for Microsoft

Quick Install Manual
OnTime® for Microsoft version 6.4.x

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 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 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 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

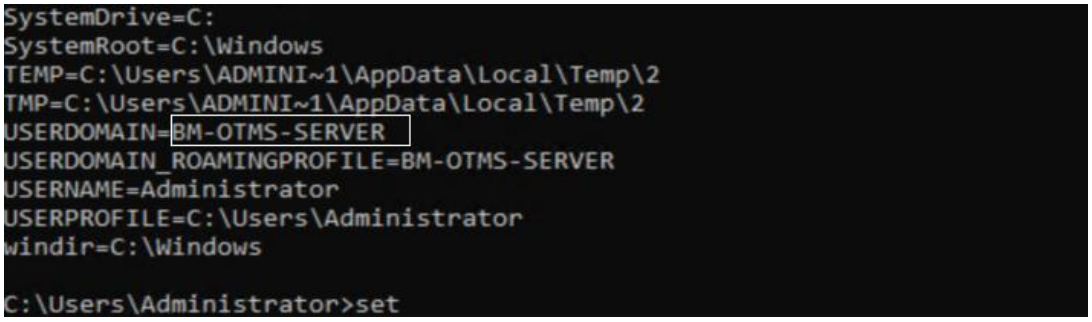
- OnTime requires a license key with the required number of users enabled to run.
- These keys are delivered directly by IntraVision or an OnTime Partner.
- A list of OnTime Partners is available at www.ontimesuite.com.

For obtaining a license key, provide the following info:

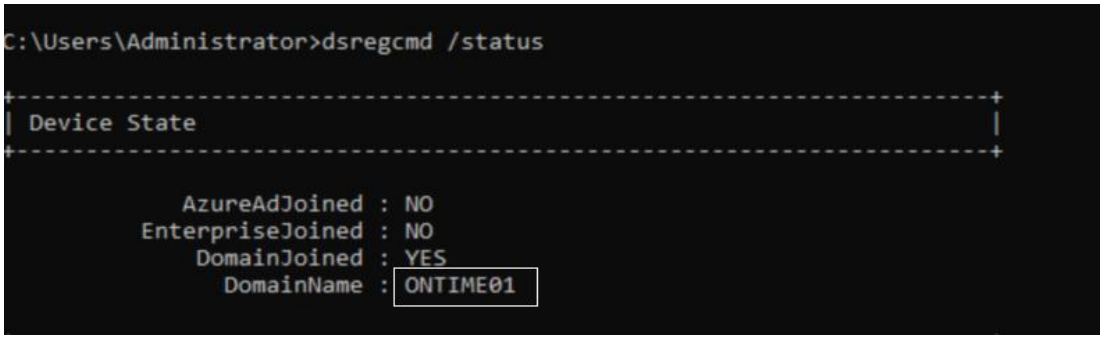
- your Company name
- total number of users, including rooms and equipment
- a. OnTime server in an AD domain,

  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
It is the easy way of installing OnTime with a local, silent installation of the MS SQL Server 2019-2022 at 'C:\Program Files', runs a single command to create the OnTime database, installs the 'OnTimeMSAuth' Windows service for SSO authentication, and installs the Tomcat server for web access.

Note: Dynamic Distribution Groups from Microsoft 365 are supported.

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

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

To install the SQL server, Example:

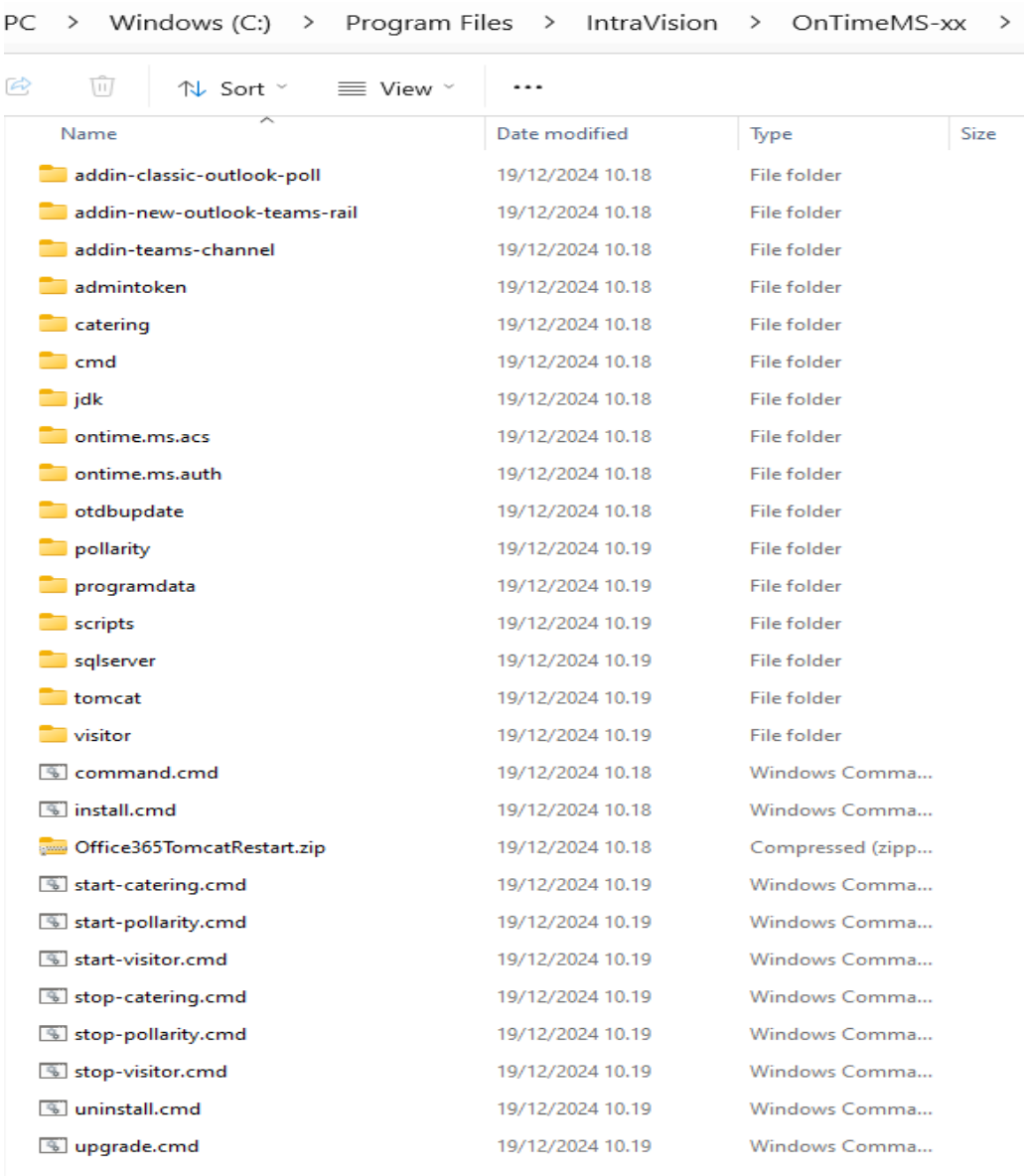
1. Open Command Prompt in administrator mode
2. Run 'sql_express_full_setup.cmd'
3. Wait for installation to complete

If you see other messages than "Installing SQL Express Server" your Windows server probably needs some updates from Microsoft. Resolve these prerequisites and rerun the command.
It may take 5-10 minutes to execute the installation of SQL Server Express.

Result:
The SQL Server is installed in the path:
C:\Program Files\Microsoft SQL Server

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

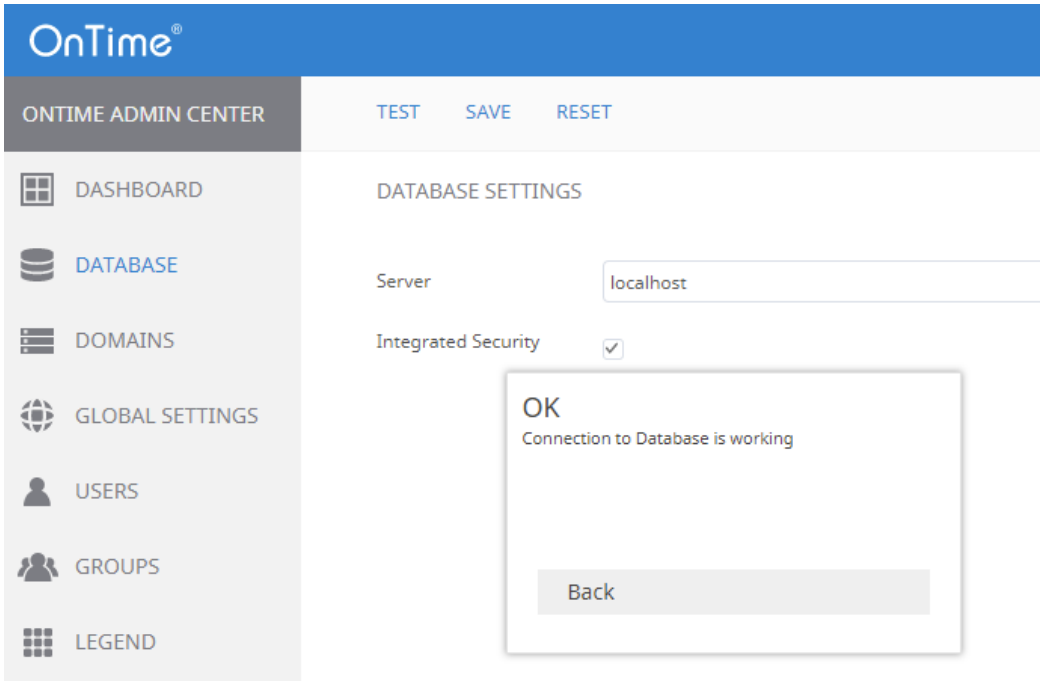
From a browser - Open the administration URL – for example:
https://ontime.example.com:8443/ontimegcms/admin
Note: Insert your relevant URL instead of 'ontime.example.com'.

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)

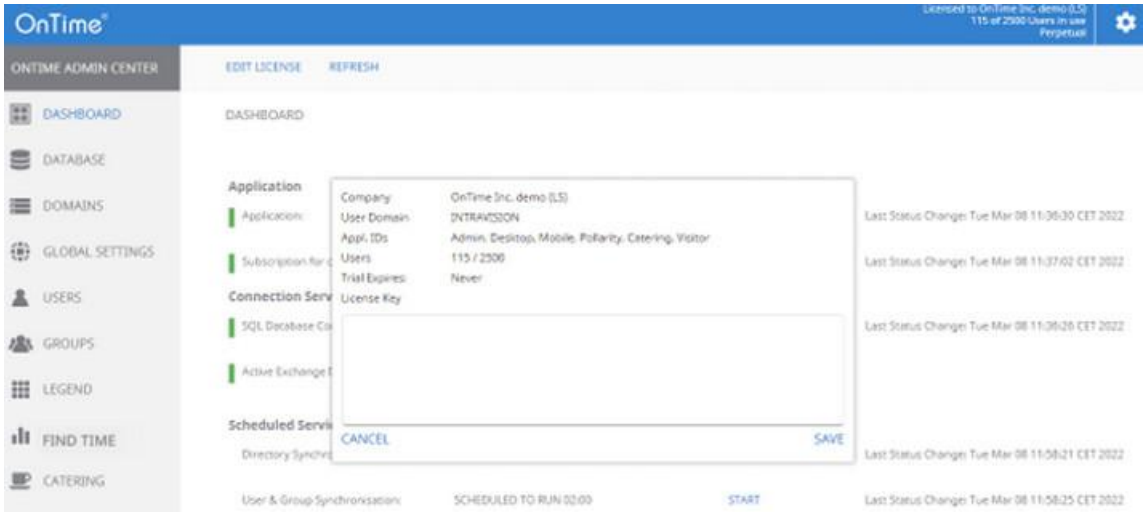
Database

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

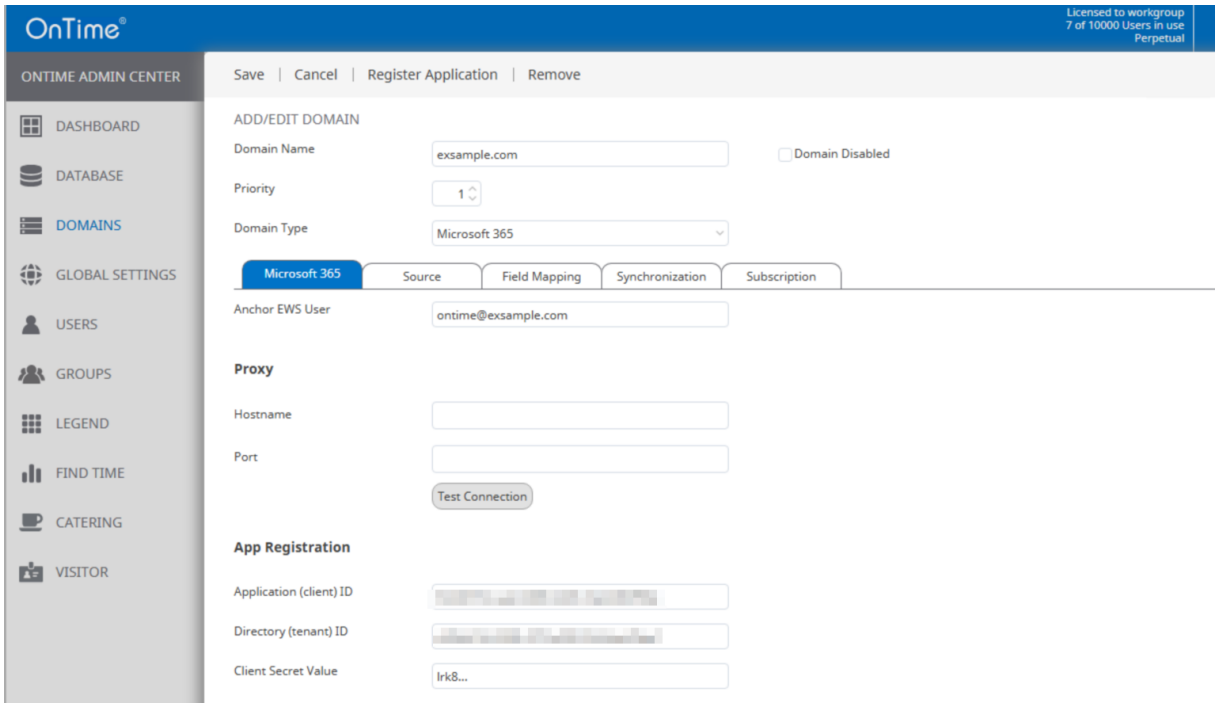
Click ‘Dashboard’
– Enter your license key by clicking ‘License’ in the upper right corner of the dashboard. Click ‘Save’



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 permissions are required.

Application.Read.All	Allows OnTime to read all permissions that are granted to the user.
Mail.Send	App-only access, without user context
Calendars.ReadWrite	get Online Meeting event, build Online Meeting event or add to existing event.
Group.Read.All	Allows the app to read group properties and memberships, and read conversations for all groups, without a signed-in user.
GroupMember.Read.All	Allows the app to read memberships and basic group properties for all groups without a signed-in user and allows to read membership Teams Group and members.
MailboxSettings.ReadWrite	Used for automaticRepliesSetting and make it possible to get and update AutoReply for mailboxes.
People.Read.All	Allows the app to read any user’s scored list of relevant people, without a signed-in user. The list can include local contacts, contacts from social networking, your organization’s directory, and people from recent communications
Place.Read.All	Allows the app to read company places (conference rooms and room lists) for calendar events and other applications, without a signed-in user
User.Read.All	Allows the app to read user profiles without a signed in user.
EWS.AccessAsUser.All	Note: This permission is required only if OnTime uses form-based authentication. Delegated permissions are used for OAuth authentication functionality.

Full-access_as_app	It allows an application (not a user) to access all mailboxes in the tenant with full mailbox permissions.

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 ten permissions:

Application.Read.All, EWS.AccessAsUser.All, Calendars.ReadWrite, MailboxSettings.ReadWrite, Group.Read.All, GroupMember.Read.All, Place.Read.All, User.Read.All, People.Read.All, Mail.Send, Full-access_as_app

You may remove ‘User.Read’, if already selected.

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.

Introducing the OnTime Subscription

For many years, the notification mechanism in OnTime for Microsoft has relied on streaming subscriptions, a technology that in turn depends on Exchange Web Services (EWS). However, Microsoft has officially announced the deprecation of EWS in Microsoft 365, and with it the end of streaming subscriptions. This change is currently scheduled to take effect on Early, 2027.

Once EWS is removed, the existing subscription-based notifications used by OnTime in Microsoft 365 will no longer function. Exception is that streaming subscriptions will continue to work for OnTime connected to an Exchange on-premises environment.

From OnTime version 6.4.x onward, tree subscription methods are available: The OnTime Server EWS Based (legacy) method, will be available until Microsoft will stay support it; OnTime Server Graph Based method and the External Subscription Hub Graph Based method, also referred to as the 'Subscription Hub'.

Prerequisites for Graph-Based OnTime Server Configuration

Network & Connectivity Requirements

Graph is a cloud API, so no on-prem server is required—but connectivity matters.

- Firewall rules:

  Allow Microsoft 365 endpoints

  Firewall roles need to be opened for http (port 80) or https (port 443) between the server running OnTime® Group Calendar and Microsoft 365® Exchange® server(s).

- Inbound HTTPS access:

  HTTPS access to the 'Notice URL' (e.g., https://ontime.example.com:443)"

- Outbound HTTPS access:

  https://graph.microsoft.com

  (Check the ports for Microsoft 365)

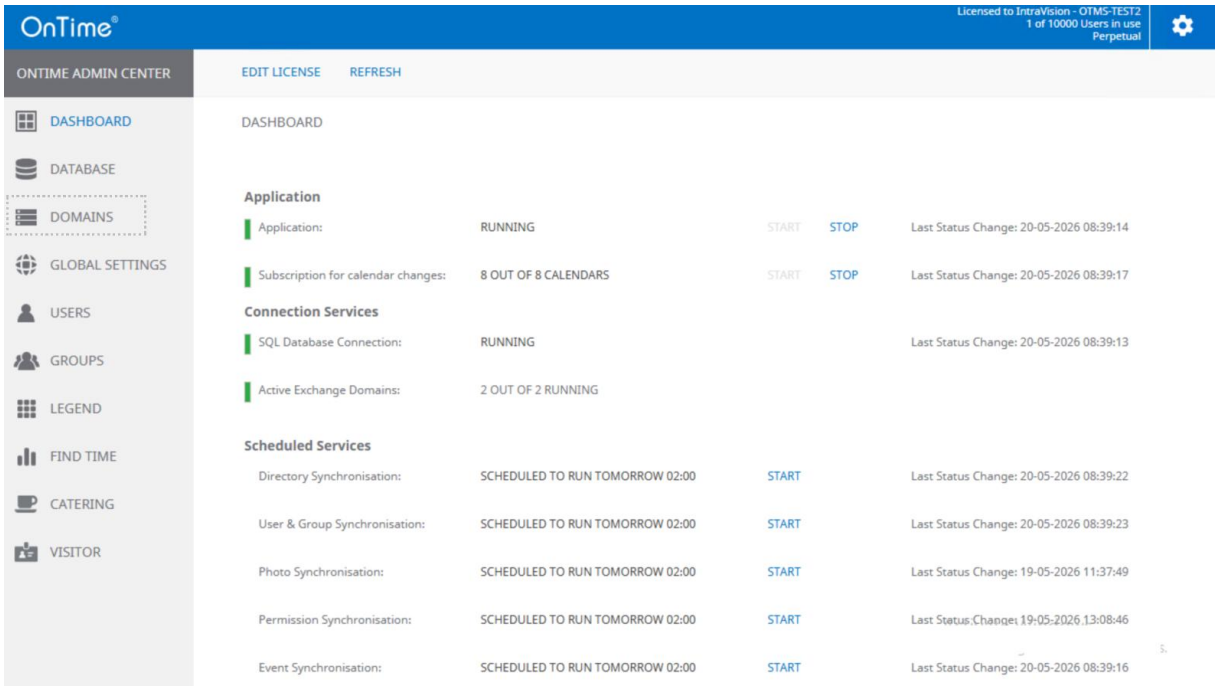
- DNS resolution must be reliable

Optional but common:

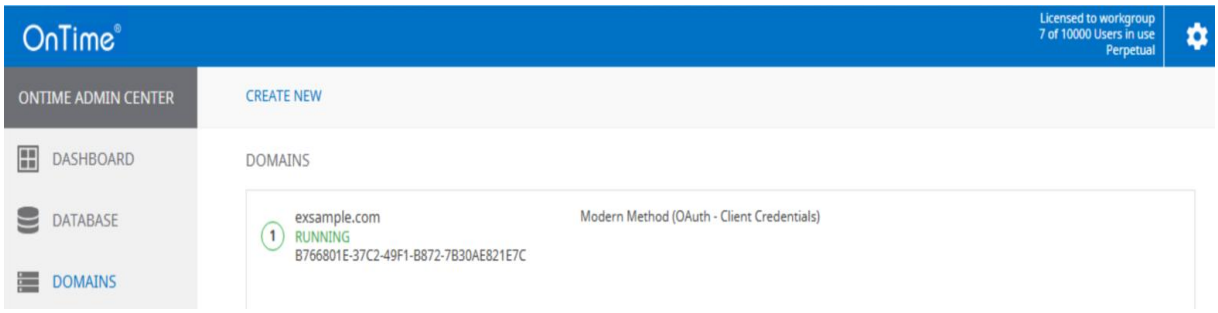
- Reverse Proxy configuration for Incoming (internet → server)
- Private endpoints (advanced scenarios via Microsoft Entra ID)

Configuration of Subscription Methods in OnTime Admin

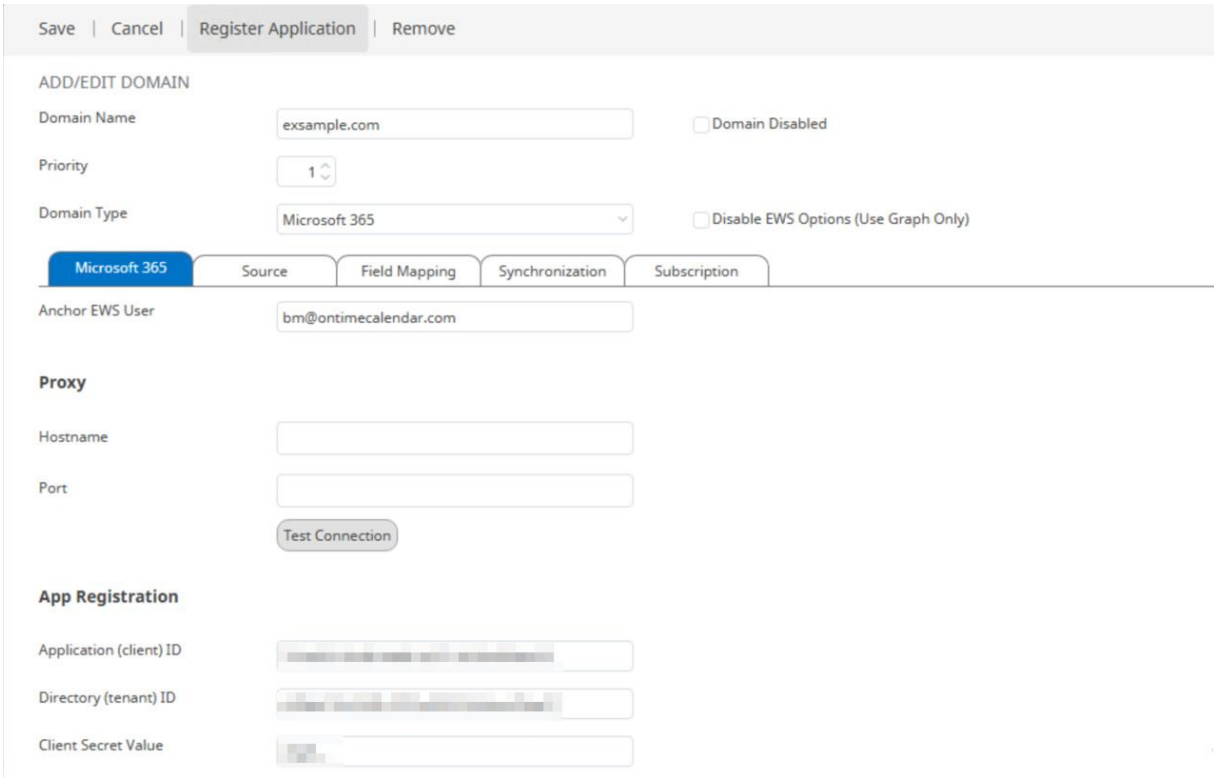
Navigate to OnTime admin dashboard



and choose ‘Domains’



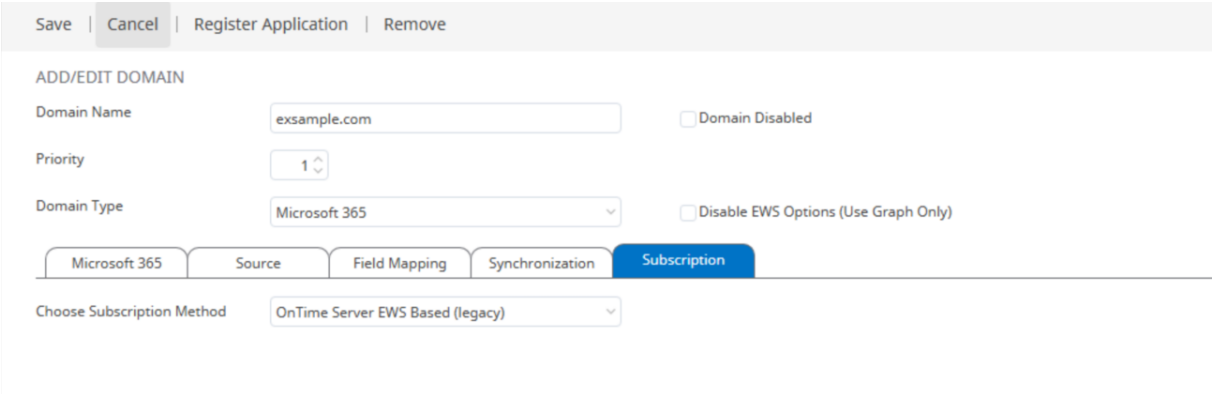
Select the ‘Subscription’ Tab



Configuring Subscription Methods in OnTime Admin

a) 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 application. (see the example below)

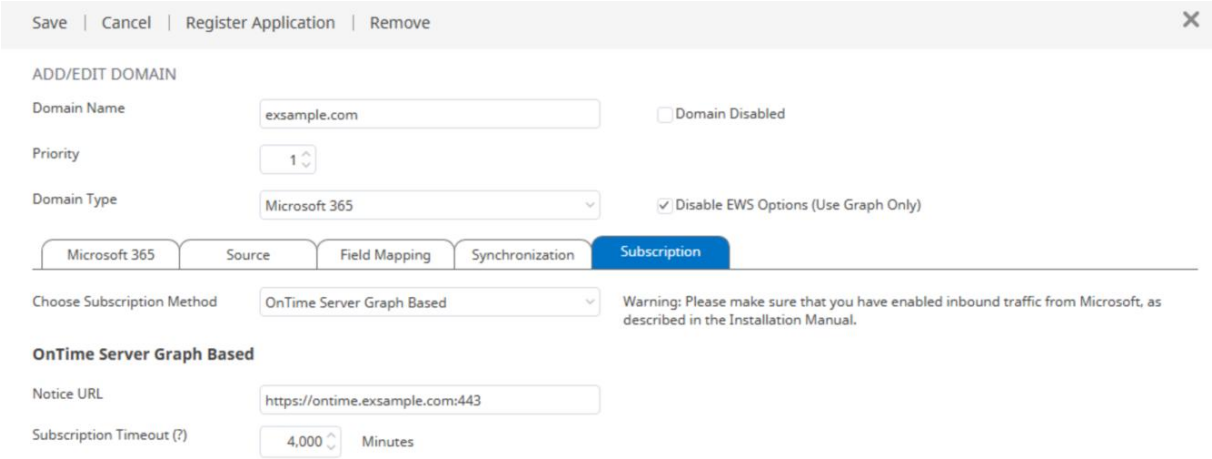


b) Using OnTime Server Graph Based event subscription

From the 'Choose Subscription Method' drop-down list, select **'**OnTime Server Graph Based'.
Follow the section "Prerequisites for Graph-Based OnTime Server Configuration"

In the **'**Notice URL' field, enter the full HTTPS OnTime server URL including the port number.

Click 'Save'. Then, in the OnTime Dashboard, stop and restart the application.



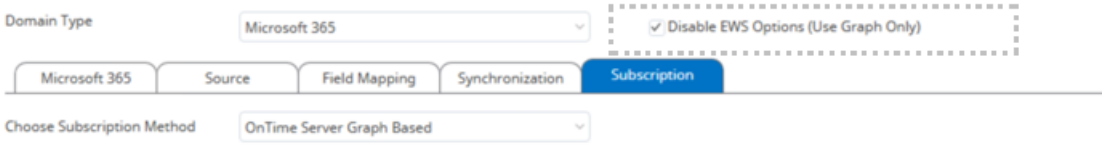
c) Using External Subscription Hub Graph-Based event subscription

From the drop-down list**,** **'**Choose Subscription Method', select **'**External Subscription Hub Graph-Based'. Go to Subscription Hub Configuration

Full disable using EWS

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.

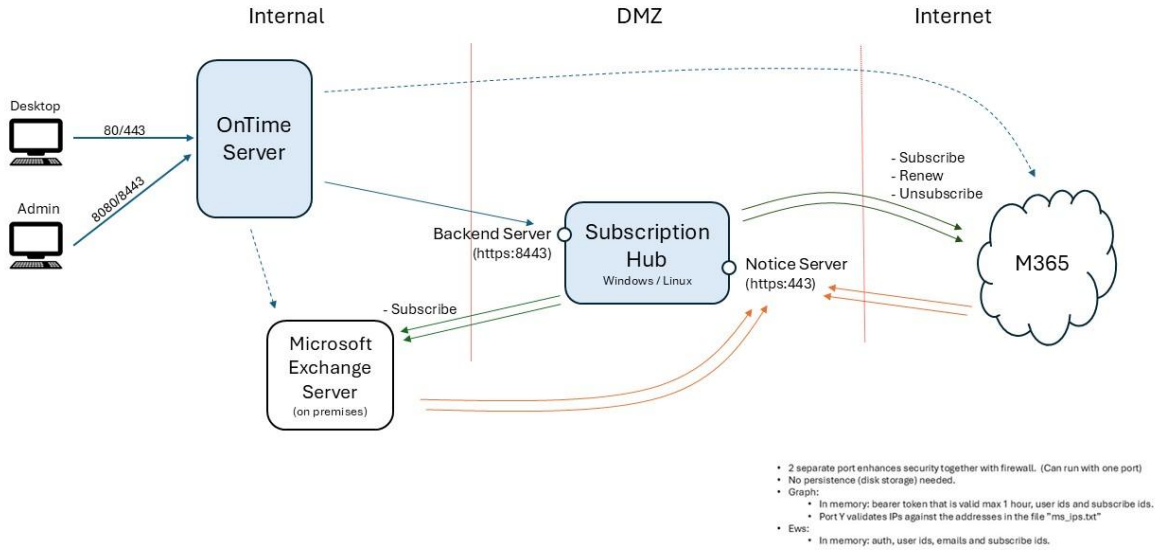
This will switch all configurations to use only Microsoft Graph, and EWS can then be disabled at the tenant level.



External Subscription Hub Graph Based / Subscription Hub Topology

For many years, the notification mechanism in OnTime for Microsoft has relied on **streaming subscriptions**, a technology that in turn depends on **Exchange Web Services (EWS)**. However, Microsoft has officially announced the deprecation of EWS in Microsoft 365, and with it the end of streaming subscriptions. This change is currently scheduled to take effect on **October 1, 2026**.
Once EWS is removed, the existing subscription-based notifications used by OnTime in Microsoft 365 will no longer function. Streaming subscriptions will continue to work for OnTime connected to an Exchange on-premises environment.

To address this – and to introduce a more robust, scalable, and future-proof synchronisation model — we have introduced the **OnTime Subscription Hub** in OnTime for Microsoft.



Why the Subscription Hub?

- **Removes dependency on EWS** by moving from streaming subscriptions to Microsoft Graph-based technology
- **Improves scalability and performance** by offloading subscription handling from the main OnTime server
- **Prepares all OnTime environments for the coming Microsoft 365 changes**

By separating the subscription handling into its own dedicated service, the Subscription Hub significantly reduces processing load on the core OnTime server. For that reason, **we in general recommend running the Subscription Hub on a separate system rather than on the main OnTime server**.

Requirements:

Operating System

- **Windows:** Windows Server 2019 or later, or Windows 10 or later
- **Linux:** Kernel 4.18 or later, glibc 2.28 or later

CPU

- The Subscription Hub service requires a single CPU core.
- Additional cores may be beneficial for the operating system but are not required by the application.

Memory

- Operating system requirements **plus 1 GB** for Subscription Hub.
- Actual memory usage depends on the number of subscriptions (users).
- The service consumes **less than 1 KB of RAM per subscription**.

Disk

- Operating system requirements **+ 1 GB** for application files and logs.

Network

- The Subscription Hub requires inbound access from the internal OnTime server on port **80 or 443**.
- It is recommended deploying Subscription Hub in a DMZ, as this avoids the need to open additional firewall ports.

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	Allows the app to read events in user calendars
User.Read	Allows users to sign in to the app and allows the app to read the user’s profile

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’

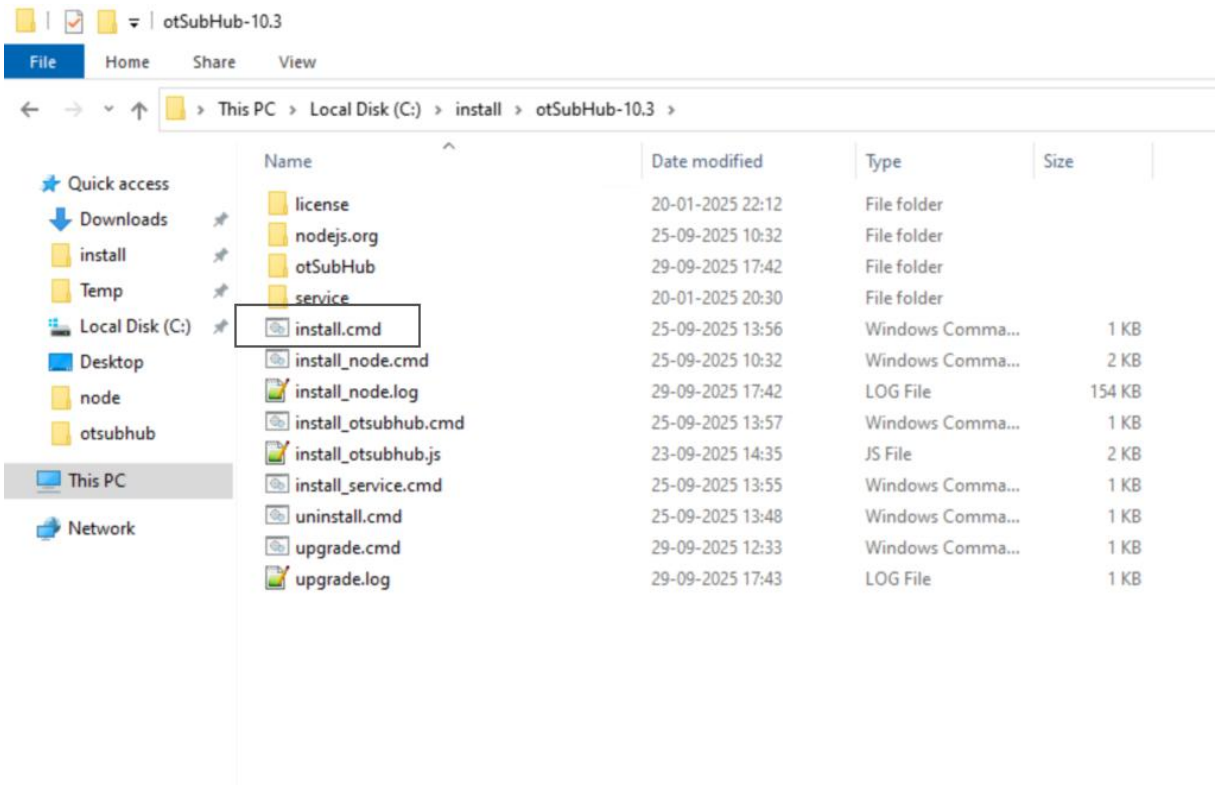
p) Click "Grant admin consent for *Your Company*"
Click ‘Yes’ to answer the question ‘Do you want to grant consent ...’

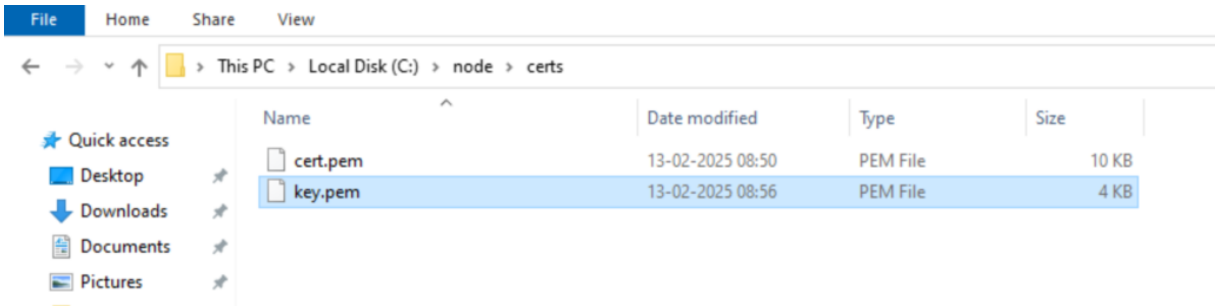
Subscription Hub "otSubHub" Installation and Configuration Steps

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'.

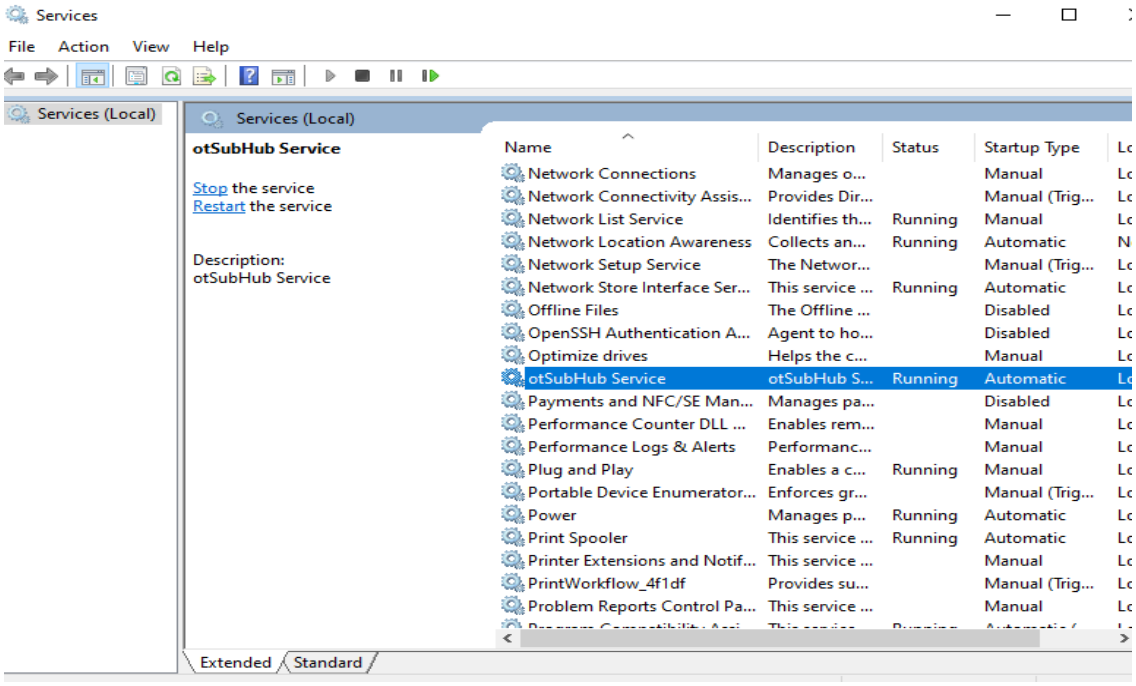

otSubHub-10.3
File
Home
Share
View
This PC › Local Disk (C:) › install › otSubHub-10.3 ›
Quick access
Downloads
install
Temp
Local Disk (C:)
Desktop
node
otsubhub
This PC
Network
Name
Date modified
Type
Size
license 20-01-2025 22:12 File folder
nodejs.org 25-09-2025 10:32 File folder
otSubHub 29-09-2025 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

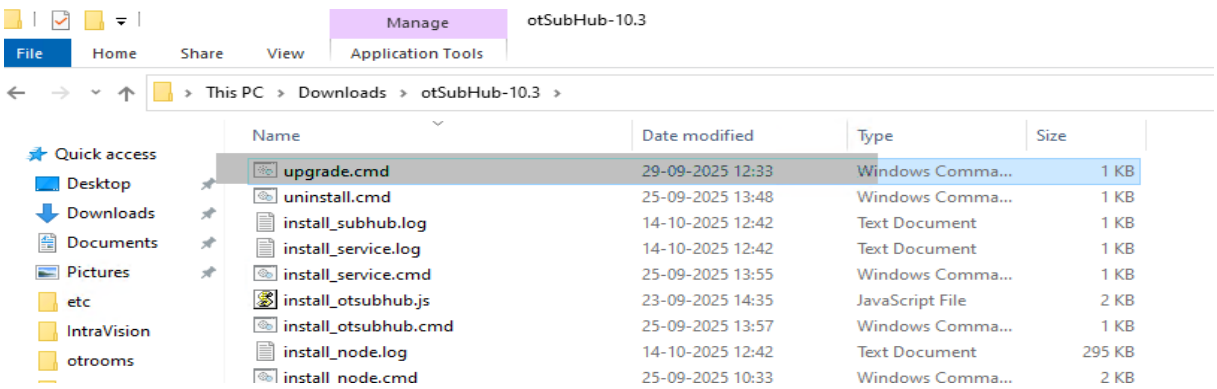
See the section *Microsoft Graph Change Notifications* for more information

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

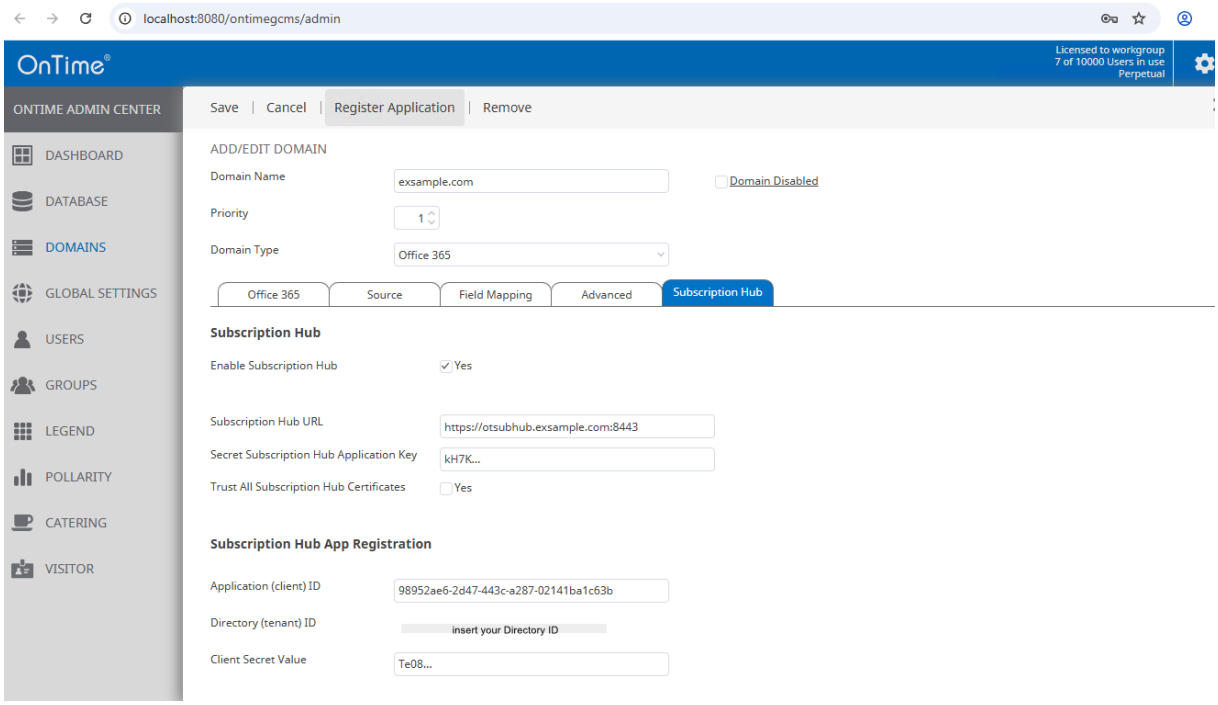
1. Copy Credentials
   Copy the values of the ‘Client Application ID’ and ‘Client Secret Value’ from the registered Subscription Hub application into a text editor, e.g., Notepad

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).

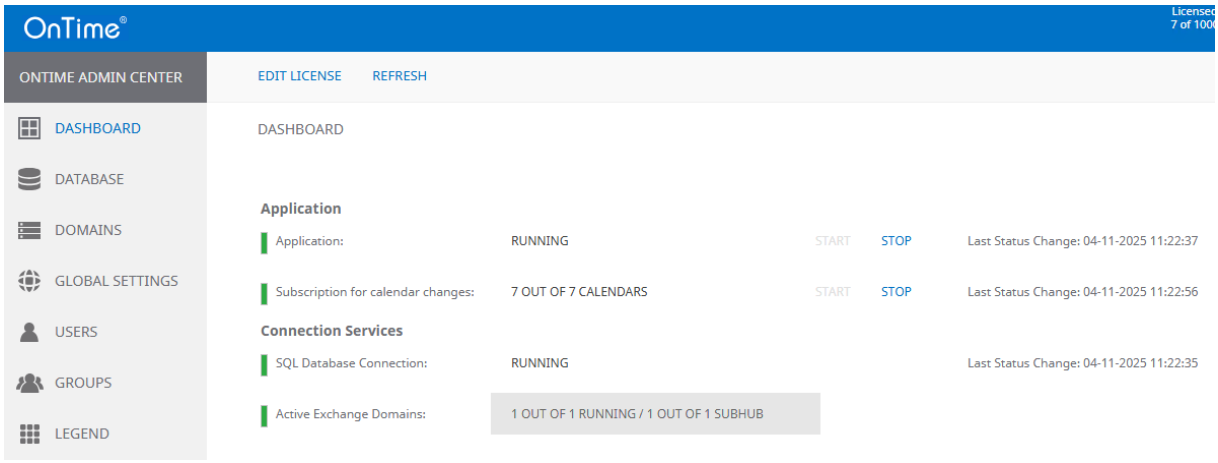
5. Set Subscription Hub URL
   Open the ‘otSubHub.json’ file located in ‘C:\node\otsubhub’ in a text editor, copy the Subscription Hub URL (including the port number) values, and paste it into the ‘Subscription Hub URL’ field (see example below).
6. Insert Secret Key
   Open the ‘otSubHub.json’ file 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).



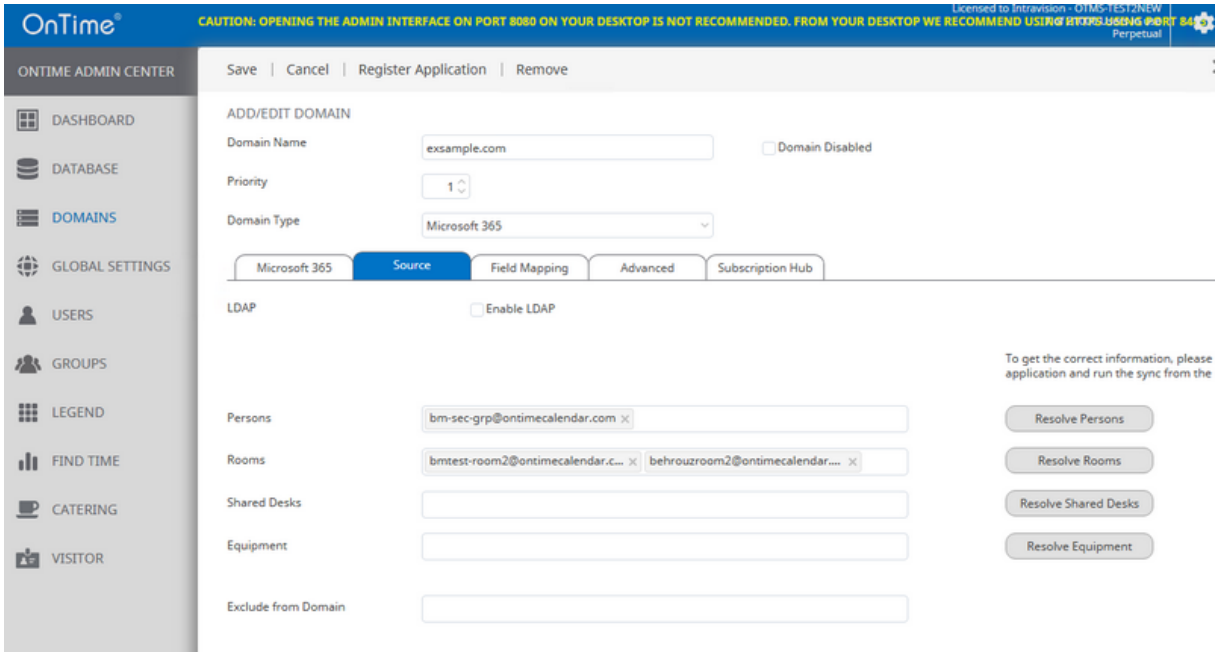
An example of the 'otSubHub.json' file is shown below.

```
{
        "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": " kH7KoGfl42Wqp5f/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.

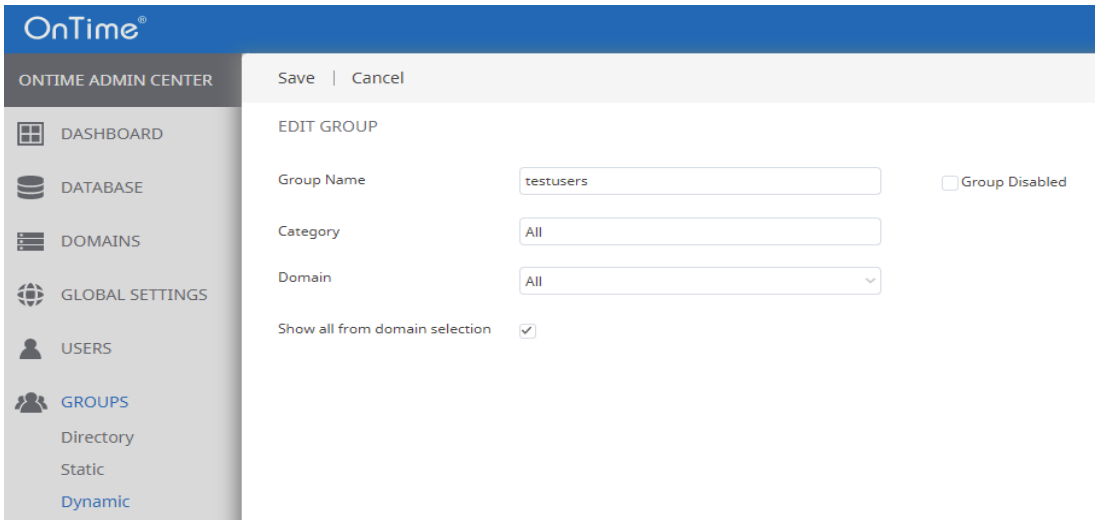
To reflect your new settings, go to the Dashboard - Stop and Start the Application. Then check that the "Database Service" and "Exchange Service" both show "Running"

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'.

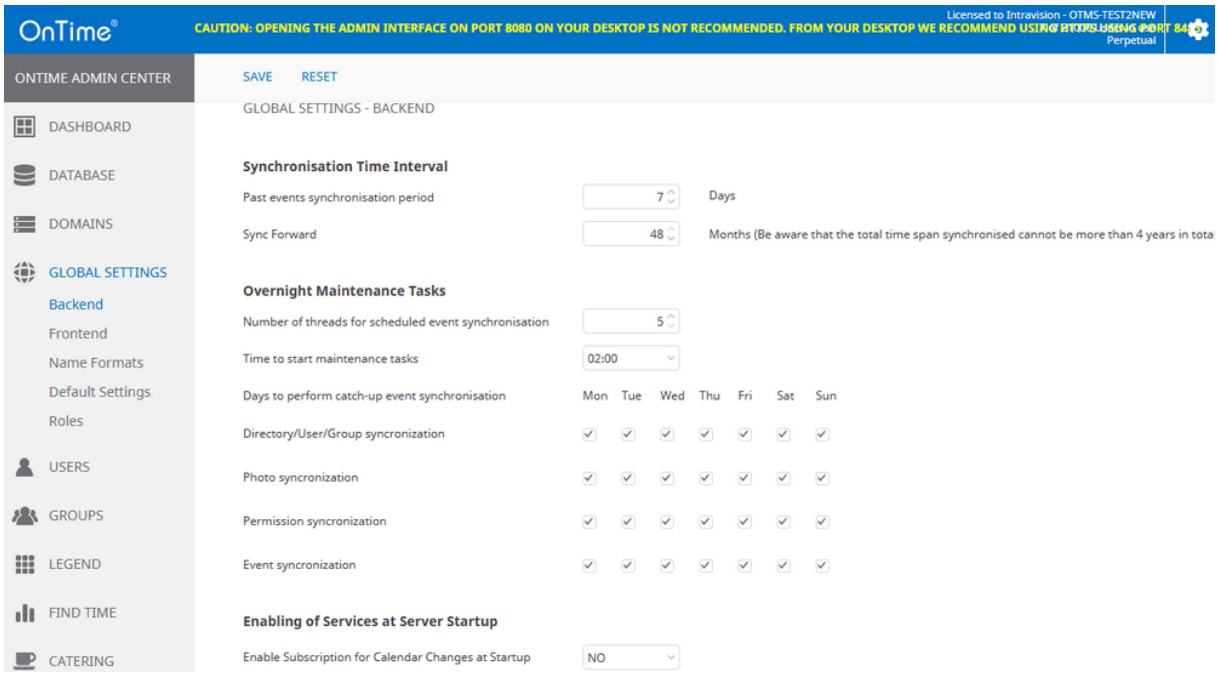
Changes in the 'dynamic groups' must be followed by clicking "Start" at "User & Group Sync" in the **Dashboard.**

Global Settings - Backend

Click Global/Backend

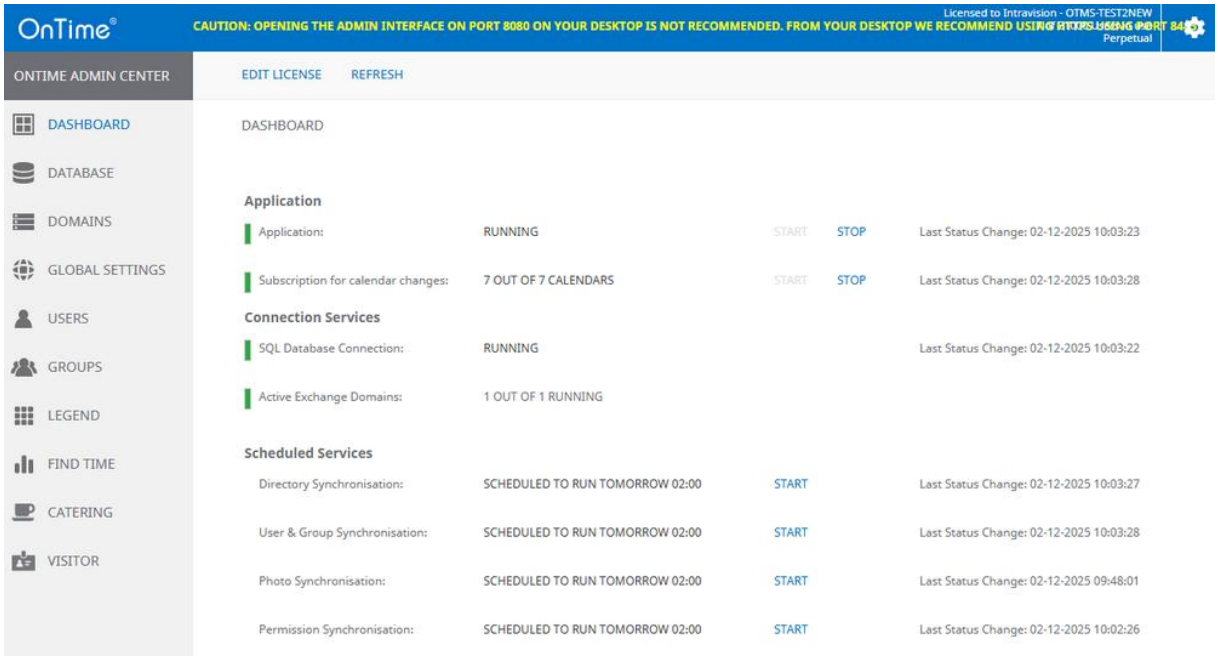
Choose 'Yes' at ‘Enable subscription for Calendar Changes at Startup'.

- 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.

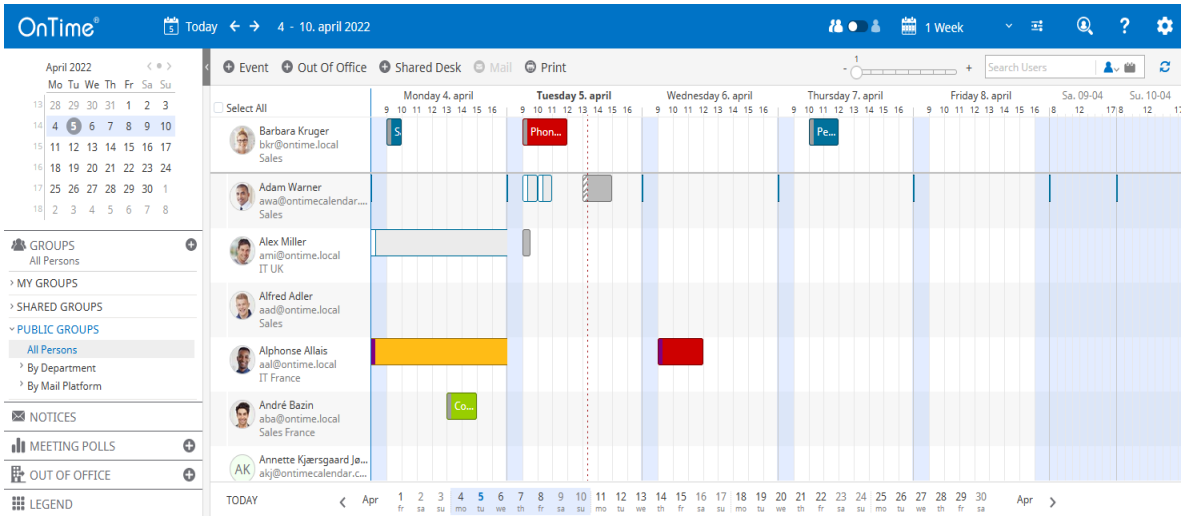
OnTime User – Calendar

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’