. Copy Credentials
   Copy the values of the 'Client Application ID' and 'Client Secret Value' from the registered Subscription Hub application into a text editor, e.g., Notepad

2. Navigate to the OnTime Admin Centre

3. Open 'Domains' Section
   From the left-hand navigation bar, select Domains.

4. Configure Subscription Hub
   Select the Subscription Hub tab and enter the two values from step 1 under 'Subscription Hub App Registration' (see example below).

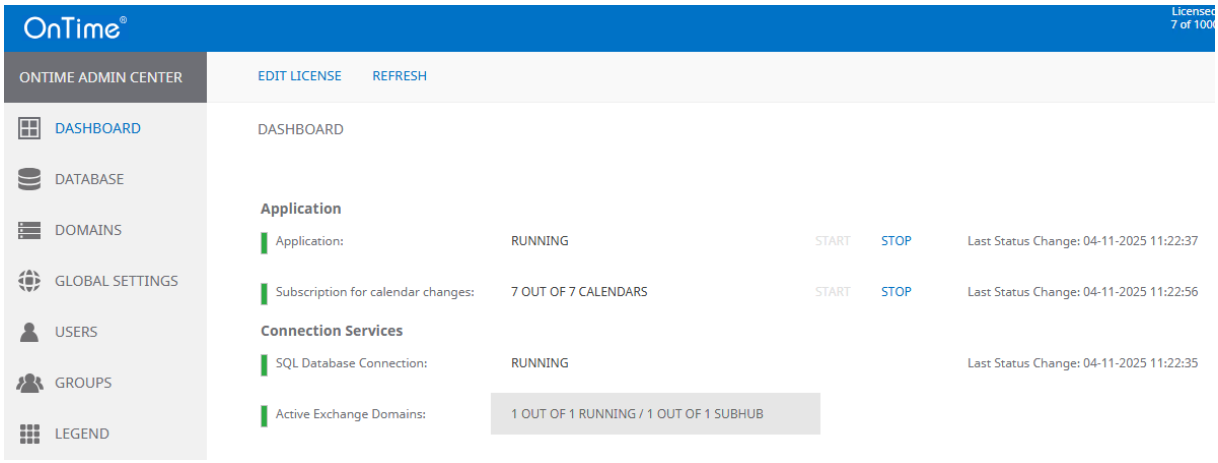
5. Set Subscription Hub URL
   Open the 'otSubHub.json' file located in 'C:\node\otsubhub' in a text editor, copy the Subscription Hub URL (including the port number) values, and paste it into the 'Subscription Hub URL' field (see example below).
6. Insert Secret Key
   Open the 'otSubHub.json' file located in 'C:\node\otsubhub' in a text editor, copy the 'secretKey' value, and paste it into the 'Secret Subscription Hub Application Key' field (see example below).
7. Enable Subscription Hub
   Enable the option Enable Subscription Hub and save the changes. (see example below).



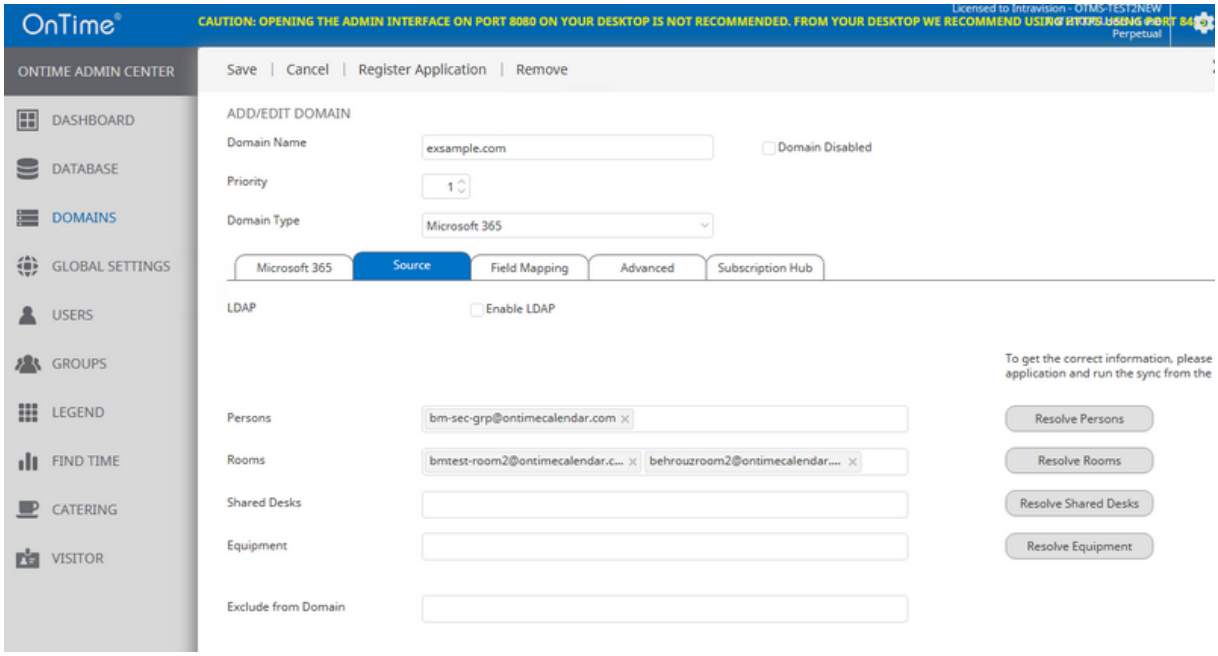
An example of the 'otSubHub.json' file is shown below.

```
{
        "noticeServer": {
                "protocol": "https",
                "port": 443,
                "key": "c:/node/certs/key.pem",
                "cert": "c:/node/certs/cert.pem",
                "payload": {
                        'URL': "https://otsubhub.example.com",
                        "clientState": " 05vy+WNM2JurnOc/HuEFg+tsVco= "
                }
        },
        "backendServer": {
                "protocol": "http",
                "port": 8443,
                "secretKey": " kH7KoGfI42Wqp5f/flKrCBJnB2I "
        },
        "graph": {
                "expiration_min": 60,
                "subscribe_threads": 3,
                "renew_threads": 3,
                "unsubscribe_threads": 5
        },
        "ews": {
                "subscribe_threads": 5
        }
}
```

8. *Now by navigating to the OnTime Admin Dashboard, you may view the status of 'SUBHUB'* when it is running (see example below)



Domains/Source



Source is where you configure users included in your OnTime setup.

'Untick' 'Enable LDAP'.

Add distribution groups of persons, rooms, shared desks, equipment you want to be included in the OnTime calendar. The email addresses of these distribution groups are written into the fields. More groups or individuals can be added, separated by commas.

Click **'Save'** to save your Domain Settings.

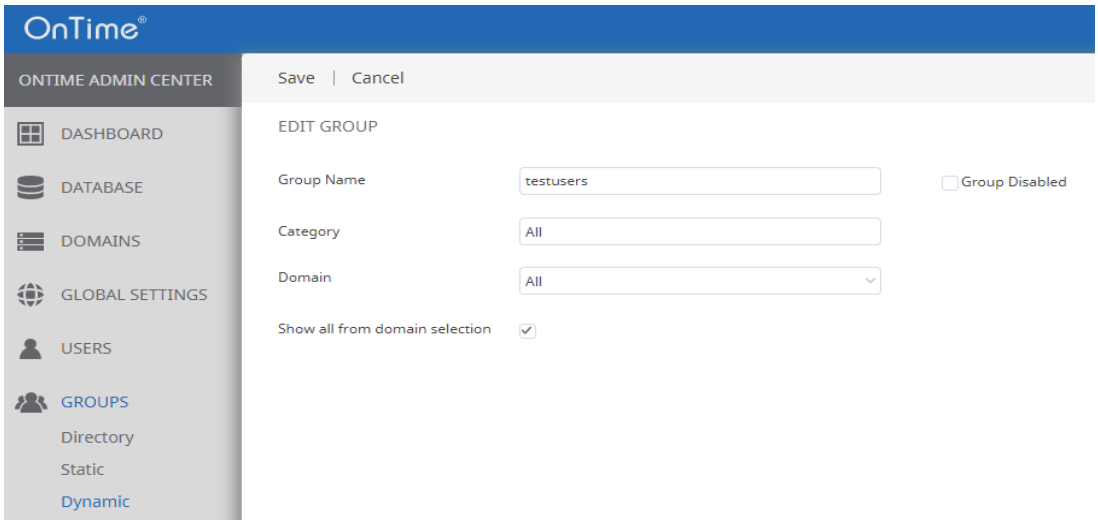
To reflect your new settings, go to the Dashboard - Stop and Start the Application. Then check that the "Database Service" and "Exchange Service" both show "Running"

Groups

Select 'Groups/Dynamic' to create a group of persons included in OnTime selected above in the 'Synchronization Source' section in your **Domain settings.**

Click 'Create New'. Creating at least one group will ensure that users will see more than one user in OnTime.

Enter a Group name, enter a Category (text) to be shown in the user interface, choose 'All' in Domain, tick 'Show all from domain selection'.



Click 'Save'.

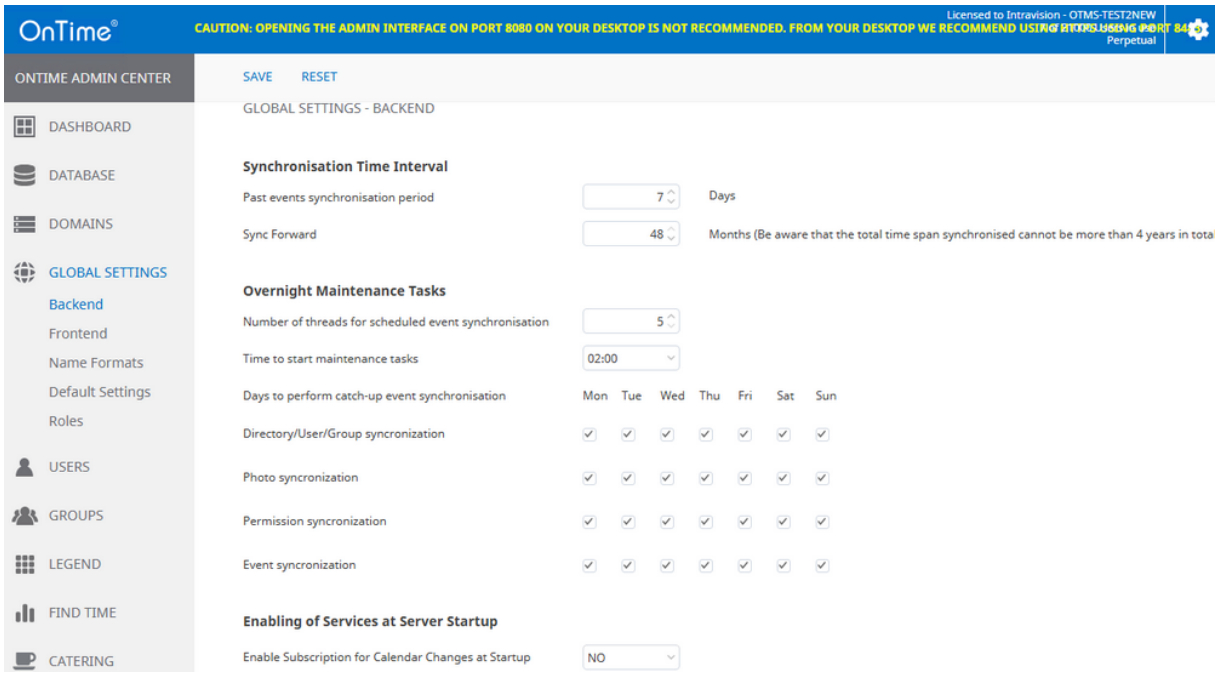
Changes in the 'dynamic groups' must be followed by clicking "Start" at "User & Group Sync" in the **Dashboard.**

Global Settings - Backend

Click Global/Backend

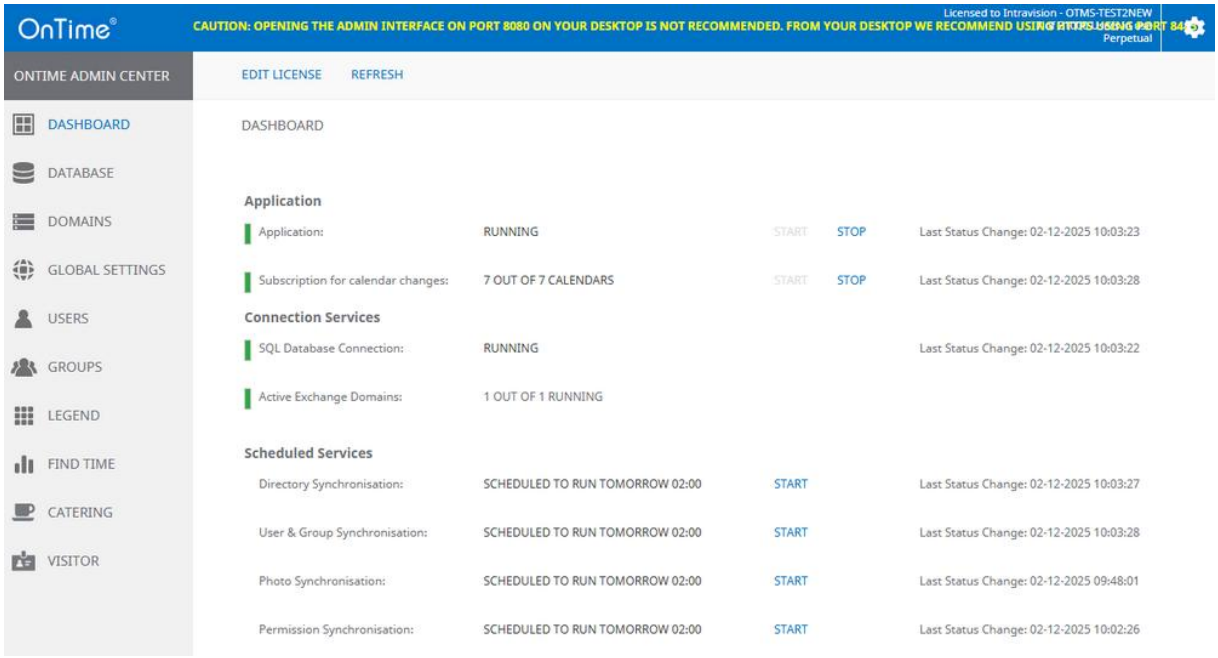
Choose 'Yes' at ‘Enable subscription for Calendar Changes at Startup'.

- Click ‘Save’ to ensure the synchronisation subscription service starts every time you click stop/start at the ‘Application Status’ in the Dashboard.



Dashboard

The main page of the ‘OnTime Admin Center’ is the Dashboard. This page presents an overview of the processes in OnTime. When you change the values in the other pages, you must restart the OnTime application by clicking “Stop/Start” in the according section.



The section **Persistent** shows the status of the OnTime Application and the automatic subscription of calendar changes. Both should be running within normal production.

The section **Connection** shows the status of the connections to the OnTime SQL database and the Exchange service. Both should be running within normal production.

The section **Scheduled** normally shows the status stopped because running is done automatically at midnight. But the five positions within this section can be started on-demand to reflect changes at once.

Directory Sync takes care of updating users/groups from Exchange.

User & Group Sync synchronises the Exchange users/groups onto the OnTime SQL tables.

Photo Sync imports the users' photos/avatars from the Exchange server

Permission Sync updates the users' permissions to update other users' calendars

Event Sync is synchronising all users calendar entries and may take a considerable amount of time.

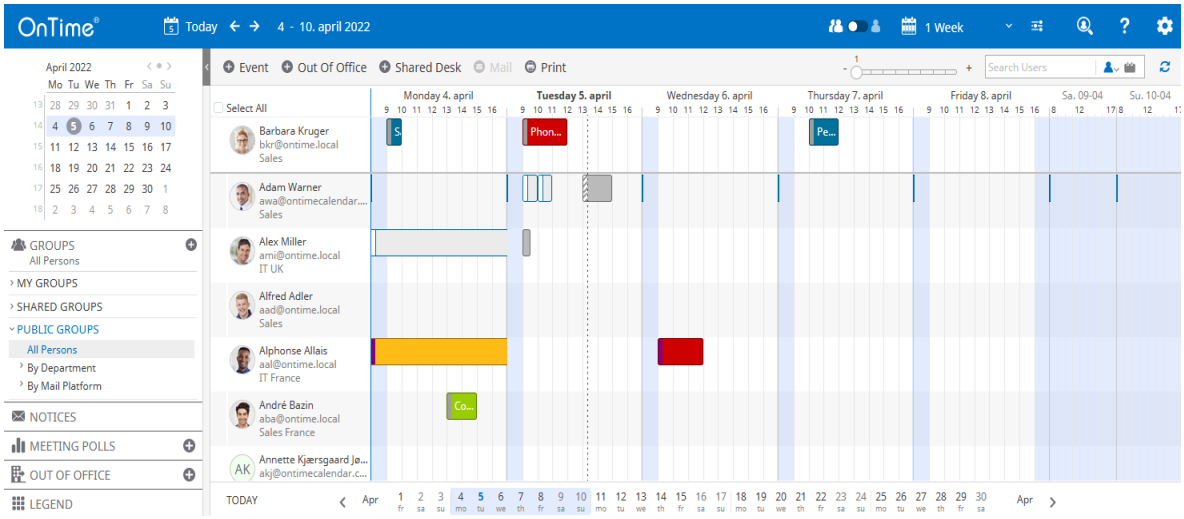
OnTime User – Calendar

OnTime Client Web Desktop

OnTime from the user perspective:

From a browser, open the user URL — for example:

http://ontime.example.com/ontimegcms/desktop
Note: Insert your relevant URL instead of 'ontime.example.com'.



OnTime Client Web Mobile

OnTime from the user perspective:

From a mobile browser - Open the user URL – for example:

http://ontime.example.com/ontimegcms/mobile

Note: Insert your relevant URL instead of ‘ontime.example.com’