for Microsoft

Installation & Configuration Manual
OnTime® for Microsoft version 6.4.x

Revision 11

OnTime is a registered community trademark (#004918124). The trademark is registered with the Trade Marks and Designs Registration Office of the European Union.
OnTime is a registered Japanese trademark (#5569584). The trademark is registered with the Japan Patent Office

OnTime® for Microsoft

© IntraVision ApS,

IntraVision

Installation Manual

The main audience for this manual is Microsoft administrators with proper experience in Windows Server and Exchange on-premises /Microsoft 365 (Previously known as Office 365) administration. The reader of this manual is expected to be familiar with the Microsoft environment.

Table of Contents

About OnTime® for Microsoft 6
OnTime API 7
Pollarity 7
Catering 7
Visitor 7

Structure of the technical part of this manual 8

Preparing the new OnTime installation 9
OnTime Topology 9
Server requirements 10
Ports for Microsoft 365 11
Ports for Exchange on-premises 11
Prerequisites 12
External access to OnTime 12
User requirements 13
Supported internet browsers 13
OnTime Mobile add-on requirements 14
License key 15

OnTime Installation 16
Quick installation 17
Installing the SQL Server Express 17
Install OnTime 20
Manual installation 22
Command-line scripts 22
Create the OnTime database at the SQL server 23
Pollarity 33
Catering 35
Visitor 37
OnTime Server 39
OnTime add-on products 39
Database 40
Local SQL server 40
External SQL server, same Windows domain 41
External SQL server, outside the Windows domain 41

OnTime Configuration 42
OnTime Setup 42
License key 45
Domains 46
Authentication 46
Add Domain 47
Microsoft Exchange Online Subscriptions Methods 54
1. Legacy EWS Streaming Subscription 54
2. Microsoft Graph Subscription – Integrated OnTime Server 56
3. Microsoft Graph Subscription – External Subscription Hub 60

On-Premises configuration 66
Source *69*
Source, LDAP *71*
Field Mapping *73*
Add/Edit Domain - Advanced *74*
Synchronisation settings *75*
Global Settings *76*
Name Formats *87*
Name Formats/Advanced *88*
Default Settings *89*
Roles *97*
Users 100
Members *100*
API Users *106*
Combined Rooms *107*
Groups 108
Directory Groups *108*
Static Groups *109*
Dynamic Groups *111*
Linked AD Groups *113*
Legend 115
Definition *117*
Appearance *118*
Importance *118*
Languages *118*
Find Time 119
Configuration of Pollarity *120*
Configuration of 'Share my Time' *121*
Catering 122
Administering Catering *123*
URLs for 'Catering Manager' *124*
Visitor 125

OnTime User – Calendar 127
OnTime client Web Desktop 127
OnTime client Web Mobile 128

Add-ins for OnTime 129
Add-in for OnTime New Microsoft Outlook and in Microsoft Teams Navigation Panel *130*
User setup for Teams Channels *131*
Upload of add-ins for OnTime first time 133
Upload of add-ins for OnTime, Upgrade 134
How to add OnTime to a Teams Shared Channel: *136*
OnTime Pollarity - add-in in Microsoft Outlook 138
Your Microsoft Outlook, with OnTime Poll-add-in *138*
OnTime Catering add-in Microsoft Outlook *139*

Logfiles 142
OnTime, Pollarity Catering, Visitor Logs *142*

Appendices 144
Subscription Hub Platform Requirements 144
Register External Subscription Hub in "Microsoft Entra ID" *145*

Installation and Configuration of the External Subscription Hub 'otSubHub' *147*
Upgrading Subscription Hub (otSubHub) *150*
Configuring the Subscription Hub in OnTime Admin *151*
Register External Subscription Hub in "Microsoft Entra ID" *155*
Installation and Configuration of the External Subscription Hub 'otSubHub' *157*
Upgrading Subscription Hub (otSubHub) *160*
Configuring the Subscription Hub in OnTime Admin *161*
OnTime server components and ports 163
Integrating OnTime Group Calendar with other systems 164
Integrating and launching OnTime from other solutions using custom URLs 164
Creating Integrations with OnTime Desktop 166
Open the desktop client with a specified user selected. *166*
Open the desktop client with a public group selected *167*
Open the desktop client creating a new entry *168*
Open the desktop client creating a poll *168*
Open the desktop client in a view *169*
Open the desktop client a certain date with 'View start' *170*
Open the mobile client with a selected group *170*
Open the mobile client with an existing Entry Selected *171*
Redirection whitelists 173
CORS 174
SSL certificates for the OnTime Tomcat Server 175
SSL certificates for the OnTime Auth Service 177
SSL root certificates for the OnTime server 179
OnTime Authentication Token 181
OnTime Domain Authentication (SSO) 182
Customisation of the "OnTimeMS Auth" service 183
Browser setup for SSO 184
ADFS login (SSO) 185
Whitelist 189
SQL Server network protocol setup 190
External access to OnTime 191
Mapping of directory fields 196
Configuring private settings for Rooms 197

About OnTime® for Microsoft

OnTime® for Microsoft (hereafter OnTime) provides your organisation with an overview of where people are, what they are doing right now, and what they will be doing in the future. Further, OnTime provides youOnTime is configured and administrated through an admin web interface. a rich graphical interface and simple access.

OnTime presents other users' calendar information according to the individual Exchange access rights of the logged-in user combined with access rights granted by roles in OnTime. If user access rights are determined by groups in Exchange, OnTime supports non-hidden groups.

OnTime is configured and administrated through an admin web interface. A server task allows for almost real-time updates of the group calendar when a user creates, updates, or deletes a calendar entry in the personal Microsoft Outlook calendar.

We offer the following clients and interfaces:
OnTime Web Desktop

- OnTime Add-in for Microsoft Teams
- OnTime Add-in for Microsoft Outlook
- OnTime API – Licensed separately for other applications than standard OnTime
- OnTime Web Mobile – Licensed as an OnTime add-on
- OnTime Pollarity – Licensed as an OnTime add-on
- OnTime Catering – Licensed as an OnTime add-on
- OnTime Visitor – Licensed as an OnTime add-on

Note: The OnTime server must be configured with a certificate from a publicly trusted certification authority - unless you run OnTime with an on-prem Exchange Server without add-ins for Microsoft Teams, Microsoft Outlook, etc. We highly recommend running OnTime with secure communication.
Ref. to SSL certificates for the OnTime Auth Service

OnTime API

If you have developed calendar applications based on the OnTime API v1, you must adapt the applications to API v3.
OnTime API ver. 1 is no longer supported. Documentation for OnTime API v3 is available from www.ontimesuite.com upon request.

Pollarity

Pollarity is an optional module which supports voting for the most suitable meeting time.

Catering

Catering is an optional module which is the organisation's one-stop shop for managing catering within the organisation, in a simple and time-saving way for everyone involved.

Visitor

Visitor is an optional module for the organisation's ability to register and manage visitors within the organisation, in a simple and time-saving way for everyone involved.

Flyway database tool

An OnTime tool called 'otdbupdate.cmd' is used to install and update databases. This tool is powered by the open-source tool 'Flyway'.

Structure of the technical part of this manual

In the “Preparing the new OnTime installation” section we will provide you with an overall understanding of the main technical components of the OnTime product and what you need to have prepared before you can begin the actual installation process.

The manual then continues with the installation and configuration of your OnTime environment.

The actual installation process can be performed as either a ‘Quick installation’ or a ‘Manual installation’.

Quick installation
- a MSSQL server 2019/2022/2025 Express database server is installed on the OnTime server

Manual installation
- additional configuration options are described, including the use of an MSSQL server installed externally to the OnTime server.

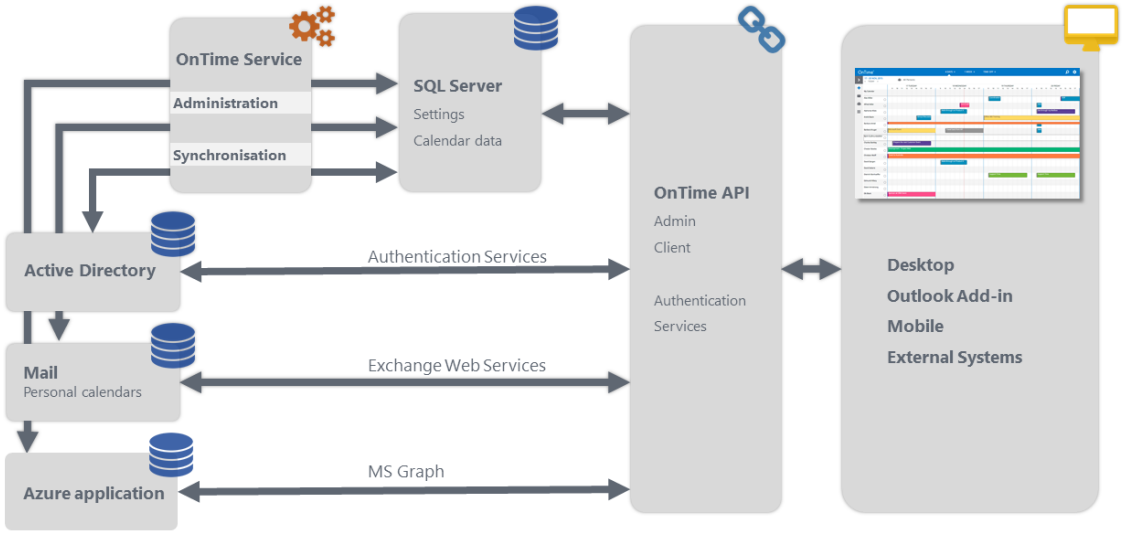
OnTime configuration
- the ‘OnTime Admin Centre’ with the ‘Dashboard’ for stopping and starting the different processes in the backend
- configuration of user synchronisation
- different types of user groups.

OnTime clients
- OnTime Web Desktop, Microsoft Teams, OnTime Web Mobileand an add-in for Microsoft Outlook

Preparing the new OnTime installation

OnTime Topology

The diagram below shows the overall topology of the OnTime Group Calendar for Microsoft.



Server requirements

The following requirements represent the minimum specifications based on our experience from multiple installations of OnTime Group Calendar. These guidelines provide the foundation for a functional system. However, as the number of users increases or additional modules are deployed, the resource requirements will also grow. Furthermore, factors such as backup processes, antivirus software, or other server activities can significantly impact performance and must be considered. We strongly recommend utilizing performance measurement tools in your specific environment to assess whether additional resources are necessary to support the increased demands of your installation.

The following server requirements are based on our experience from several installations.

OnTime must be installed while logged in as a Windows administrator.

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

For small and medium-sized installations of OnTime, you can use Microsoft SQL Server® 2019/2022/2025 Express which is free.

We recommend using the full Microsoft SQL Server if your OnTime installation has more than 2,000 users.

For further comparison between the Express and the full version of the SQL Server: https://learn.microsoft.com/en-us/sql/sql-server/editions-and-components-of-sql-server-2019?view=sql-server-ver15&preserve-view=true

Processor
Intel-compatible processor(s) with a minimum speed of 2 GHz or higher

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 of dedicated disk space for the OnTime solution

The above specification has been tested with environments with 2000 users.

As with most software solutions, we prefer a dedicated server for the OnTime solution. Should you, however, choose to install on a multi-purpose server we have the following minimum requirements:

Installing OnTime on a Windows Server running a Microsoft Exchange Server is not recommended.

If you want to use an existing MS SQL Server installation, it must have TCP/IP enabled on TCP port 1433.

The Tomcat application server must be dedicated exclusively to OnTime.

Ports for the OnTime server

Ports 80 and 9080 must be 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.
Port 8443 is required for the admin client; HTTPS is supported remotely.

Ports for Microsoft 365

If OnTime configuration for Microsoft 365, please verify outbound firewall access (port 443) from the OnTime server:

https://login.microsoftonline.com
https://graph.microsoft.com
https://portal.azure.com

Ports for Exchange on-premises

Port 443 must be open to the Exchange server.

Prerequisites

AD domain

The OnTime server can be part of your user Active Directory domain to ensure your OnTime users' web authentication (SSO) without requiring users to enter their AD passwords.
An OnTime server installed in a Windows workgroup is supported. However, this configuration is recommended only for test or isolated installations.

SQL Server 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.
Note: For larger installations, we do not recommend SQL Server Express

Note: Microsoft mainstream support for SQL Server 2016 ended in July 2022.

SQL Server Express Limitations

Maximum Database Size	10 GB
Compute Capacity	1 socket or 4 cores
Maximum Memory	1 GB

Create a user for OnTime in Exchange/Microsoft 365

Mailbox user (minimum type 1, if in Microsoft 365)

External access to OnTime

OnTime is most often installed on a server in the internal network. When external access to desktop and mobile clients is required, the configuration of the firewall and DMZ must be considered.

Solutions include VPN access or a reverse proxy server in the DMZ. Scenarios are described in the appendix External access to OnTime.

User requirements

Supported internet browsers

Due to the increased rate at which vendors are now releasing new versions of their browsers, support for browser updates will only be maintained for the most recent shipping release of OnTime. OnTime product testing on new browser versions will continue at periodic intervals which may or may not align with the browser vendor's release schedule. Should a problem be found when using a browser update with the most recent release of OnTime, we will make every effort to resolve the issue. To expedite this resolution, we recommend that you contact the browser vendor as well as IntraVision Support about the situation.

For the desktop users, Catering and Visitor Manager clients:
Refer to the OnTime Web Desktop client.
- The following browsers are supported:

	Chrome (Latest)	Safari (Latest)	Firefox (Latest)	Edge Chromium (Latest)
Windows	Supported	N/A	Supported	Supported
macOS	Supported	Supported	Supported	Supported

For the admin client
- The following browsers are supported:

	Chrome (Latest)	Safari (Latest)	Firefox (Latest)	Edge Chromium (Latest)
Windows	Supported	Not Supported	Not Supported	Supported

Only ports 80 and 443 are supported for the desktop client, and the browsers need to have cookies enabled.

OnTime Mobile add-on requirements

The OnTime Mobile add-on is a web app which uses a browser on the device. Due to the increased rate at which vendors are now releasing new versions of their mobile browsers, support for mobile browser updates will only be maintained for the most recent shipping release of OnTime. OnTime product testing on new mobile browser versions will continue at periodic intervals which may or may not align with the browser vendor's release schedule. Should a problem be found when using a browser update with the most recent release of OnTime, we will make every effort to resolve the issue. To expedite this resolution, we recommend that you contact the browser vendor as well as IntraVision Support about the situation.

Please refer to OnTime client Web Mobile
-The following browsers are supported:

	Chrome (Latest)	Safari (Latest)
Android (14 and later)	Supported	
iOS (18 and later)	Supported	Supported

-
OnTime Mobile web app add-on has the following specific requirements

- A smartphone with touch gestures
- JavaScript enabled
- Cookies enabled

License key

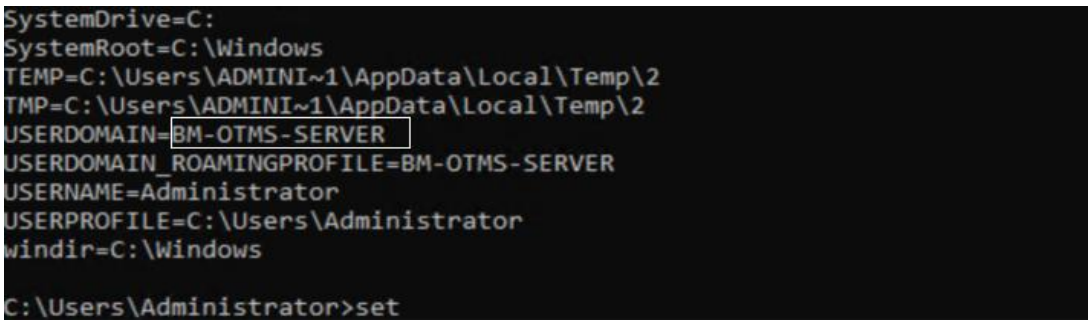
- OnTime requires a license key with the required number of users enabled to run.
- These keys are provided directly by IntraVision or an OnTime partner. A list of OnTime Partners is available at www.ontimesuite.com.

To obtain a license key, please provide the following info:

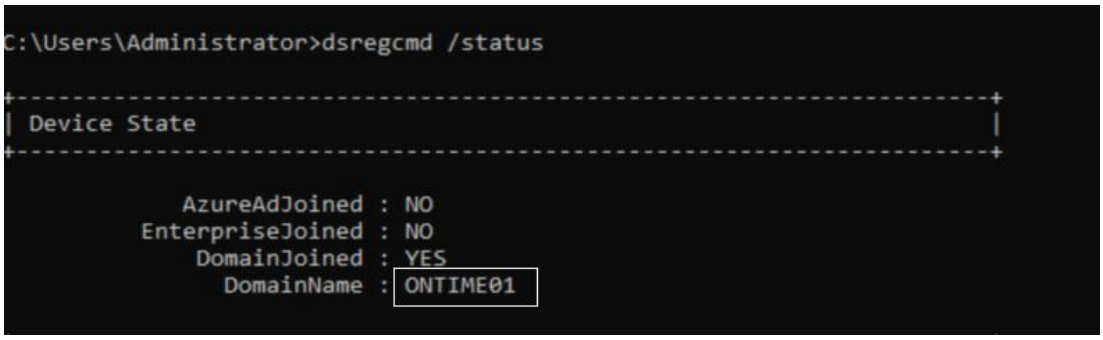
- your company name
- the total number of users, including rooms and equipment
- a. OnTime server in an AD domain,

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

  In a Command prompt > set (Enter) – to view your 'USERDOMAIN' and device name"



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



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

OnTime Installation

There are two options for installing OnTime: Quick installation or Manual installation.

Quick installation

The simplified installation procedure of installing OnTime
- with a local, silent installation of the MS SQL Server 2019/2022/2025 at 'C:\Program Files'
- one 'install' command file that in turn creates a database for OnTime, and installs Windows services for OnTime

Microsoft 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

Note: Run the SSMS tool as an administrator to obtain the required permissions to run queries against the OnTime database.

Manual installation

This method applies when you need to configure custom settings applicable if you need to be able to configure custom settings for the SQL server.
Please refer to the Manual installation.

Quick installation

Quick installation requires:

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

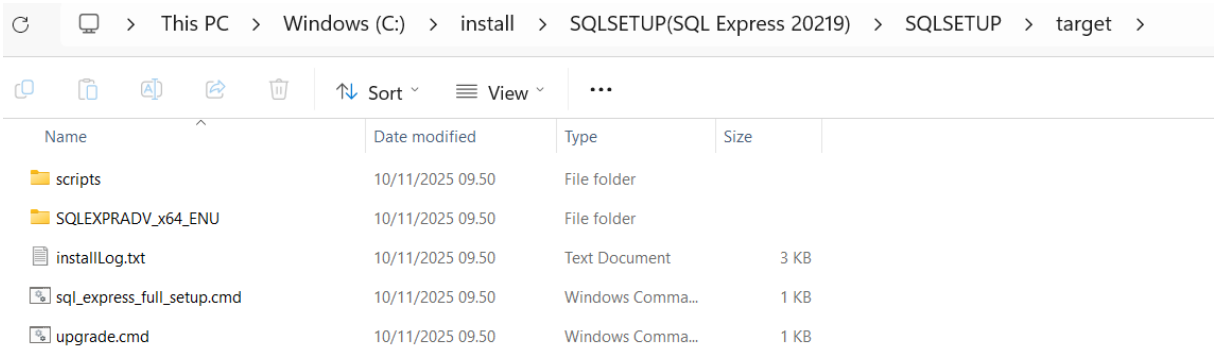
- Integrated Security is used, instead of SQL Server Security

- 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.

Installing the SQL Server Express

Extract the file downloaded from SQL Server 2019 Express



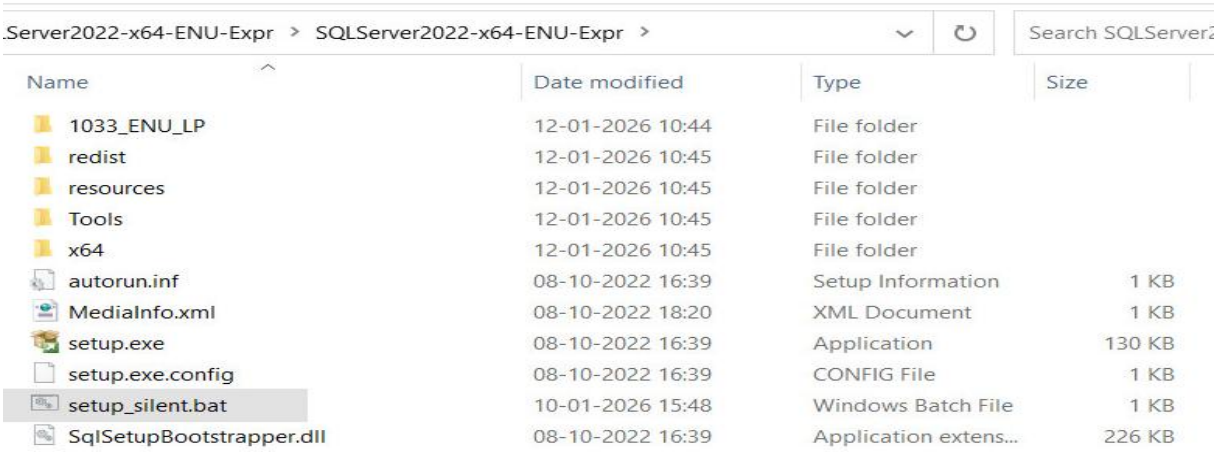
To install the SQL server, start a Command Prompt in administrator mode in the OnTime (silent) folder.

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

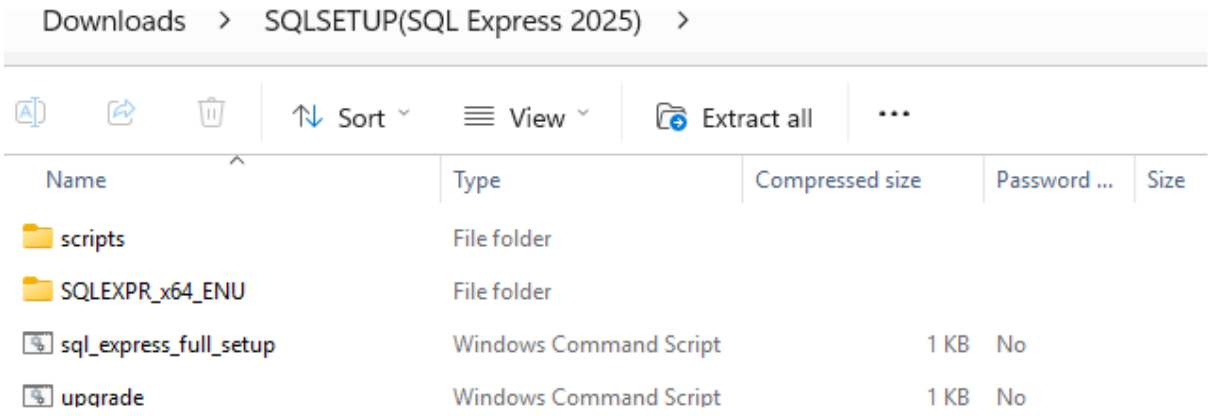


To install the SQL server, start a Command Prompt in administrator mode in the OnTime (silent) folder.

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.

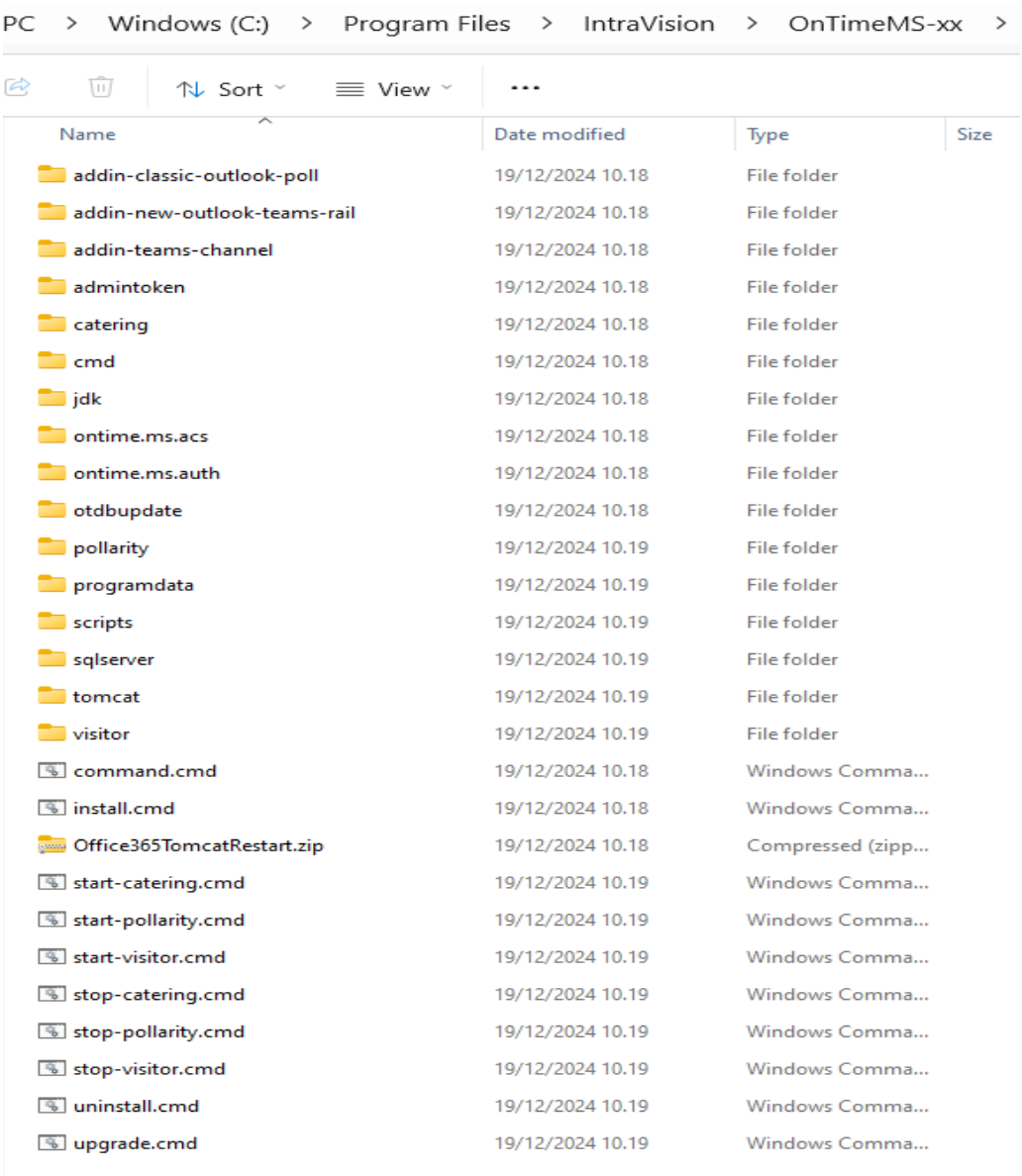
Run the command:
sql_express_full_setup.cmd

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

Unzip the downloaded OnTime package to a temporary location, move the directory OnTimeMS-x.x to the recommended path:
C:\Program Files\IntraVision\



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

This command will execute the following tasks:

1. You will be asked for a new password for the OnTime admin
   Note: Special characters may make the Tomcat server to fail to start
2. It will create the ‘ontimems’ database 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 server for OnTime.
   Windows service – ‘Apache Tomcat x.x OnTimeTomcat’
6. It will create a database, ‘pollarity’ for Pollarity
7. **Note:** Pollarity has an optional License.
8. It will create a database, ‘catering’ for Catering
9. It will create a database, ‘visitor’ for Visitor

   Note: Pollarity, Catering, and Visitor each have an optional license.

Proceed to OnTime Configuration

Manual installation

All components can be configured after completing the Quick installation. The only exception is the SQL Server.
This manual option is based on your installation of MS SQL Server, locally or externally to your OnTime server.

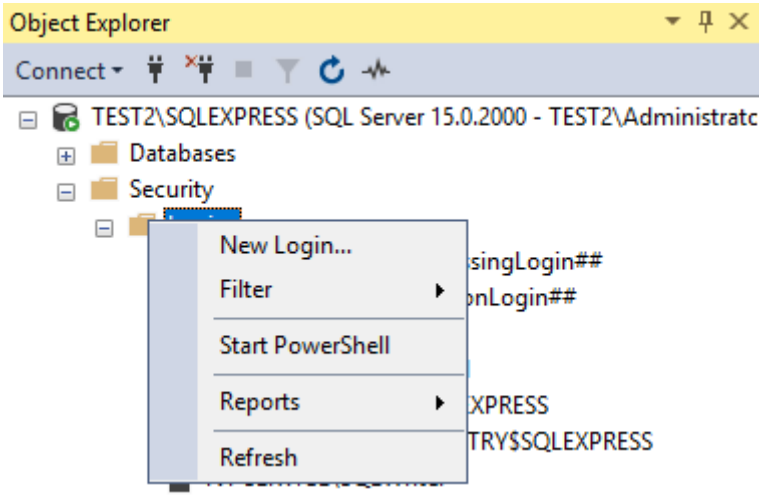
The network protocol TCP/IP must be enabled for the SQL Server; the default port is 1433. If you want to use another port, remember to enter your chosen port in the OnTime Admin client's Database section.
Refer to the SQL Server network protocol setup

'SQL Server Management Studio', SSMS is used in this section.

Command-line scripts

In order to run OnTime 'otdbupdate.cmd' scripts later in the SQL server, an administrative user 'BUILTIN\Administrators' is required with the database role 'db_owner'.

In SSMS right-click the SQL-servers Security section, click 'New Login'

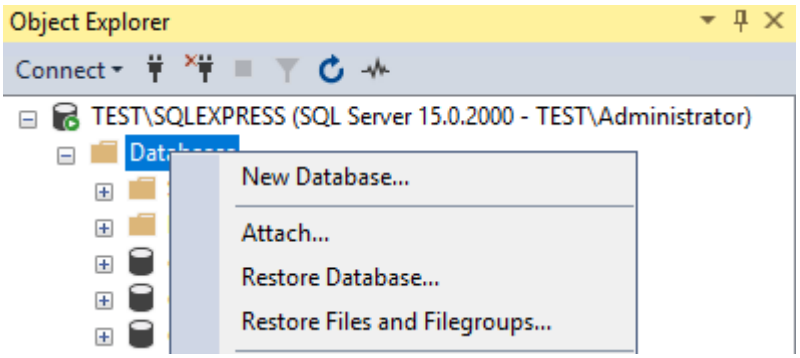


Enter the login name 'BUILTIN\Administrators'

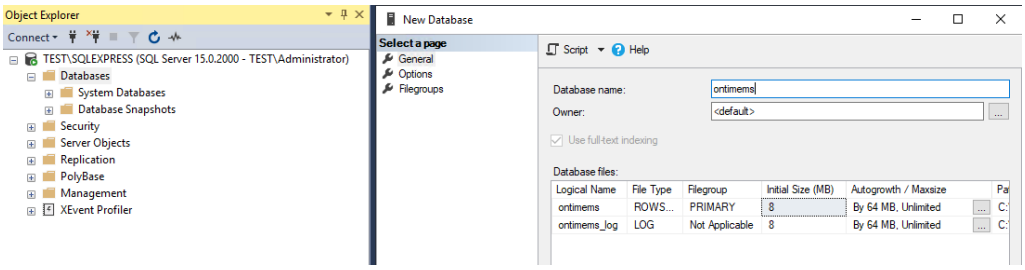
Click 'OK'

Create the OnTime database at the SQL server

At your MS SQL server create a new database with the name ‘ontimems’ for OnTime. In SSMS right-click ‘Databases’

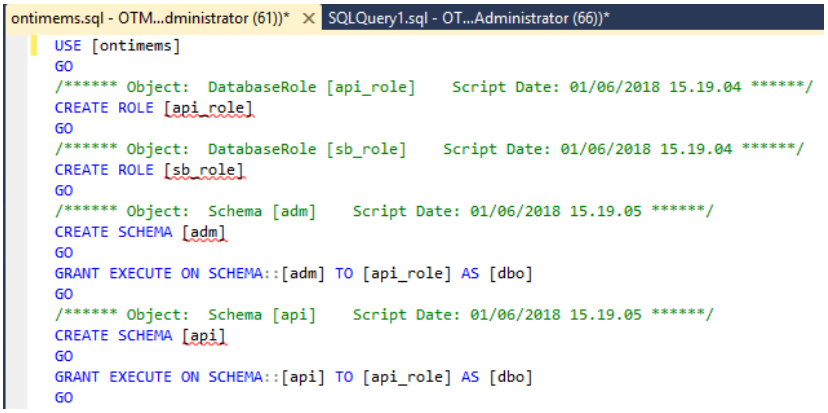


Click ‘New database’. Enter the database name ‘ontimems’. Click ‘OK’



In the folder: C:\Program Files\IntraVision\OnTimeMS-x.x\sqlserver\
you will find the sql-script – 'ontimems.sql'

You may open the script in "SQL Server Management Studio" or a text editor. Check the first line of the script. The first line must be changed to 'USE [ontimems]' instead of a programmatic parameter for the database name.



Two methods are possible to create the tables in the database 'ontimems', in SSMS or in the command-line.

1. SSMS: Click 'New Query'
   Copy all the text from the script, 'ontimems.sql' to the new Query Window. Click 'Execute'.

2. Alternatively run the SQL script from the command-line.

   C:\Program Files\IntraVision\OnTimeMS-x.x\sqlserver>

   sqlcmd -S .\SQLExpress -i ontimems.sql

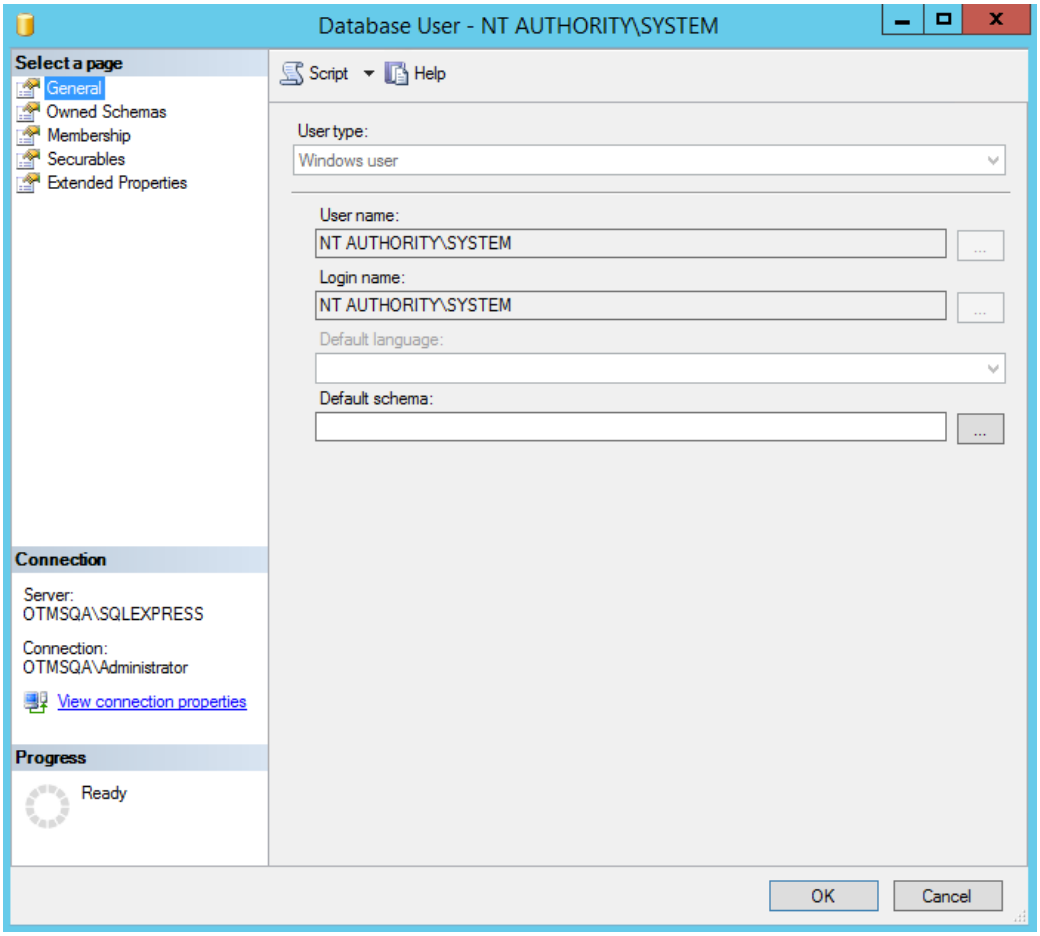
   - here SQLExpress is representing your SQL server's instance.

After running the SQL-script open the database and check that the database tables have been created.

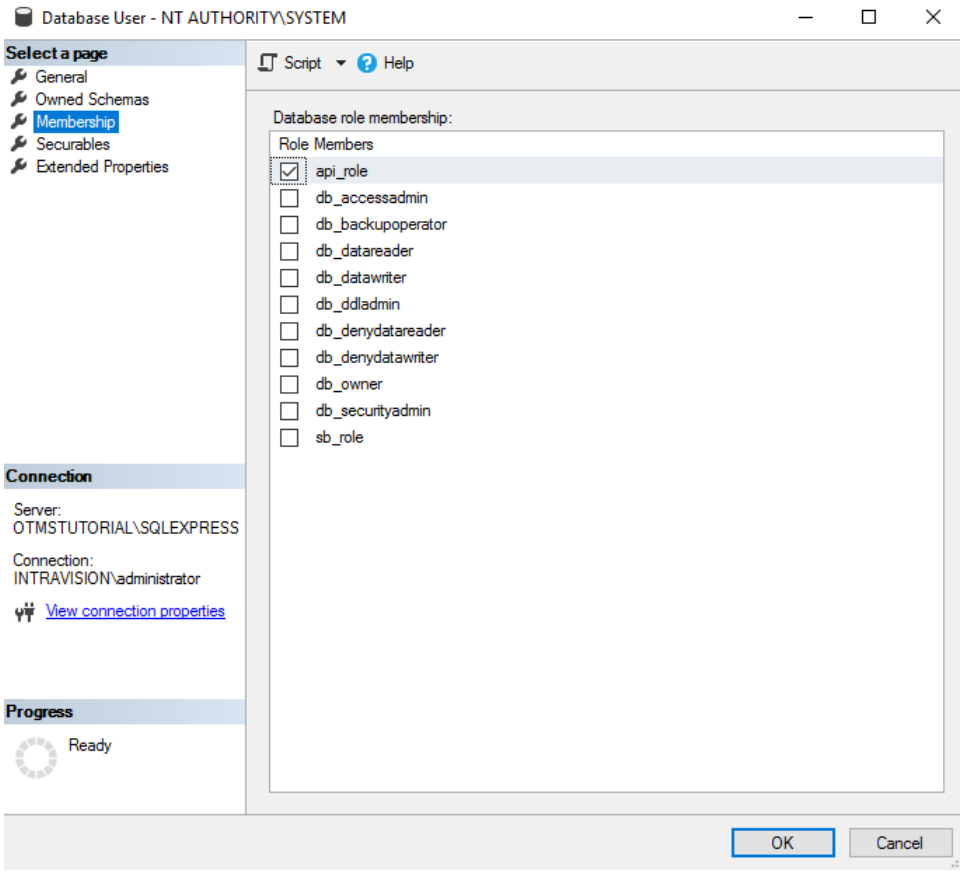
The OnTime application user, local SQL Server

1. In the OnTime database's Security section, right-click 'Users' and choose 'New User'. Click the button by 'Login name' and click 'Browse' Among the possible 'Logins', select 'NT AUTHORITY\SYSTEM' as the OnTime application user in the OnTime database. Click 'OK'.

Additionally, add 'NT AUTHORITY\SYSTEM' to the 'Username' field. Click 'OK'.



2. Click ‘Membership’ and select the ‘api_role’. Click ‘OK’.



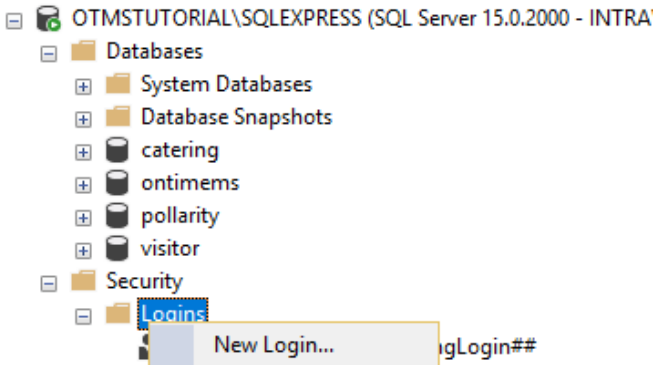
3. A configuration with the ‘NT AUTHORITY SYSTEM’ allows you to choose ‘integratedSecurity=yes’ in the database configuration.

   Please refer to **Database** in the ‘OnTime Configuration’ section.

4. Add an administrative user ‘BUILTIN\Administrators’ in the ‘ontimems’ database’s security section in the same way as above.
   In the ‘membership’ for ‘BUILTIN\Administrators’, tick ‘db_owner’ and click ‘OK’.

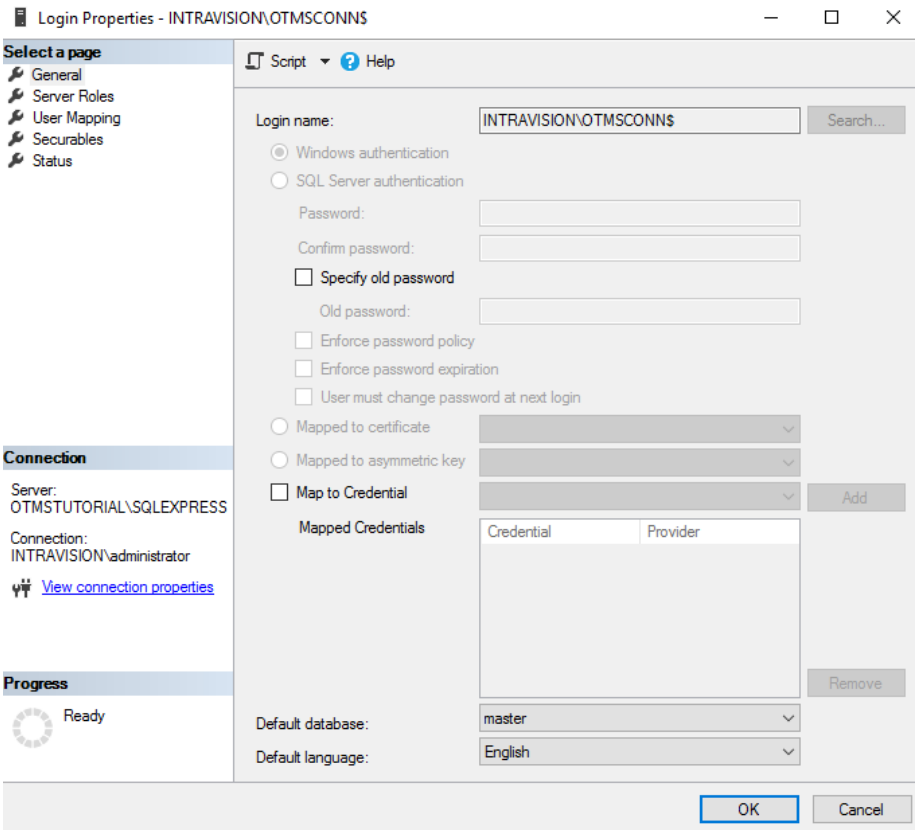
The OnTime application user, external SQL Server, same Windows Domain

In the SQL server's Security section, create a Login for access from the OnTime server. Right-click 'Logins', select 'New Login'.

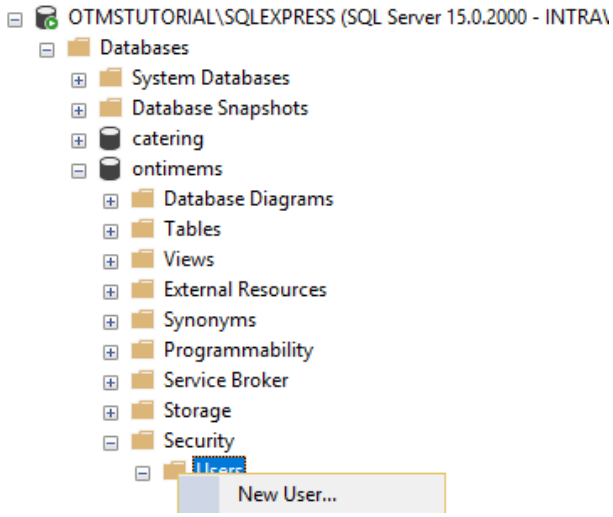


1. As 'Login name' you manually enter your OnTime server's hostname in the format: DOMAINNAME\HOSTNAME$
   - remember the '$' character at the end of the server's hostname.
   In the SQL server, this name is for authenticating your OnTime server.
   Note: Searching for the hostname is not possible – the name entered cannot be verified.

   Example:



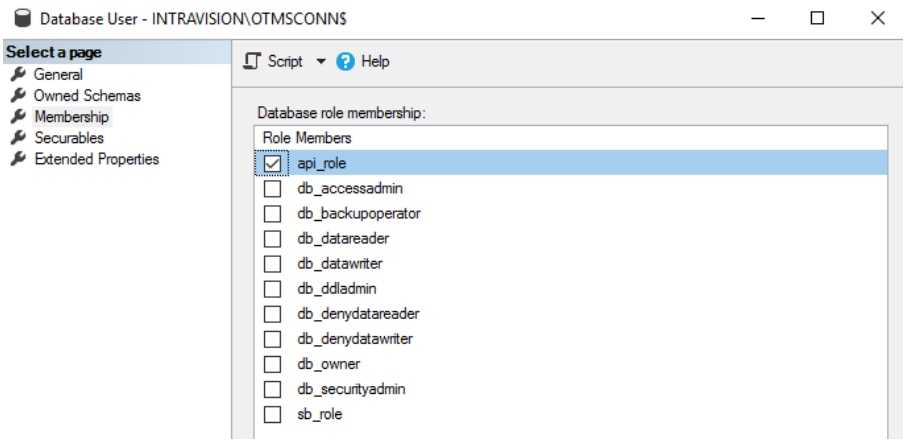
2. In the Security section of your new OnTime database, right-click Users, choose ‘New User’.



Click the button at ‘Login name’, click ‘Browse’ and choose the server Login entry you entered above.

Copy the ‘Login name’ to the field ‘Username’. Click OK

3. The server Login entry must have the role ‘‘api_role’



Click ‘OK’

4. Add an administrative user ‘BUILTIN\Administrators’ in the ‘ontimems’ database’s security section in the same way as above.
   In the ‘membership’ for ‘BUILTIN\Administrators’, tick ‘db_owner’ and click ‘OK’.

5. The database is now ready for access with ‘Integrated Security’ from the OnTime server within the same domain.

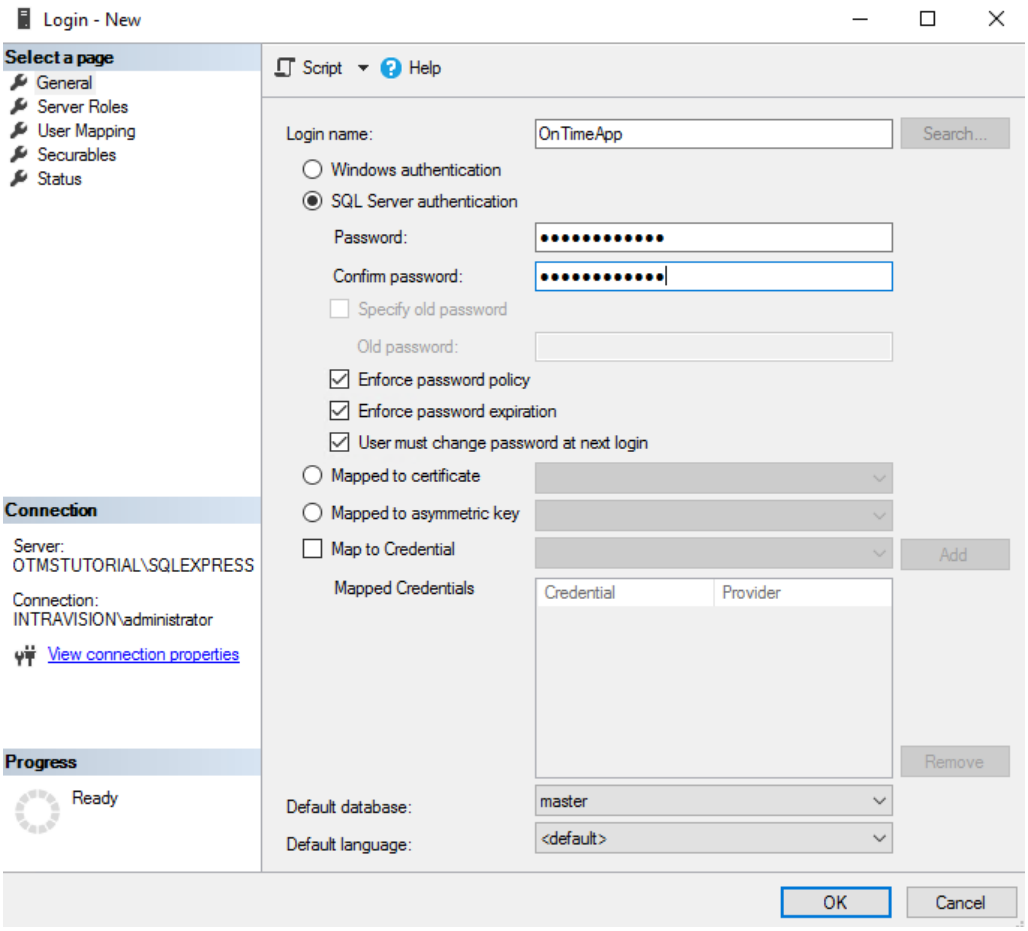
   Please refer to **Database** in the ‘OnTime Configuration’ section.

The OnTime application user, external SQL Server, outside the Windows Domain

The SQL server must be enabled for 'SQL Server and Windows Authentication'. If you have installed with 'Windows Authentication', you may change the authentication mode:

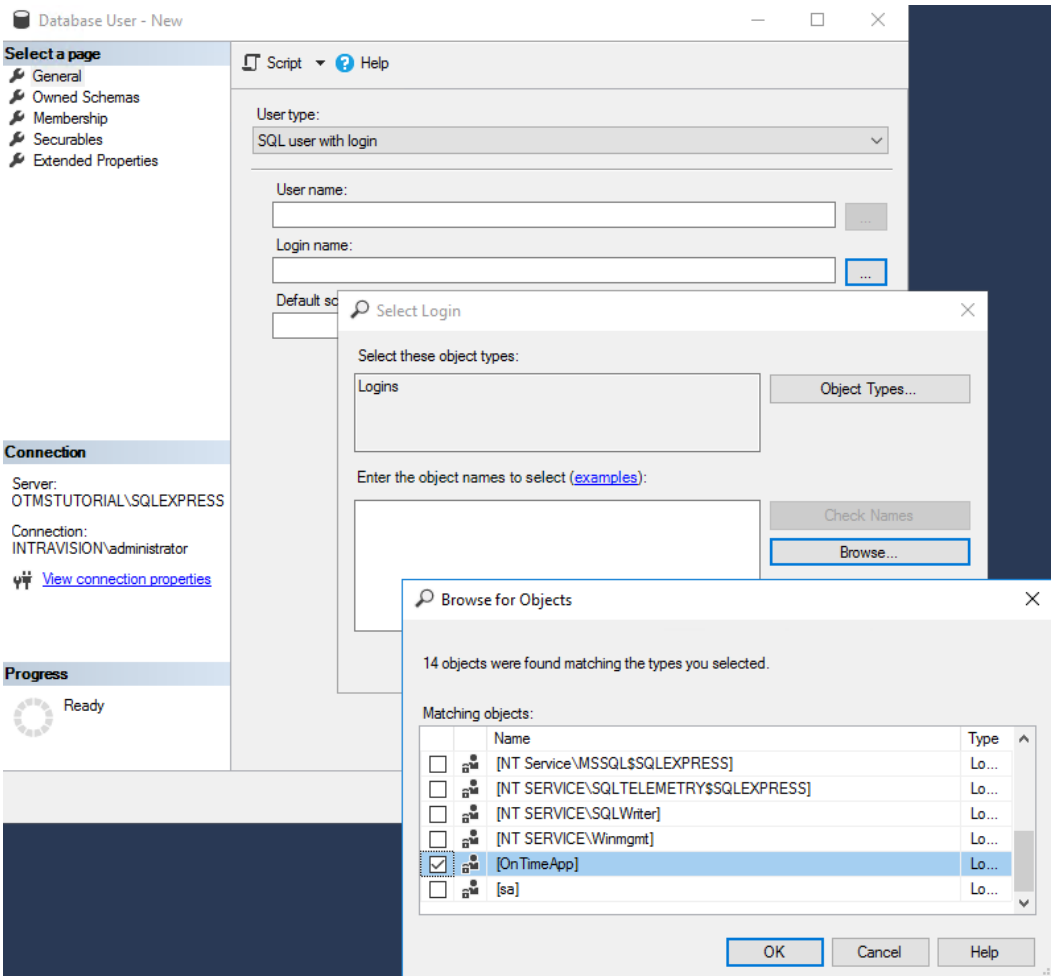
https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode?view=sql-server-ver15

1. In the SQL server's Security section, create a Login for access from the OnTime server. Right-click 'Logins', select 'New Login'.
   Enter a login name 'OnTimeApp'. Choose 'SQL Server Authentication. Enter a password twice. Make a note of the password. Click 'OK'

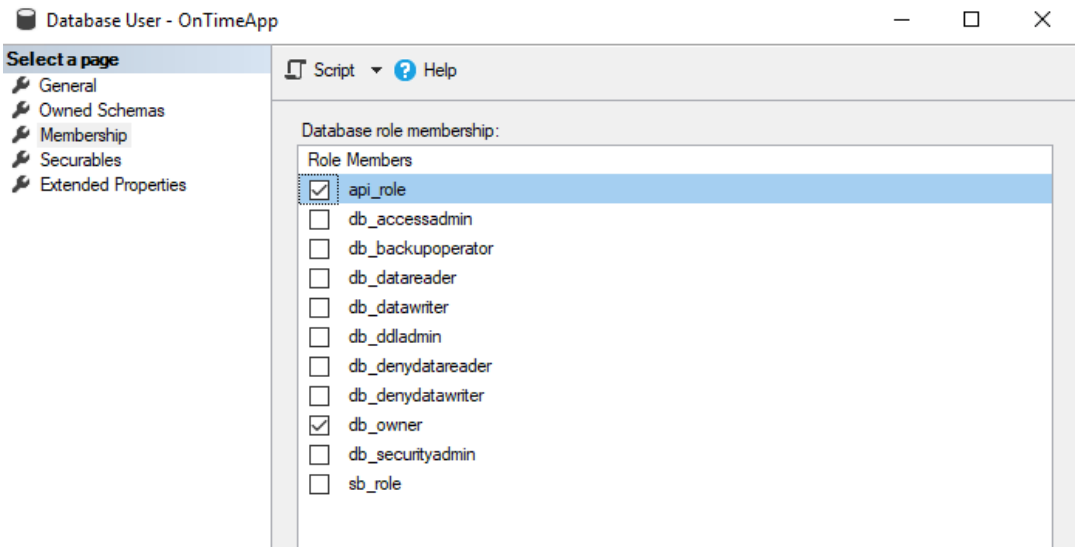


2. In the Security section of your new OnTime database, right-click Users, choose ‘New User’.

   At ‘Login Name’ click the button with the 3 dots. Click ‘Browse’. Choose the OnTimeApp user. Click ‘OK’. Copy the login name ‘OnTimeApp’ to the ‘Username’ field. Click ‘OK’



3. Right-click your new user ‘OnTimeApp’, choose properties.
   In the section ‘Membership’ select the api_role and the db_owner. Click ‘OK’



4. The database is now ready for access with ‘SQL Server Authentication’ from the OnTime server.

   Please refer to **Database** in the ‘OnTime Configuration’ section.

Update the OnTime database using 'otdbupdate.cmd'

From the folder C:\Program Files\IntraVision\OnTimeMS-x.x. open a command window as Administrator.

Note: Requires OpenJDK 17 or later (included with OnTime 6.4.x)

otdbupdate.cmd requires an environment variable for JAVA_HOME in your OnTime installation files.

Set the environment variable for **JAVA_HOME** by running the command:

```
set JAVA_HOME=C:\Program Files\IntraVision\OnTimeMS-x.x\jdk
```

Set the environment variable for **Path** by running the command:

```
set PATH=%JAVA_HOME%\bin;%PATH%
```

Navigate to `C:\Program Files\IntraVision\OnTimeMS-x.x\otdbupdate`

Run this command, if you are using integratedSecurity:

```
otdbupdate.cmd -skipDefaultCallbacks=true
-url=jdbc:sqlserver://localhost:1433;databaseName=ontimems;
encrypt=true;trustServerCertificate=true;
integratedSecurity=true migrate
```

All parameters must be entered on one line.

Run the following command if you are using a specific database user:

```
otdbupdate.cmd -skipDefaultCallbacks=true
-url=jdbc:sqlserver://localhost:1433;databaseName=ontimems;
encrypt=true;trustServerCertificate=true;
 -user=OnTimeApp -password=xxxx migrate
```

All parameters must be entered on one line.

Pollarity

Pollarity requires a database and the installation of an application on the Tomcat OnTime server.

Pollarity database

Depending on your setup of the SQL server, local or external to the OnTime server the process is similar to the section Create the OnTime database.

1. Create a database named '**pollarity'** in the SQL Server.
2. In the database's security section add a database user, the same as the database user of the 'ontimems' database.
3. Double-click the database user, select 'Membership', select db_owner, click 'OK'

Update the Pollarity database using 'otdbupdate.cmd'

From the folder C:\Program Files\IntraVision\OnTimeMS-x.x. open a command prompt as administrator.

otdbupdate.cmd requires an environment variable for JAVA_HOME in your OnTime installation files.

Set the environment variable for **JAVA_HOME** by running the command:

```
set JAVA_HOME=C:\Program Files\IntraVision\OnTimeMS-x.x\jdk
```

Set the environment variable for **Path** by running the command:

```
set PATH=%JAVA_HOME%\bin;%PATH%
```

Navigate to `C:\Program Files\IntraVision\OnTimeMS-x.x\pollarity\otdbupdate`

Depending on your setup, use 'integratedSecurity' or 'SQL Server Authentication'.:

Run this command, if you prefer 'integratedSecurity' in your SQL server:

```
otdbupdate.cmd -skipDefaultCallbacks=true
 -url=jdbc:sqlserver://localhost:1433;databaseName=pollarity;
encrypt=true;trustServerCertificate=true;integratedSecurity=true migrate
```

All parameters must be entered on one line.

Run this command if you prefer SQL Server Authentication:

```
otdbupdate.cmd -skipDefaultCallbacks=true
 -url=jdbc:sqlserver://localhost:1433;databaseName=pollarity;
encrypt=true;trustServerCertificate=true;
 -user=OnTimeApp -password=xxxx migrate
```

All parameters must be entered on a single line.

Pollarity application

1. Copy Pollarity files to the Tomcat server. This can be accomplished by running the command 'start-pollarity.cmd' in the directory: C:\Program Files\IntraVision\OnTimeMS-x.x\pollarity\cmd\
2. Restart the Tomcat service 'Apache Tomcat 10.x OnTimeTomcat'.

Catering

Catering requires a database and the installation of an application on the Tomcat OnTime server.

Catering database

Depending on your setup of the SQL server, local or external to the OnTime server the process is similar to the section Create the OnTime database.

1. Create a database named '**catering'** in the SQL Server.
2. In the database's security section add a database user, the same as the database user of the 'ontimems' database.
3. Double-click the database user, select 'Membership', tick db_owner, click 'OK'

Update the Catering database using 'otdbupdate.cmd'

From the folder C:\Program Files\IntraVision\OnTimeMS-x.x. open a Command Prompt as Administrator.

Otdbupdate.cmd requires an environment variable for JAVA_HOME in your OnTime installation files.

Set the environment variable for **JAVA_HOME** by running the command:

```
set JAVA_HOME=C:\Program Files\IntraVision\OnTimeMS-x.x\jdk
```

Set the environment variable for **Path** by running the command:

```
set PATH=%JAVA_HOME%\bin;%PATH%
```

Navigate to `C:\Program Files\IntraVision\OnTimeMS-x.x\catering\otdbupdate`

Depending on your setup use 'integratedSecurity' or 'SQL Server Authentication'.:

Run this command, if you prefer 'integratedSecurity' in your SQL server:

```
otdbupdate.cmd -skipDefaultCallbacks=true
 -url=jdbc:sqlserver://localhost:1433;databaseName=catering;
encrypt=true;trustServerCertificate=true;
integratedSecurity=true migrate
```

All parameters must be entered on one line.

This command, if you prefer 'SQL Server Authentication':

```
otdbupdate.cmd -skipDefaultCallbacks=true
 -url=jdbc:sqlserver://localhost:1433;databaseName=catering;
encrypt=true;trustServerCertificate=true;
 -user=OnTimeApp -password=xxxx migrate
```

All parameters must be entered on one line.

Catering application

1. Copy Catering files to the Tomcat server. This is accomplished by running the command 'setup-catering.cmd' in the directory:

   C:\Program Files\IntraVision\OnTimeMS-x.x\catering\cmd\

2. Restart the Tomcat service 'Apache Tomcat 10.x OnTimeTomcat'.

Visitor

VisitorOnTime add-on product requires a database and the installation of an application on the Tomcat OnTime server.

Visitor database

Depending on your setup of the SQL server, local or external to the OnTime server the process is similar to the section Create the OnTime database.

1. Create a database named '**visitor'** in the SQL Server.
2. In the database's security section add a database user, the same as the database user of the 'ontimems' database.
3. Double-click the database user, select 'Membership', tick db_owner, click 'OK'

Update the Visitor database using 'otdbupdate.cmd'

From the folder C:\Program Files\IntraVision\OnTimeMS-x.x, open a command window as Administrator.

Otdbupdate.cmd requires an environment variable for JAVA_HOME in your OnTime installation files.

Set the environment variable for **JAVA_HOME** by running the command:

```
set JAVA_HOME=C:\Program Files\IntraVision\OnTimeMS-x.x\jdk
```

Set the environment variable for **Path** by running the command:

```
set PATH=%JAVA_HOME%\bin;%PATH%
```

Navigate to `C:\Program Files\IntraVision\OnTimeMS-x.x\visitor\otdbupdate`

Depending on your setup use 'integratedSecurity' or 'SQL Server Authentication'.:

Run this command, if you prefer 'integratedSecurity' in your SQL server:

```
otdbupdate.cmd -skipDefaultCallbacks=true ^
 -url=jdbc:sqlserver://localhost:1433;databaseName=visitor;
encrypt=true;trustServerCertificate=true;integratedSecurity=true migrate
```

All parameters must be entered on one line.

This command, if you prefer 'SQL Server Authentication':

```
otdbupdate.cmd -skipDefaultCallbacks=true ^
 -url=jdbc:sqlserver://localhost:1433;databaseName=visitor;
encrypt=true;trustServerCertificate=true;
-user=OnTimeApp -password=xxxx migrate
```

All parameters must be entered on one line.

Visitor application

1. Copy the Visitor files to the Tomcat server. This is accomplished by running the command 'setup-visitor.cmd' in the directory:

   C:\Program Files\IntraVision\OnTimeMS-x.x\visitor\cmd\

2. Restart the Tomcat service 'Apache Tomcat 10.x OnTimeTomcat'.

OnTime Server

In the folder C:\Program Files\IntraVision\OnTimeMS-x.x\cmd - you will find the command ‘install-ontime-services.cmd’

Run it as administrator to install the Tomcat server and the ‘OnTimeMS Auth’ service.

The Tomcat service for OnTime is now running within Windows Services as ‘Apache Tomcat 10.x OnTimeTomcat’.

The OnTime Auth service is now running as a Windows service as ‘OnTimeMS Auth’.

OnTime add-on products

If you have licenses for the OnTime add-on products, Catering, Pollarity, Visitor, you may run the scripts below to enable the applications.

In the folder C:\Program Files\IntraVision\OnTimeMS-x.x - you will find the commands:

start-catering.cmd

start-pollarity.cmd

start-visitor

Database

Local SQL server

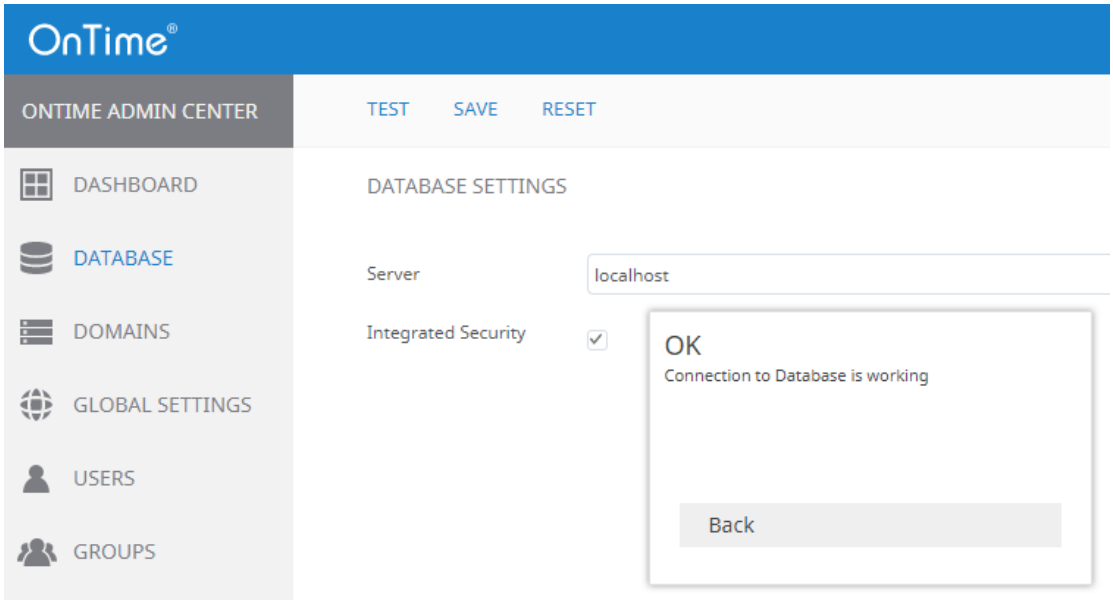
In the web administrator interface, “OnTime Admin Centre”, click “Database”.

If you followed the ‘Quick installation’ procedure, the fields are already populated with Server, ‘localhost’ and ‘Integrated Security’, checked.

Click “Test” in the upper menu line to test the database connection.

Upon the response “OK Connection to Database is working” click “Back”.

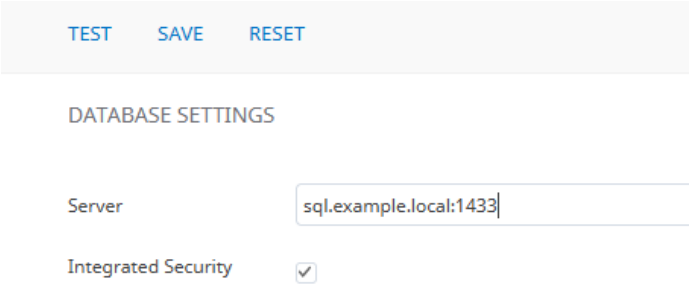
Click Save.



If the SQL Server is external to the OnTime server, there are two possible configurations:

External SQL server, same Windows domain

You have to reference the SQL server and optionally a port number



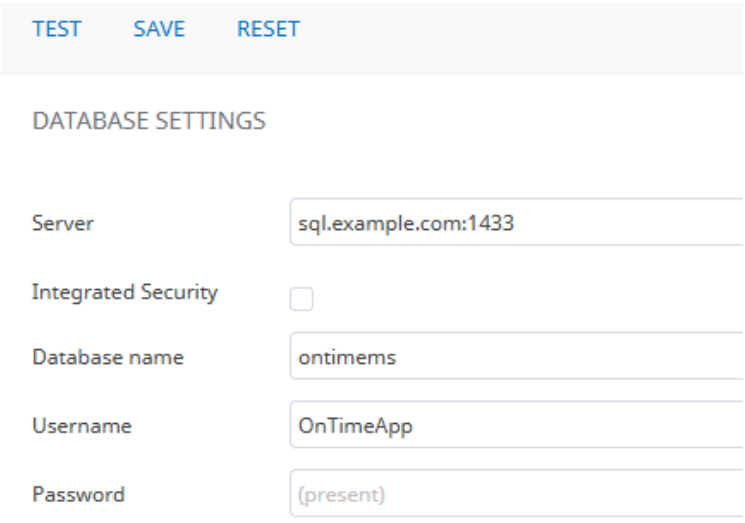
External SQL server, outside the Windows domain

Enter the reference to the SQL server and optionally a port number

Deselect the ‘Integrated security’ setting.

Enter the database name ‘ontimems’

Enter username, OnTimeApp, and the corresponding password

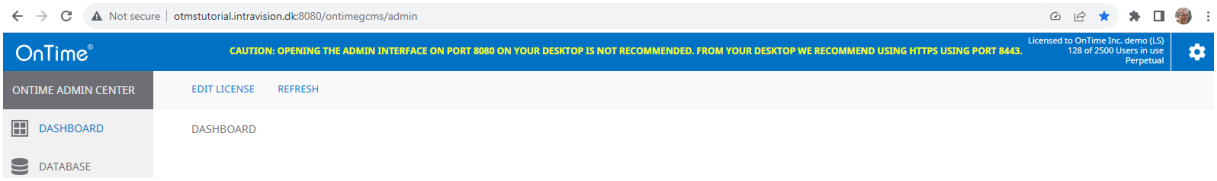


OnTime Configuration

OnTime Setup

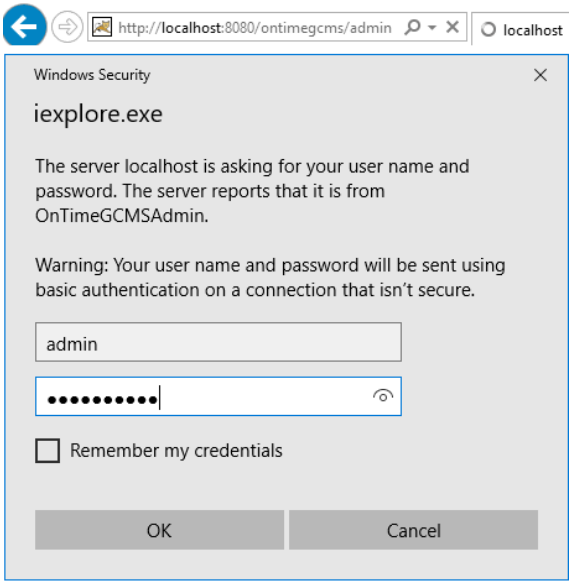
Open a web browser and navigate to the administration URL. The Exchange server has to be configured for 'Basic Authentication
https://ontime.example.com:8443/ontimegcms/admin
- or only on localhost, at the OnTime server.
http://127.0.0.1:8080/ontimegcms/admin

Note: Replace 'ontime.example.com' with your actual OnTime server URL.
If you access the administration interface remotely using HTTP on port 8080, to the OnTime server you will get a yellow warning: 'Caution: Opening the admin interface on port 8080 is not recommended …'



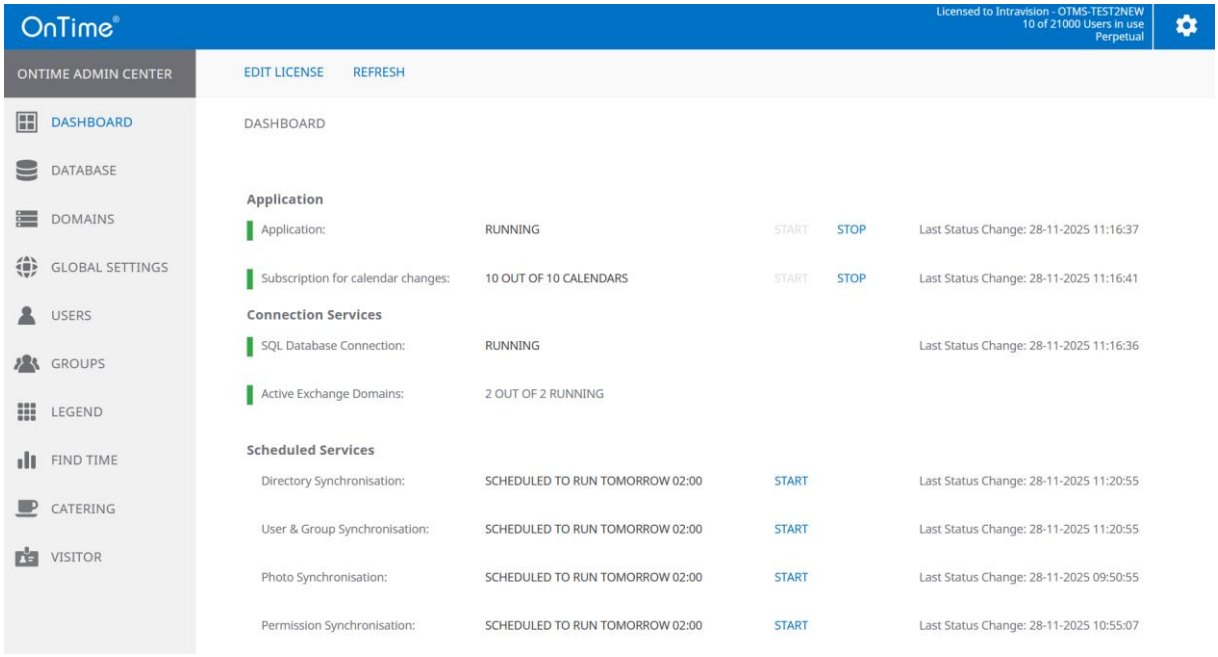
Administrator: admin		(Administrator username: admin (case-sensitive; use lowercase only)
Password:	*****	(Password: [the password set during installation])

Resetting the password if it is lost:
In the folder C:\Program Files\IntraVision\OnTimeMS-x.x\cmd
- you will find the command 'change-tomcat-password.cmd'.
Run it as an administrator to reset the admin password.
Note: Special characters may prevent the Tomcat service from starting


http://localhost:8080/ontimegcms/admin
localhost
Windows Security
iexplore.exe
The server localhost is asking for your user name and password. The server reports that it is from OnTimeGCMSAdmin.
Warning: Your user name and password will be sent using basic authentication on a connection that isn't secure.
admin
Remember my credentials
OK
Cancel

Dashboard

The main page of the OnTime Admin Centre 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 corresponding section.



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

The section **Connection** shows the status of the connections to the OnTime SQL database and the Exchange service(s). Both should appear green during normal operation.

The section **Scheduled** normally shows the time when the services will be started automatically. The time can be configured in the Global -> Backend settings.

Five services within this section can be started manually to reflect changes at once.

Directory Sync updates users/groups from Exchange.

User & Group Sync synchronises the Exchange users/groups onto the OnTime SQL tables (starts automatically whenever Directory Sync finishes)

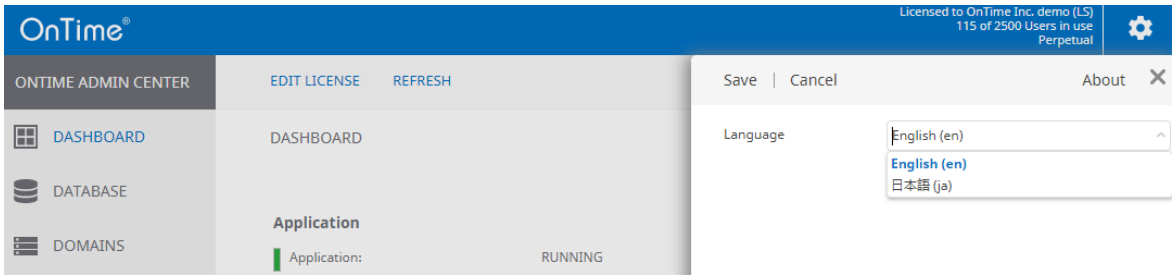
Photo Sync imports the users’ photos/avatars from the Exchange 2013 server

Permission Sync updates the users’ permissions to modify other users’ calendars

Event Sync synchronises all users’ calendar entries and may take a considerable amount of time.

Japanese language support is available in the OnTime Administration Centre.

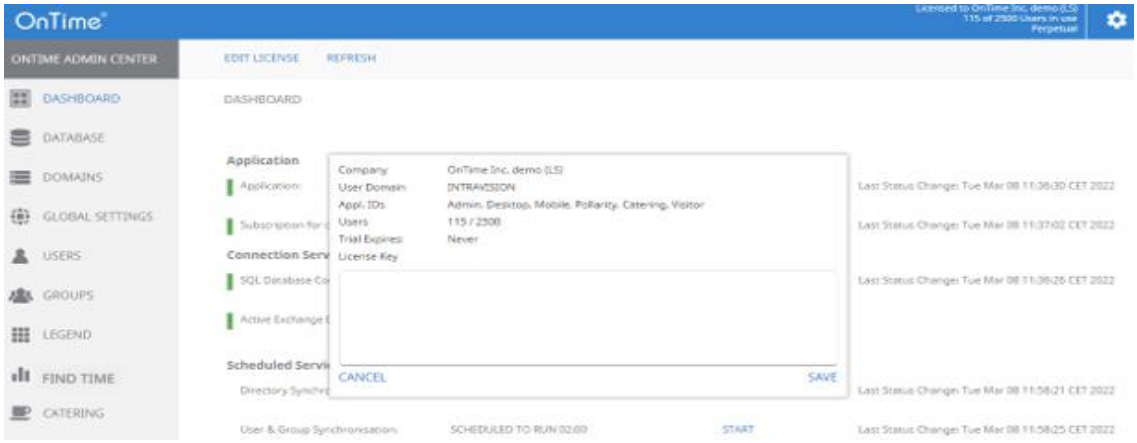
- The settings in the upper right corner of the dashboard allow for the change of the preferred language in the OnTime Admin Centre.



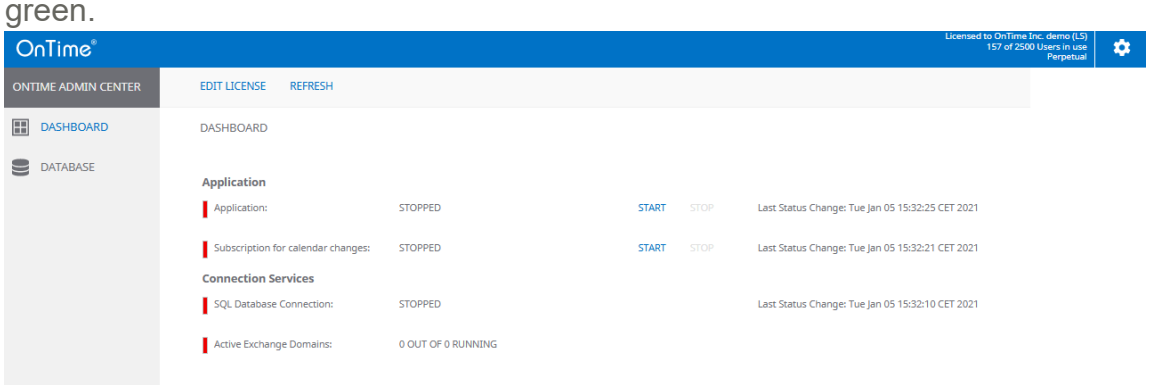
License key

Click ‘Dashboard’

– In the Dashboard, click **License**, enter your license key, and click **Save**



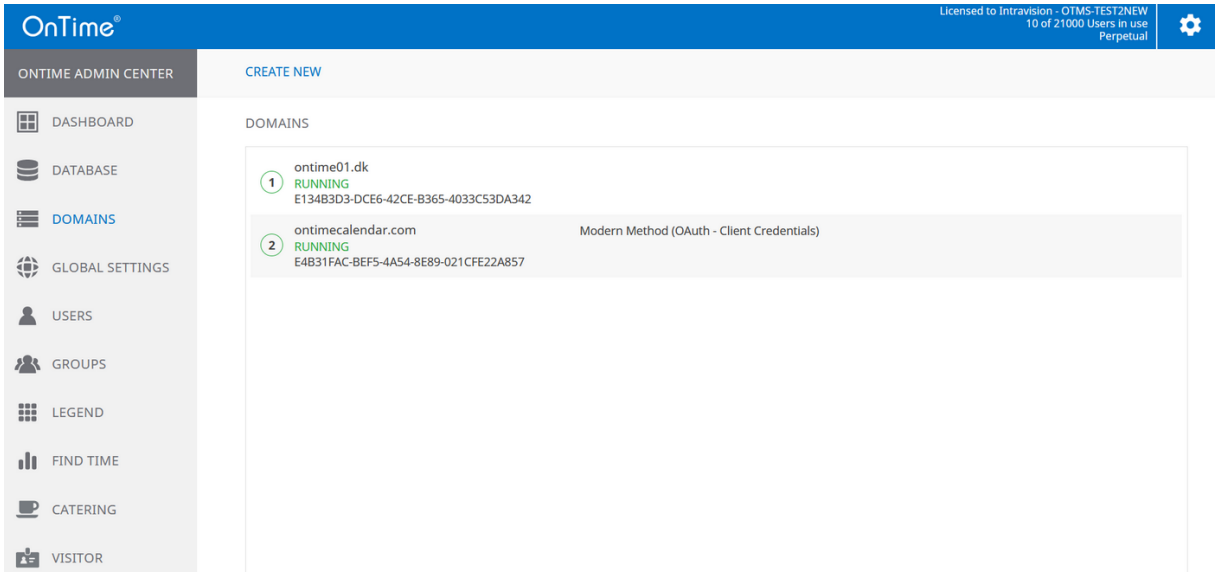
In the ‘Dashboard’ click ‘Start’ at ‘Subscription’ – the state colour should change into green.



Note: **When you see the Connection Services/SQL Database Connection - “Running” (green), press ‘**F5’ **to refresh the whole web page from the database.**

Domains

Click “Domains” to configure the directory settings.



If you are upgrading from an OnTime version earlier than 2.8 you will see an entry ‘Imported Domain’, it represents the single domain configuration from before the upgrade.

Authentication

OnTime supports two authentication methods in Microsoft 365:

1. OAuth – Client Credentials
2. OAuth – Impersonation User

If you connect to Exchange Online, Microsoft 365, you should choose OAuth, Microsoft recommends ‘OAuth – Client Credentials’ authentication – it supports multi-factor authentication.

OnTime does not support **multi-factor** authentication for the ‘OAuth - Impersonation user’, in Microsoft 365.

Note: Basic authentication is deprecated by Microsoft for Microsoft 365.

Note: Basic authentication/Form Based – Pass-through with multi-factor authentication in Microsoft 365 is not supported.

Note: Microsoft Teams configuration works only with OAuth authentication. Ref. **Add-ins for OnTime**.

Note: If you choose the authentication type Legacy Method (Basic), you will miss details such as room ‘Capacity’ and ‘Floor’ in OnTime.

Prerequisites

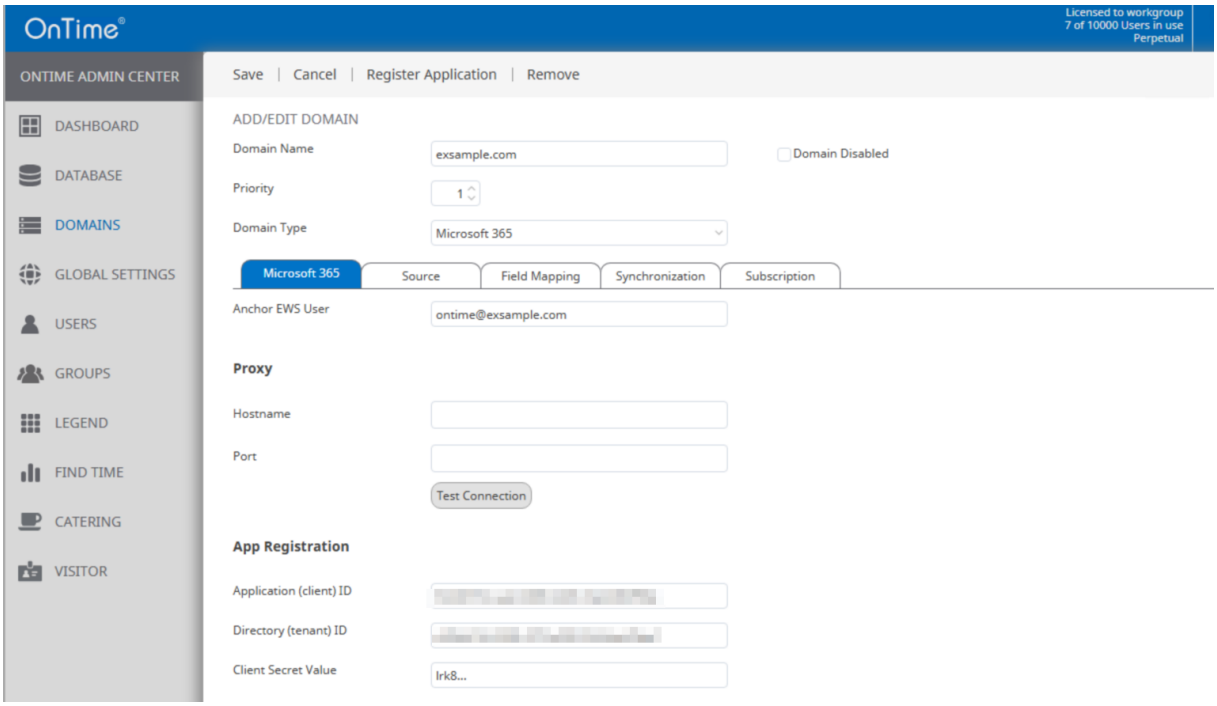
To retrieve data from Microsoft 365, Microsoft Entra ID, Graph we need access from the OnTime server to the internet - with the following URL's:

https://login.microsoftonline.com
https://graph.microsoft.com
https://portal.azure.com

Note: The secure connection from the OnTime server to these Microsoft sites has been an issue for one customer. Please check appendix SSL root certificates for the OnTime server

Click 'Create New' to add a domain. If you already have a domain configured you may click the domain name to 'Edit'.

Add Domain



Domain Name - is a text field for naming your domain setup.

Domain Disabled – 'checked' is used when you are working on setup, not ready for production.

Priority - is for prioritising the users in OnTime. Priority '1' is the highest priority. If a users' email address is found in more than one domain, the one from the domain with the highest priority will be synchronised into OnTime.

Domain Type – choose between a configuration for 'Microsoft 365' or 'On-Premises'

Anchor EWS User – A user required only for technical purposes.

EWS API fails when a user is not provided for a call. Some calls have an explicit user, others don't. There must be a user in the call, so that EWS does not fail, we

introduced an anchor user, which is simply a valid user that has no special abilities, apart from making EWS API succeed on the user-less calls.

Impersonation User: is the user in Exchange On-premises that has the **role** “ApplicationImpersonation”. This user is used by OnTime to read and edit all users’ calendars.

Proxy
If the Exchange server is behind a proxy server, you may enter DNS name (or IP) and a port number for access from the OnTime server.

The three values, for Application (client) ID, Directory (tenant) ID, Client Secret Value - are obtained from Microsoft Entra admin center (portal.azure.com), see below.

Missing permissions in the Microsoft Entra ID configuration, will be listed in red characters.

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 following permissions:

s)

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.

t) Click 'Add a permission'.

u) Click 'Microsoft Graph'

v) Click 'Delegated permissions'

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

x) Click ‘Add a permission’

y) Click ‘APIs my organization uses’

z) In the field for search, enter ‘Office’

aa) Click ‘Microsoft 365 Exchange Online

bb) Click ‘Application permissions’

cc) Tick ‘full-access_as_app’

dd) Click ‘Add permissions’

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

ff) 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. Methods 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.

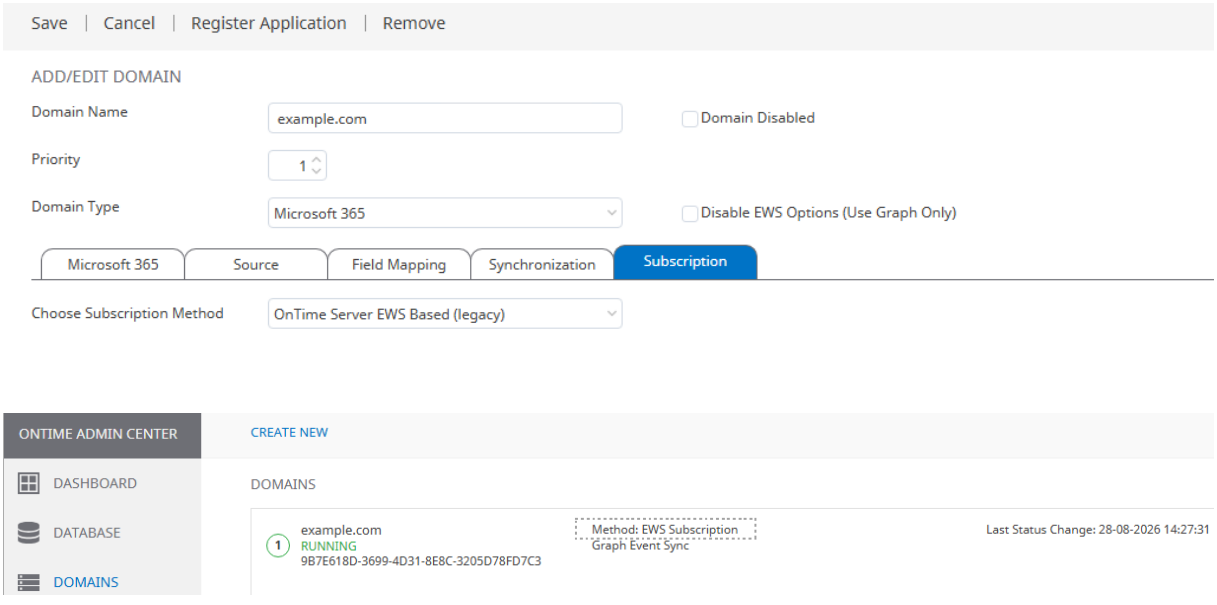
Selecting the Legacy Subscription Method

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)

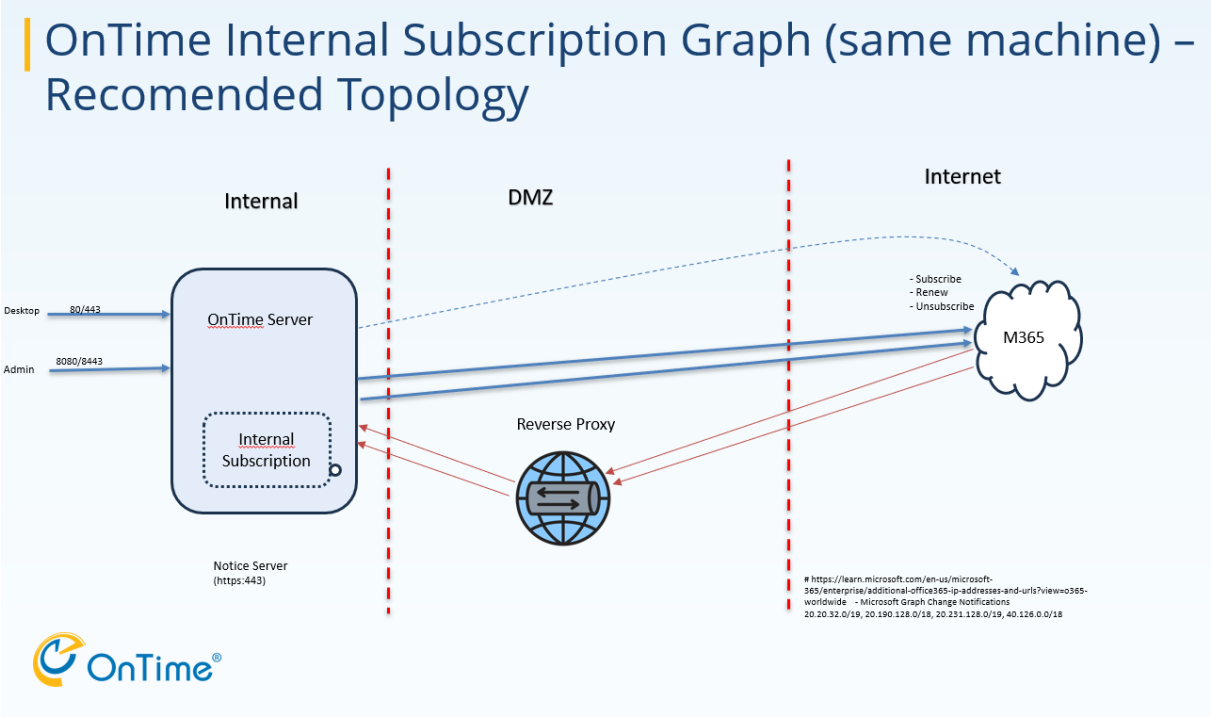


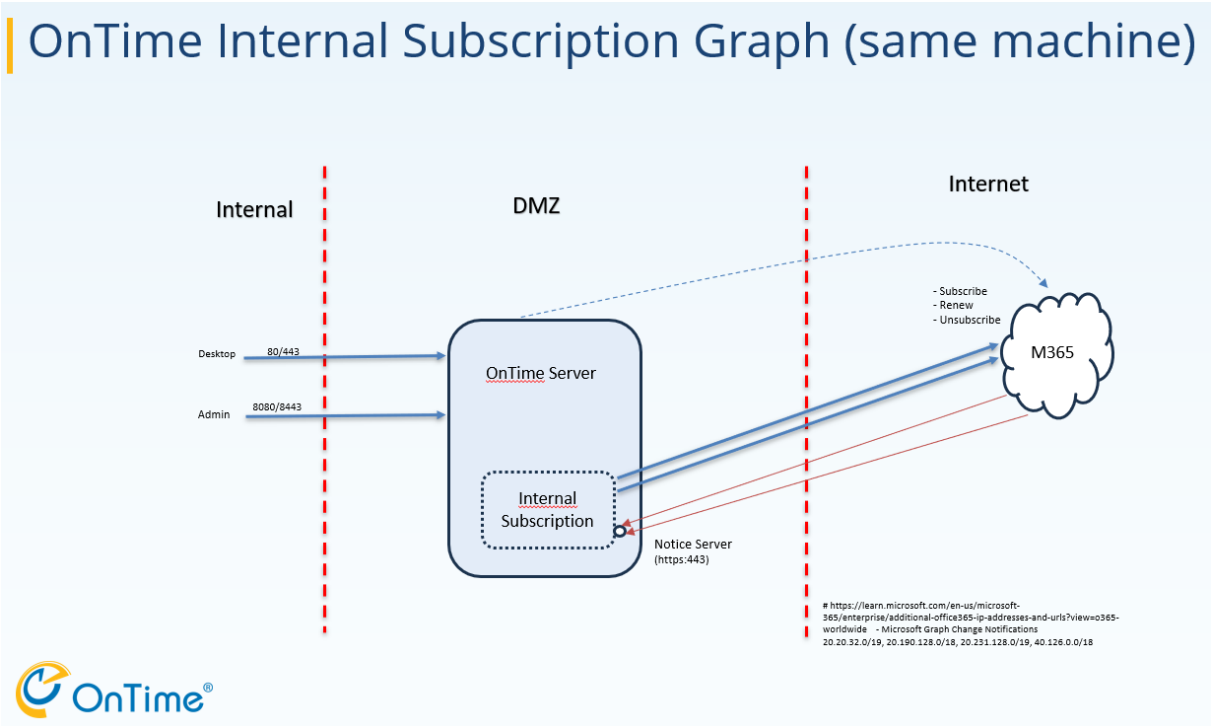
2. Microsoft Graph Subscription – Integrated OnTime Server

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

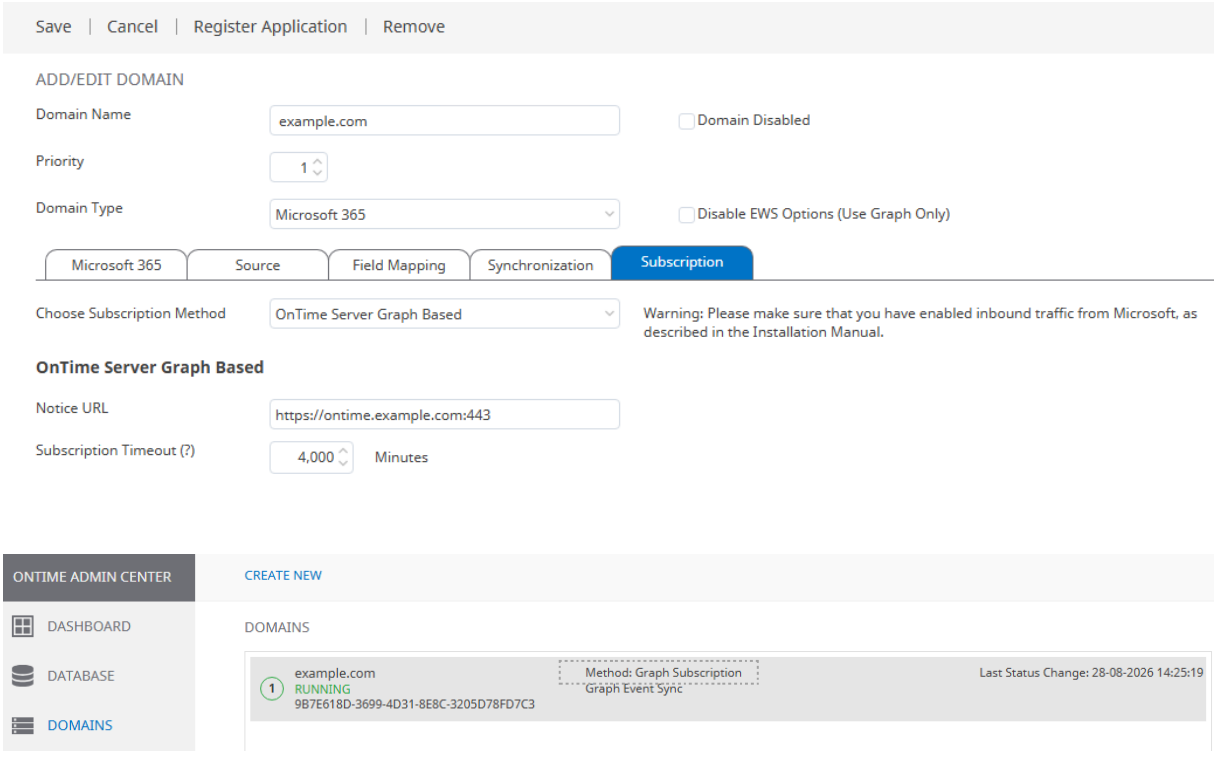
In the OnTime Admin Centre:

`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)



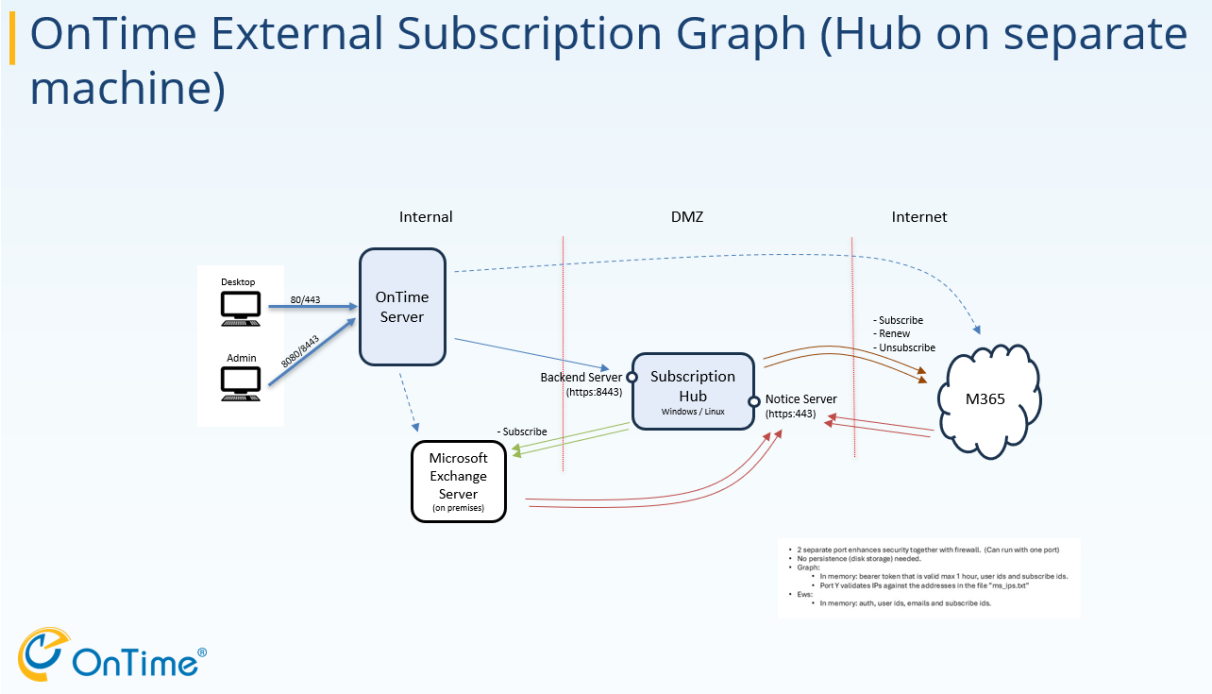
3. Microsoft Graph Subscription – External Subscription Hub

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 models 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.

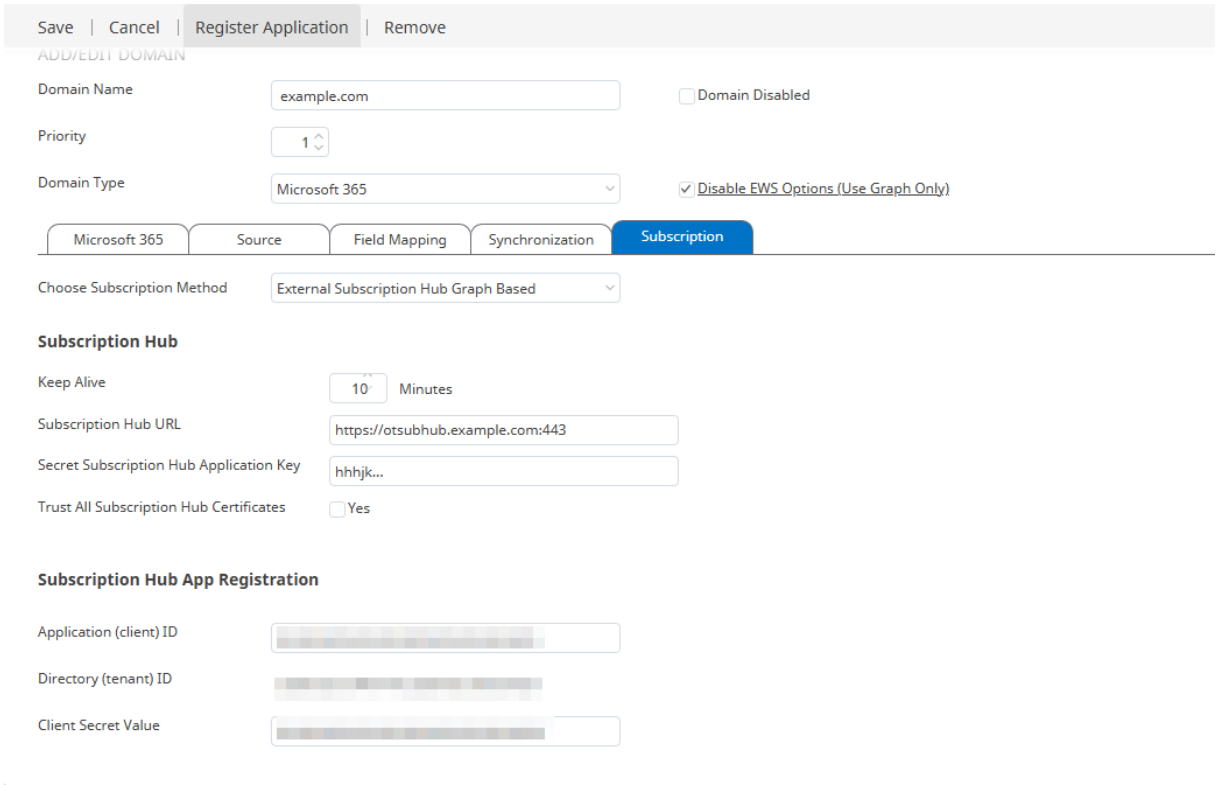
Trust All Subscription Hub Certificates: When selected, OnTime accepts all certificates presented by the Subscription Hub. This option should only be enabled when required, for example when using a self-signed or privately issued certificate.

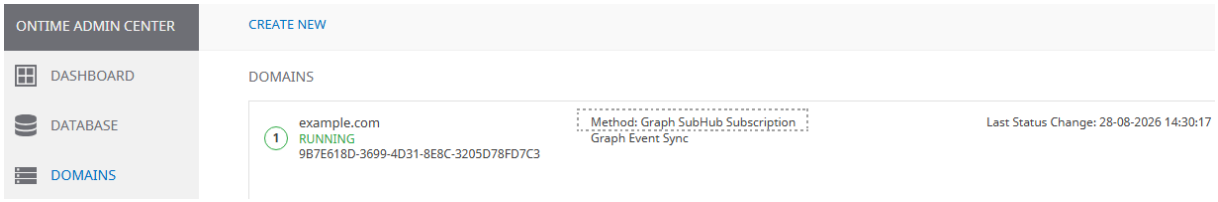
Application (client) ID: Enter the Application (client) ID of the Microsoft Entra ID app registration. (go to)

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.

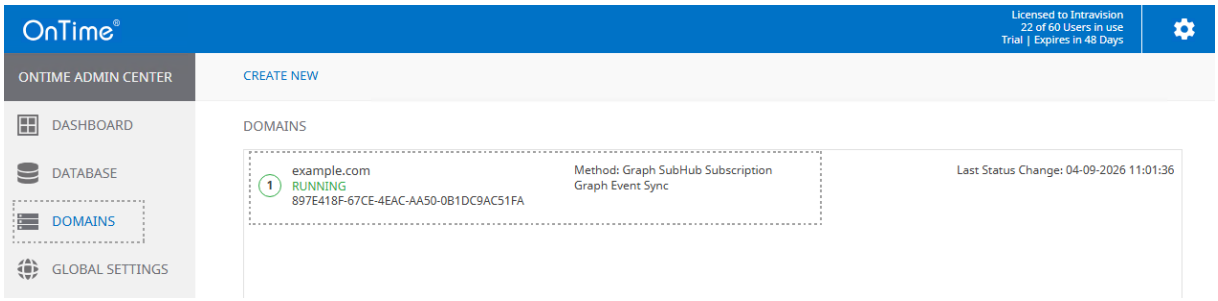
Click 'Save'. Then, in the OnTime Dashboard, stop and restart the OnTime application. (see the example below)


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

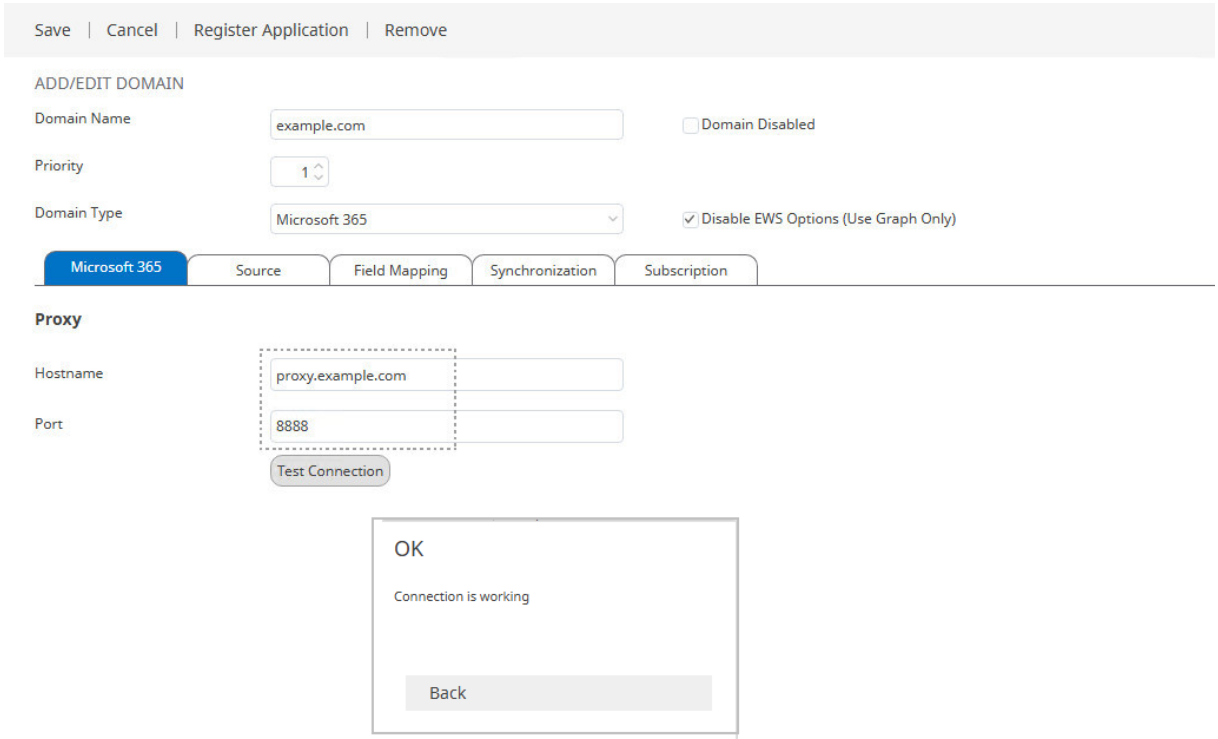
How to Configure Subscription hub using a Proxy

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)



Comparison of the Three Models

	EWS Streaming	Integrated Graph	External Graph Subscription Hub
Technology	EWS Streaming Subscription	Microsoft Graph Change Notifications	Microsoft Graph Change Notifications
Subscription service	OnTime Server	OnTime Server / Tomcat	Subscription Hub
EWS dependency for subscriptions	Yes	No	No
Incoming Graph notifications	No	OnTime server	Subscription Hub
Public HTTPS endpoint required	No	Yes	Yes
DMZ deployment possible	N/A	Via network / reverse proxy architecture	Yes – recommended architecture
Reverse proxy possible	N/A	Yes	Yes
Subscription workload separated from OnTime	No	No	Yes, when deployed separately
Exchange Online long-term model	Legacy	Yes	Yes
Exchange on-premises	Yes	Not the primary use case	Not the primary use case

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)
```

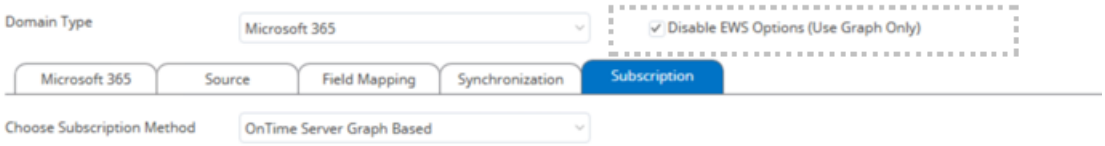
When enabled, OnTime switches its applicable configurations to Microsoft Graph only. EWS can subsequently be disabled at the Microsoft 365 tenant level.

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.

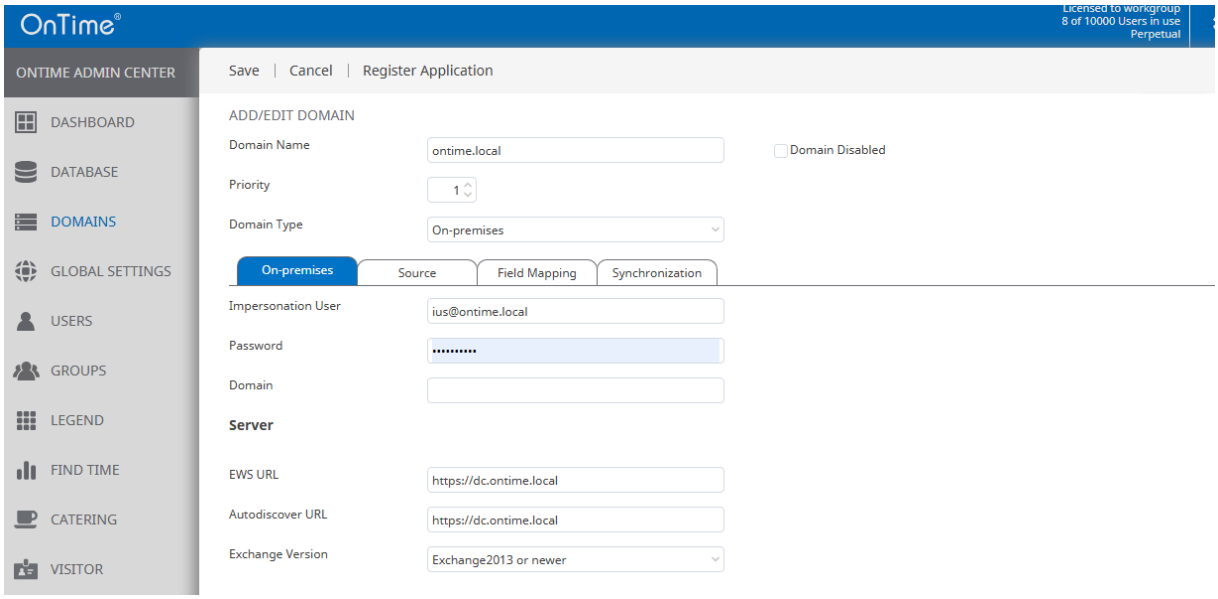
This will switch all configurations to use only Microsoft Graph, and EWS can then be disabled at the tenant level.(see the example below)



On-Premises configuration

The example below is with a local 'On-premises' Exchange server:

Note: The Exchange server must be configured for Basic Authentication.



Domain Name - is a text field for naming your domain setup.

Domain Disabled – 'checked' is used when you are working on setup, not ready for production.

Priority - is for prioritising the users in OnTime. Priority '1' is the highest priority.
If a users' email address is found in more than one domain, the one from the domain with the highest priority will be synchronised into OnTime.

Impersonation User - is the user in Exchange that has the role "ApplicationImpersonation". This user is used by OnTime to read and edit all users' calendars. Normally this username is written as an email address (UPN name), then the domain name is not required.

Password – OnTime supports passwords with numbers, letters (uppercase and lowercase). Special characters tested **:.;,-_*=@!#%&/()?'+[]{}\£$€.**
If you change the password, please stop/start the OnTime application in the OnTime Dashboard.

Server

The "Server URLs" are preconfigured for Microsoft 365, the URLs must be changed accordingly if the Exchange backend is on-premises.

'Exchange Version'

- Exchange On Prem including Microsoft 365

Proxy

If the Exchange server is behind a proxy server, you may enter DNS name (or IP) and a port number for access from the OnTime server.

Teams

Use Teams – select 'Yes' to configure Teams.
In this section, it is possible to configure parameters for Microsoft Teams. you will have to recheck your parameters



Get the values from the section below. In case you see a value in the field 'Missing parameters' you must verify your parameters again from 'Microsoft Entra ID' portal.

Registering the OnTime application in the Microsoft Entra ID portal for Teams

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

GroupMember.Read.All

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

b) Click 'View' at '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'.
Enter the 'Redirect URI, example https://localhost:8443/ontimegcms/code.html
Click 'Register'.

f) Click 'Add a certificate or secret' tab

g) Click 'New client secret'
h) Copy the value

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

j) Click ‘Microsoft Graph’

k) Click ‘Application permissions’

l) Select the following API permission, Type a few letters in the search field and tick the permission
(GroupMember.Read.All)

m) At the bottom click ‘Add permissions’

n) Click "Grant admin consent for *Your Company*"

o) Click ‘Yes’ to answer the question ‘Do you want to grant consent ...’

p) Copy the three values from Microsoft Entra ID to the page ‘OnTime Admin Centre’ –
‘Domains Add/Edit Domain/Teams’.
Click Overview - in the Microsoft Entra ID portal
Copy the values ‘Application (client) ID’, Directory (tenant) ID and ‘Client Secret Value’ to the corresponding fields in ‘Domains Add/Edit Domain/Authentication’ page.

Source

In this section, the users included in the OnTime Calendar can be configured. Users may generally be People, Rooms, or Equipment.

Shared desks

Note: OnTime also supports booking of 'Shared Desks', which is not a resource type (Mailbox type) in Exchange.

Register 'Shared Desks' as rooms – not as equipment. When registered as rooms, they will be searchable by location in Exchange. OnTime will allow booking and overview of 'Shared Desks'.

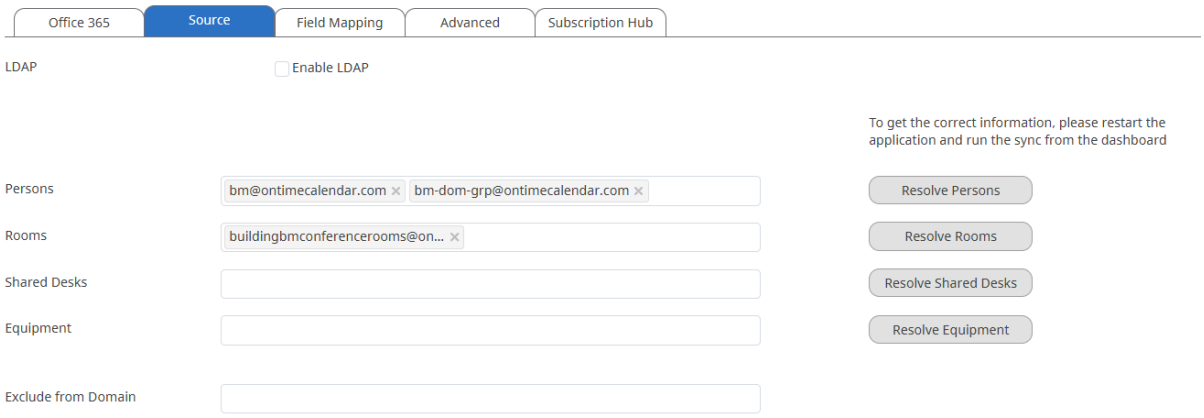
The Users in the OnTime Calendar can be included in two ways:

1. Distribution groups from the Exchange server (EWS, Exchange Web Services)
2. Through LDAP lookup from Active Directory.

For LDAP setup please refer to Source, LDAP.

Untick 'Enable LDAP' to include users from the 'Exchange distribution groups'.

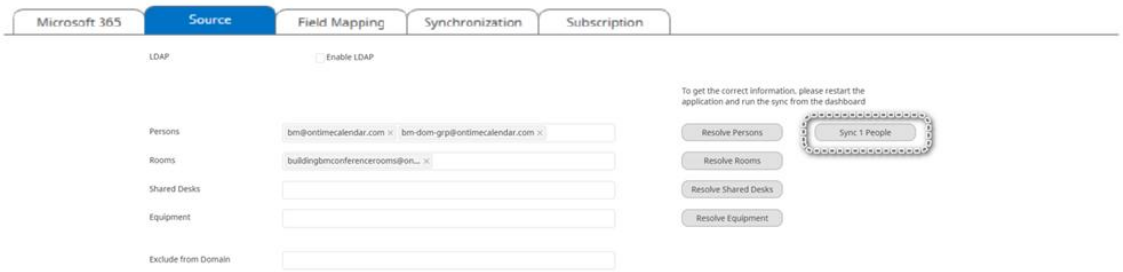
The section describes the Persons, Rooms, Shared Desks, Equipment groups that can be seen in the OnTime group.



The email addresses of these distribution groups are entered into the fields. More groups or individuals can be added, separated by commas. To check the content Click the Resolve button.
The configuration for 'Exchange distribution groups' means that the lookup is performed using Exchange Web Services (EWS), Exchange Web Services.

Click **‘Save’** to save your Domain Settings.
To reflect your new domain settings go to the Dashboard - Stop and Start the Application. Then check that the “Database Service” and “Exchange Service” both show “Running”.

During production, if additional users have been added to the resources to reduce server load, you have the option to run a synchronization for only the recently added people. This eliminates the need to perform a full ‘Directory synchronization’ through the OnTime Admin Dashboard.



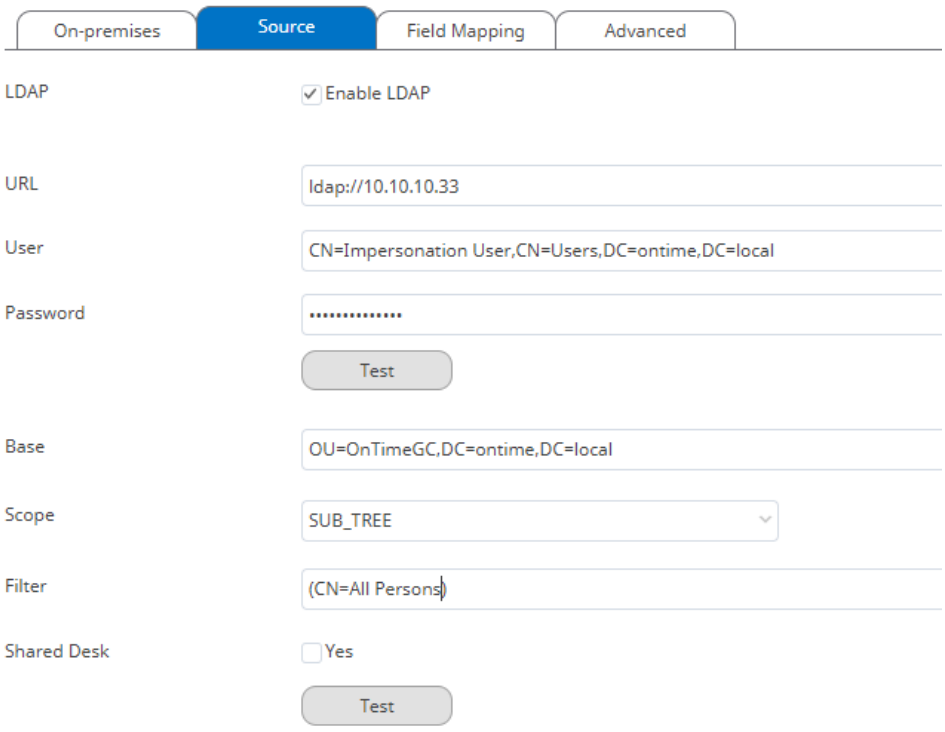
Source, LDAP

Tick 'Enable LDAP (Save) to use LDAP/LDAPS as the source of users in OnTime.

With this configuration for LDAP, the lookup of all types of OnTime users (persons, rooms, shared desks, equipment) are received via the LDAP service from a domain controller.
The OnTime backend will figure out what is rooms/shared desks, equipment or persons.

In the 'Source' section a domain controller is referenced, the URL states the LDAP or the LDAPS protocol.
We recommend to use 'We recommend using 'LDAPS' to ensure a secure connection to Active Directory. This also supports environments where the domain controller is configured for 'LDAP Signing'.. The non-secure 'LDAP' setup is meant for testing or initial setup for OnTime.

The LDAP authentication (bind) user's name is written in the distinguished name format.
Username and password is required if the LDAP service does not accept 'Anonymous' access. Click the "Test" button to check that you have access to the LDAP service. The response should show "Connections to LDAP is working". Click Back to clear the popup box.



In the ‘Base’ section, the distinguished name format is used as a base for searching the AD. The scope One_Level will only find members within the base mentioned above, not from OUs below this base. The scope Sub_Tree will add members also from OUs below the base.

Shared Desks are included by including a Base reference to a group, like ‘All Shared Desks’ and ticking ‘Shared Desk ‘Yes’.’

Example 1:
All mail users from the OU ‘Test’ including mail users from OUs below.

```
Base:           OU=Test,DC=ontime,DC=local
Scope:          SUB_TREE
Filter:         (mail=*)
```

Example 2:
Finding all members of a certain group, with canonical name:
CN=Test_grp,OU=Test,DC=ontime,DC=local

```
Base:           OU=Test,DC=ontime,DC=local
Scope:          ONE_LEVEL
Filter:         (cn=Test_grp)
```

Click the “Test” button to check your search entries – a good response could be “Connection to LDAP is working, Matches found: 23”.

More base entries are possible, to add different parts of the AD tree to the search.

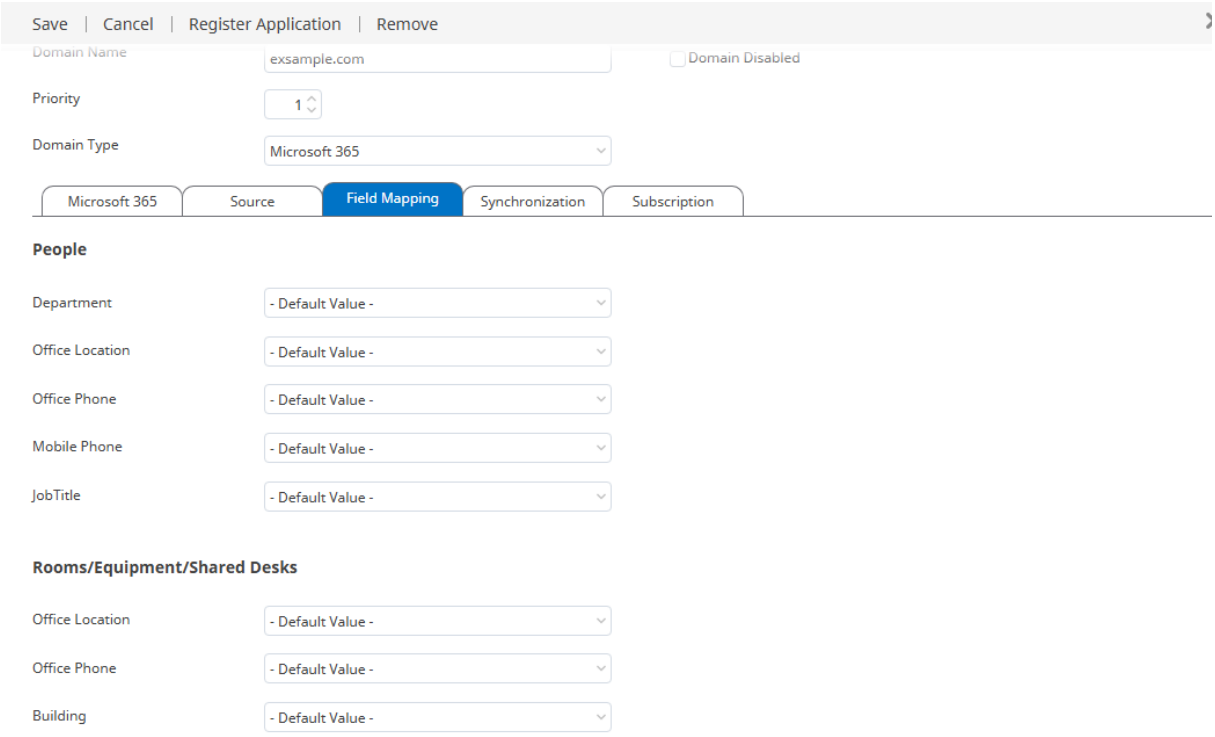
Click ‘Save’ to save your Domain settings.

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”.

Field Mapping

Here you may configure parameters included in the business card.



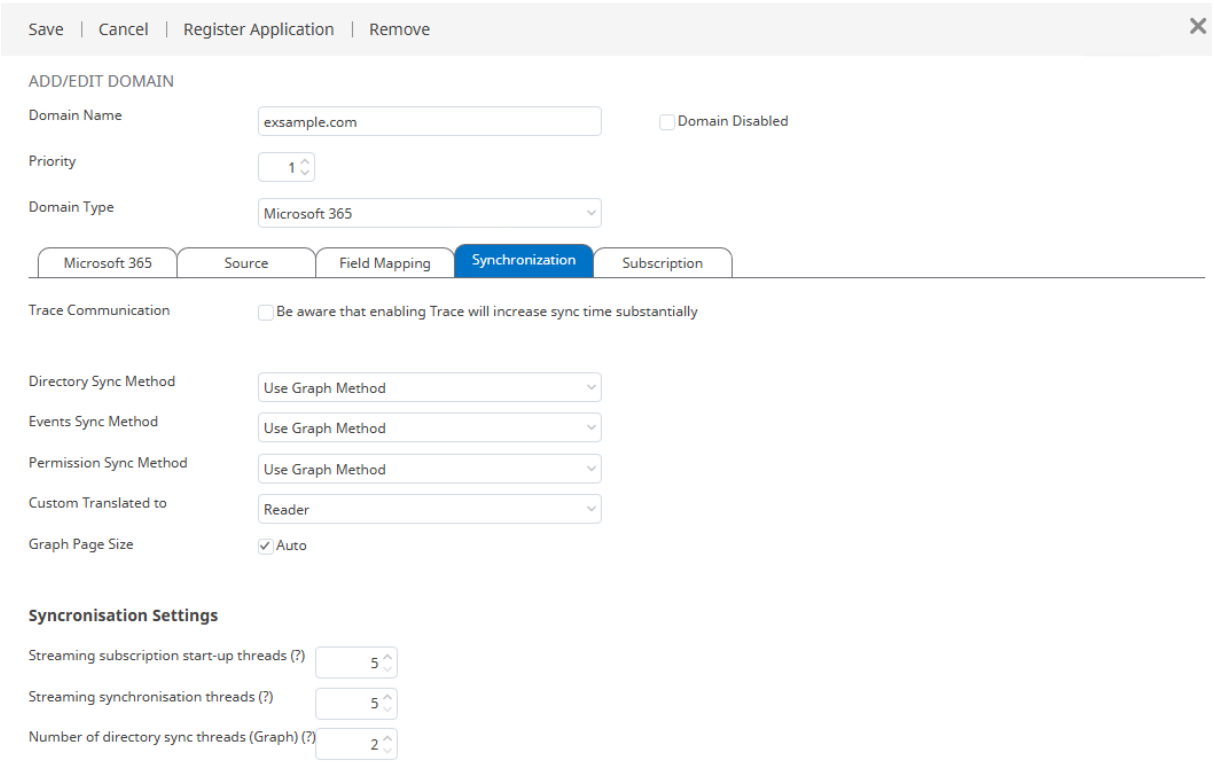
Parameters for the business card includes values from the AD like

- Department
- Office Location
- Office Phone
- Mobile Phone
- Job Title

Values can be retrieved from Active Directory extension attributes.

Note: if you make changes here, remember to run 'User and Group Synchronization' in the Dashboard.

Add/Edit Domain - Advanced



Trace Communication - may be enabled in case of trouble-shooting the OnTime service.
Please refer to **Trace Communication**

Directory Sync Method – Choice between 'Use Graph Method' and 'Use Legacy EWS Method'.

According to the current Microsoft Graph documentation, these Exchange/Microsoft 365 group types are supported: **Microsoft 365 Group**, **Security Group**, **Mail-enabled Security Group** and **Distribution Group / Distribution List**.

Note: If Use **Graph Method** is selected, **Dynamic Distribution Groups** often refers to **Dynamic Distribution Lists** are not supported in Microsoft Graph. Please refer to the relevant Microsoft Support documentation for more information.

Note: Microsoft 365 Groups can be used provided that the groups are not hidden from Microsoft Outlook in Microsoft Entra ID.

Event Sync Method – Choice between 'Use Graph Method' and 'Use Legacy EWS Method'. By choosing one of these methods all event processing will belong to it.

Permission Sync Method – Choose between 'Use Graph Method' and 'Use Legacy EWS Method'. These methods produce different results depending on the underlying data sources used.

Custom Translated to – Choice between 'NoAccess, Busy, Limited, Reader, Author, Editor'. The default is 'Reader' and used only in case to choose 'Use Graph Method' for Permission sync.

Synchronisation settings

Note: These default settings should not be changed normally.

Streaming subscription start-up threads – '5' is the minimum.

Streaming synchronisation threads – '5' is the minimum.
Recommendations are 5 threads for 1000 users, 25 threads for 8000 users.

Number of directory sync threads (Graph) – '2' is the minimum, '10' is the maximum.

Throttling

OnTime is a highly scalable application that has been optimized for both performance and throughput. However, when optimizing these aspects, it's common to encounter throttling for certain functions. Throttling is when the number of API requests a user or system can make within a specified time is limited, and Microsoft applies these limits in various ways through the Graph / EWS API.

To handle more API requests simultaneously, OnTime splits tasks across multiple threads. While this improves performance, it also increases the risk of throttling. If the throttling limit is exceeded, Microsoft Graph will restrict further requests from that client for a period. When throttling occurs, Microsoft Graph responds with an HTTP status code 429, 503, 509 (Too Many Requests), causing the requests to fail.

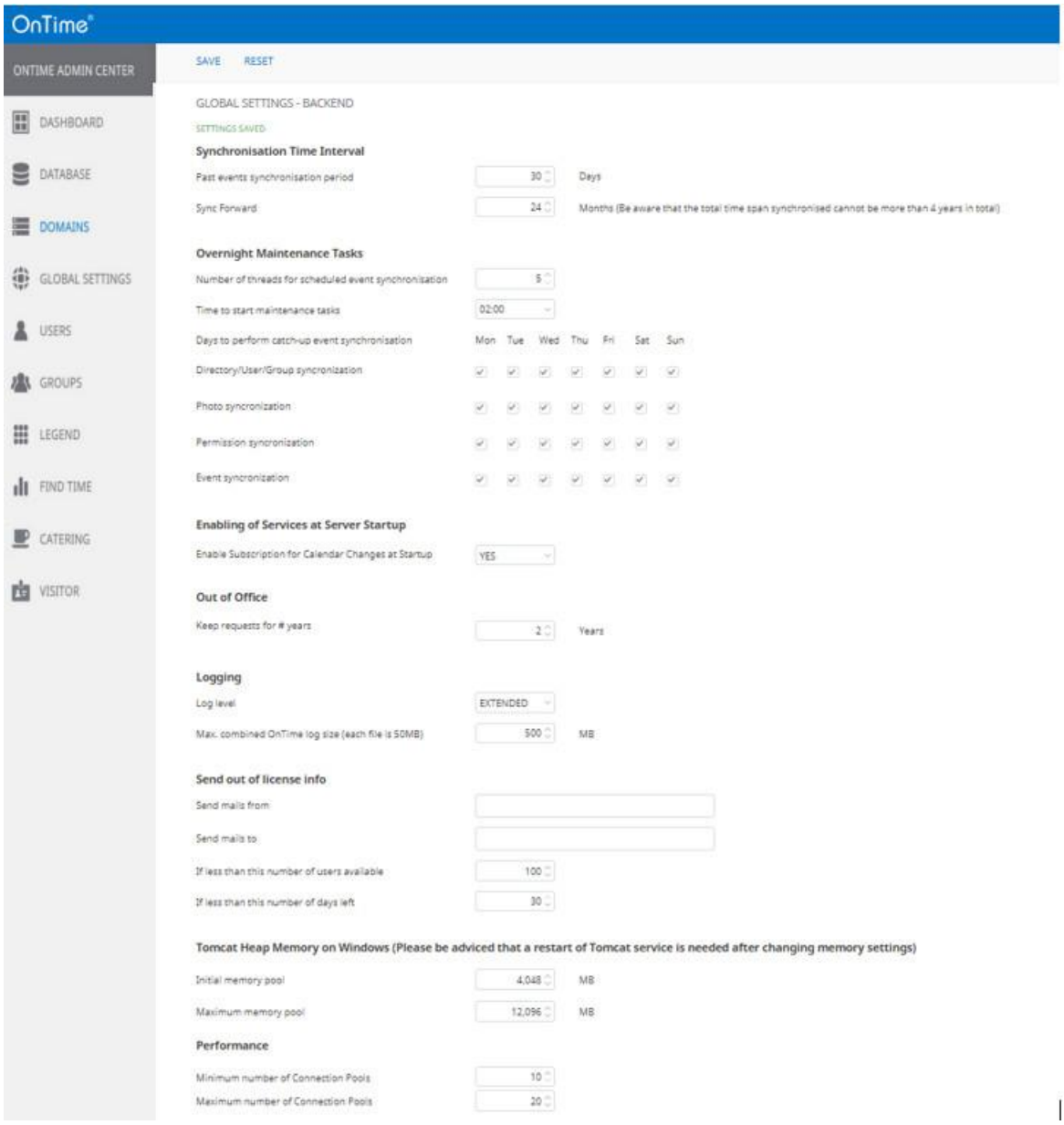
The default values for the maximum number of simultaneous threads in the Graph / EWS API, as shown in the screenshot above, have been successfully tested by IntraVision. However, these values may need to be adjusted over time based on your specific environment. We recommend consulting with your OnTime partner or IntraVision before making any changes to these values.

Global Settings

Global settings for the OnTime Application

Backend

Click “Global>Backend” to enter the “Global Settings-Backend” page.



Synchronisation Time Interval

Here you set the number of days for synchronising the past calendar events. The total synchronisation time frame is four times the selected number of days. The maximum value for ‘Past events synchronisation period’ is 180 days.

Overnight Maintenance Tasks:

Number of threads for scheduled event synchronisation – Minimum value is 5.

Specify the maintenance task start time (0–24, server time).

Weekdays to perform event synchronisation

You may choose to tick certain weekdays to run the event synchronisations.

Enabling of Services

When enabled, this setting loads the synchronisation service every time you start the Tomcat service. Normally you set it to “No” while you do your installation. After confirming all configurations, enable this option.

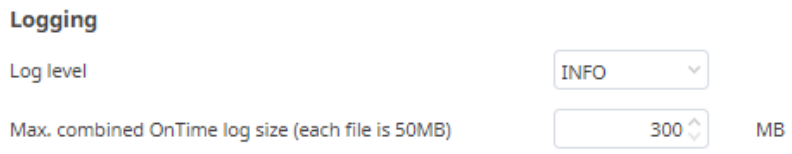
Click ‘Save’ and go to the Dashboard. Stop/Start the Application.

Out of Office

Specify how many years Out of Office requests are retained in the database (default: 2 years)

Logging

Here you can decide the level of logging for troubleshooting purposes and limiting of the log file size in MBs. Default setting is ‘INFO’.



Refer to the section

Logfiles section for references to the log files.

Send out of license info

Send emails from – OnTime user that is mentioned as sender in a license info mail

Send email to – any internet mail user, optionally multiple recipients

If less than this number of users available – warning threshold of users left within the OnTime license limit

If less than this number of days left – warning threshold of days before the OnTime license expiry

Tomcat Heap Memory on Windows:

Dependent on your setup and amount of users you may increase the memory for the Tomcat server.
When a user installs or upgrades OnTimeGCMS and the Tomcat memory settings has not been configured, then the memory will be configured automatically.
By default that would be Initial Memory Pool of 2 GB and Maximum Memory Pool of 4 GB.
If the server has more than 8Gb of RAM then the Initial Memory Pool will be 3 Gb and the Maximum Memory Pool of 6 GB.

Note: A restart of the Tomcat in Windows Services is required if you change the values for the memory pool.

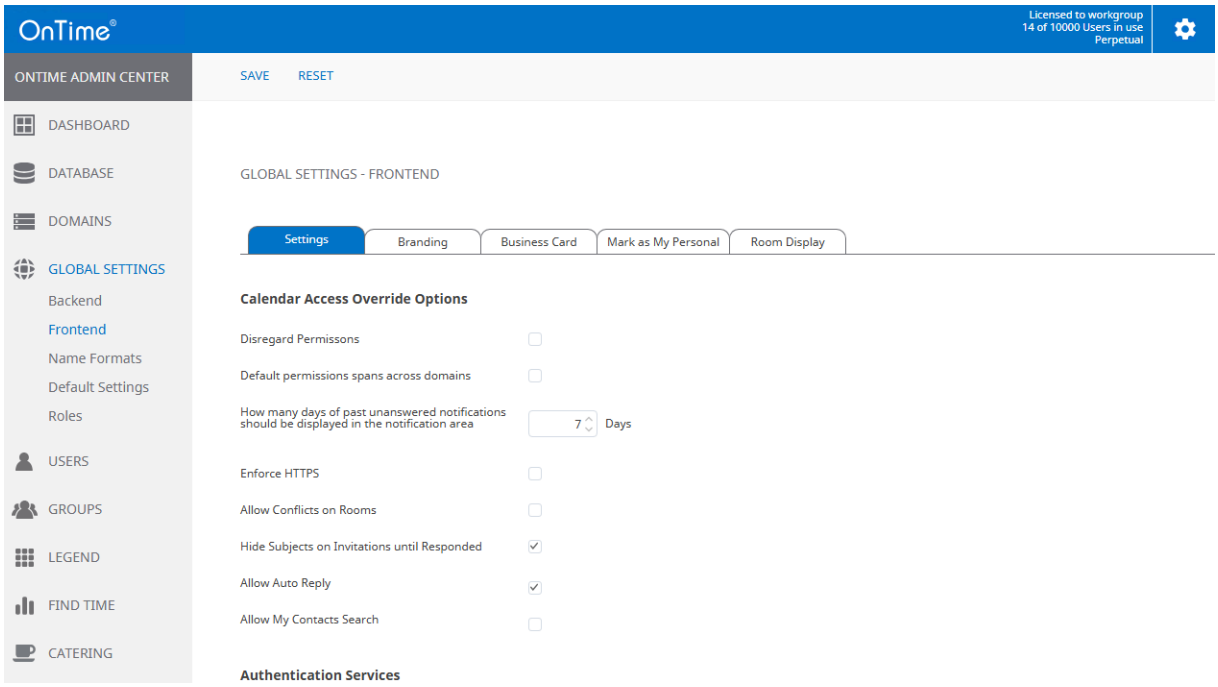
Performance

Connection pools define the connection between the Tomcat and SQL servers.
Default values are minimum 10 and maximum 30.

After changing the values, a restart of the OnTime application is required.

Frontend

Click “Global Settings>Frontend” to enter the “Frontend” page.



Settings

In Exchange/Outlook, the default permissions granted by a user do not span across other domains See browser setup for SSO. In OnTime we allow the administrator to set that these default permissions should span across domains. It is, for example, useful if your organisation has two domains and you want the users to have the experience as if they were all within the same domain from a permissions perspective without using a federated domain.

Default permissions span across domains = Unchecked, default permissions set on users are ignored across domains.

Default permissions span across domains = Checked, default permissions set on users are included in the permissions across domains. If set to ‘Yes’ your personal level of ‘Organizational permissions’ in Exchange/Outlook is used for all users across all the domains.

Specify how many days of past unanswered notifications are displayed the notification area – Number of days unanswered invitations are kept in OnTime.

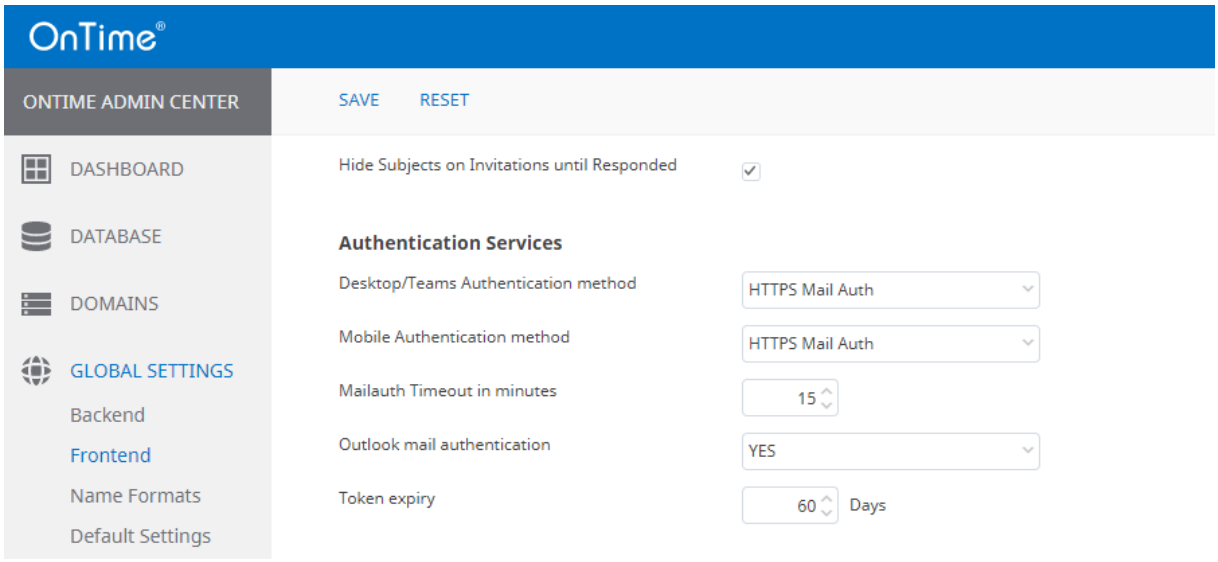
Enforce HTTPS – web clients with http are redirected to https (port 443).

Allow conflicts on Rooms – tick to allow calendar conflicts on rooms.

Hide subjects on invitations until responded – check to enable.

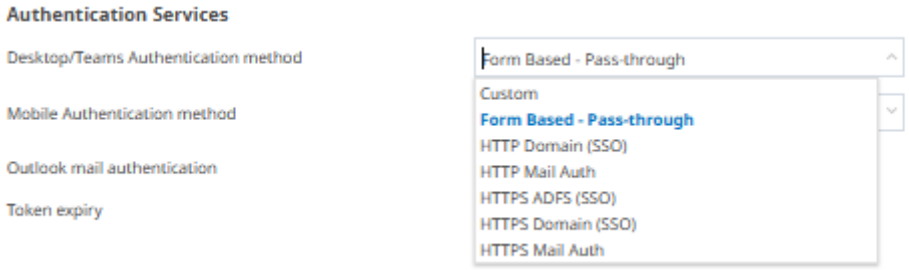
Allow my Contacts Search - tick to allow OnTime uses a user's personal contacts as an additional source for attendee searches and contact information.

Authentication Services



This section describes different methods for users to obtain an OnTime authentication token for access to OnTime calendar data.
For more details about the token, see the section OnTime Authentication Token.

Desktop/Teams login methods in OnTime:



Note: Basic authentication and form-based pass-through with multi-factor authentication in Microsoft 365 are not supported.

– a drop-down menu shows the different choices for authentication.

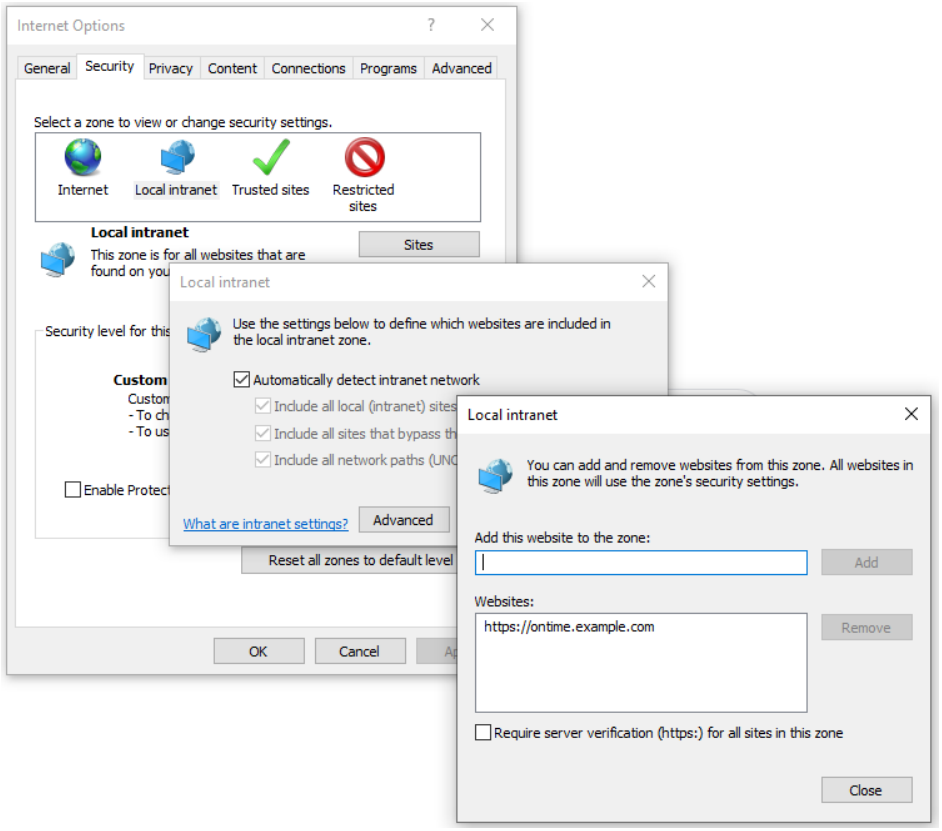
Form-Based – Pass-through authentication is only supported when the domain Windows AD has the 'userPrincipalName' value the same as the 'mail' address.

HTTP(S) Domain (SSO). The choice of HTTP may be preferable instead of HTTPS in the OnTime setup phase when you have not yet acquired a certificate for your OnTime server. This choice relies on the 'OnTimeMS Auth' (NTLM) service.
Ref. to **OnTime Domain Authentication (SSO)**

Note: The choice of HTTP(S) Domain (SSO) is not supported with the reverse proxy server for external access from the internet. Ref. **External access to OnTime.**
It is only supported if you provide a VPN-solution for external access from desktops.

See bBrowser setup for SSO for the browser to trust your OnTime server.

HTTPS ADFS (SSO) : is described further in the appendix



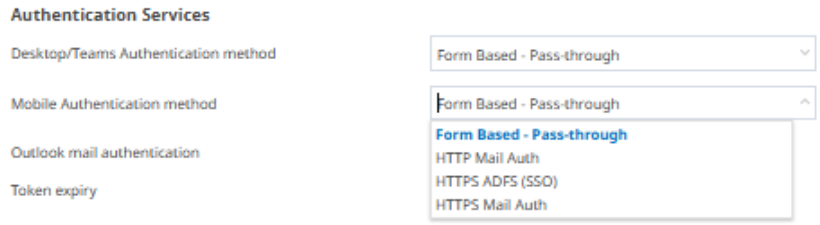
ADFS login (SSO)

HTTP(S) Mail Auth – OnTime supports authentication by email. A request with an email address is sent from the user, and OnTime responds with an email containing a link for the user to click. The link is valid for 15 minutes.

Custom – In case you have a special setup, you can select custom and type in your customised Authentication URL.

Note: ADFS is supported but no longer recommended by Microsoft. Entra ID (Microsoft Entra ID) cloud-based SSO is

Mobile Authentication Method



– a drop-down menu shows the different choices for Mobile authentication.

Form-Based – Pass-through authentication is only supported when the Windows AD has the 'userPrincipalName' value the same as the 'mail' address.

HTTP(S) Mail Auth – OnTime supports authentication by email. A request with an email address is sent from the user, and OnTime responds with an email containing a link for the user to click. The link is valid for 15 minutes.

HTTPS ADFS (SSO) - is described further in the appendix **ADFS login (SSO)**

Note: *"ADFS SSO is still supported, but Microsoft recommends migrating to Entra ID federation or cloud-native SSO solutions."*

Mailauth Timeout in minutes

-default 15 minutes timeout for Mail authentication

Outlook Mail Authentication

– enables the Outlook mail authentication in the 'Outlook add-in'. Set to 'Yes' when authenticating through ADFS; otherwise optional.

Please refer to the appendix **ADFS login (SSO)**.

Token expiry

– the OnTime user's authentication token lifetime in days. Which means how long the users can remain idle in OnTime before they need to log in again.

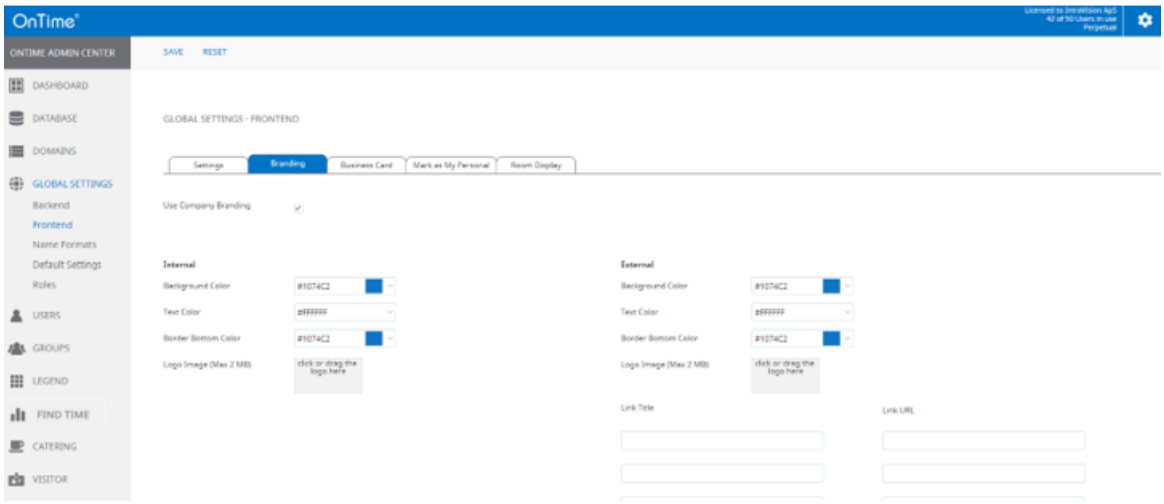
Default is 7 days. The minimum value is 1 day.

For details about the OnTime token, see the section **OnTime Authentication Token**.

Click 'Save' and go to the Dashboard.

Stop/Start the Application.

Branding



The tab ‘Branding’ is used for customizing the look and feel of the OnTime.

The lefthand column ‘Internal’ is for the Desktop.
The righthand __column ‘External’ is for applications like ‘Pollarity’

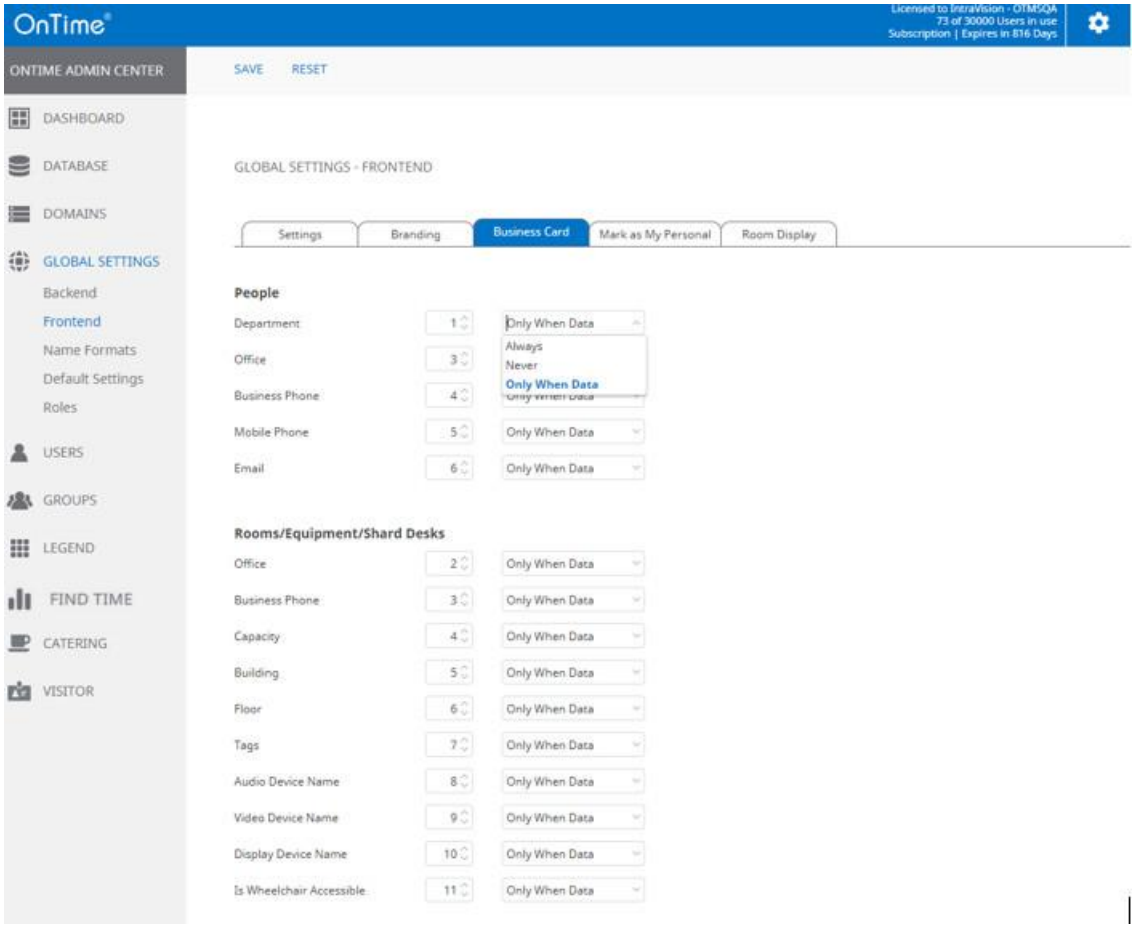
Use Company Branding – tick to enable.
Background Color – use the arrow to select a color.
Text Color - tick the arrow to choose the background color.
Border Bottom Color - tick the arrow to choose the Border Bottom color.
Logo Image (Max 2 MB) – click or drag the logo to the field.

Links in the Column ‘External’ are for Pollarity only – used for customizing the form for Pollarity. You may enter ‘Link Title’ and the ‘Link URL’.

Business Card:

The display of information in the business cards may be configured here. Business cards specify individual data for People, Rooms, Shared Desks, Equipment.

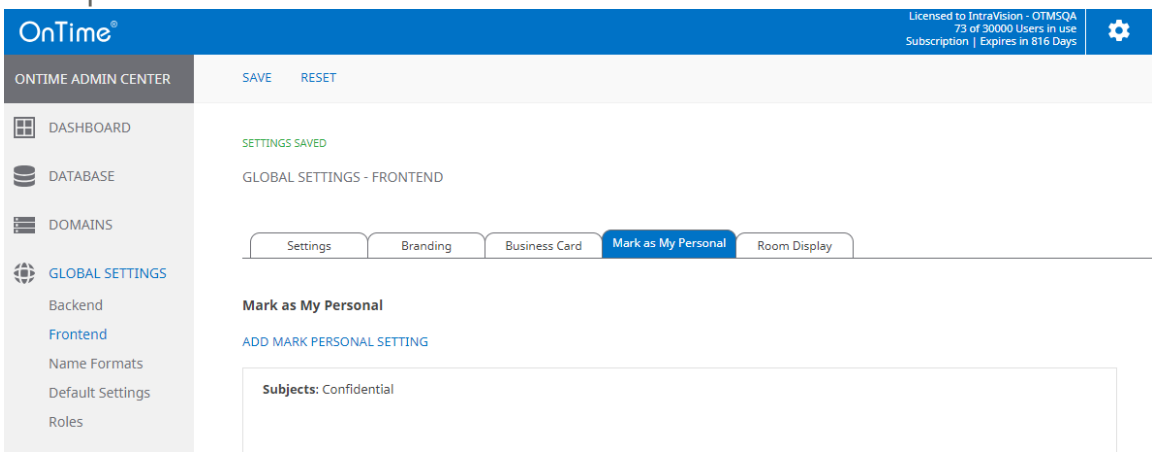
The column with numbers specifies the line numbers in the business card. In the righthand column you may specify if data is displayed.
Choice of ‘Only When data’, ‘Always’, ‘Never’.



Mark as My Personal

The setup in this section is used to restrict other users from viewing calendar entries which are “My Personal”.

Example:



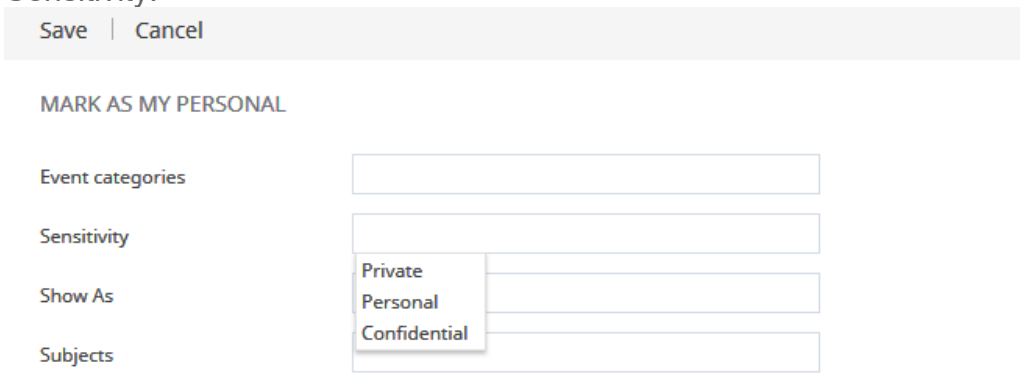
Click ‘Add Mark Personal Setting’ to setup.

Sensitivity is the levels as in Microsoft Outlook.

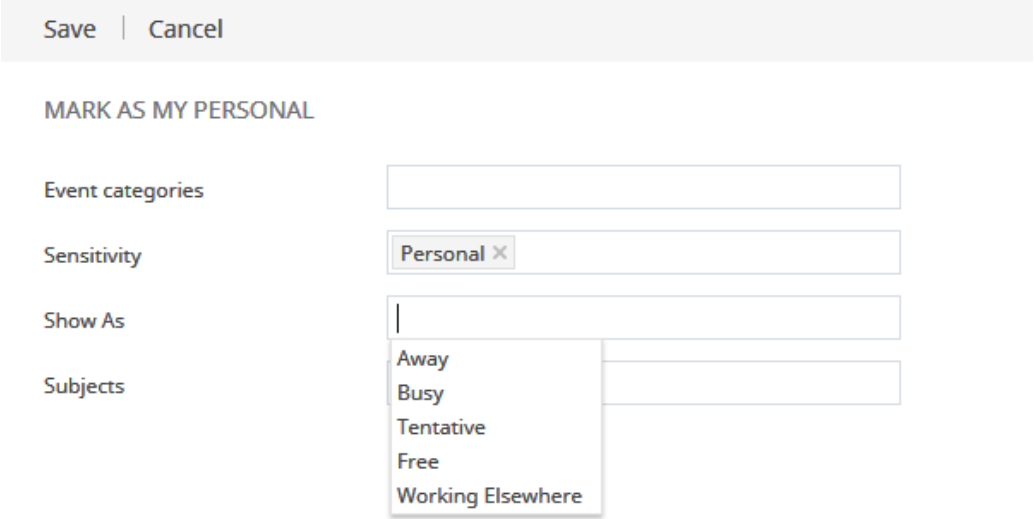
All the parameters in the ‘Mark as My Personal’ section must be true to take effect.

The calendar ‘Event categories’ are configured within the **Legend** section.

Sensitivity:

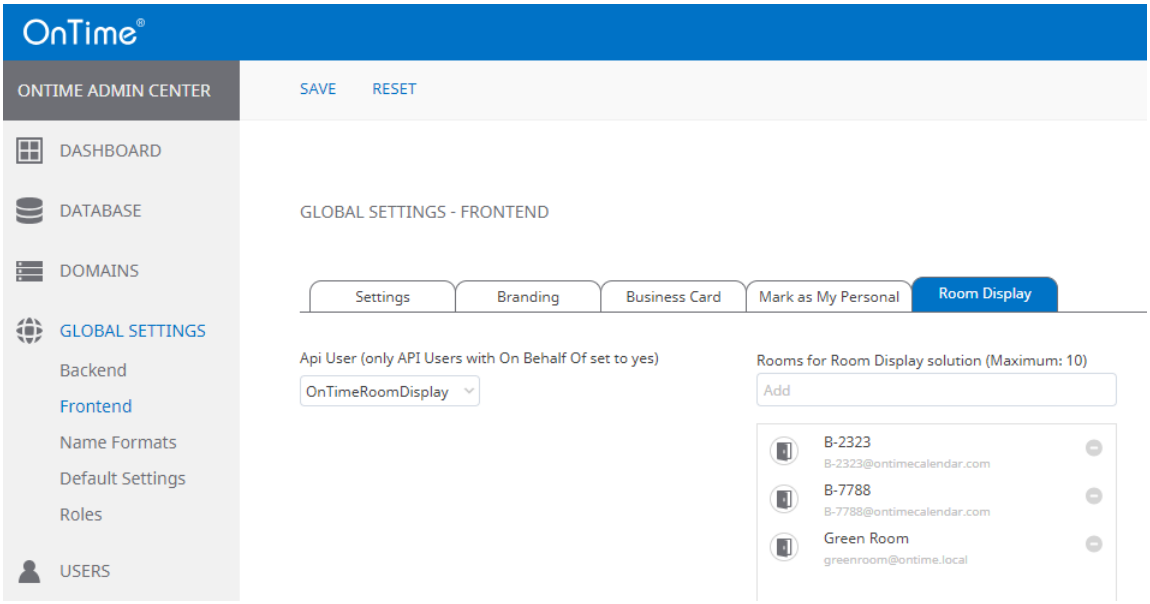


Show As:



Click ‘Save’ twice. Go to the **Dashboard**. Click Stop/Start the Application.

Room Display



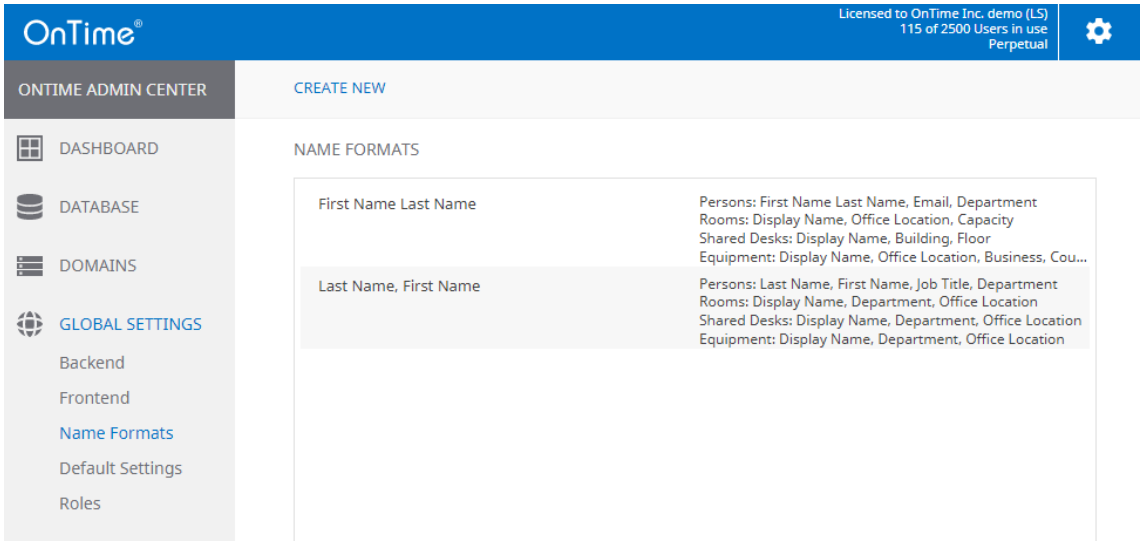
Choose an API User, with ‘On Behalf Of’ set to yes.

Add rooms with Room Display solution. The Maximum value shows your licenses for ‘Rooms Display Solution’ – allowed number of Rooms in the list.

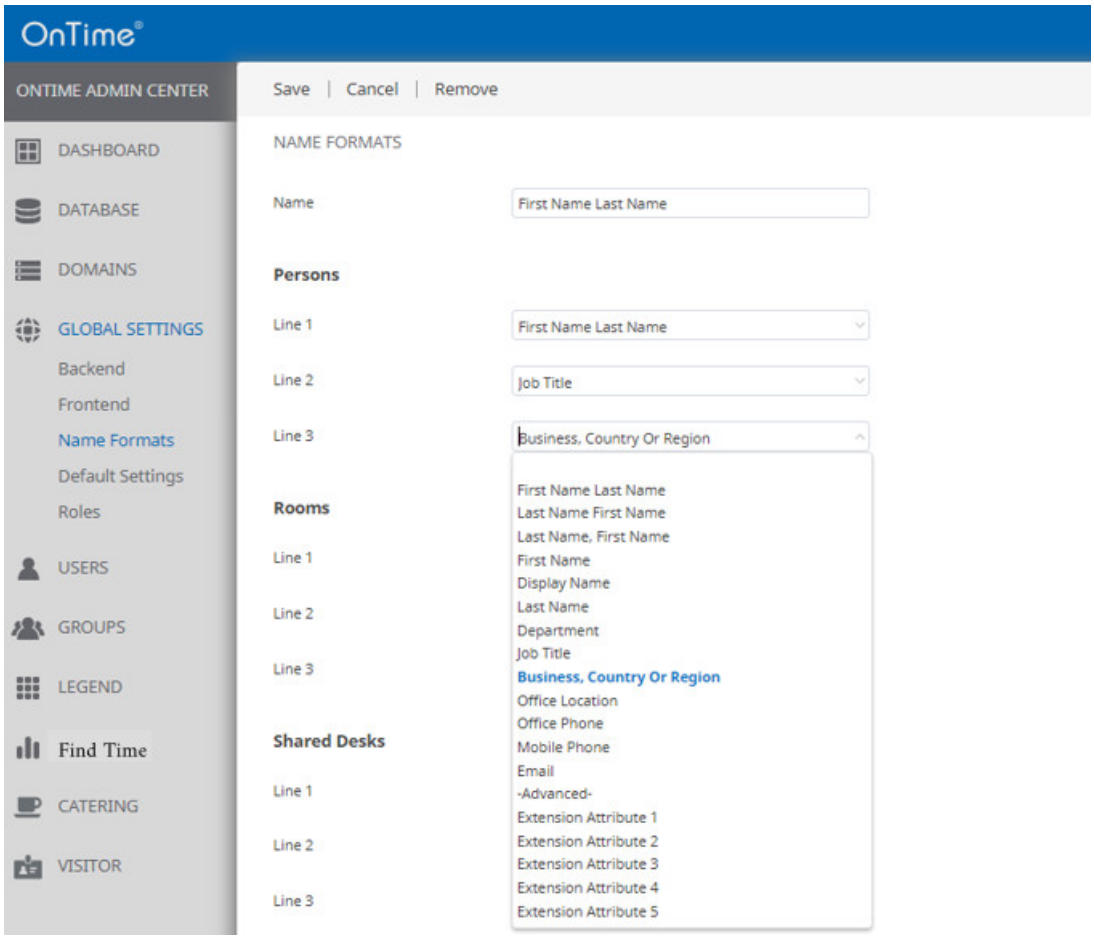
Click ‘Save’ – and restart the OnTime application in the Dashboard.

Name Formats

Click “Global – Name Formats” to work with the display of names etc.



Click “Create New” or click an existing entry to edit. The dropdown menus let you choose the content of Line1, Line 2, Line 3 for Persons, Rooms, Shared Desks, Equipment.



Name Formats/Advanced

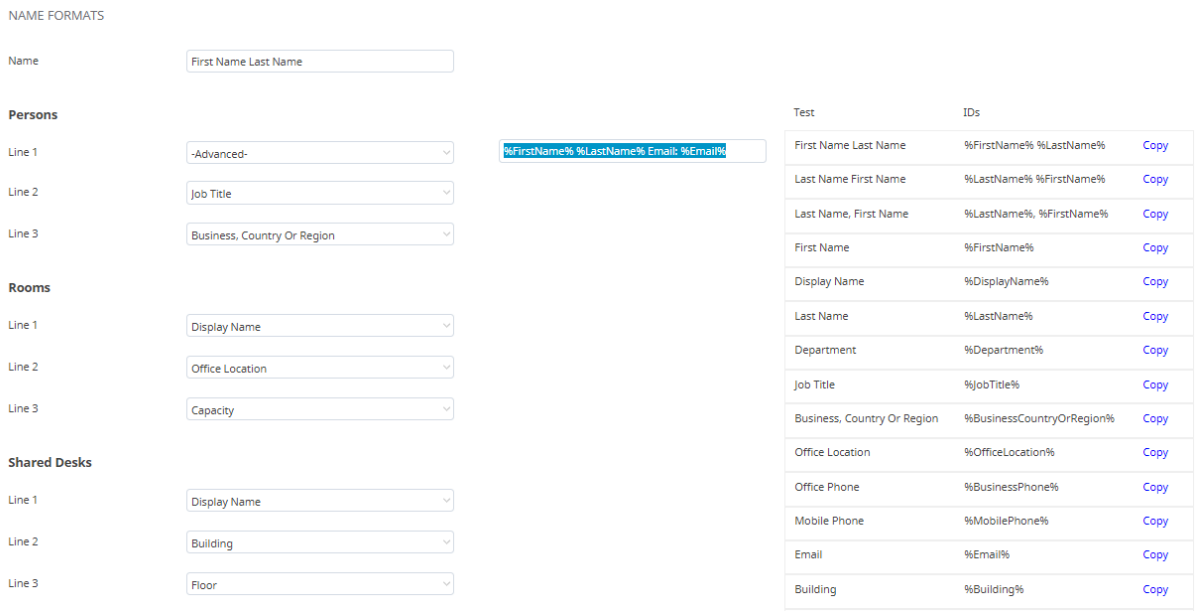
If you choose ‘Advanced’ in the dropdown menus, you can have more information in each line. You may add more parameters to the field in the middle column. The parameters are enclosed with ‘%’ characters. To avoid misspelling click ‘Copy’ and ‘Paste’ into the field in the middle column. You may add text/characters in between the parameters.

Example of field in the middle column:

```
%FirstName% %LastName% Email: %Email%
```

Line 1 may display as:

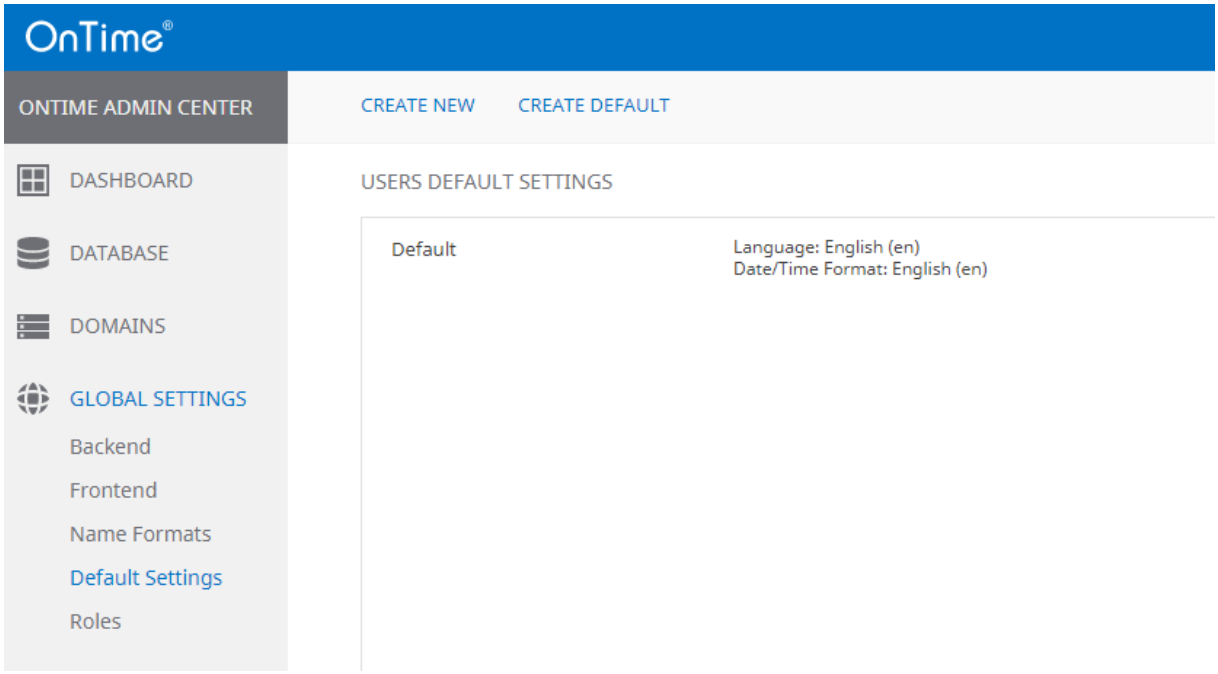
FirstName Lastname Email: email@example.com



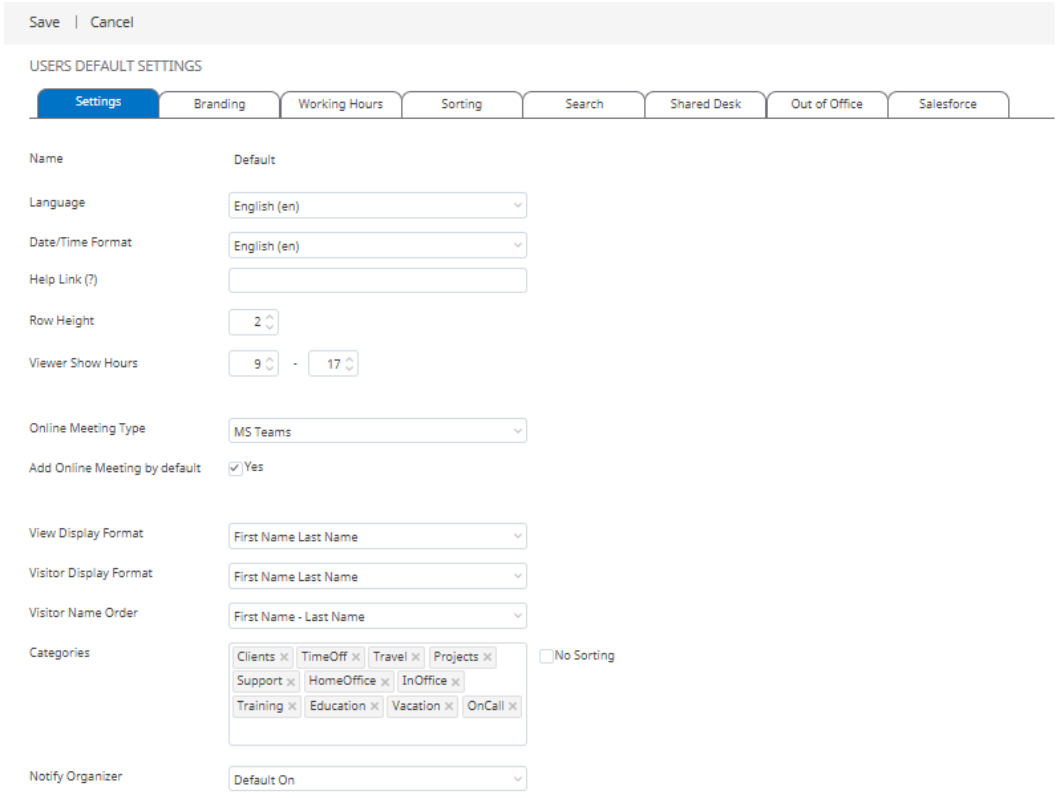
Click ‘Save’ to save your configuration

Default Settings

Click ‘Default Settings’.



Click ‘Create New’, or choose an existing entry, to change the OnTime User’s Default Settings.



Settings

Name - Name of the Setting.

Regional settings, like **Language** and **Date/Time Format** may be chosen.

Help Link(?) - Reference to customized help.

Row Height – number of lines per user

Viewer Show Hours – time span for showing the users appointments/meetings.

Online Meeting Type – choose between 'Microsoft Teams'.

Add OnLine Meetings by Default – checked by the administrator, the user may individually choose to untick Online meetings as default

View Display Format – order of 'First Name', 'Last Name'

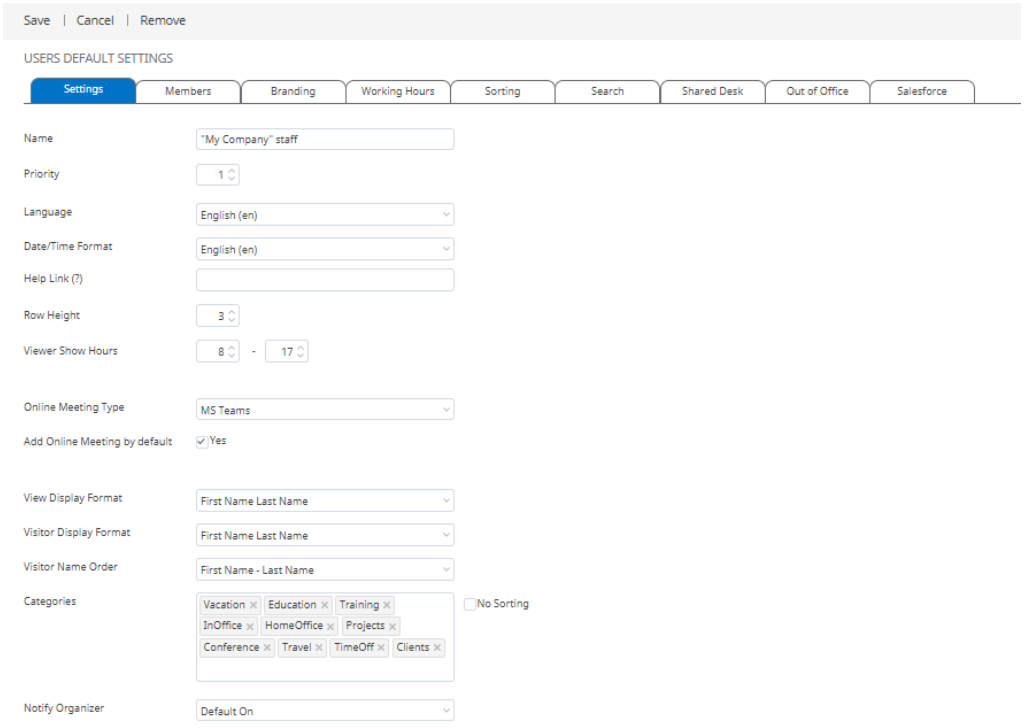
Visitor Display Format – order of 'First Name', 'Last Name'

Visitor Name order - order of 'First Name', 'Last Name'

The **Categories** entered will be visible as options when the user creates a calendar event. The categories originate from the legends left-hand defined in the Legends section. Please refer to

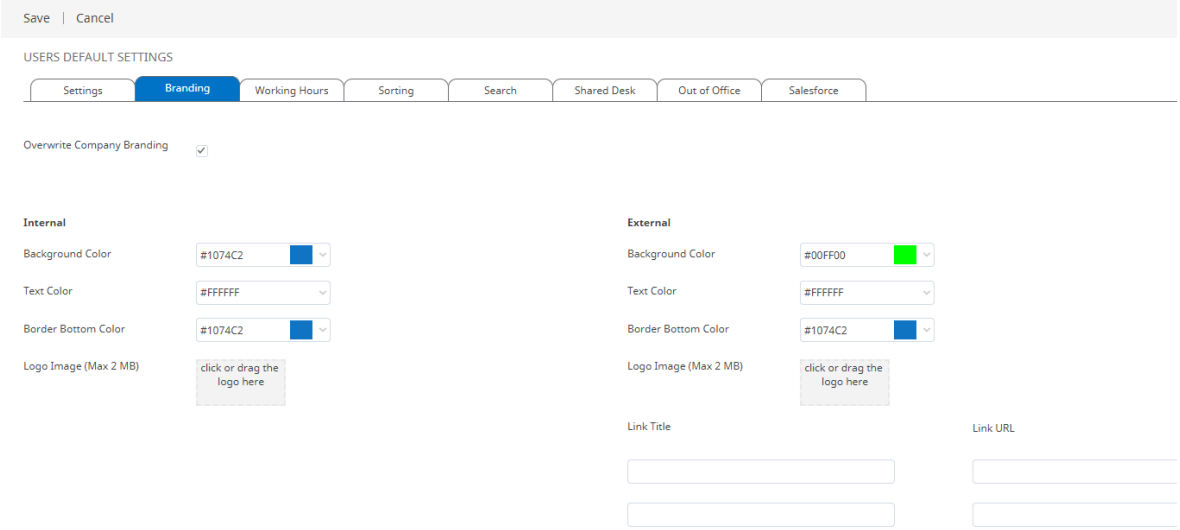
Members

If you create 'Default Settings' other than 'Default' you may work with **members**, include and eventually exclude persons for this particular 'Default Setting'



Branding

The tab ‘Branding’ is used for customizing the look and feel of the OnTime.



For the users you may overwrite the ‘Company Branding’ chosen in ‘Global Settings>Frontend’. The user settings have priority over ‘Company Branding’.

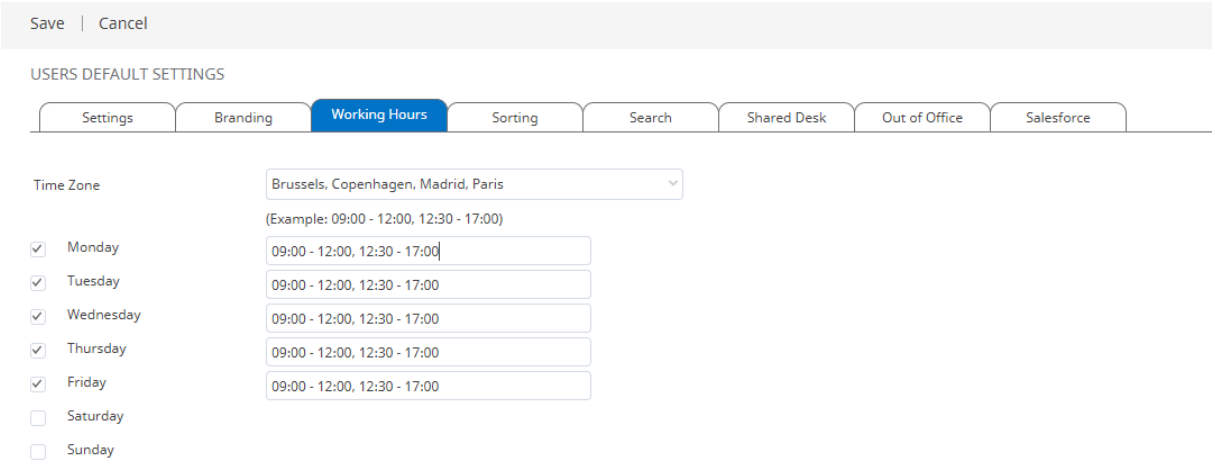
The lefthand column ‘Internal’ is for the Desktop.
The right-hand column ‘External’ is for applications like ‘Pollarity’

Overwrite Company Branding – tick to overwrite
Background Color – use the arrow to select a color
Text Color - tick the arrow to choose the background color
Border Bottom Color - tick the arrow to choose the Border Bottom color
Logo Image (Max 2 MB) – click or drag the logo to the field

Links in the Column ‘External’ are for Pollarity only – used for customizing the form for Pollarity. You may enter ‘Link Title’ and the ‘Link URL’.

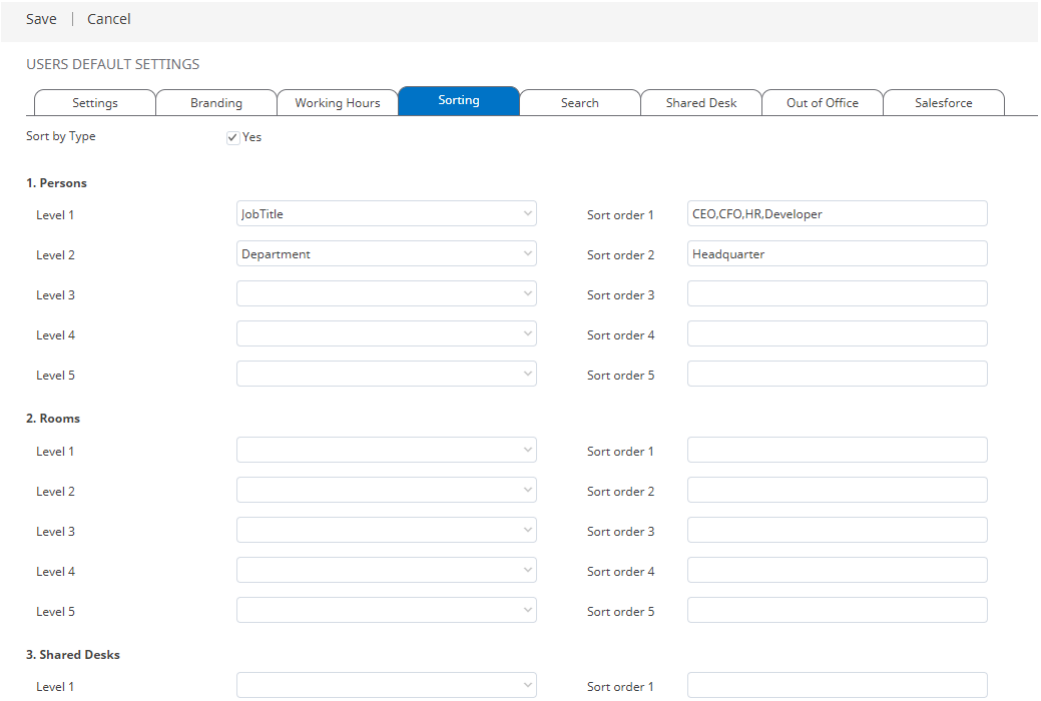
Working Hours

– in the section ‘Working Hours’ you may configure the Time Zone and the working hours each day.



Sorting

– in the section, ‘Sorting’ you may determine the sort order of Persons, Rooms, Shared Desks, Equipment. Tick ‘Sort by Type’.



Sorting of persons, rooms, shared desks, equipment is done alphabetically by name. When you activate the "Sort by Type" feature in the "Sorting" tab, the desktop views will be organized based on user types.

Specifically, individuals (Persons) will be prioritized first, followed by Rooms, and so forth.

If both Level and Sort orders are specified, the configuration might look like this:

Level 1: Job Title

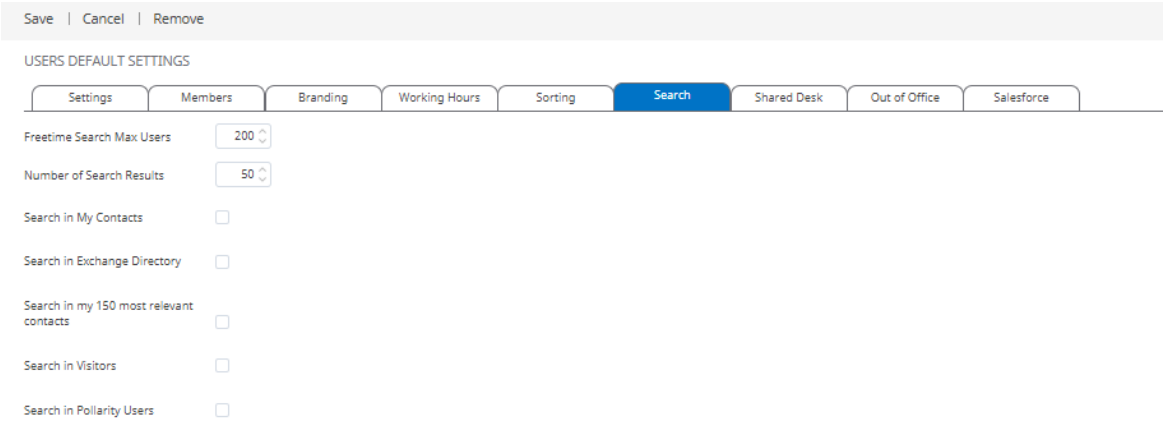
Sort order 1: CEO, CFO, HR, Developer

Level 2: Department

Sort order 2: Headquarters

As a result, the desktop views will display people sorted by their job titles, with CEOs appearing first, followed by CFOs, HR personnel, and Developers.
In cases where multiple individuals share the same job title, a secondary sorting will be applied based on the Department, placing those from the Headquarter at the forefront. If there are still multiple people with identical job titles and departments, the final sorting criterion will be alphabetical, based on their name format.

Search



Freetime Search Max Users: This performance parameter limits the time spent searching Freetime in a view with many users.

Number of Search Results: This number limits the number of persons and rooms shown in the list when the user types characters to search for people and rooms.

Search in My Contacts – Tick to exclude searches in private contacts.

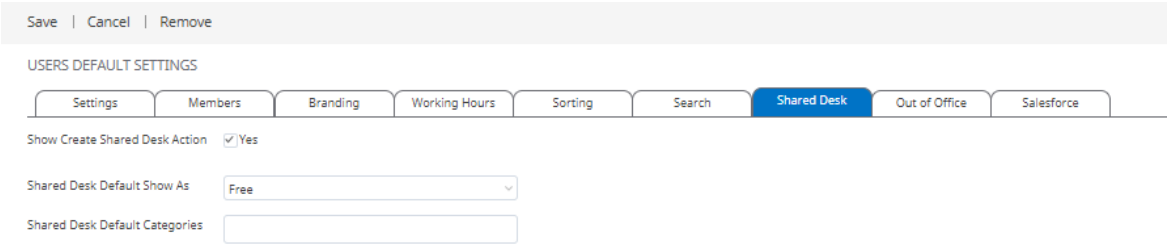
Search in Exchange Directory – tick to enable

Search in my 150 most relevant contacts – tick to enable

Search in Visitors – tick to enable

Search in Pollarity Users - tick to enable

Shared Desk

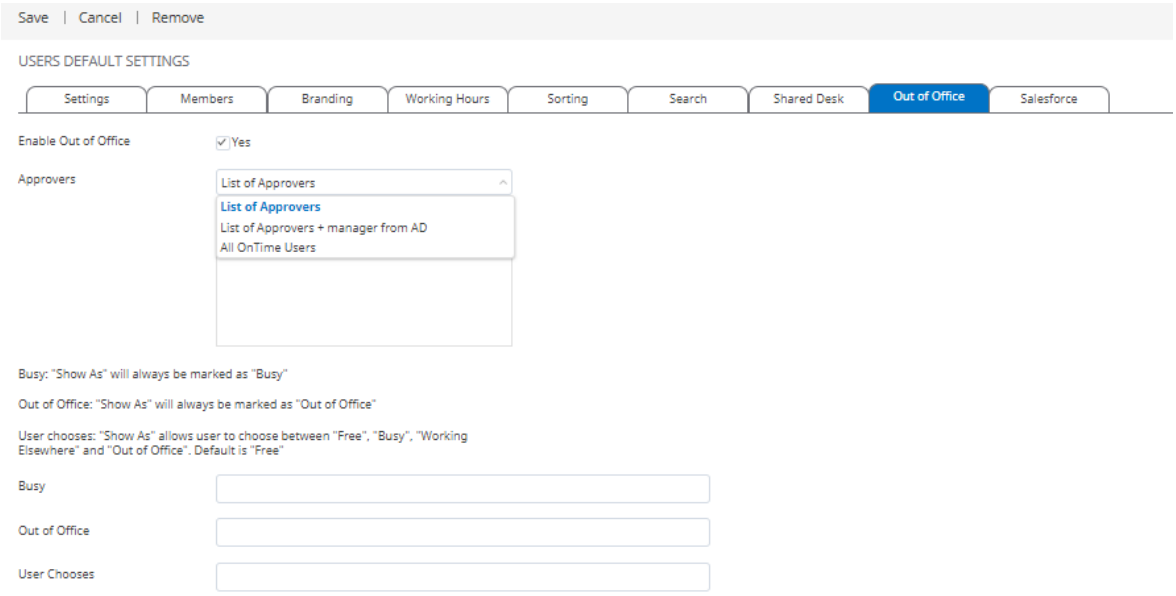


Show Create Shared Desk Action – tick 'Yes' to show the action button in the user's desktop

Shared Desk Default Show As – The availability shown for user reserving a Shared Desk.

Shared Desk Default Categories – Defines the legend (colour) shown for users reserving a shared desk.

Out of Office



Enable Out of Office: Tick 'Yes' to enable.

Approvers: Choose 'List of Approvers', '+ manager from Active Directory', 'All OnTime Users'.

In the 'Add' field type a few letters to search for people.

Enter categories available in 'Out of Office' for the user.

If the categories correspond to your definitions of legends, they will be coloured according to the legends in the user interface.

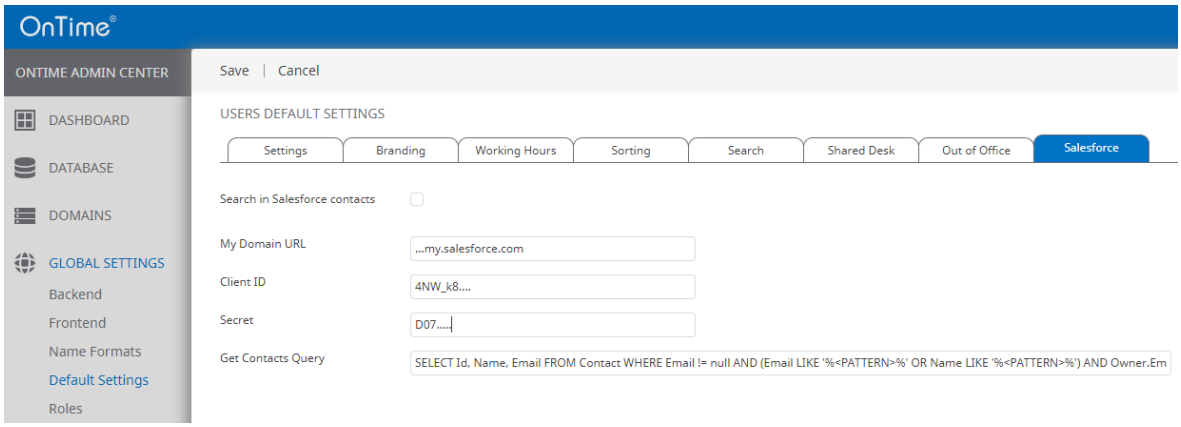
Busy: 'Show As' will be marked as 'Busy'

Out of Office: 'Show as' will be marked as 'Busy'

User Chooses: The user may decide Busy/Available

Salesforce

Search in Salesforce contacts is supported in OnTime.



Search in Salesforce contacts – tick to enable.

My Domain URL – Your domain registered with Salesforce

Client ID – Your Salesforce Client ID

Secret – The secret for accessing your Salesforce account

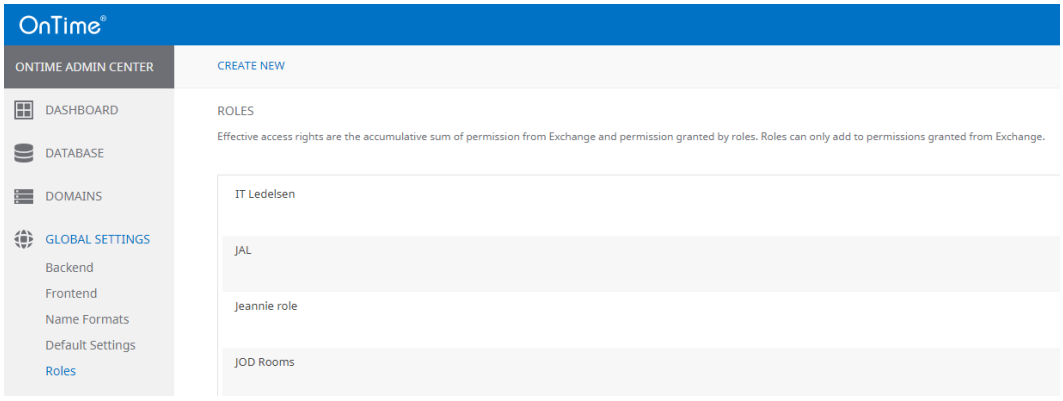
Get Contacts Query – Example: 'SELECT Id, Name, Email FROM Contact WHERE Email != null AND (Email LIKE '%<PATTERN>%' OR Name LIKE '%<PATTERN>%') AND Owner.Email = '<USER_EMAIL>'LIMIT 20'

Roles

In Exchange/Outlook the access to the users' calendar is configured as permissions like 'Busy/Available', 'View Titles and Locations', 'View all details' and 'Edit'.

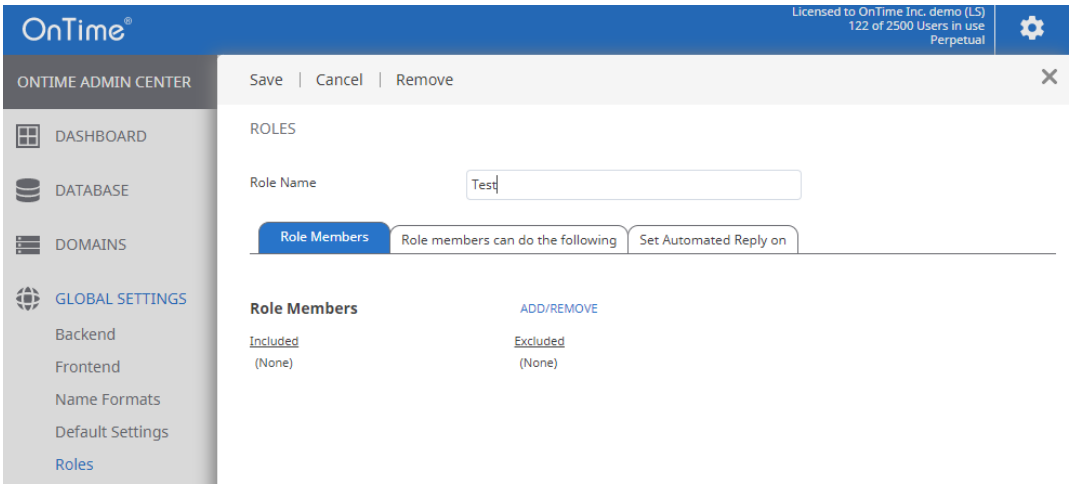
In the OnTime Calendar, a system with Roles has been added to override the individual settings of calendar permissions. With Roles, the administrator may give certain users a level of access to the users' calendars, which are different from the configured permissions in Exchange/Outlook. The permissions will be the cumulated value of the Exchange/Outlook permissions and the role setup, which means that the roles setup cannot be used to lower the permissions.

Click "Global Settings – Roles" to Create/Edit the users' roles.

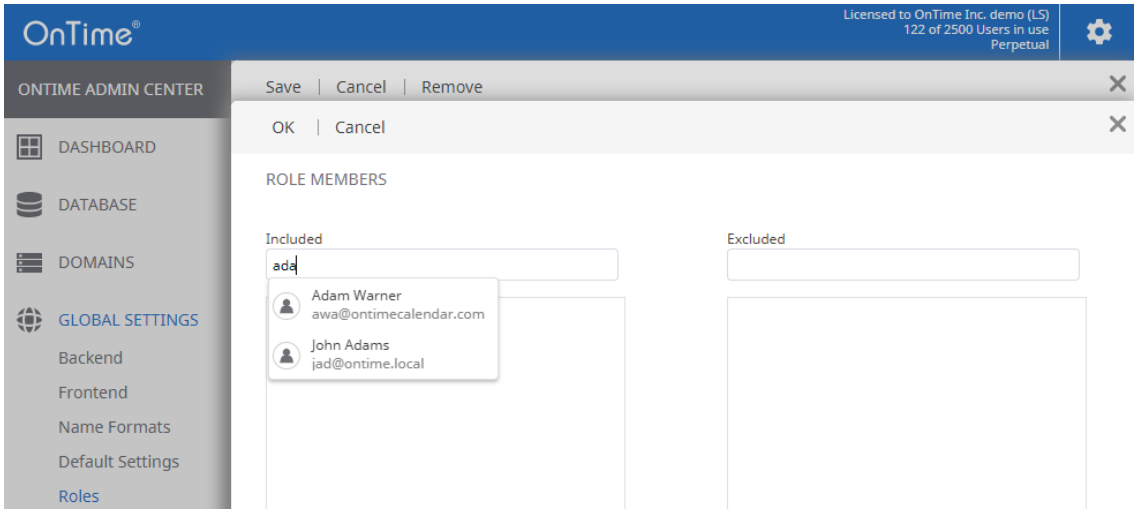


Click 'Create New' to create a role.

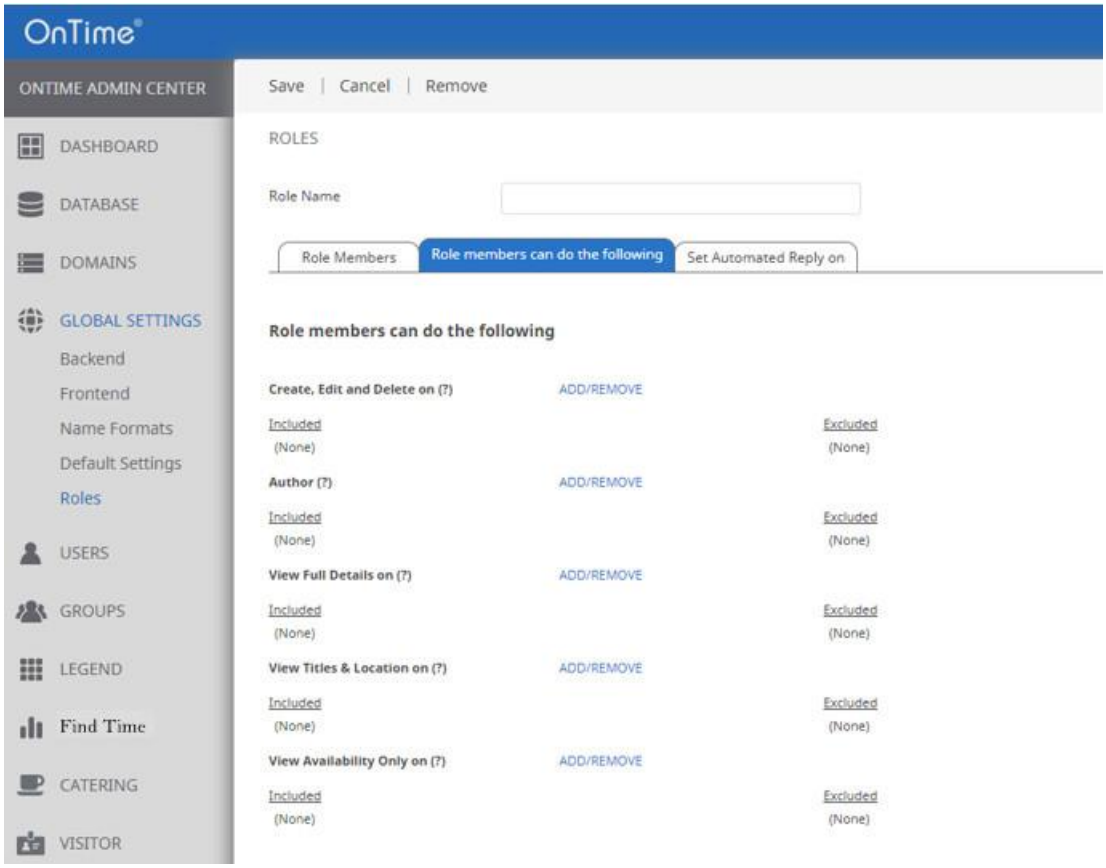
Enter a 'Role Name'.



Click ‘Add/Remove’ at ‘Role Members’ to configure the selection of users in this role. Enter characters to look up persons or groups from the directory. Click the persons to include them in the ‘Role Members’. Click ‘OK’ to save the list.



Click ‘Role members can do the following’ and ‘Add/Remove’ to select the role members’ access to the group or the users’ details.

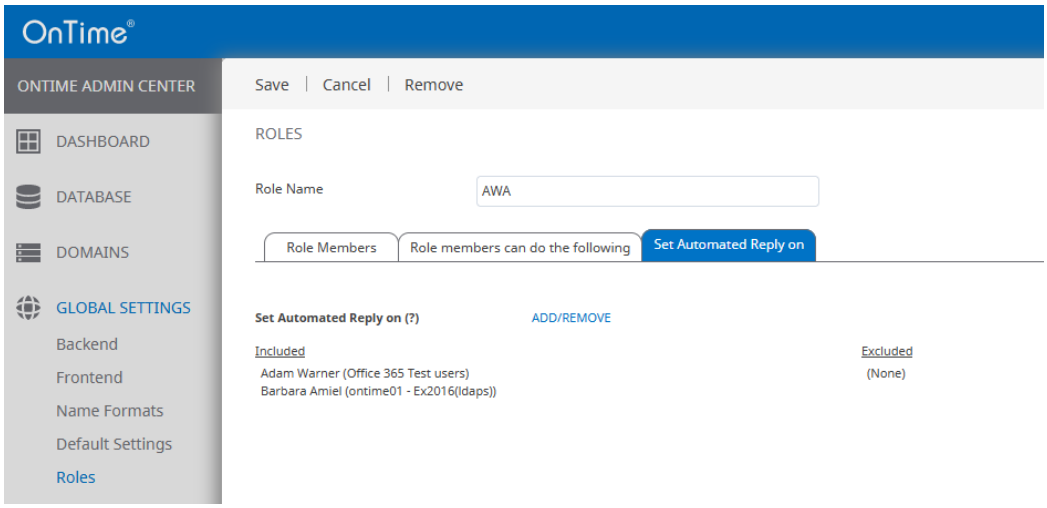


There are five different levels of what Role members can do to Calendar entries in OnTime.

Access level	Description
Create, Edit and Delete	This level allows users to Read, Create, Edit and Delete entries for the people that the users have been granted this access for Private appointments still have all information hidden by default.
Author	This level allows users to Read, Create, Edit and Delete entries for the people that the users have been granted this access for. The Author may only edit their own entries. Private appointments still have all information hidden by default
View full details	This level allows users access to read all details of a calendar entry. Private appointments still have all information hidden by default.
View Titles & Location	This level allows users access view Titles/Subjects and Locations Private appointments still have all information hidden by default.
View Availabilty Only	View Availability/Busy time information is the lowest level of access to calendar entries a user can be granted. Users can see whether the individuals are busy but not the subject of the meeting. Users can see Type and Category (Legend colour) of calendar entries.

Automated Reply

Click ‘Set Automated Reply on’ to select groups or users. The Role member may enter ‘Out of Office’ information for the users included.



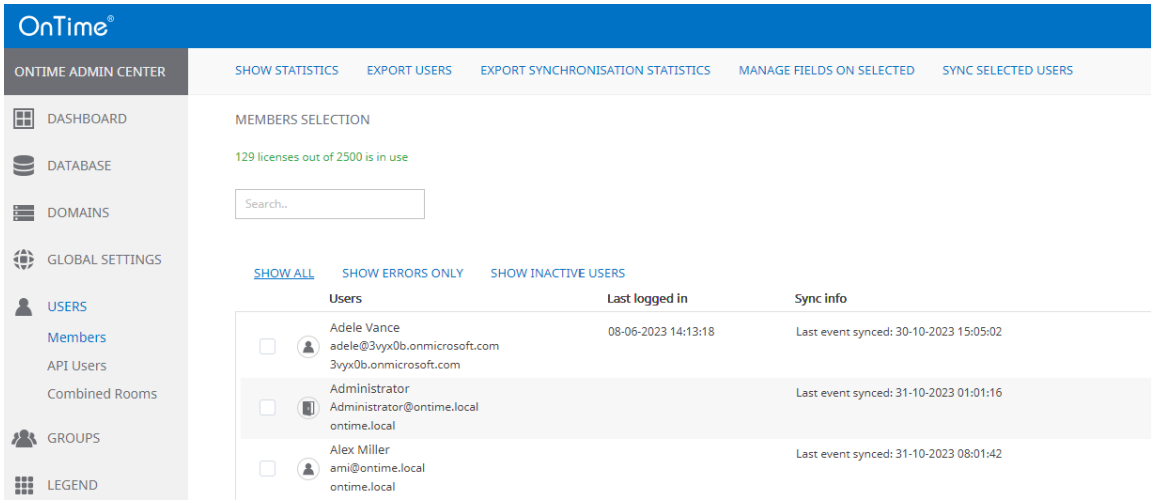
When done editing permissions, click ‘Save’ on the roles document.

The new configuration of roles is designed to be working after a few seconds.

Users

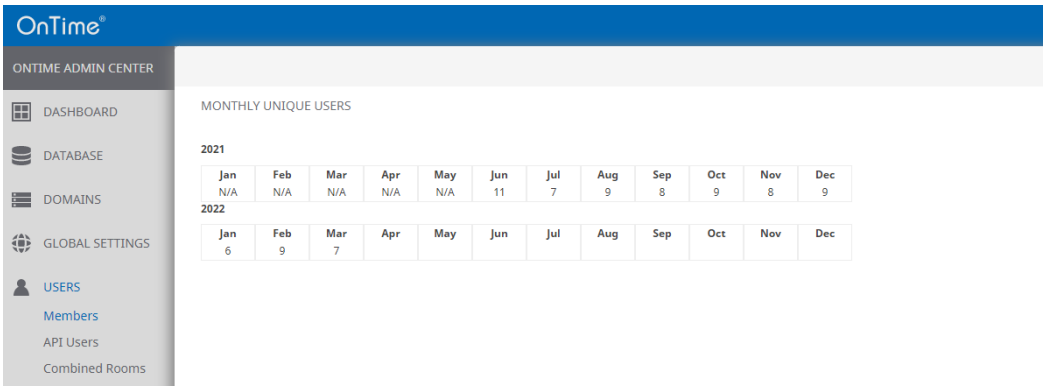
Members

Click ‘Users/Members’ to see the list of available users in OnTime.



The ‘Filter Box’ may be used to reduce the scope of searching – just add a few characters.

Click **‘Show Statistics’** at the top to view statistics about the ‘Monthly Unique Users’



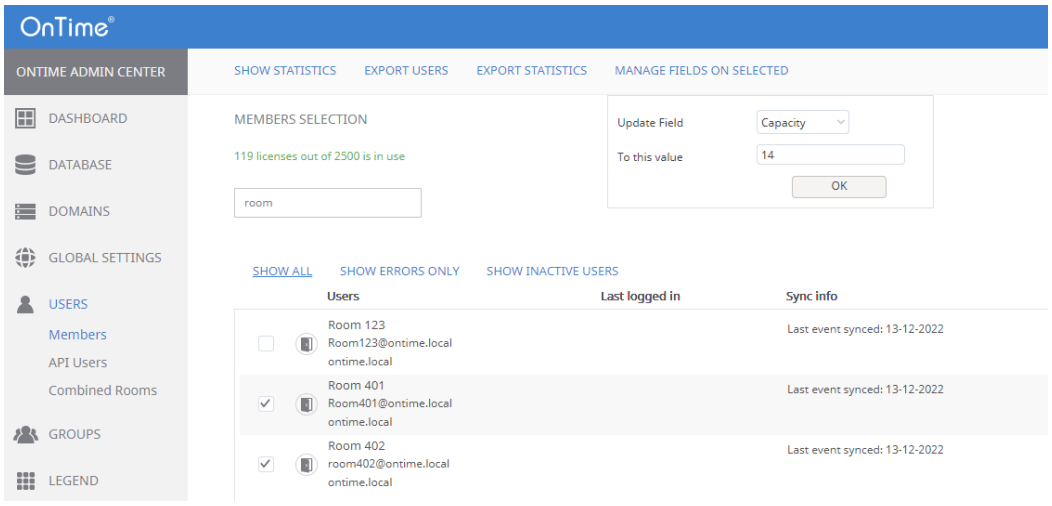
The N/A – not applicable, means no data available for the month.

Blank fields are for the months in the future.

You may export a list of OnTime users in a comma-separated file by clicking ‘Export Users’.

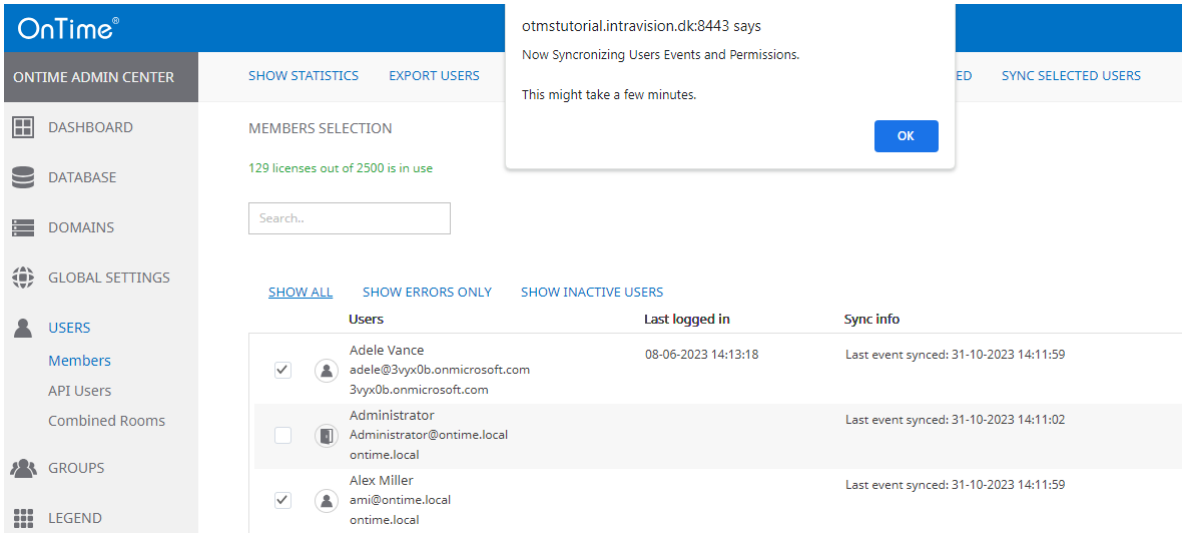
You may export statistics from OnTime in a comma-separated file by clicking ‘Export Statistics’.

The button ‘Manage Fields on Selected’ – is used for changing values in editable fields for the resources selected:

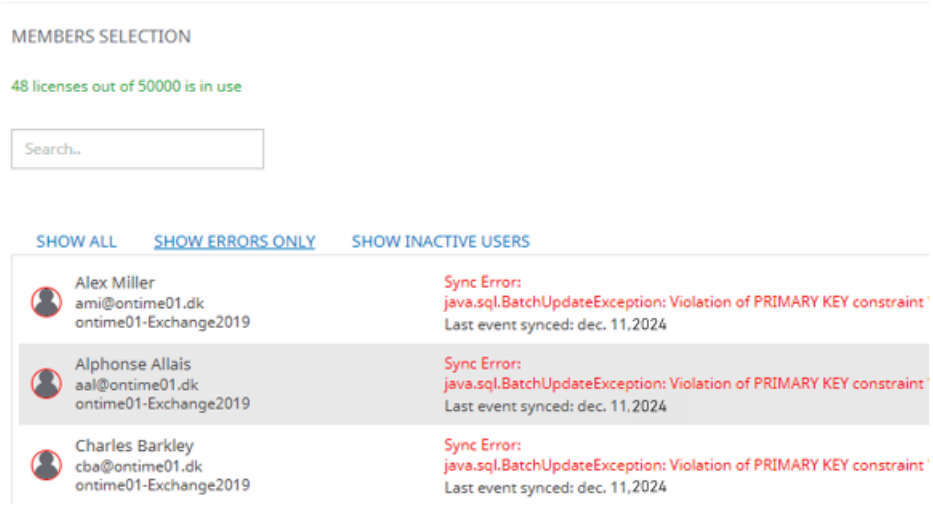


If the result box shows fewer updates than you expected – some of the resources do not have editable fields in their ‘Business Card’.

You may Sync selected users Events and Permissions by clicking ‘Sync Selected Users’.



If a user is shown in red in the list of users, it means there is a synchronisation error for that user. Click it to see the error and refer to the log for more info.

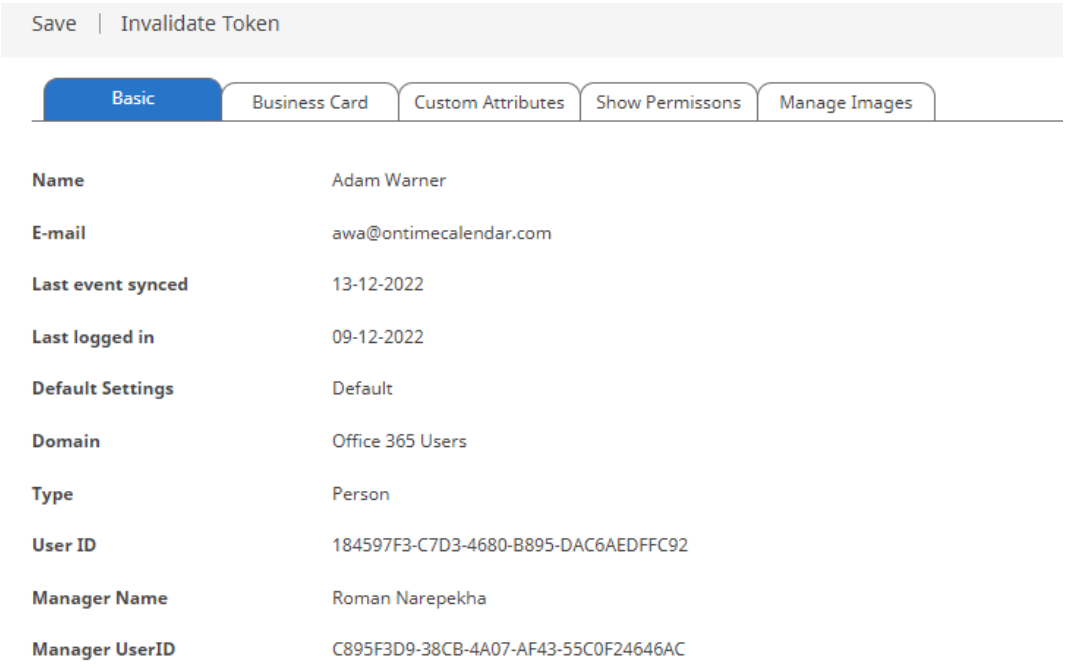


“Show Inactive Users” tab shows information about the users who are currently not active in the system. These users can be permanently removed by clicking on them and invoking action “Purge User”

For details choose a user.
We have four types of users:
Person, Room, Equipment, Shared Desk.

The screenshot below is relevant for persons.

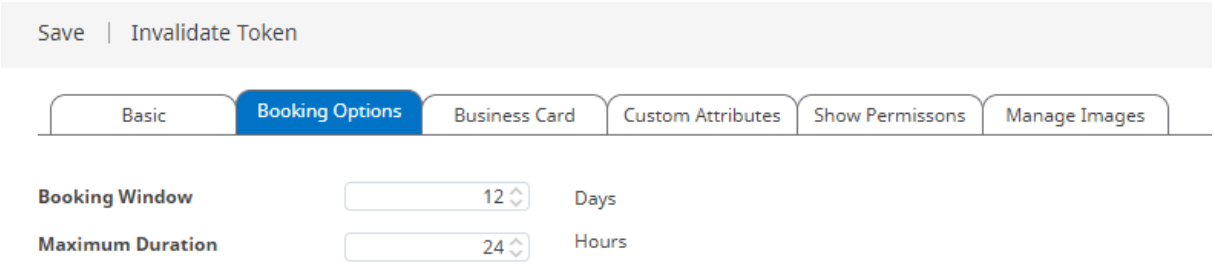
Values coming from the Active Directory are shown without a frame – and they are not editable from ‘OnTime Admin Centre’. Basic



The action button at the top - 'Invalidate Token' is used to invalidate the user's OnTimeToken.
The next login from the user requires a new authentication.
For details see the section OnTime Authentication Token

Booking Options

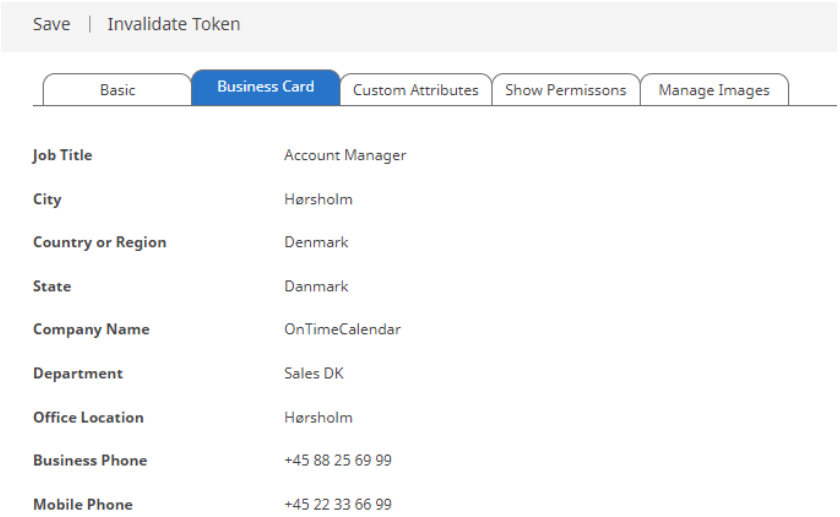
This tab is only relevant for the three user types – Room, Equipment, SharedDesk – not for the user type, person.



Booking Window – Number of days it is possible to book ahead of time.
Maximum Duration – Number of hours it is possible to book this resource.

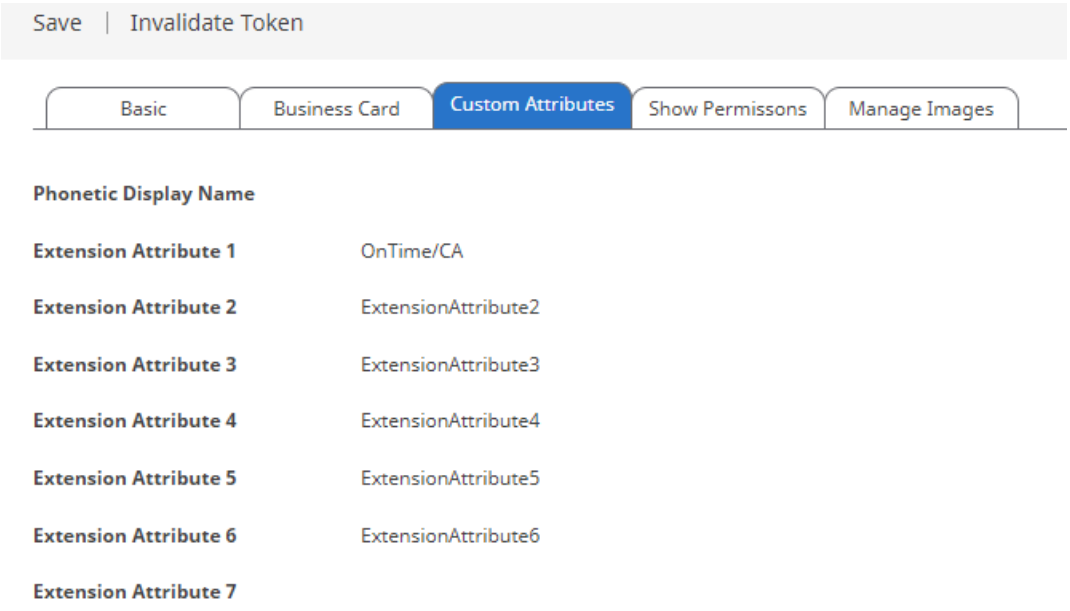
Business Card

Click 'Business Card', to see details – for a person



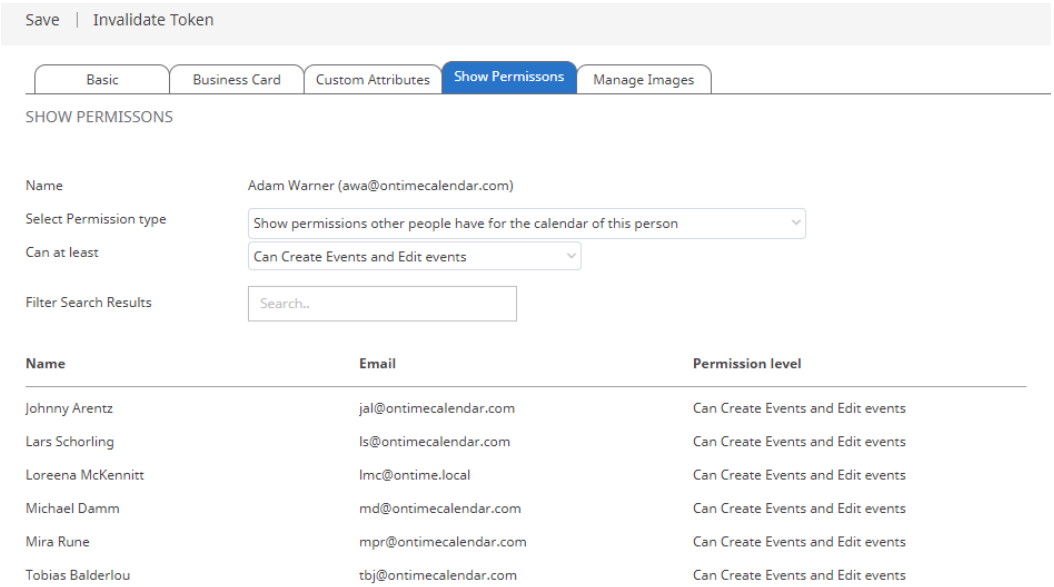
Custom Attributes

Click ‘Custom Attributes’ to see extension attributes from Active Directory



More details about the fields and their mappings to the user, EWS or Active Directory (LDAP) may be seen in the appendix Mapping of directory fields.

Show Permissions



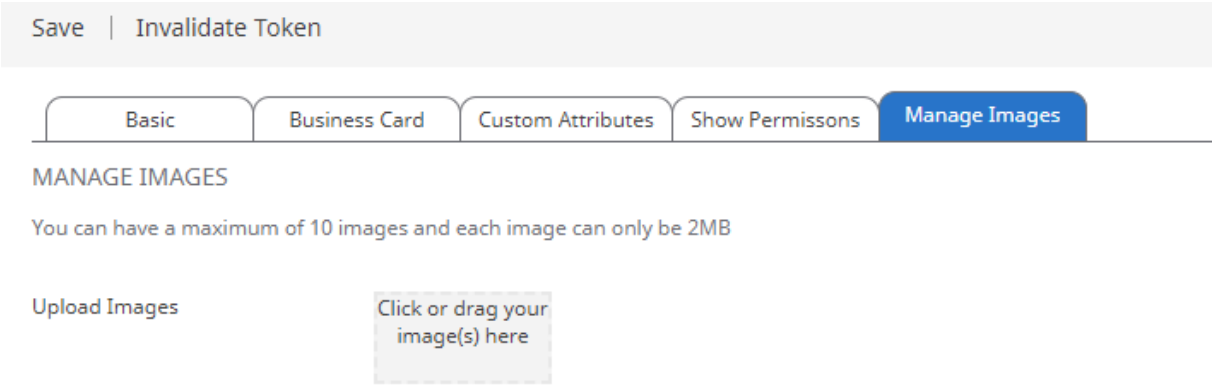
'Show Permissions' is used to get an overview of the calendar permissions for the specific user. Two selections of permission types are possible, permissions for other users to this person's calendar, and permissions that this user has to other user's calendars.

'Show permissions other people have for the calendar of this person'
'Can at least' - 'Can Create Events and Edit events'
'View availability only'

'Show permissions this person has for other people's calendar'
'Can at least' – 'Can Create Events and Edit events'
'View Full Details'
'View availability only'

Manage Images

For upload of images – max. 10 images of max. 2MB each:

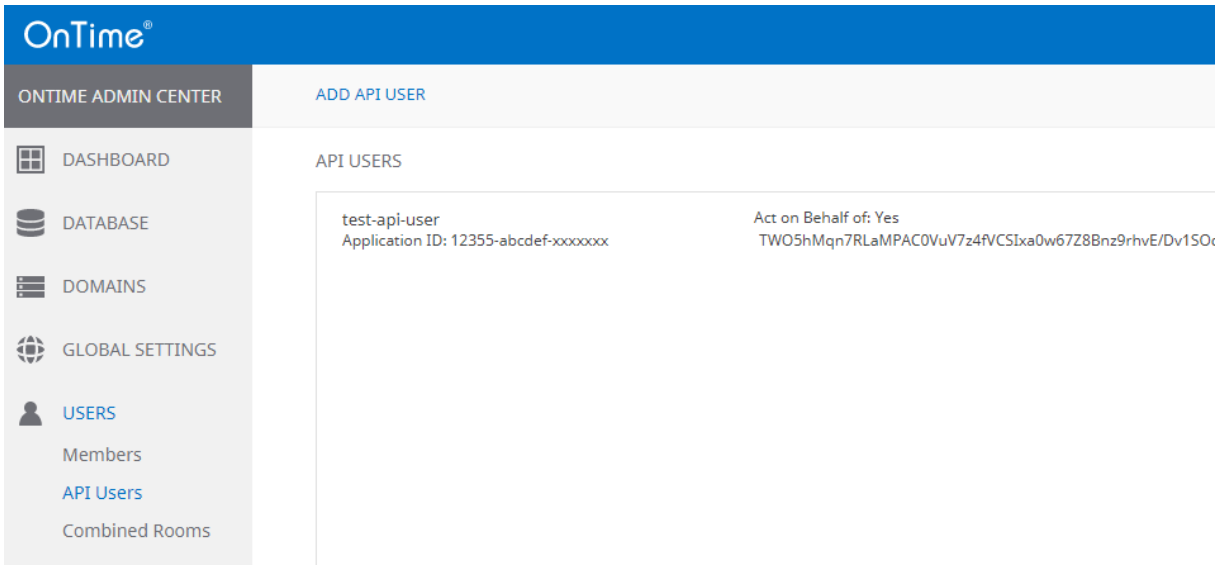


API Users

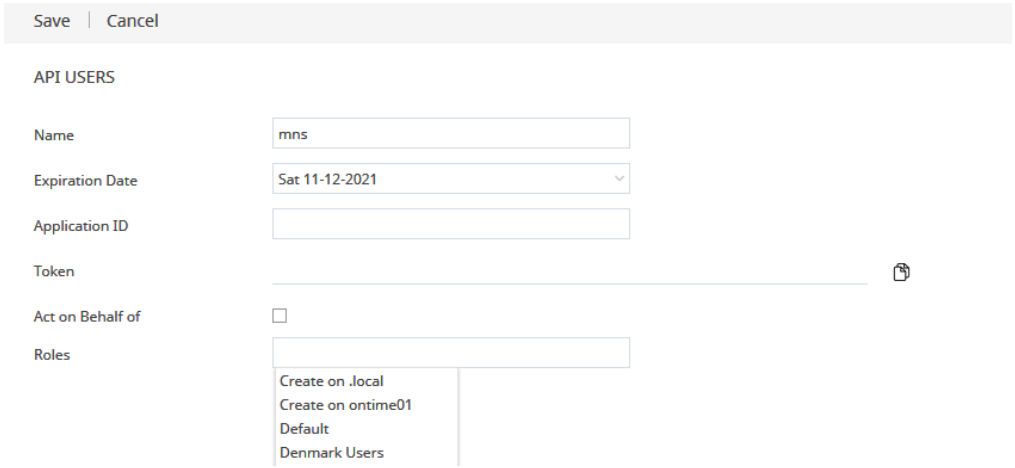
The API user is used for developing your own external applications using the OnTime API.

A special “APIUser” license key is required to enable this functionality.

Click ‘Users/API Users’



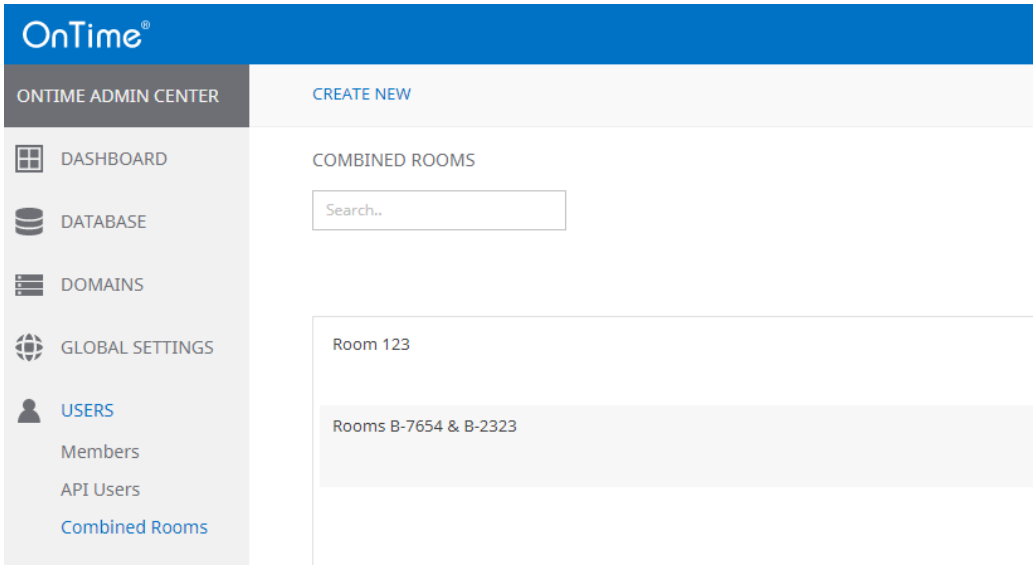
Click ‘Add API User’ to create a new OnTime API User.



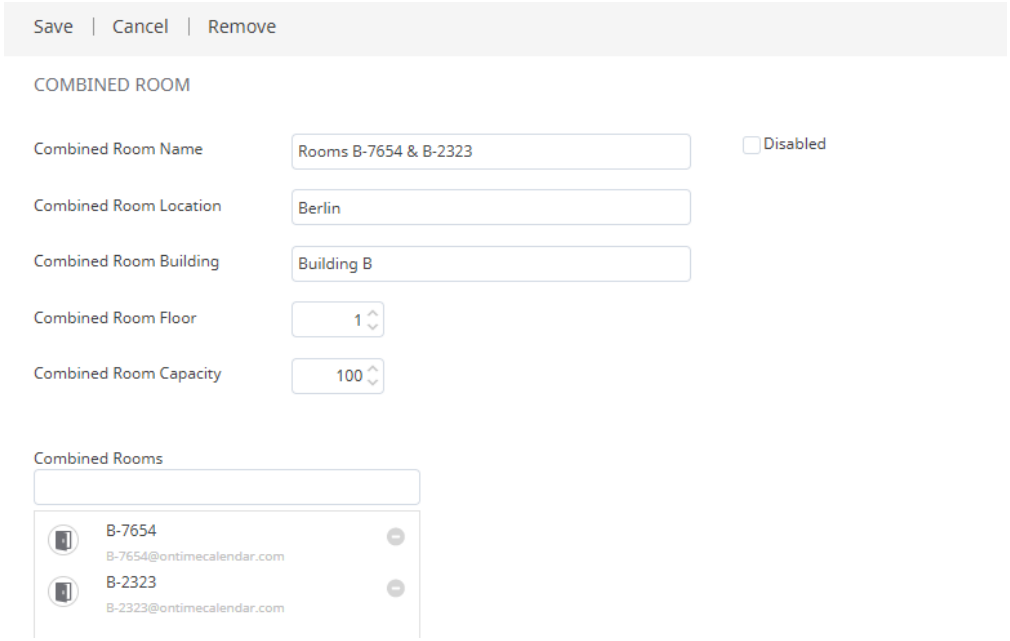
Name – enter a name of the API User.
Expiration Date – enter the expiration date for this API User
Application ID – license acquired
Token – when you click ‘Save’ a token is generated in the OnTime back-end.
Act on Behalf of – checked, means that the API User acts with the individual rights of all users (bypasses Roles)
Roles – the API User acts according to the role defined in Global\Roles.

Combined Rooms

Click ‘Users/Combined Rooms’ to view or create rooms that are combinations of two or more rooms.



Click ‘Create New’ or edit an existing ‘Combined Room’:

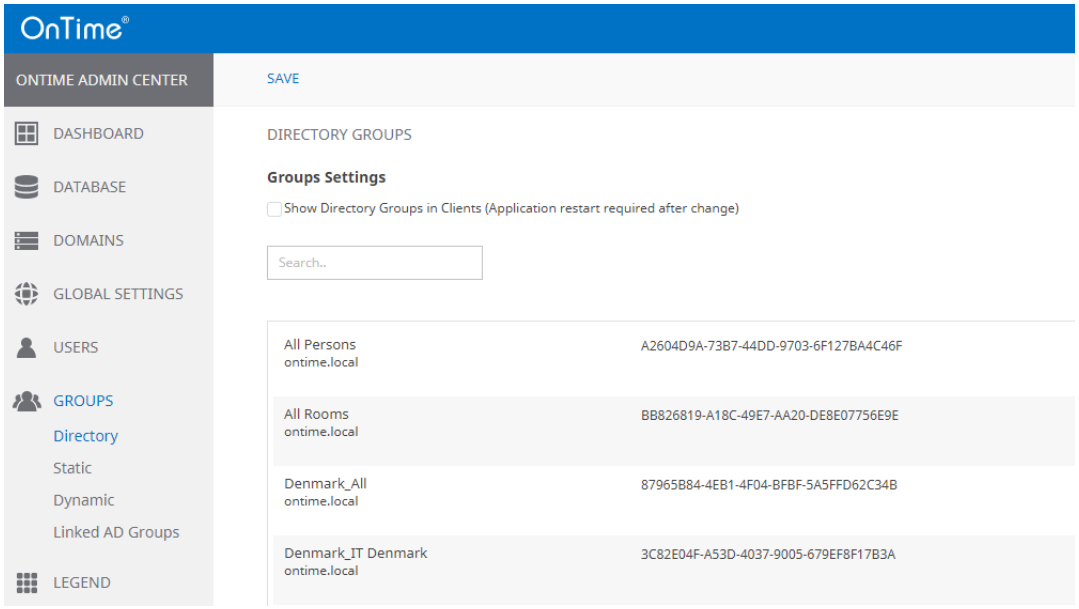


Groups

Four variants of groups are available, Directory groups, Static Groups, Dynamic groups and Linked AD Groups.

Directory Groups

Click “Groups/Directory” to see a list of Directory groups from the AD, included in the OnTime calendar.



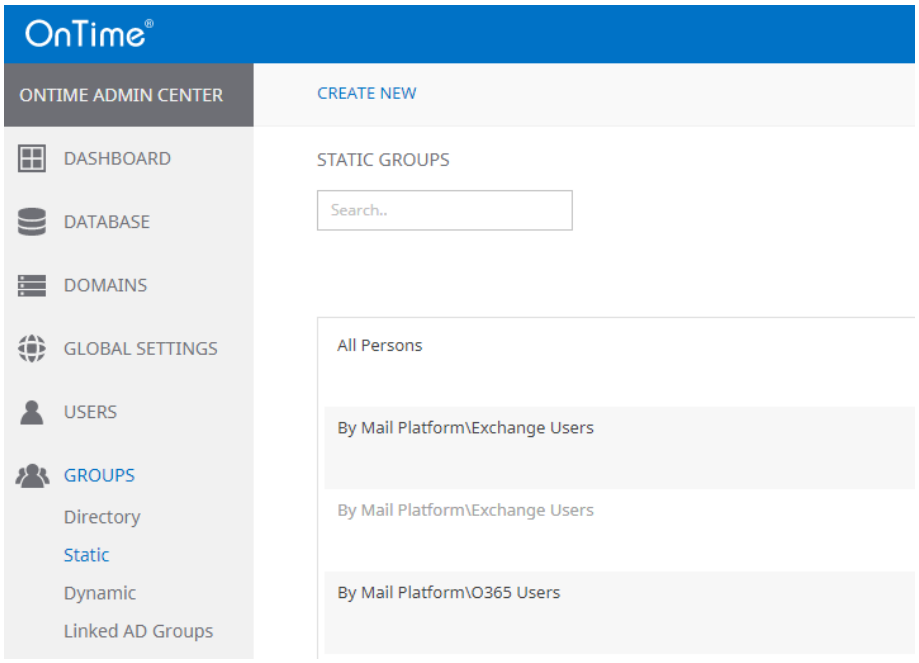
To show these groups in the OnTime client, tick ‘Show Directory Groups in Clients’ and ”Save”.

If you change your groups in Active Directory

- go to the **Dashboard** and click “Start” at “Directory Sync”.

Static Groups

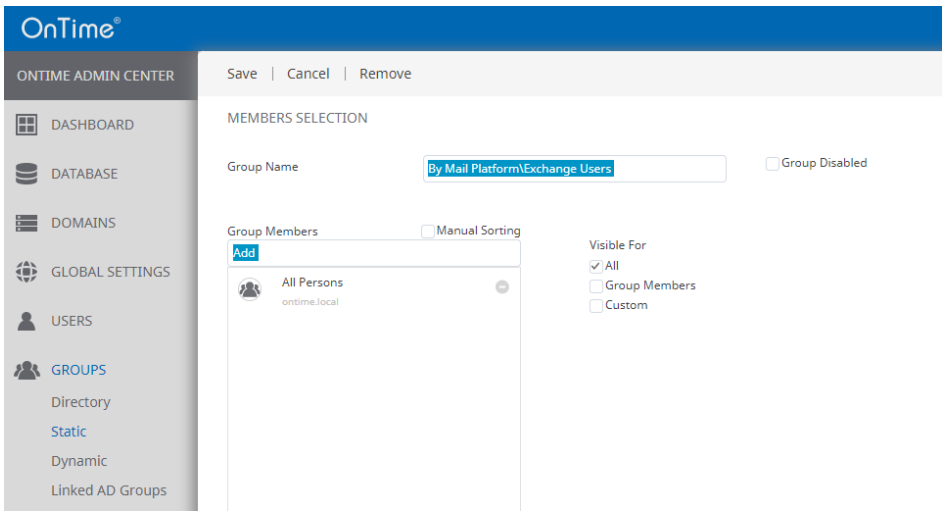
Click ‘Groups/Static’ and ‘Create New’ for groups within OnTime.



Here you can administrate an OnTime group structure that will be displayed for all users. It could be an organisational structure or maybe different projects. You can assign both Exchange groups, Persons, Rooms, and Equipment as members of your Static Groups.

Changes in the static Groups must be followed by clicking “Start” at “User & Group Sync” in the **Dashboard**

Click “Create New” to create a new Static group. You may search elements by entering a few characters, click to add members to the group.



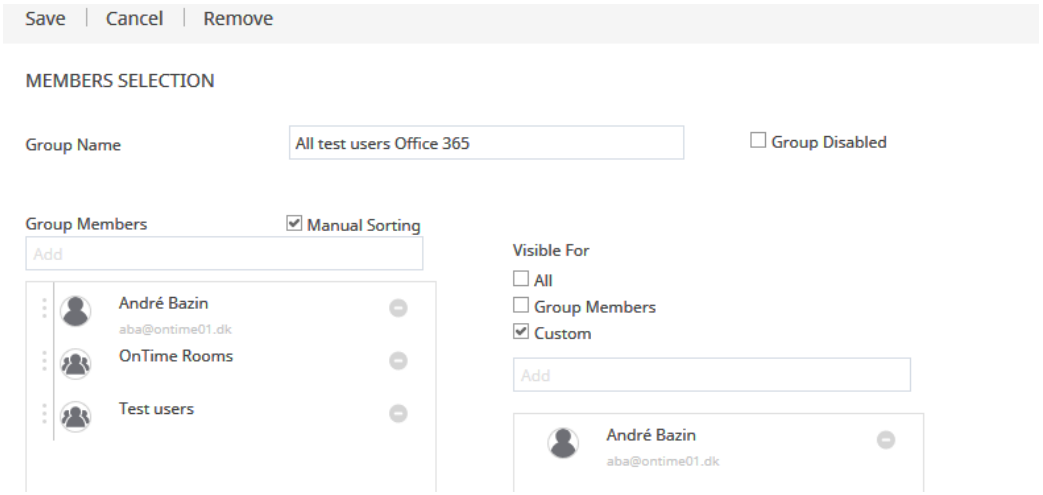
Group Name – Enter a name for the group

Group Disabled – tick, to hide it from the user interface

Manual Sorting

- 'Tick'. Hold' the grey buttons at the left-hand side of an element and drag to the position you want it.
- Click 'Save'.

The visibility of the static group may be chosen for 'All' persons, only 'Group Members' or selected users/groups in 'Custom'.



Click "Save" to save your group.

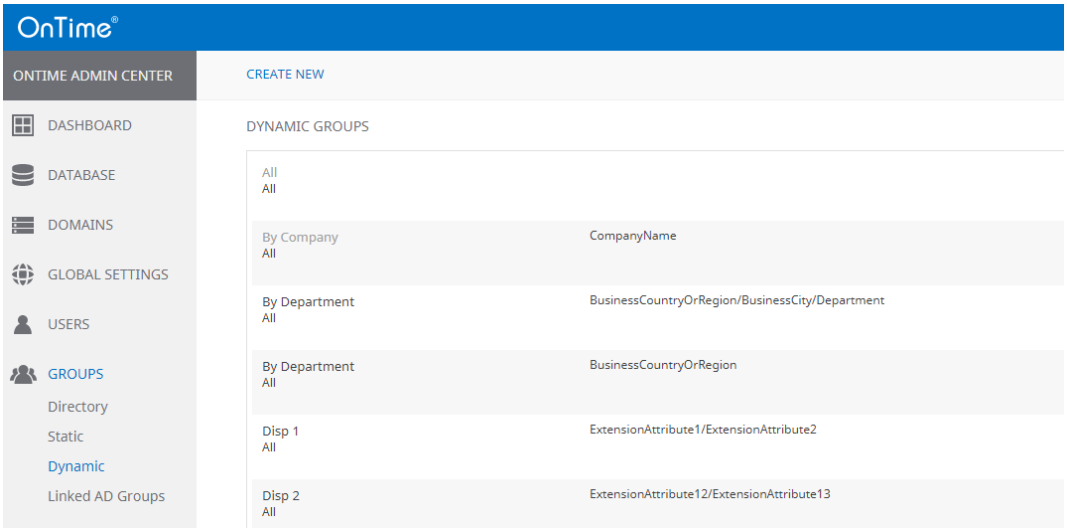
Changes in the static groups must be followed by clicking 'Start' at 'User & Group Sync' in the **Dashboard.**

Dynamic Groups

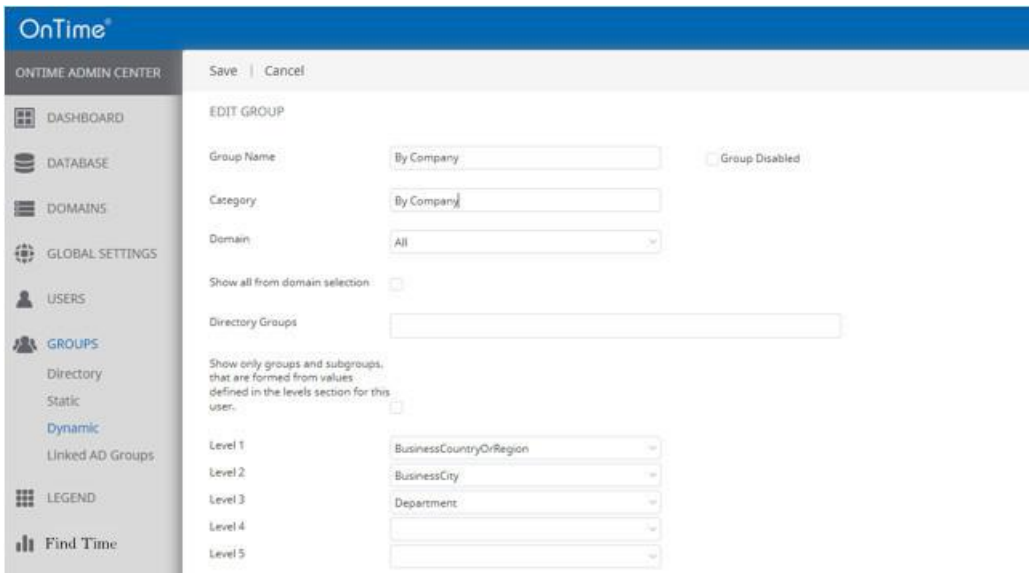
Important Note: Dynamic Distribution Groups from Microsoft 365 are not supported.

Click Groups/Dynamic to configure your dynamic groups. These groups depend on the users' attributes in 'Active Directory/Exchange'.

Click "Create New" to configure a new dynamic group
- or chose an existing entry to edit.



Click 'Create New' or select an existing Dynamic Group.



You may design a tree hierarchy for showing the users filtered by Department, Job Title, and so on.

You can decide if you want the groups created for a single domain or all domains.

Click ‘Save’.

After making changes in the dynamic groups, click ‘Start’ at ‘User & Group Sync’ in the **Dashboard.**

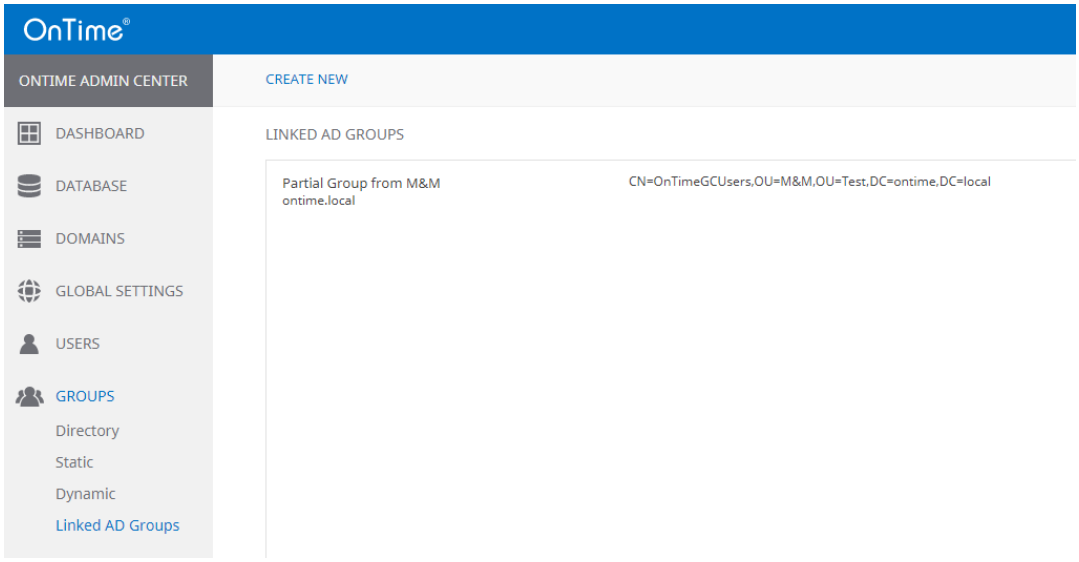
It is possible to add a “Show All” group for the OnTime clients, by adding a group and tick “Show All”. This group will contain all members in OnTime.

Linked AD Groups

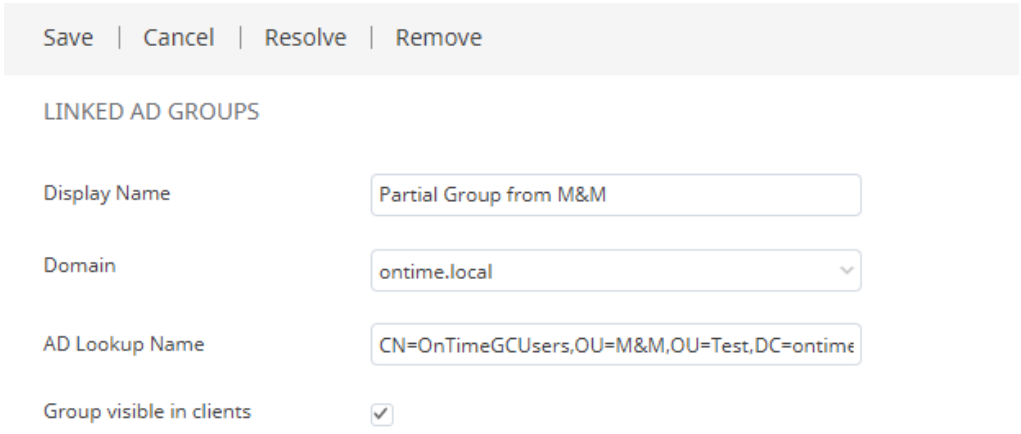
This is only possible if Domain configuration is using LDAP.

The scope of users included in the OnTime calendar is defined in the section ‘Domains/Synchronisation Source’. If you want to relate to groups outside the main scope of users in OnTime, it is possible with a definition of a Linked AD Group.

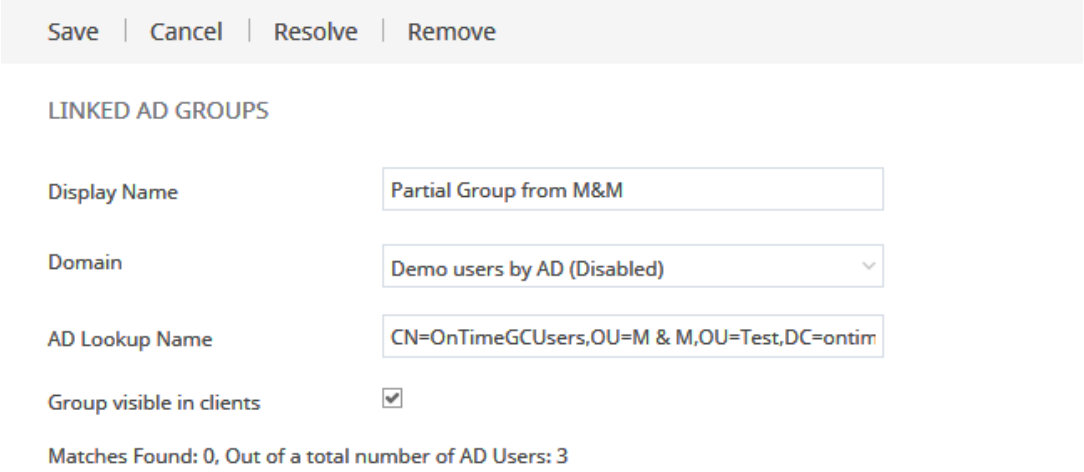
Click Groups/Linked AD Groups to configure your Linked AD Group, click ‘Create New’ or choose a group to edit.



An example:



If you click ‘Resolve’ a result of users belonging to the scope of OnTime users will be shown:

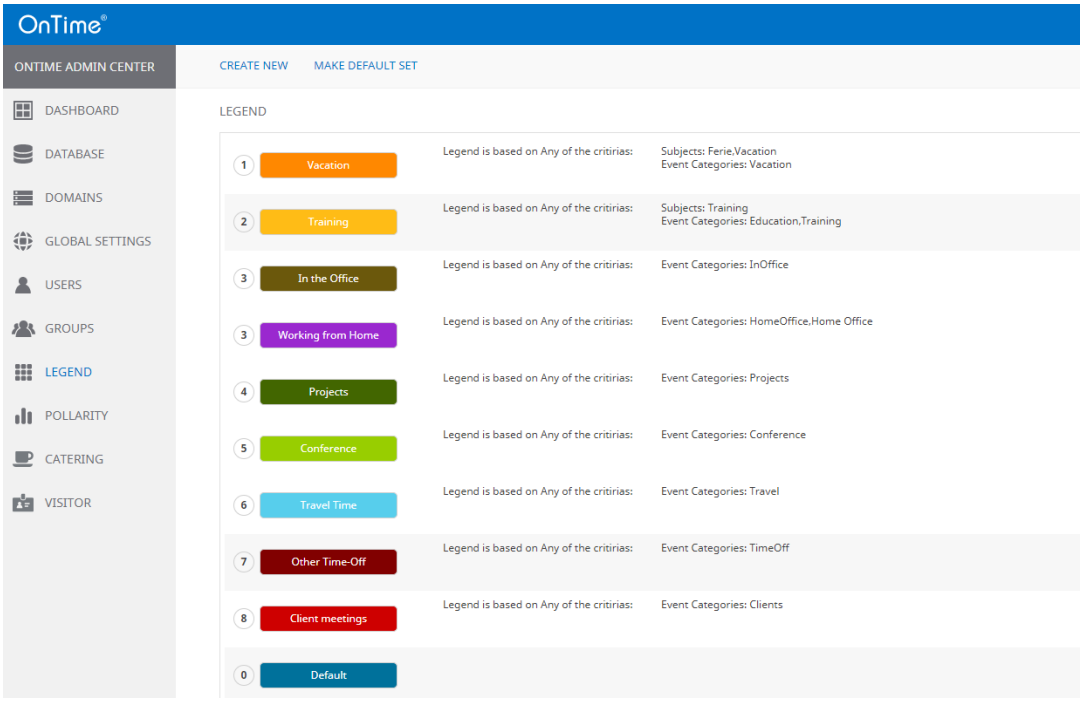


Legend

Click “Legend”.

You may configure OnTime to display different types of calendar entries in different colours, based on a set of criteria. This feature provides the user of the calendar interfaces with a better overview of colleagues’ appointments and an ability to visually filter by type.

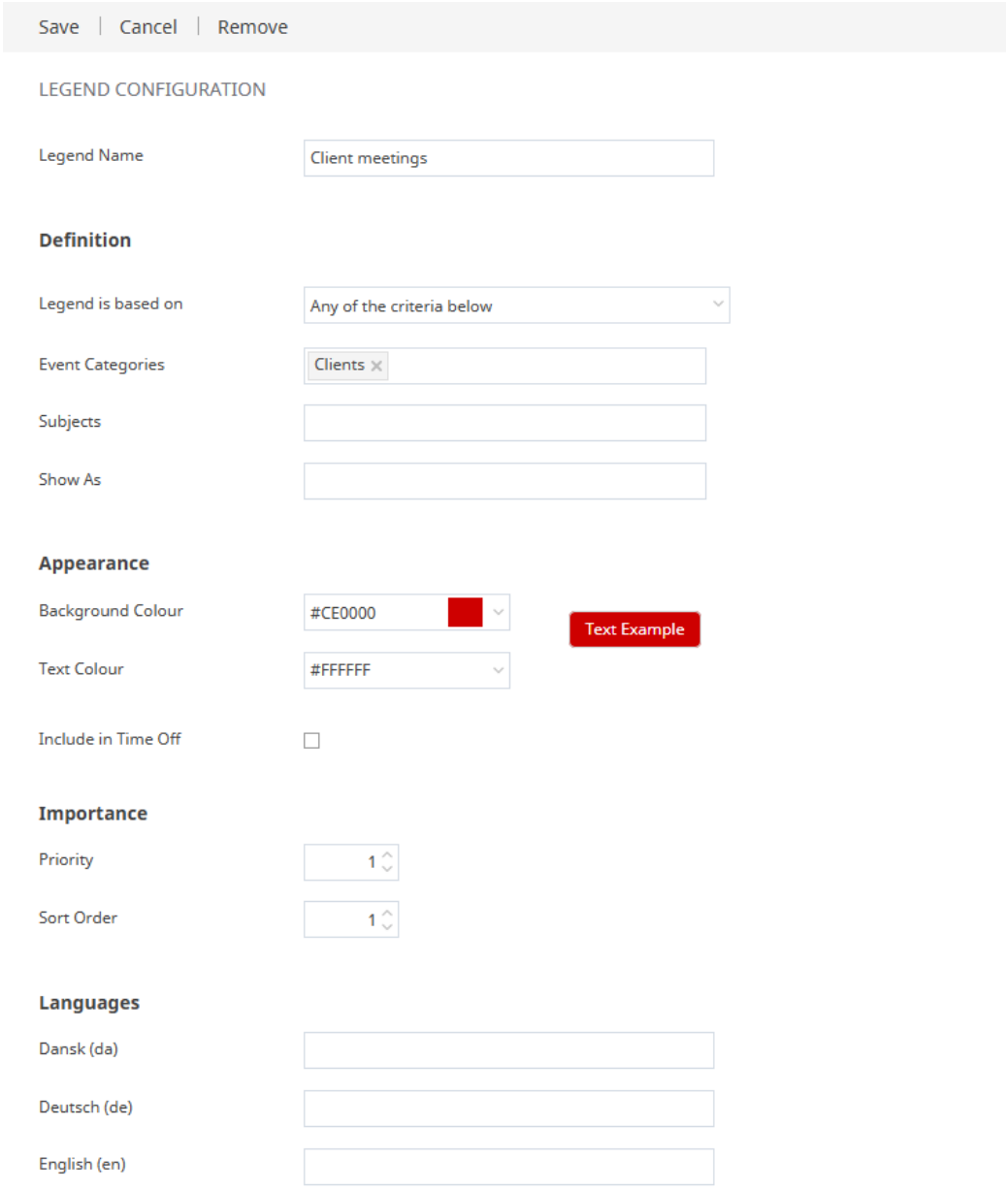
The colour coding of the categories will show in the user’s calendar overview.



The button “Create New” is for adding a new legend to the list of legends.
To remove a legend, click the legend and the button “Remove”.
“Create Default” is utilised if you have removed the default legend and you want it back.

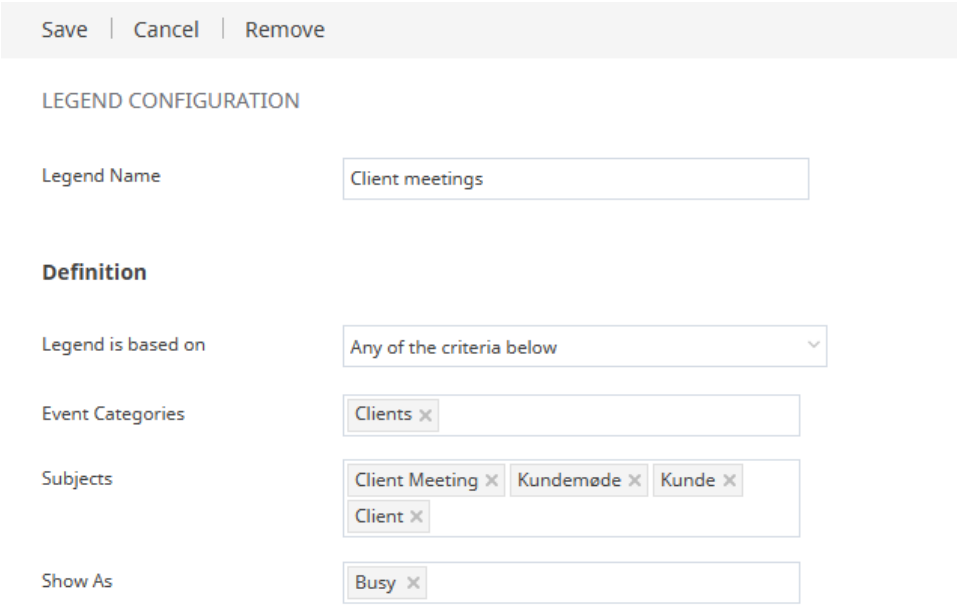
The button “Make Default Set” creates eight standard legends, as shown above.

Click the Legend name to see the details:

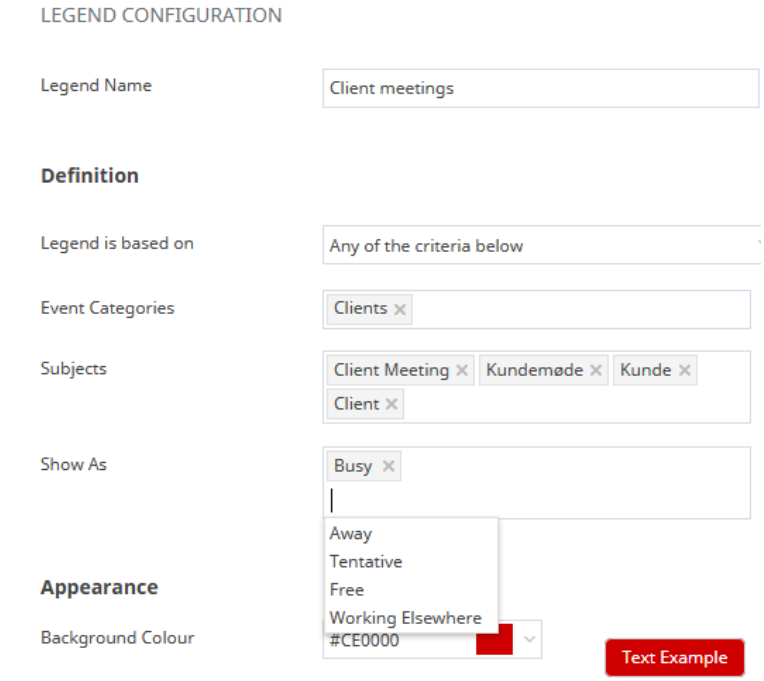


Definition

The **Legend is based on** – **Any of the criteria below**, or **All criteria below**. The criteria are “Event Categories”, “Subjects” (written in one of the ways listed) and a calendar event selection of “Show As”. If **All criteria below** are chosen, all the three criteria have to be fulfilled to fire the chosen background colour. If only one or two criteria are fulfilled the event will be shown with the default colouring.



The subjects mentioned below lets the user write one of the possibilities in the list, in his subject for the meeting.
Show As determines how the appointment is shown in the calendar.



Appearance

Background Colour, Text Colour and the setting of whether to include this legend in the users "**Time Off** view" can be set.

Importance

Priority – determines the winning legend type in case of overlapping definitions – most likely if the **Legend is based on** – **Any of the criteria below.** "1" is the highest priority.

Sort order - determines the occurrence of the different legend types when the user creates a calendar event.

Languages

Translations of the Legend Name can be entered in the different languages supported.

The translations are utilised in the left-hand navigation for the user interface when Legend is chosen.

Changes in the "Legend Configuration" only requires clicking "Save", no further actions in the Dashboard are necessary.

Find Time

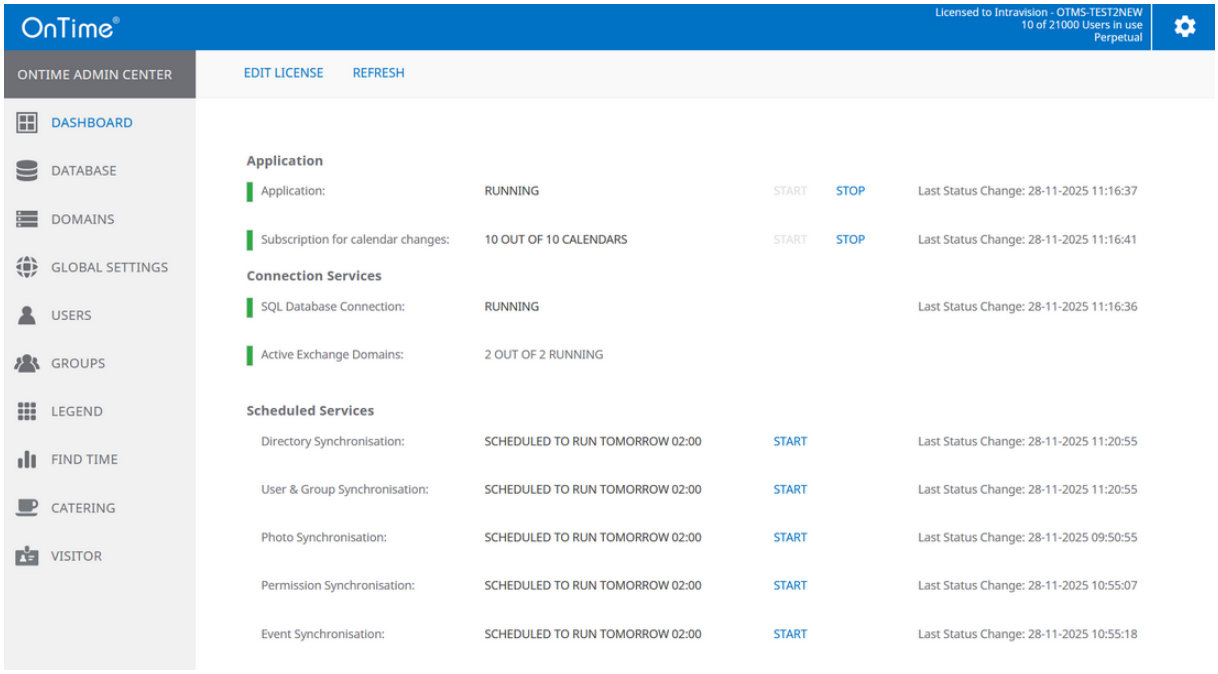
Two options determine the way of finding time for meetings in OnTime

'Pollarity' and 'Share my Time'.

The OnTime licensed option, Pollarity means that voting for meeting times is possible.

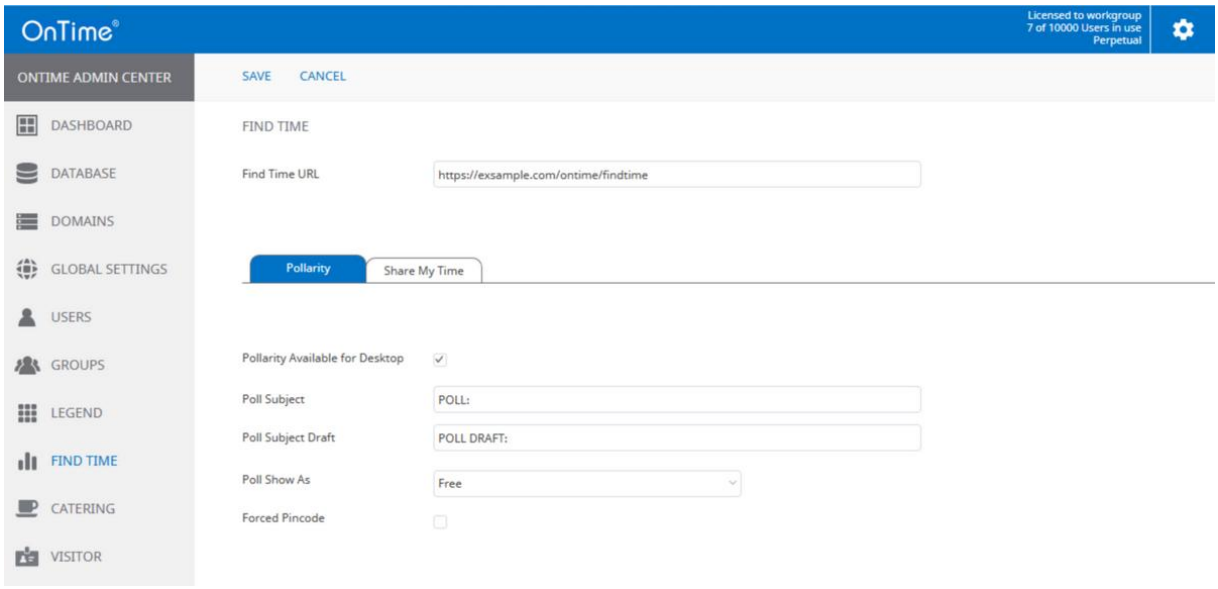
If Pollarity is used in OnTime with users external to the environment, a reverse proxy solution in the DMZ is required.
Ref. to Reverse Proxy.

When licensed for Pollarity, the admin dashboard shows Pollarity for configuration and status.



Configuration of Pollarity

In the ‘OnTime Admin Centre’ click ‘Pollarity’.



Pollarity Available for Desktop: tick, to choose availability to the users.

Find Time URL: This is the link sent to invitees for voting in Pollarity.

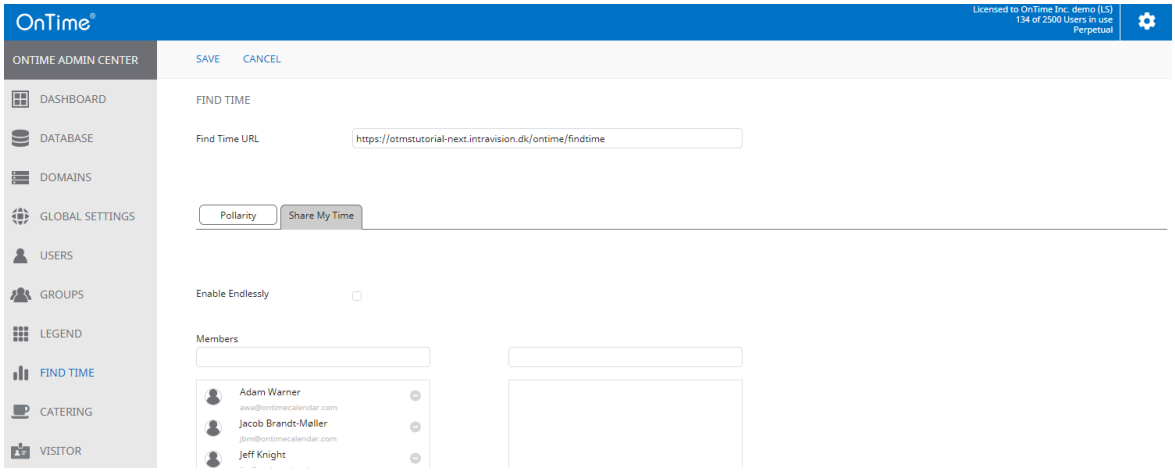
Poll Subject: This text is automatically inserted in the mail message subject field

Poll Subject Draft: In case a ‘poll owner’ saves a draft instead of sending the mail this text will be inserted in the subject of the placeholder document

Poll Show As: Determines if placeholder documents will be shown as ‘Busy’, ‘Tentative’ or ‘Free’.

Configuration of 'Share my Time'

In the ‘OnTime Admin Center’ click 'Find Time' and then ‘Share my Time’.



Find Time URL: This is the link sent to invitees in Share My Time.

Enable Endlessly – if enabled, links to 'share my time' will be reusable.

At the bottom of the page include (or exclude) groups or persons as Members of 'Share My time'.

Catering

The OnTime licensed option, Catering means that ordering of for example food and beverages for meetings can be arranged. Three roles for OnTime Catering are described in the following table:

	System Admin	Canteen Manager	Canteen Staff
Create Canteen	Yes	No	No
Edit Canteen	Yes	Yes	No
Remove Canteen	Yes	No	No
Maintain Menu item	No	Yes	No
Create Orders	No	Yes	Yes
Edit Order	No	Yes	Yes
Remove Order	No	Yes	No

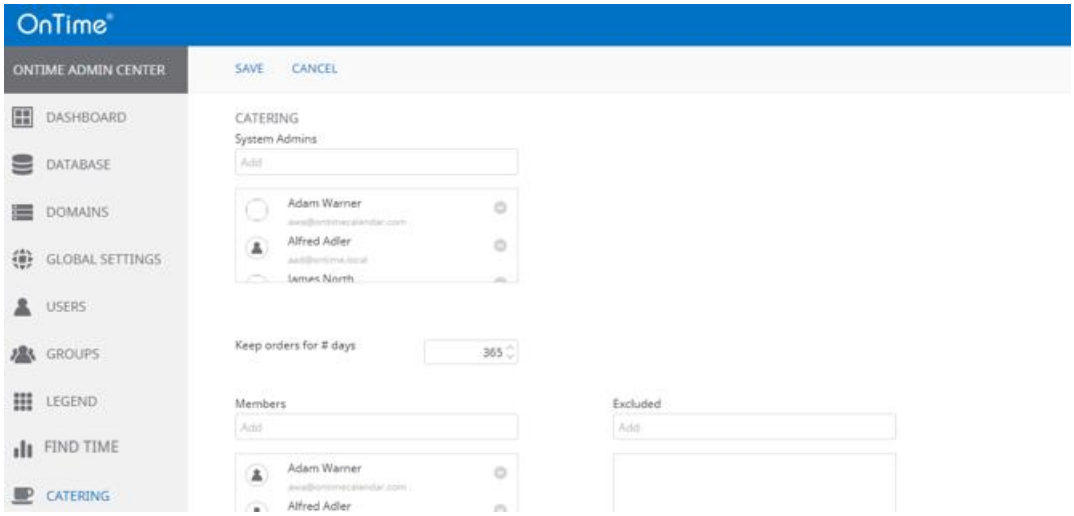
The role **'System Admin'** is to create/remove/edit canteens in the 'Catering Manager'.

The role **'Canteen Manager'** is to administer orders, add items for consumption and edit info about an existing canteen.

The role **'Canteen' Staff'** is to administer orders.

Administering Catering

Click ‘Catering’ in the ‘OnTime Admin Centre’ to administer the persons involved in Catering.



Catering ‘System Admins’
Add Catering ‘System Admins’ by entering characters and selecting persons or OnTime ‘Directory Groups’ in the ‘Add’ box.

Keep orders for # days
Enter number of days that canteen orders are kept in the system after being served. Default value is 365.

Catering ‘Members’
Add Catering ‘Members’ by entering characters and selecting persons or OnTime ‘Directory Groups’ in the ‘Add’ box.
The members in the list are dedicated to the two roles ‘Canteen Managers’ and ‘Canteen Staff’ in the ‘Catering Manager’

Catering ‘Excluded’
Person or directory groups that are excluded from a group in the Members list

Catering ‘Members’ have a button for ‘Catering Order’ when creating a meeting in Ontime.
Members have an overview with ‘My Orders’ in the lefthand navigation of the desktop client

URLs for ‘Catering Manager’

The ‘Catering Manager’ is accessed by the URLs:
https://ontime.example.com/cateringdesktop
or
https://ontime.example.com/cateringmobile
- for the touchscreen client

Note: Please insert your relevant URL instead of ‘ontime.example.com’.
- and it is further described in a tutorial video at www.ontimesuite.com

Visitor

The OnTime licensed option, Visitor, enables registering and managing visitors within the organisation.

Three roles for OnTime Visitor are described in the following table:

	System Admin	Visitor Manager	Visitor Staff
Create Location	Yes	No	No
Edit Location	Yes	Yes	No
Remove Location	Yes	No	No
Maintain Locations	No	Yes	No
Check in Visitor	No	Yes	Yes
Edit Visitor	No	Yes	Yes
Check out Visitor	No	Yes	Yes

The role **'System Admin'** is to create/edit/remove locations in the 'Visitor Manager'.

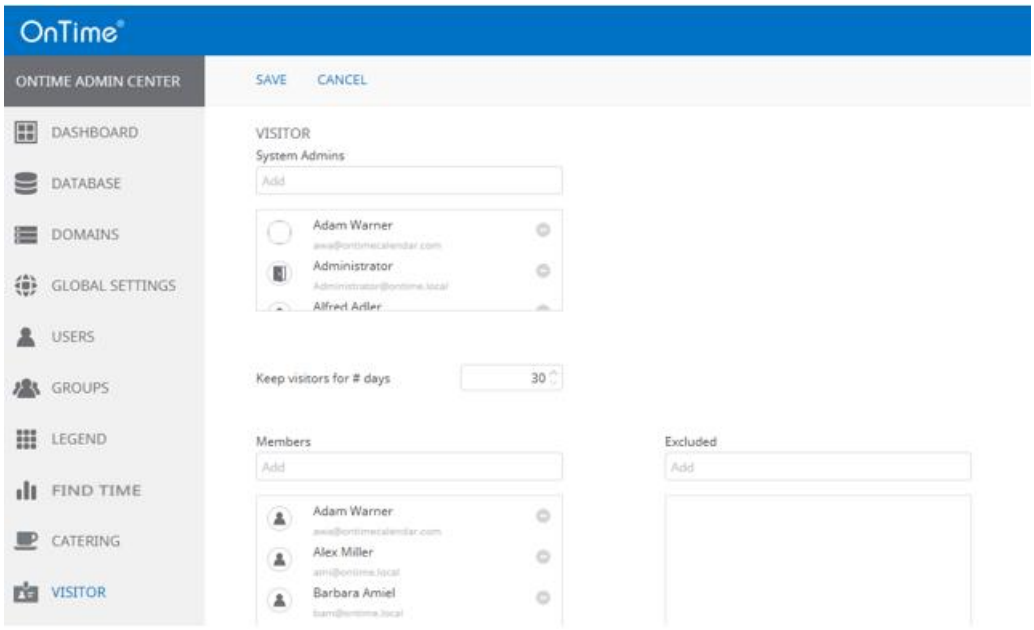
The role **'Visitor Manager'** is to edit locations - and administer visitors.

The role **'Visitor' Staff'** is to administer visitors.

The 'Visitor Manager' is accessed by the URL:
https://ontime.example.com/ontimegcms/visitormanager
Note: Please insert your relevant URL instead of 'ontime.example.com'.

- and it is further described in a tutorial video at www.ontimesuite.com

Click ‘Visitor’ in the ‘OnTime Admin Centre’ to administer the people involved in the Visitor module.



Visitor ‘System Admins’
Add Visitor ‘System Admins’ by entering characters and selecting persons or OnTime ‘Directory Groups’ in the ‘Add’ box.

Keep visitors for # days
Enter number of days that the visitors are kept in the system after the visit.
Default value is 365.

Visitor ‘Members’
Add Visitor ‘Members’ by entering characters and selecting persons or OnTime ‘Directory Groups’ in the ‘Add’ box.
The members in the list are dedicated to the two roles ‘Visitor Managers’ and ‘Visitor Staff’ in the ‘Visitor Manager’:
https://ontime.example.com/ontimegcms/visitormanager
Note: Please insert your relevant URL instead of ‘ontime.example.com’.

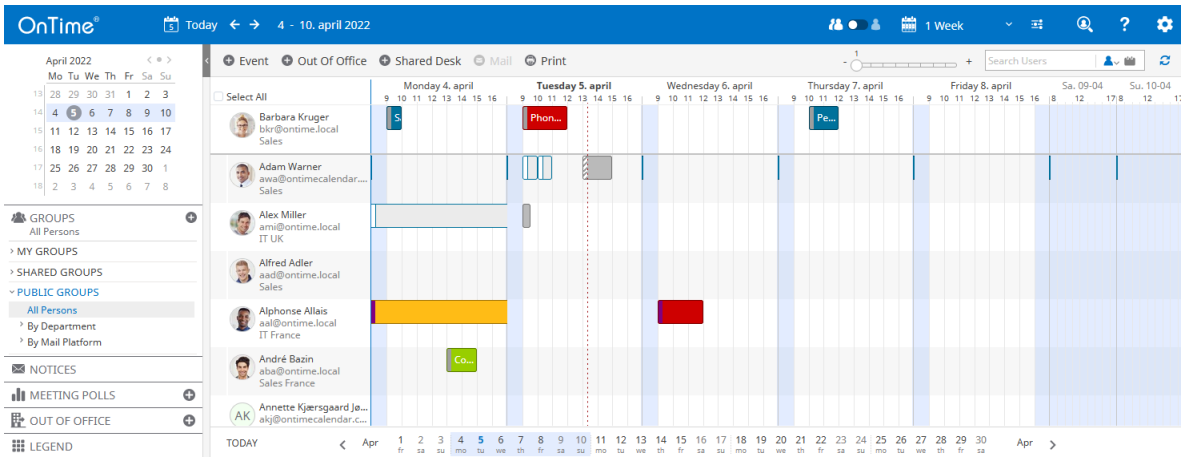
Visitor ‘Excluded’
Person or directory groups that are excluded from a group in the Members list
Visitor members have access to the ‘Visitor Registration’ button when creating a meeting in Ontime.

Note: Concerning membership - if a secretary is editing an event for a manager, the secretary also needs to be added as a member in the visitor section in the Admin UI.

OnTime User – Calendar

OnTime client Web Desktop

From a browser - Open the user URL -
https://ontime.example.com/ontimegcms/desktop
Note: Please insert your relevant URL instead of 'ontime.example.com'.

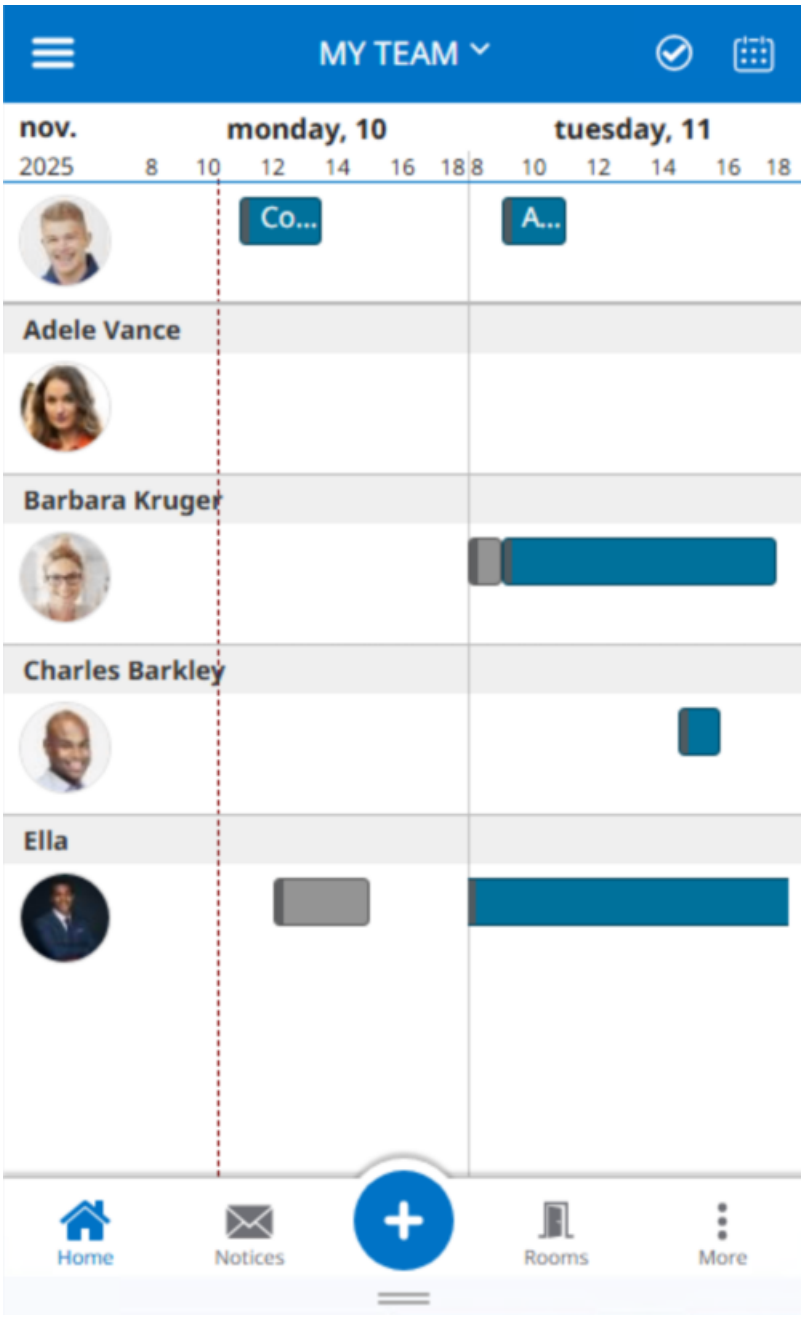


OnTime client Web Mobile

From a browser - Open the user URL –

https://ontime.example.com/ontimegcms/mobile
Note: Please insert your relevant URL instead of ‘ontime.example.com’.

Note: The ‘OnTime Mobile Client’ requires a separate license.



Add-ins for OnTime

You have the option to include the OnTime calendar inside Microsoft Teams and Microsoft Outlook.

Now while using Teams integration you will have the possibility to create Online Meetings based on Teams meeting provider.

If you are using multiple domains, you need to register an OnTime application for each of the domains you want to use in Microsoft Teams or create online meetings by users from the domain. If you have users from the same Microsoft domain in different OnTime domains, you can use the same credentials for different domains.

Note: Microsoft Teams, and Microsoft Outlook require a secure connection, only https is allowed, and the OnTime server must be configured with a certificate from a publicly trusted certification authority.
The users must authenticate to the OnTime server using https.

Note:
Registering of OnTime in Microsoft 365 is described in the section Upload of add-ins for OnTime

Add-in for OnTime New Microsoft Outlook and in Microsoft Teams Navigation Panel

Note: Microsoft Teams requires a secure connection, only https is allowed, and the OnTime server must be configured with a certificate from a publicly trusted certification authority.
The users must authenticate to the OnTime server using https.

To create the application that can be used in Microsoft Teams, a .json file needs to be edited and zipped together with some images.
In the install package a 'manifest.json' file can be found in the folder:
'C:\Program Files\IntraVision\OnTimeMS-x.x\addin-new-outlook-teams-rail'

1. Run the cmdlet build_manifest.cmd as Administrator.

2. You will be asked to enter the name (DNS name - with https!) of your OnTime

server e.g. https://ontime.example.com. A manifest.json file will be created. Refresh

the folder if you do not see it.

3. Zip the three files: color.png, outline.png, and manifest.json into a file

'teams_outlook_ navigation_panel.zip'

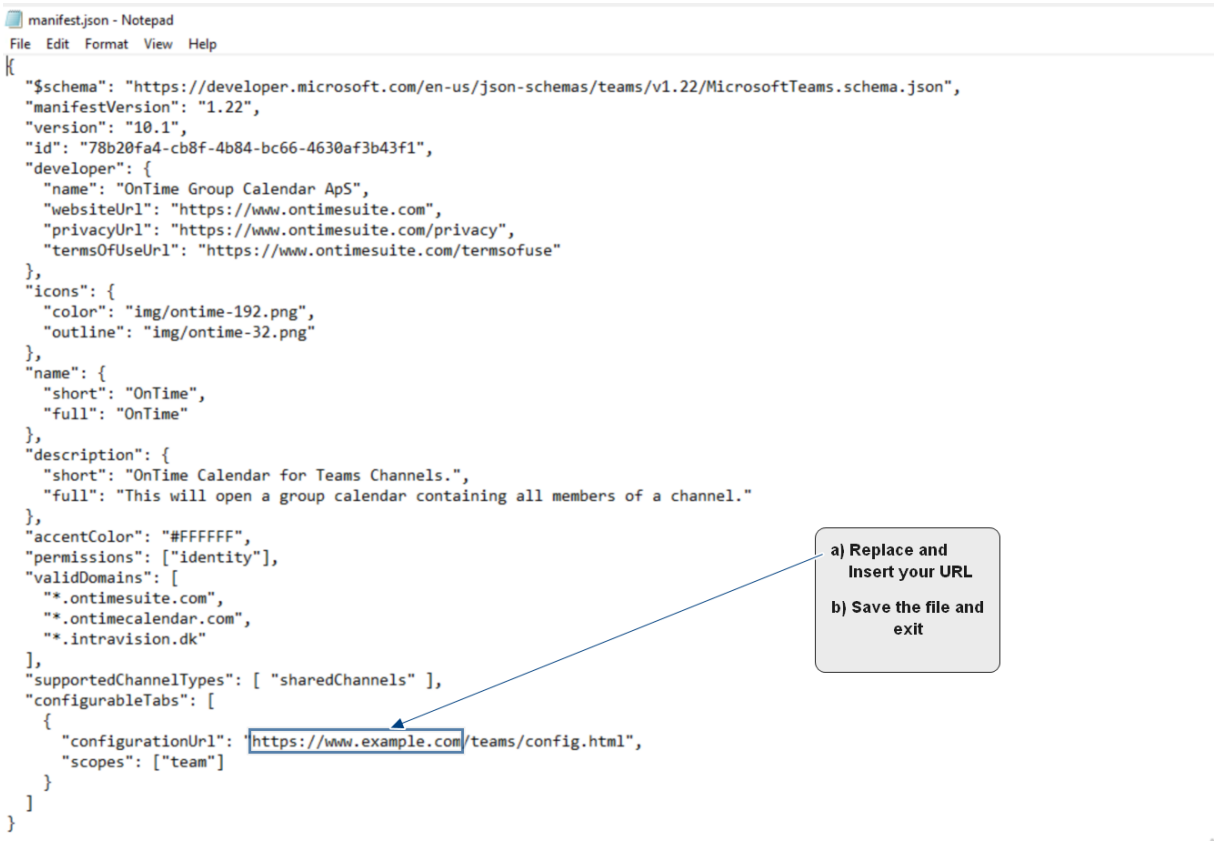
Note:
Upload of the zip-file is described in the section Upload of add-ins for OnTime

User setup for Teams Channels

Note: The following guidelines apply only to version 6.3.3 and later.

In your OnTime installation files you will find the command file ‘add-url-config.cmd’ in the folder ‘C:\Program Files\IntraVision\OnTimeMS-x.x\addin-teams-channel’

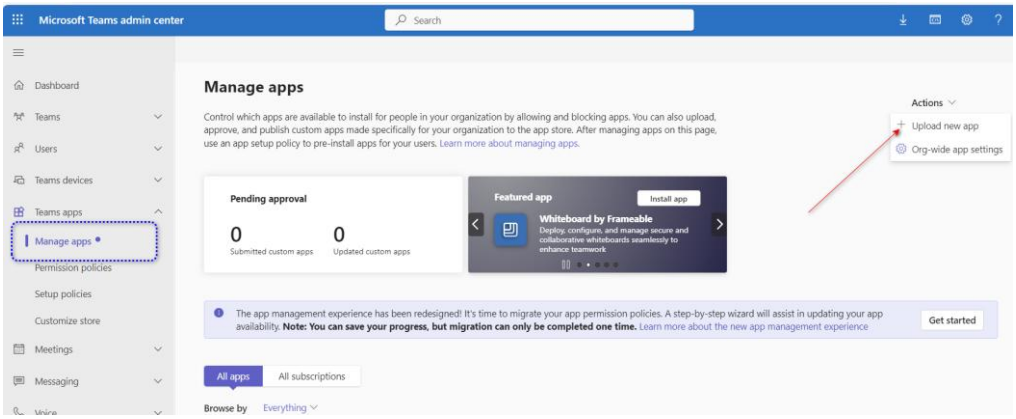
a. Run cmd file ‘add-url-config.cmd’ as Administrator
b. You will be asked to enter the name (URL) of your OnTime server
c. From the current location, edit the file named manifest.json and update it with your OnTime server DNS name, including https, as shown below:



d. From the current location, select the ‘img’ folder and the ‘manifest.json’ file, then compress them into a ZIP file. Copy the zipped file and transfer it to a location where you have access to your Microsoft Online Admin Portal.

- Go to your Company Microsoft Online Admin URL:

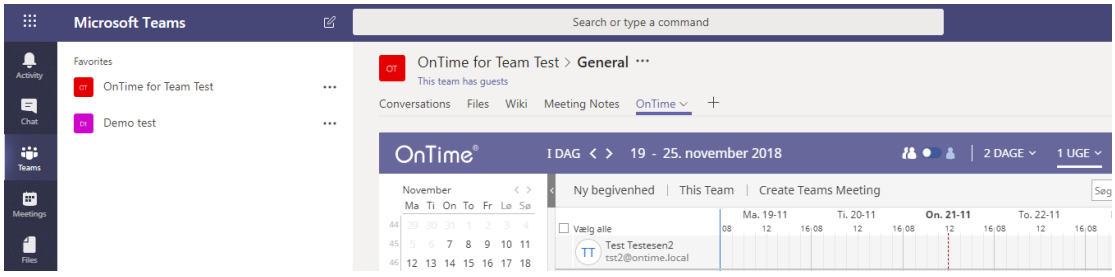
  https://admin.teams.microsoft.com/dashboard



- And upload the zipped file you created earlier
- And wait while to deployed.
- Now start your Teams App and Click on Teams and + as shown in below figure:

  When you are signed into Teams at https://teams.microsoft.com, you may click the '+' sign in one of the Teams menus.
  Click at the 'OnTime Calendar for Teams Shared Channel'.
  Click 'Use these settings' and 'Save'.

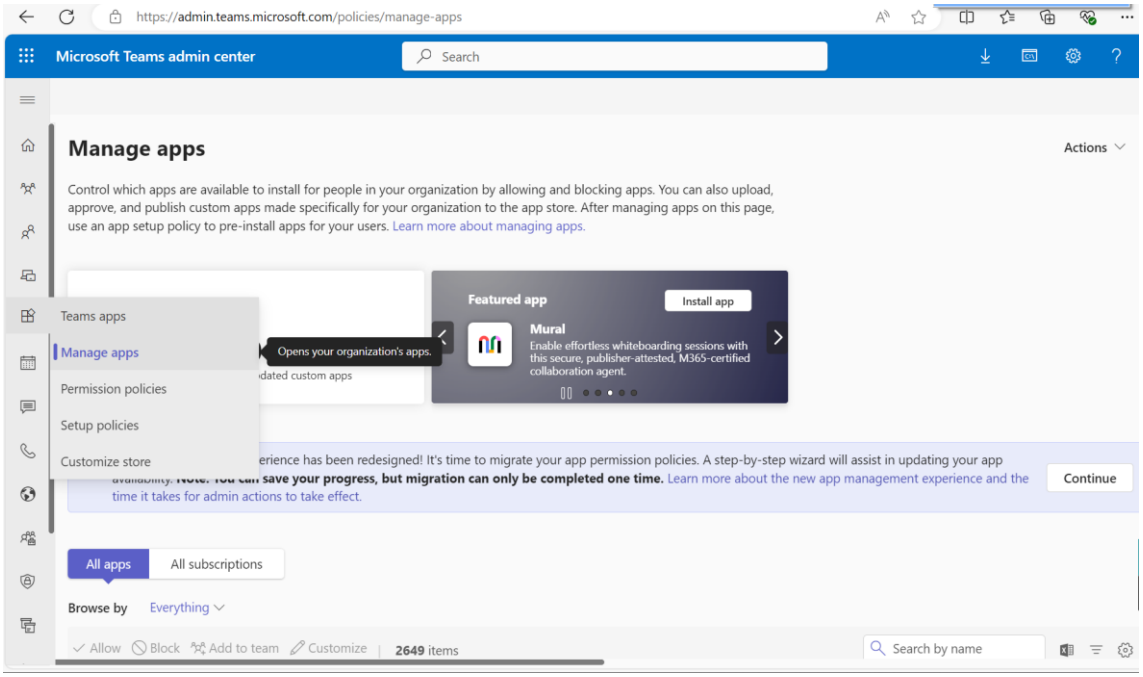
Click 'OnTime' in the Teams menu to see the OnTime calendar for your team.



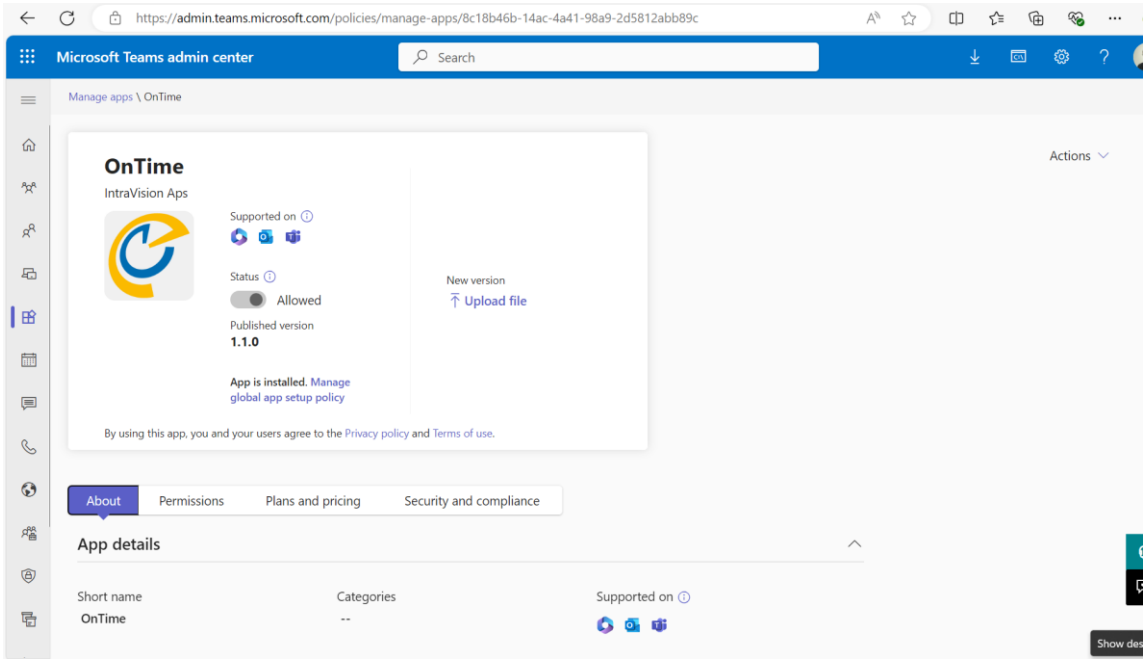
Upload of add-ins for OnTime first time

To add the OnTime add-in into the new Microsoft Outlook and Microsoft Teams Navigation Panel, login as 'Teams Admin' into https://admin.teams.microsoft.com

In the 'Microsoft Teams Admin Center' choose 'Teams apps/Manage apps' in the lefthand navigation:



At the top right corner Click 'Actions' and click 'Upload new app' Select the zip file you made.



To allow or designate users to the OnTime application, a Teams Admin has to setup ‘Permission policies’ and ‘Setup policies’ for the OnTime application.
In the section ‘Permission policies’ you designate the users for the application.
In the section ‘Setup policies’ you configure the position of OnTime in the ‘Rail’ – the lefthand navigation in Teams.

For help regarding details of managing Teams, please refer to:
https://learn.microsoft.com/en-us/microsoftteams/teams-overview

For uninstalling existing OnTime Add-ins

Go to Microsoft Teams Admin Center, https://admin.teams.microsoft.com/dashboard

In the Microsoft Teams Admin Center, navigate to **Teams apps > Manage apps** in the left-hand menu. Locate the desired add-in, select it, and then click **Delete** under the **Actions** menu in the top-right corner.

Upload of add-ins for OnTime, Upgrade

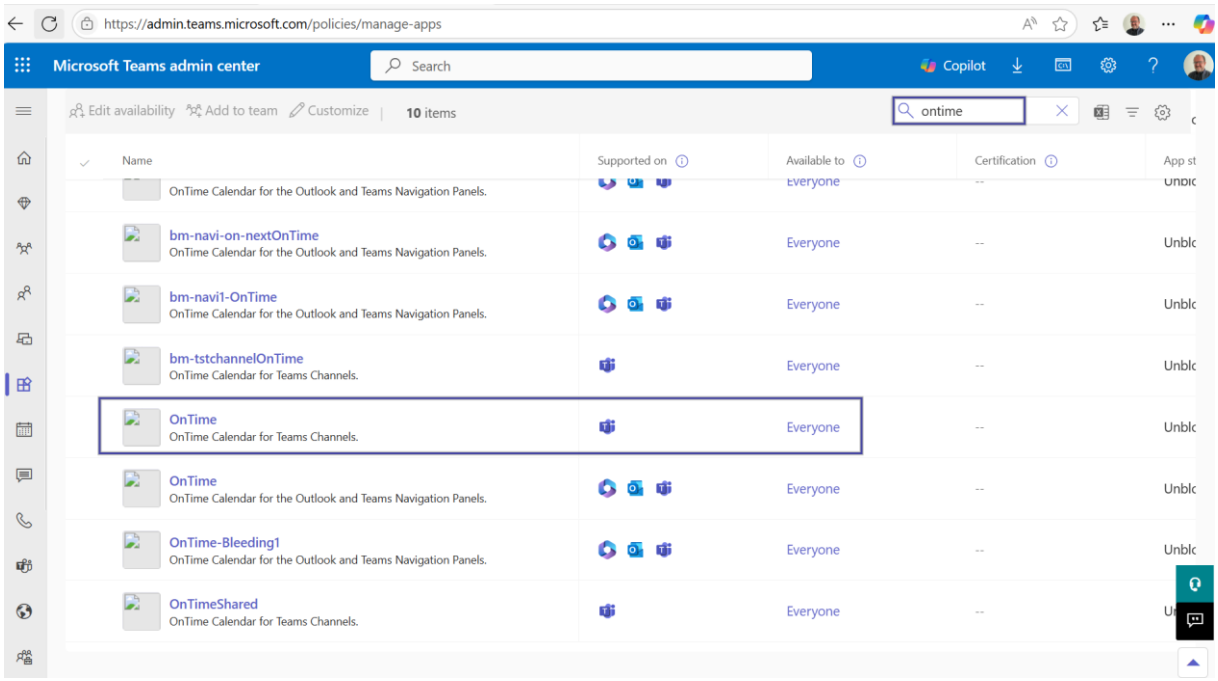
Upgrading the OnTime Add-in for Microsoft Outlook and Microsoft Teams

1. Log in as a **Teams Admin** at https://admin.teams.microsoft.com.

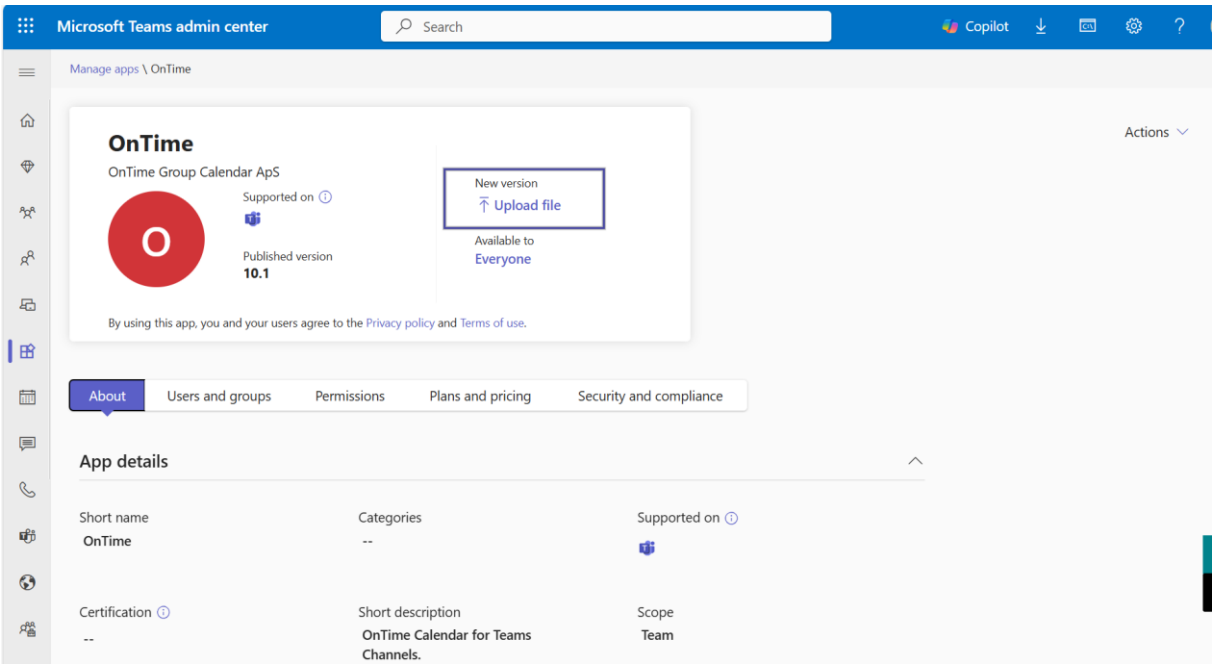
2. In the **Microsoft Teams Admin Center**, go to **Teams apps > Manage apps** in the left-hand navigation panel.

3. In the search field, type **OnTime**.

4. From the list of results, locate the **OnTime add-ins** that require an upgrade, as shown below.



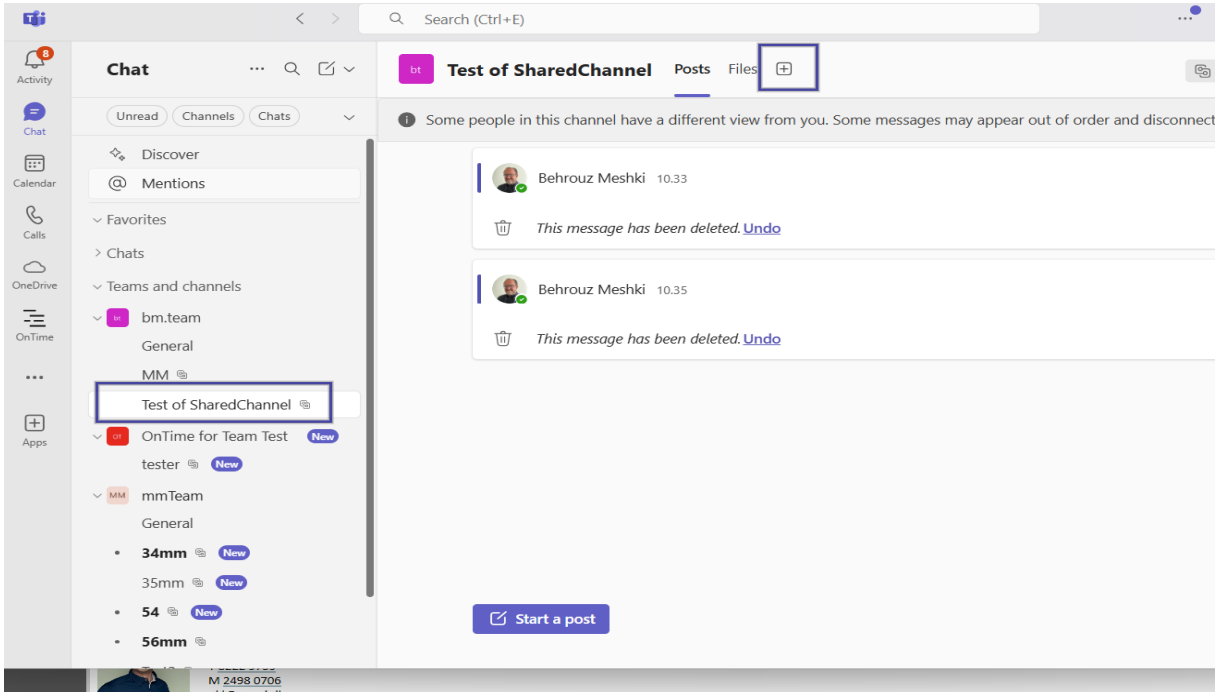
Select the add-in you want to replace, then upload the new version of the manifest file you created, as shown below.



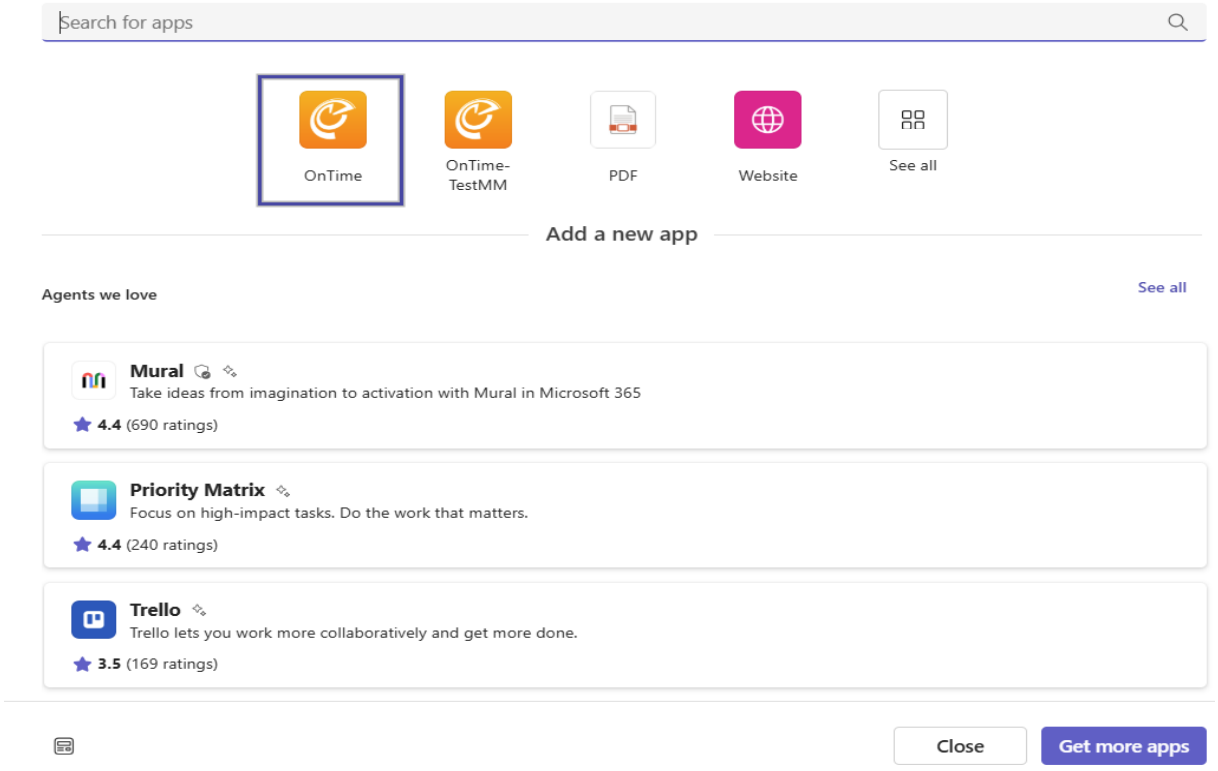
How to add OnTime to a Teams Shared Channel:

Note: This feature is currently unavailable in current OnTime version.

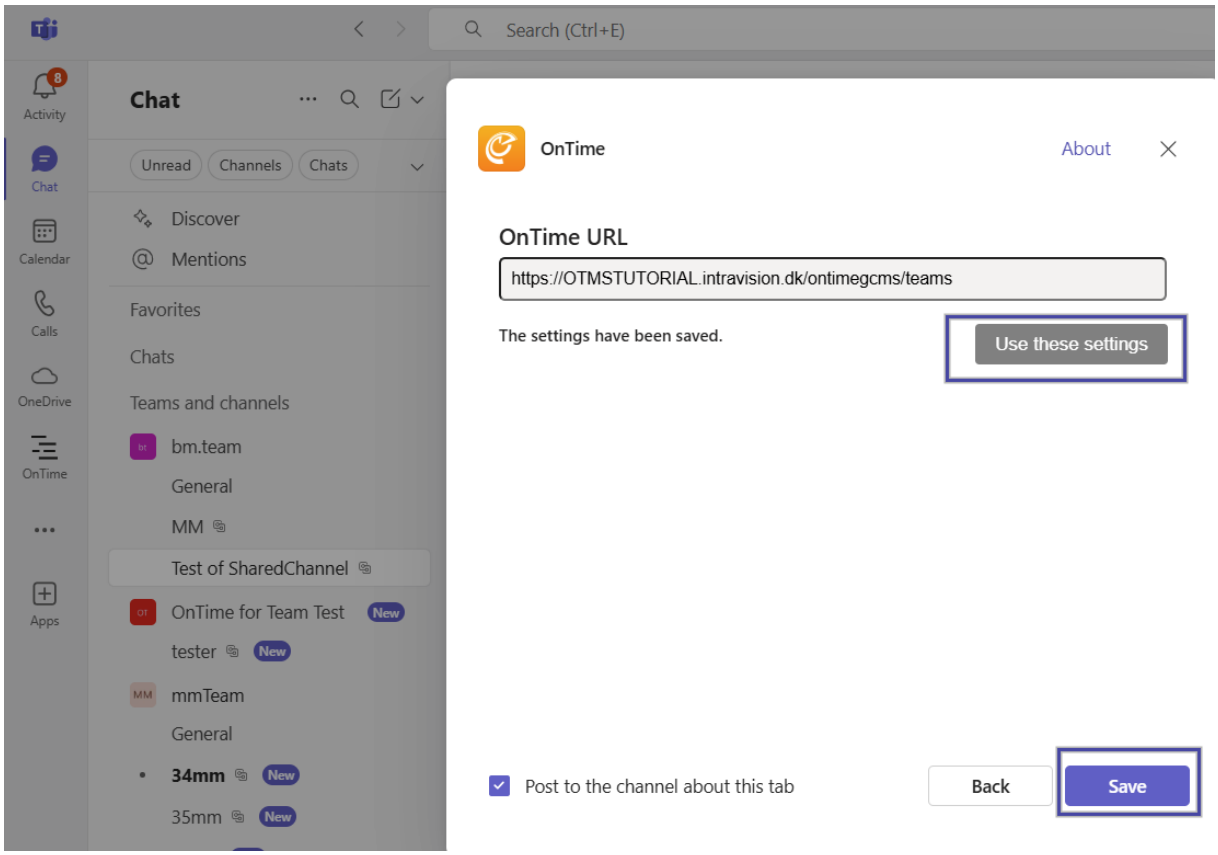
Open the Teams app or Teams web, create a Shared Channel, invite members, and then click the '+' (Add a tab) icon.



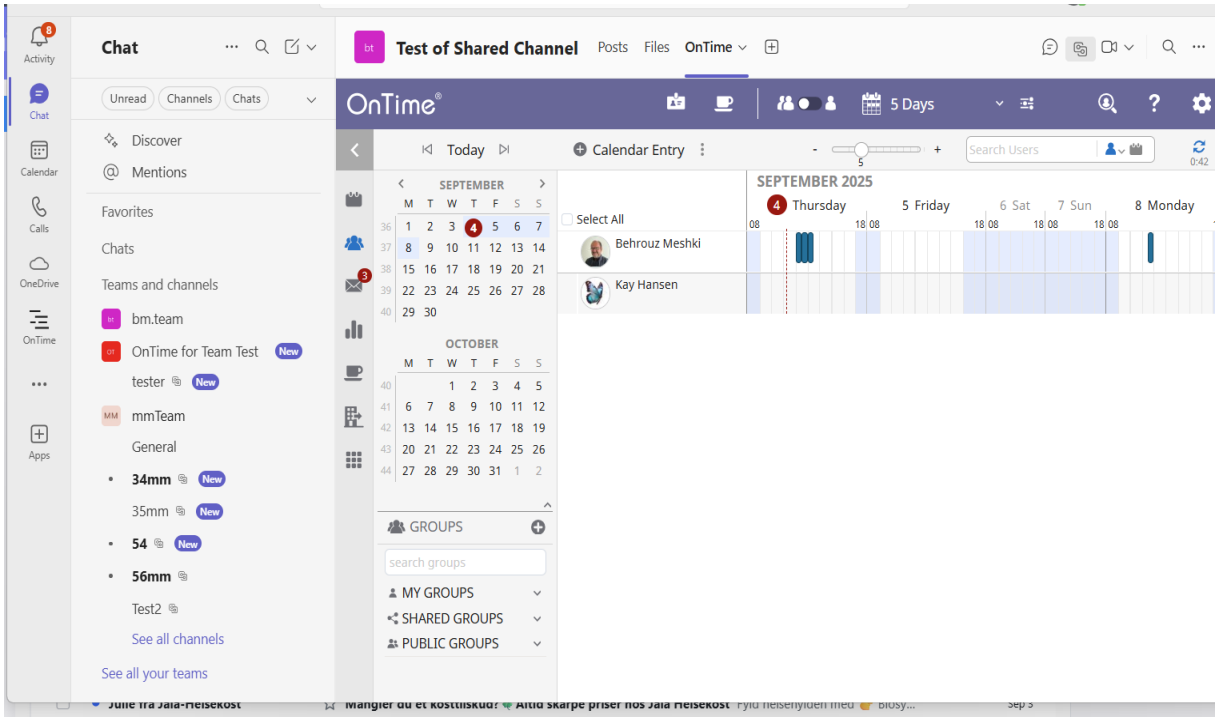
From the list, select 'OnTime' as shown below



Accept the URL link, then click ‘Use these settings’ followed by ‘Save



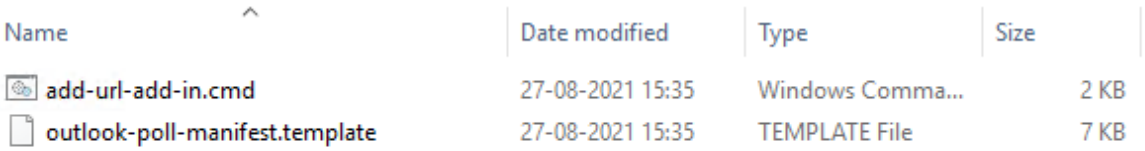
Finally, ‘OnTime’ will be added to your Shared Channel.



OnTime Pollarity - add-in in Microsoft Outlook

Installation

To get the add-in to work, you need to create a manifest file. You can do this from the 'C:\Program Files\IntraVision\OnTimeMS-x.x\addin-classic-outlook-poll' folder.



Right-click the 'add-url-add-in.cmd' file and choose 'Run as administrator' to start up the process.

Enter your OnTime server name (DNS name with https), and the manifest file will be created.

The generated file 'ontime-outlook-poll-manifest.xml' lets you deploy on the admin Microsoft 365 account. Remember to choose "add from file" in the selection, when adding.

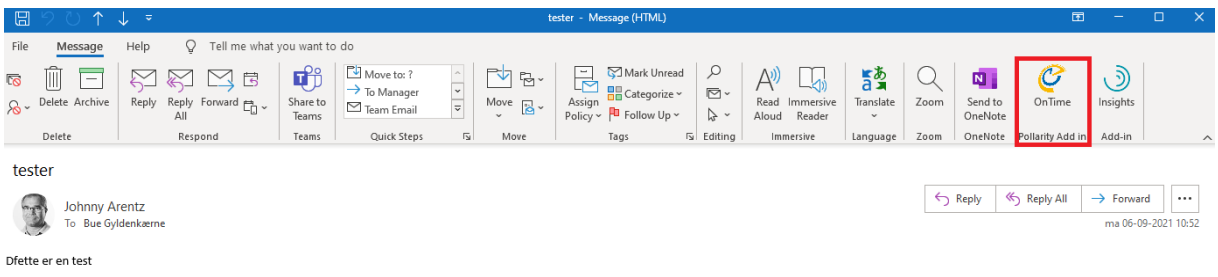
Note:
Upload of the zip-file is described in the section Upload of add-ins for OnTime

For more information:

https://support.office.com/en-us/article/Manage-deployment-of-Office-365-add-ins-in-the-Office-365-admin-center-737e8c86-be63-44d7-bf02-492fa7cd9c3f

Your Microsoft Outlook, with OnTime Poll-add-in

- visible when you open an incoming mail



OnTime Catering add-in Microsoft Outlook

In your OnTime installation files you will find a .cmd file ‘add-url-add-in.cmd’ in the folder \outlook-catering-add-in
- Run it as Administrator
- you will be asked to enter the name (URL) of your OnTime server

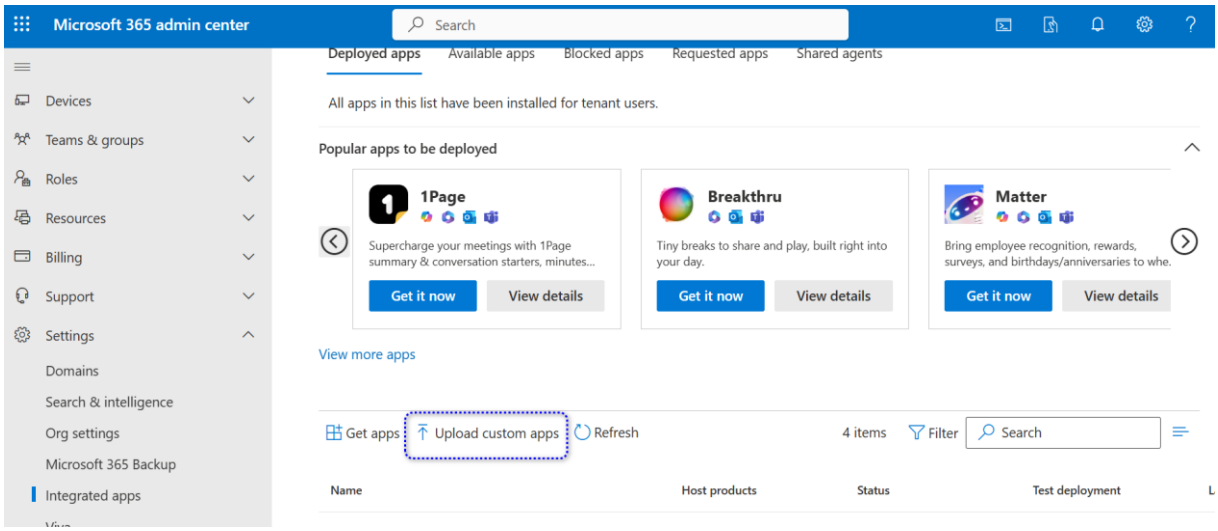
Example: https://ontime.example.com

The manifest file ‘outlook-catering-manifest.xml’ has been created in the ‘\outlook-catering-add-in’ folder. Copy the file to a temporary folder on your PC where you have access to the ‘Microsoft 365 Admin Centre’.

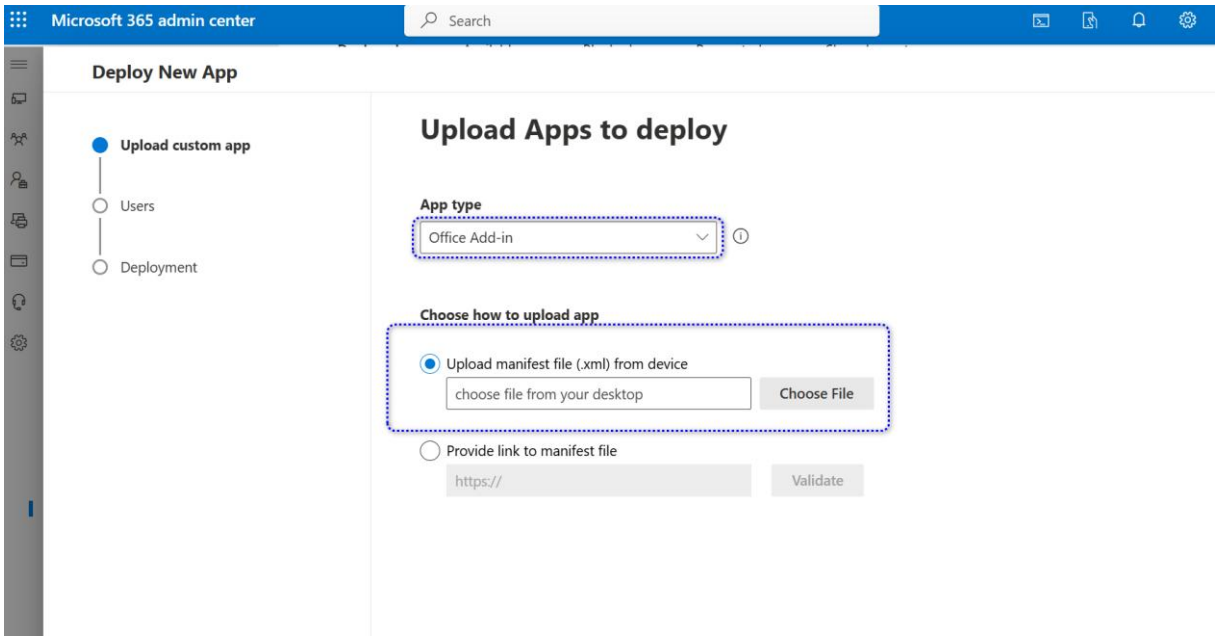
For deploying catering-add-in from Microsoft 365 admin centre choose below link:

Integrated Apps - Microsoft 365 Admin Centre

In the **Microsoft 365 Admin Center**, go to **Settings** and select **Integrated Apps**. From there, choose **Upload Custom Apps**.



And choose File ‘outlook-catering-manifest.xml’ and upload it ‘App type’ as ‘office add-in’ from below:



After the ‘outlook-catering-manifest.xml’ file has been deployed, and depending on Microsoft’s update cycle, you can launch the Microsoft Outlook client and search for the ‘OnTime Catering’ add-in.

From the left-hand navigation panel in Microsoft Outlook, select **"Add Apps"**.
In the search field, type **"OnTime Catering"**.

When it appears in the list of available apps, click **"Add"** to install the “**OnTime Catering**” add-in.

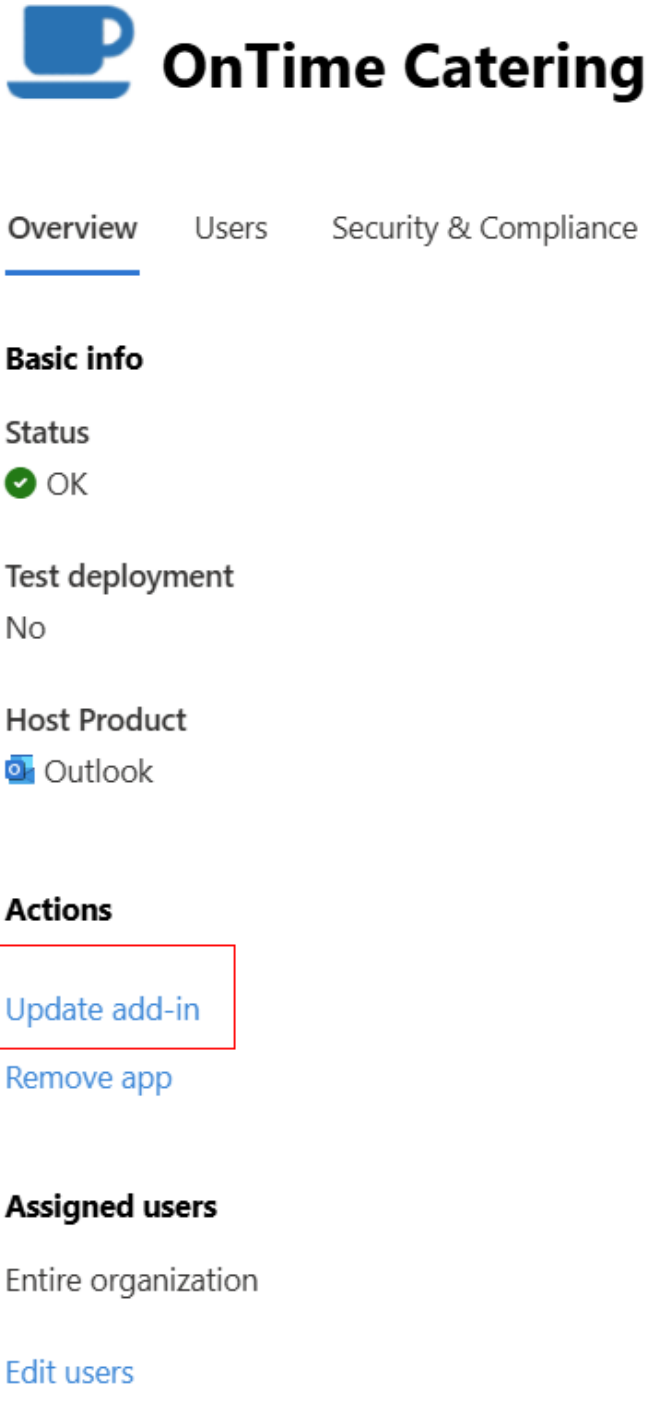
Update the custom app/Update ‘outlook-catering-manifest.xml’

In your OnTime installation files you will find a .cmd file ‘add-url-add-in.cmd’
in the folder \outlook-catering-add-in
- Run it as Administrator
- you will be asked to enter the name (URL) of your OnTime server

The manifest file **‘outlook-catering-manifest.xml’** has been created in the **‘\outlook-catering-add-in’** folder. Copy this file to a temporary folder on your device.

Go to Integrated Apps - Microsoft 365 Admin Centre

Find the **“OnTime Catering”** app under **“Integrated apps”** and click on it



Choose 'Update add-in' and update the **'outlook-catering-manifest.xml'** file by browsing to the file on your local device, then upload it to replace the existing file.

Logfiles

OnTime, Pollarity Catering, Visitor Logs:

C:\Program Files\IntraVision\OnTimeMS-x.x\tomcat\logs
- in the \logs directory the newest log file from the OnTime application:
  ontimegcms.log
- in the \tomcat\logs directory look for **'pollarity.log', 'catering.log', 'visitor.log'.**
- in the\logs\dev directory you will find logfiles for Support from IntraVision

There are many other log files in the `tomcat\logs` folder. Some of them are Tomcat generated.

`commons-daemon`, `ontimetomcat-stderr` and `ontimetomcat-stdout` are the log files generated by the Tomcat Service. Because Tomcat runs as a service, there is no open output console, and the `ontimetomcat-stderr and ontimetomcat-stdout` are the files, which capture the console output and they may contain interesting information, especially the `ontimetomcat-stderr`, which captures errors. The `commons-daemon` is the logger especially for Tomcat Service and does not contain anything interesting for us.

The following log files are provided by Tomcat by default:

`catalina` - Tomcat output, similar to `ontimetomcat-stderr` and `ontimetomcat-stdout`

`Localhost` - Usually of no interest, only when something is really wrong this file may help. ServletAppender logs go here.

`localhost_access_log` - All requests to the server are logged here

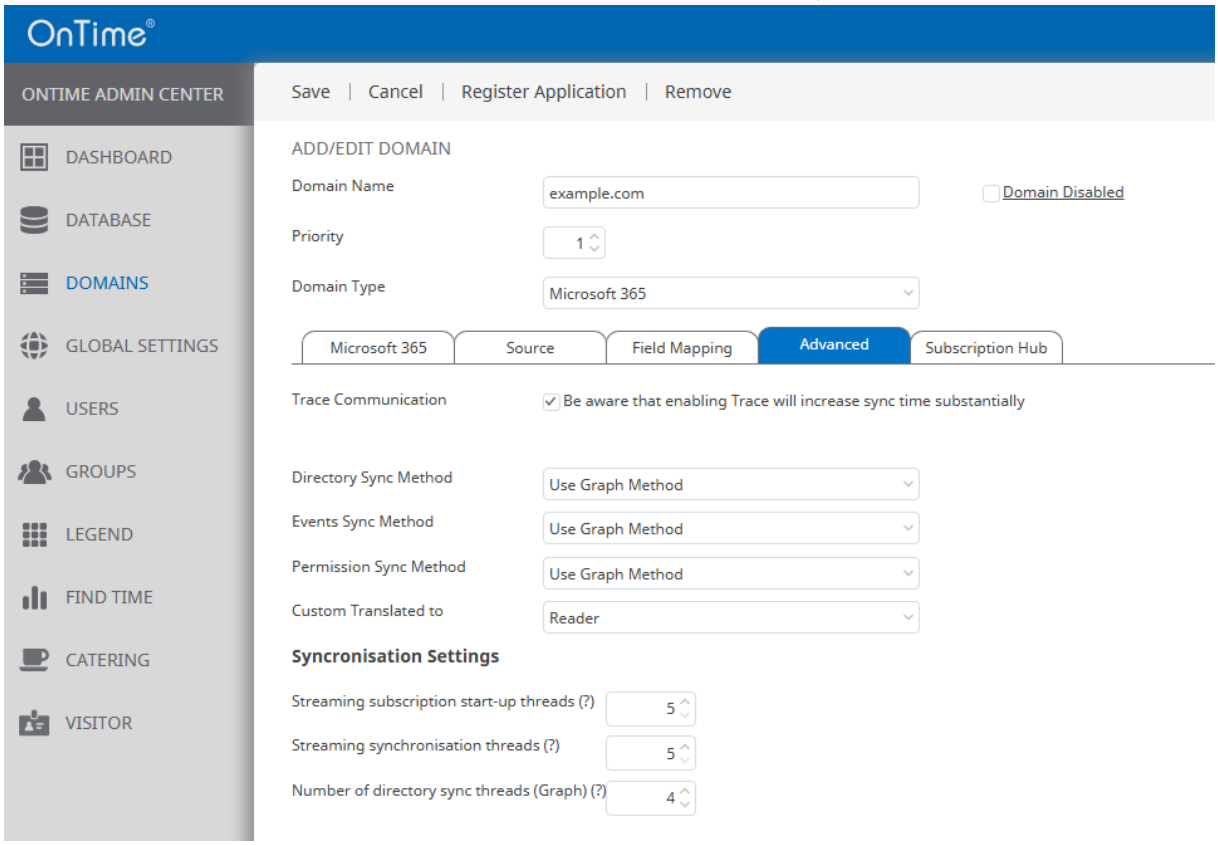
`manager` - Log for the `manager` application which is shipped with Tomcat by default

`host-manager` - Log for the `host-manager` application which is shipped with Tomcat by default

Trace Communication

A deeper level of error tracing in OnTime can be obtained in the “OnTime Admin Centre” – click “Domains”, choose your domain for tracing.

In the ‘Advanced’ section ‘Tick’ at ‘Trace Communication’, click ‘Save’.



Restart the OnTime Application from the Dashboard.

Remember to untick ‘Trace Communication’, – click ‘Save’ and restart the OnTime application when you have obtained the required info. Tracing communication will increase the sync time substantially.

In the C:\Program Files\IntraVision\OnTimeMS-x.x\tomcat\logs directory the trace log is found as the filename starting with ontimetomcat-stdout (current date).

- like

ontimetomcat-stdout.2025-xx-xx.log

Appendices

Subscription Hub Platform Requirements

Subscription Hub Platform Requirements
The Subscription Hub is a lightweight service and supports both Windows and Linux.

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 requires one CPU core. Additional CPU resources may be required depending on the operating system and the number of subscriptions.

Memory
Allow sufficient memory for the operating system, plus approximately 1 GB of RAM for the Subscription Hub.

Disk
Allow sufficient disk space for the operating system, plus approximately 1 GB for the Subscription Hub application and log files.

Subscription Hub Security and Communication

Notice Server

The Notice Server receives Microsoft Graph change notifications and provides the Internet-facing HTTPS endpoint used by Microsoft 365.

The configuration includes:

- protocol;
- listening port;
- SSL certificate;
- private key;
- public notification URL;
- clientState.

The clientState value is included in Graph change notifications and can be used to verify that incoming notifications correspond to the subscription created by OnTime.

Backend Server
The Backend Server interface handles communication between the OnTime server and the Subscription Hub.

A separate secretKey is used to authenticate communication between the OnTime server and the Subscription Hub.

This separation means that the Internet-facing Microsoft Graph interface does not have to expose the main OnTime application server.

Firewall Protection

Only the HTTPS endpoint required for Microsoft Graph Change Notifications needs to be Internet-accessible.

Where possible, the firewall should restrict incoming traffic to the relevant Microsoft 365 infrastructure. The installation manual therefore recommends applying an IP filter to the Internet-facing Subscription Hub endpoint.

Register External 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’

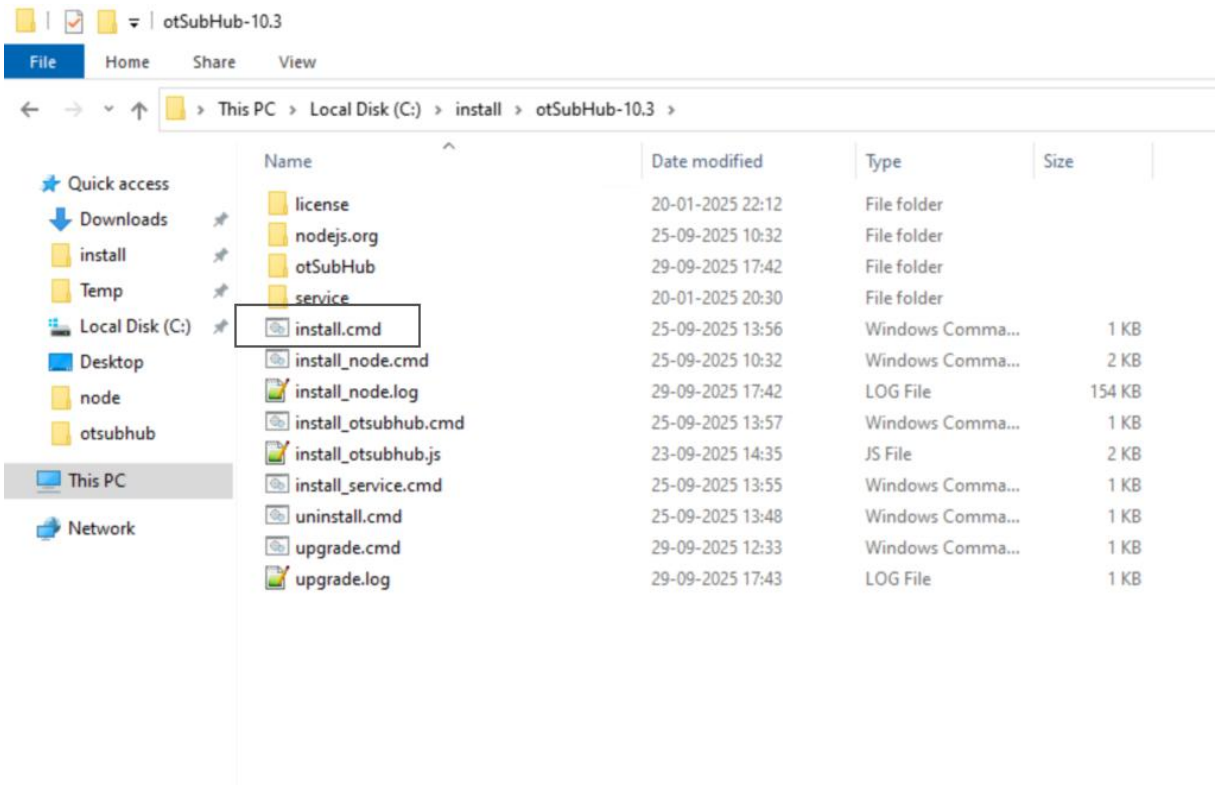
p) Click "Grant admin consent for *Your Company*"
Click ‘Yes’ to answer the question ‘Do you want to grant consent ...’

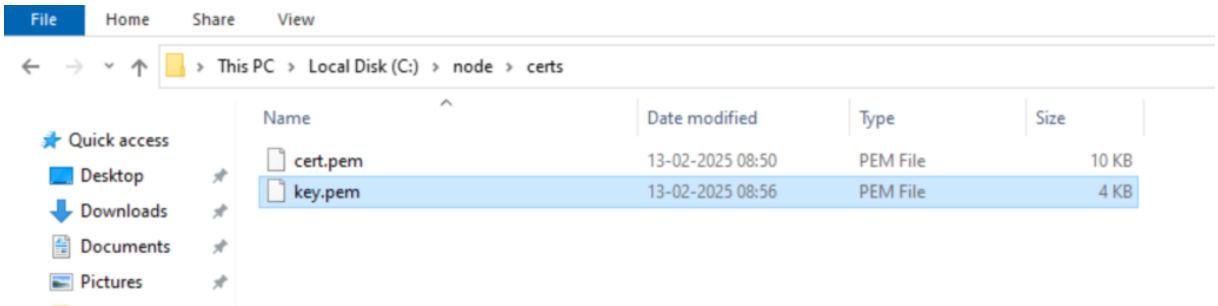
Installation and Configuration of the External Subscription Hub 'otSubHub'

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 can 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:

- 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'.

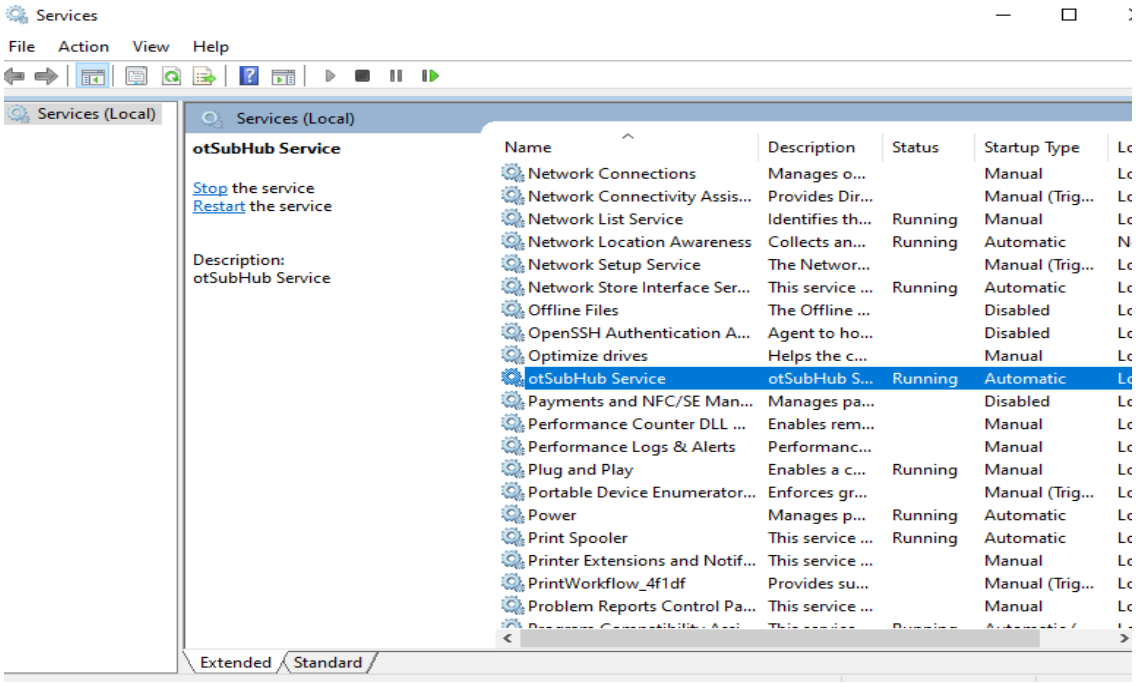

otSubHub-10.3
File
Home
Share
View
This PC › Local Disk (C:) › install › otSubHub-10.3 ›
Quick access
Downloads
install
Temp
Local Disk (C:)
Desktop
node
otsubhub
This PC
Network
Name
Date modified
Type
Size
license 20-01-2025 22:12 File folder
nodejs.org 25-09-2025 10:32 File folder
otSubHub 29-09-2025 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/fIKrCBJnB2I "
        },
        "graph": {
                "expiration_min": 60,
                "subscribe_threads": 3,
                "renew_threads": 3,
                "unsubscribe_threads": 5
        },
        "ews": {
                "subscribe_threads": 5
        }
}
```

You can 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

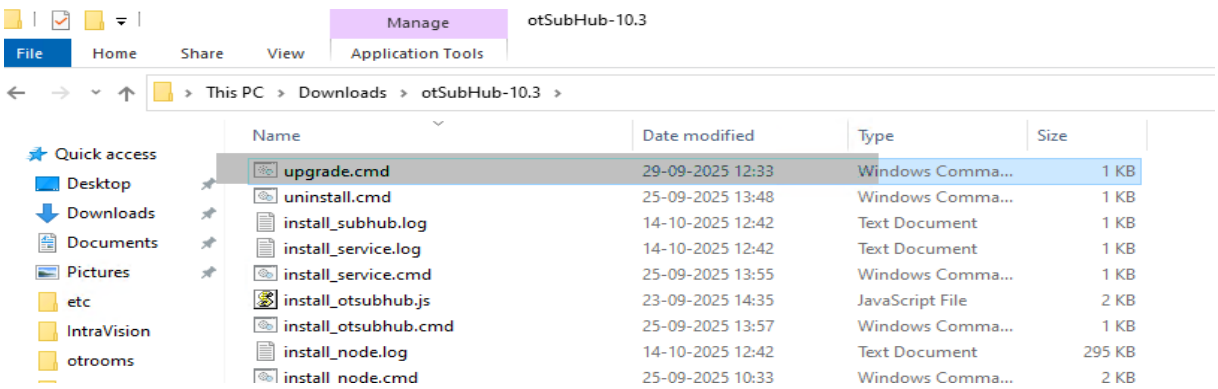
See the section *Microsoft Graph Change Notifications* for more information

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 can 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

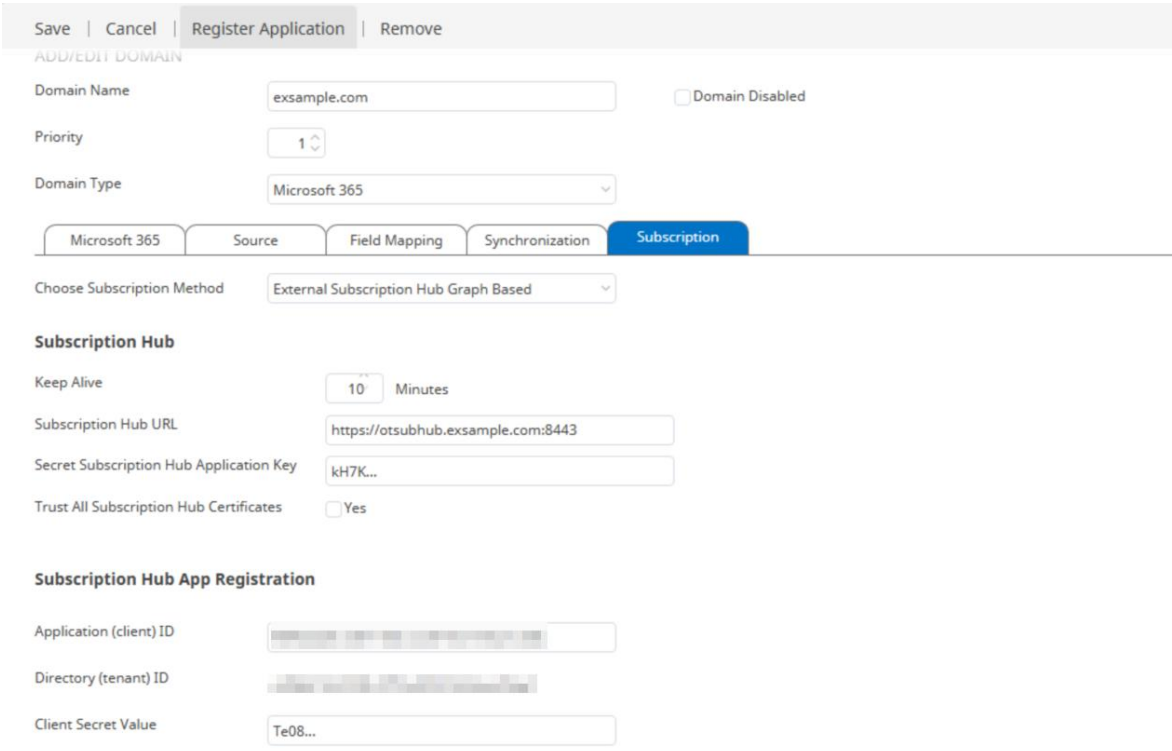
1. Copy Credentials
   Copy the values of the 'Client Application ID' and 'Client Secret Value' from the registered Subscription Hub application into a text editor, e.g., Notepad

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).

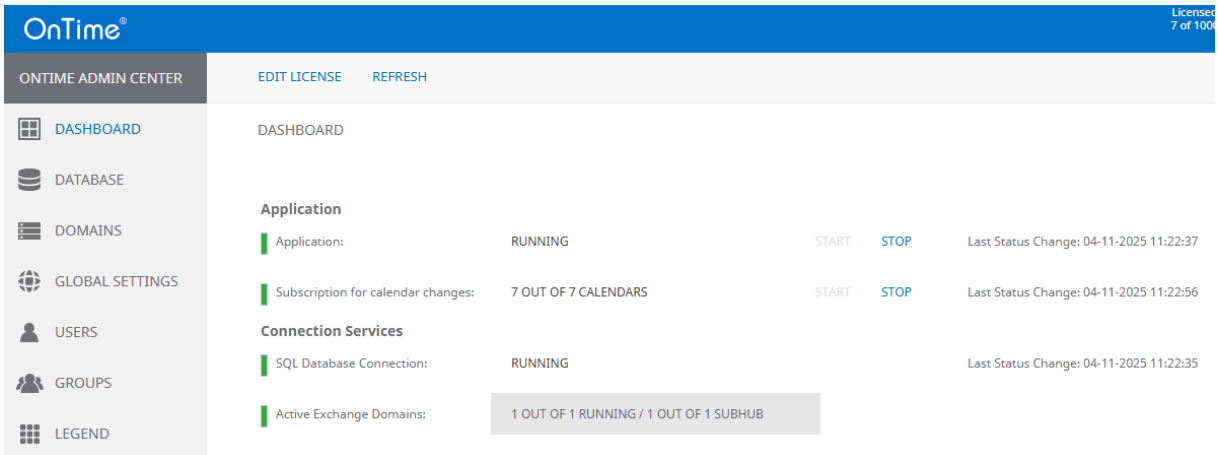
5. Set Subscription Hub URL
   Open the 'otSubHub.json' file located in 'C:\node\otsubhub' in a text editor, copy the Subscription Hub URL (including the port number) values, and paste it into the 'Subscription Hub URL' field (see example below).
6. Insert Secret Key
   Open the 'otSubHub.json' file 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": " o5vy+WNM2JurnOc/HuEFg+tsVco= "
                }
        },
        "backendServer": {
                "protocol": "http",
                "port": 8443,
                "secretKey": " kH7KoGfI42Wqp5f/fIKrCBJnB2I "
        },
        "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 can view the status of ‘SUBHUB’* when it is running (see example below)



OnTime server components and ports

Deployment Options

Option A – Subscription Hub in the DMZ – Recommended

The recommended architecture is to place the Subscription Hub on a dedicated server in the DMZ.

```
Internet / Microsoft 365 → HTTPS Change Notifications → Subscription Hub – DMZ →
OnTime Server – Internal Network
```

This architecture keeps the main OnTime server inside the internal network while only the Subscription Hub is exposed to Microsoft Graph.

The OnTime server must be able to communicate with the Subscription Hub using the configured HTTP or HTTPS port, typically port 80 or 443. The manual specifically recommends DMZ deployment because this avoids the need to open additional firewall access directly to the internal OnTime server.

Option B – Subscription Hub on a Separate Internal Server

In this scenario, the organisation must provide an externally reachable HTTPS endpoint for the Subscription Hub. This can normally be achieved by using:

- a reverse proxy;
- NAT/firewall publishing; or
- equivalent application delivery infrastructure.

This retains the performance benefit of separating subscription processing from the main OnTime server while allowing the organisation to use its existing Internet-facing security infrastructure.

Option C – Subscription Hub on the OnTime Server

The Subscription Hub can also be installed on the same machine as the OnTime server.

This can be useful for smaller installations or where additional server infrastructure is undesirable.

However, this architecture does not provide the same workload separation as running the Subscription Hub on a dedicated system. The manual therefore generally recommends a separate system.

Option D – Subscription Hub Behind a Reverse Proxy

A Subscription Hub installed either internally or in a DMZ can be published through a reverse proxy.

Microsoft Graph → HTTPS → Reverse Proxy → Subscription Hub → OnTime Server

This allows the organisation's existing reverse-proxy infrastructure to handle the public HTTPS endpoint and forward validated traffic to the Subscription Hub.

Register External 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

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

r) Select View ‘Manage Microsoft Entra ID’

s) Click ‘App Registrations’

t) Click ‘New registration’

u) 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’.

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

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

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

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

z) Choose expiration. Click Add

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

bb) Click ‘Microsoft Graph’

cc) Click ‘Application permissions’

dd) 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)

ee) Click ‘Add a permission’

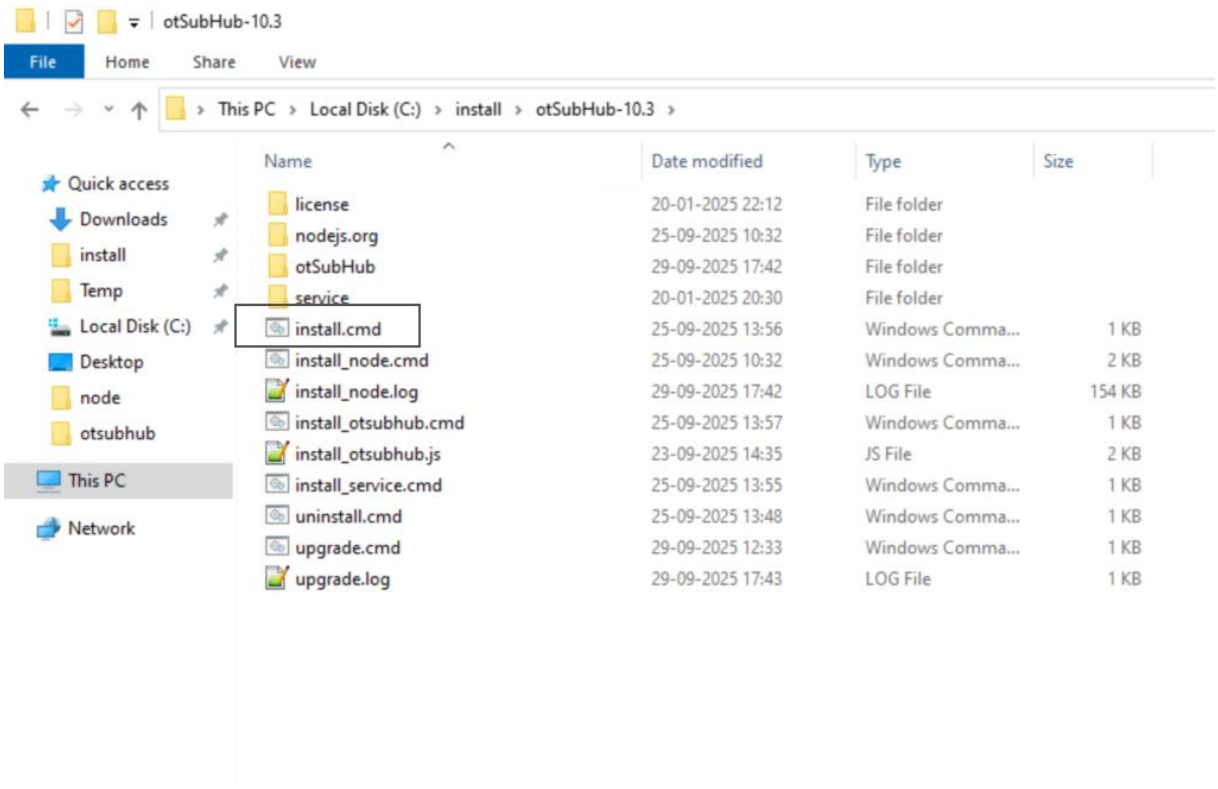
ff) Click "Grant admin consent for *Your Company*"
Click ‘Yes’ to answer the question ‘Do you want to grant consent ...’

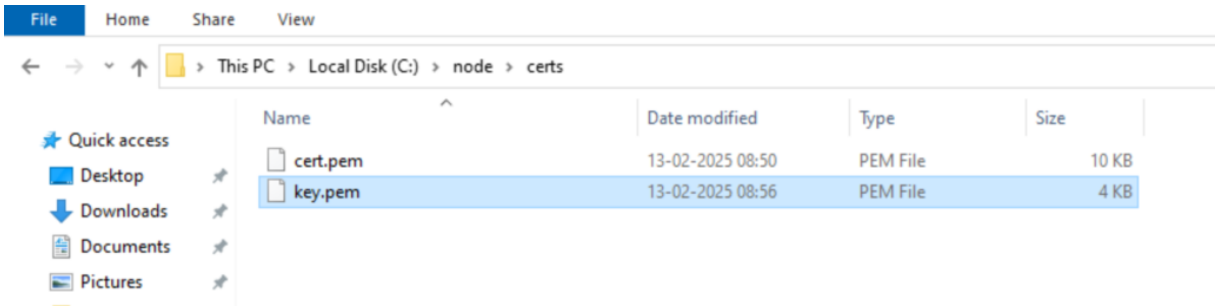
Installation and Configuration of the External Subscription Hub 'otSubHub'

8. **Unzip the installation file**
   Copy the otSubHub-10.x.zip installation file from the OnTime server to the Subscription Hub server and extract it to a temporary folder (Required when installing the Subscription Hub on a separate machine). If the OnTime server and Subscription Hub are installed on the same machine, extract the installation package locally on that server. (For both options, see example below)
9. **Run the installer**
   Navigate to the folder where the installation files were extracted, right-click install.cmd, and select **Run as administrator**. (see example below)
   The Subscription Hub service will be installed in the folder 'c:\node\otsubhub'.
10. **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)
11. **Edit the configuration file**
    Open the configuration file 'otSubHub.json' located in 'C:\node\otsubhub'.
12. **Set the certificate paths**
    In the 'otSubHub.json' configuration file, update the paths to the 'key.pem' and 'cert.pem' certificate files. (see example below)
13. **Set the service URL**
    In the URL property of the 'otSubHub.json' file, enter the full public HTTPS URL of the Subscription Hub. (see example below)
14. **Save and restart the service**
    Save your changes and 'restart the Subscription Hub service' on the server. (see example below)

Additional Notes:

- The Notice Server and Backend Server can be configured to use the same server. However, each service must use an appropriate and non-conflicting port configuration
- Log files for the Subscription Hub service are stored in the folder. 'C:\node\otsubhub'.

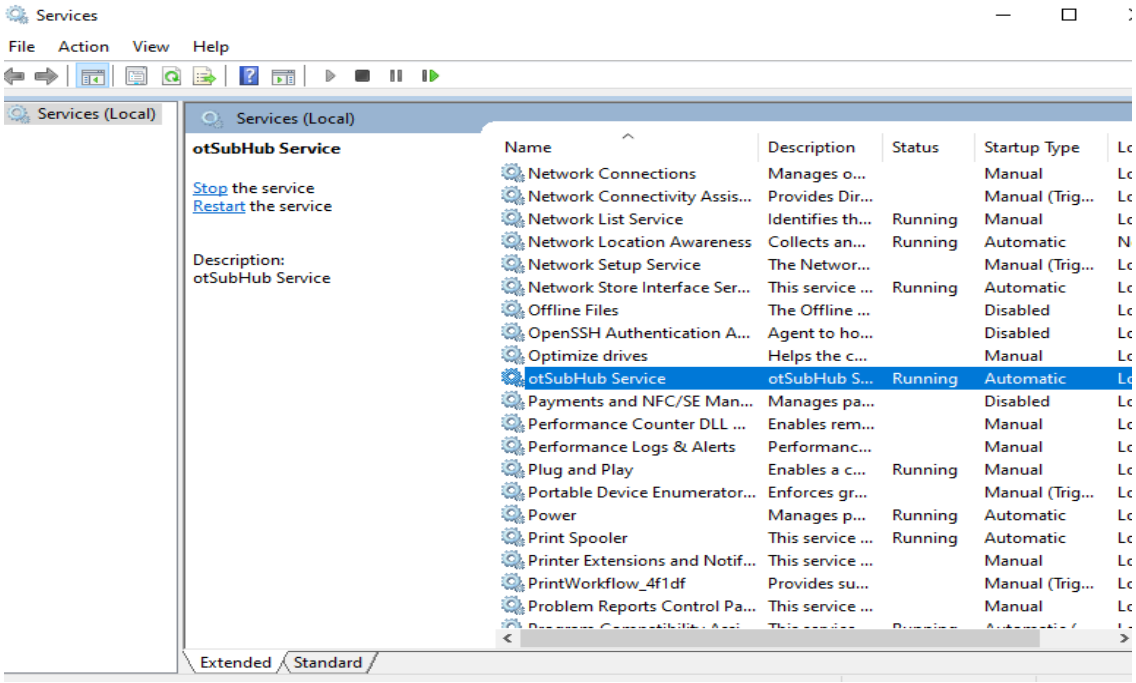

otSubHub-10.3
File
Home
Share
View
This PC › Local Disk (C:) › install › otSubHub-10.3 ›
Quick access
Downloads
install
Temp
Local Disk (C:)
Desktop
node
otsubhub
This PC
Network
Name
Date modified
Type
Size
license 20-01-2025 22:12 File folder
nodejs.org 25-09-2025 10:32 File folder
otSubHub 29-09-2025 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 can now find ‘otSubHub’ listed under Windows Services, as shown below:



Because the Subscription Hub requires inbound HTTPS connectivity for Microsoft Graph change notifications, we recommend restricting inbound firewall access as much as possible. 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

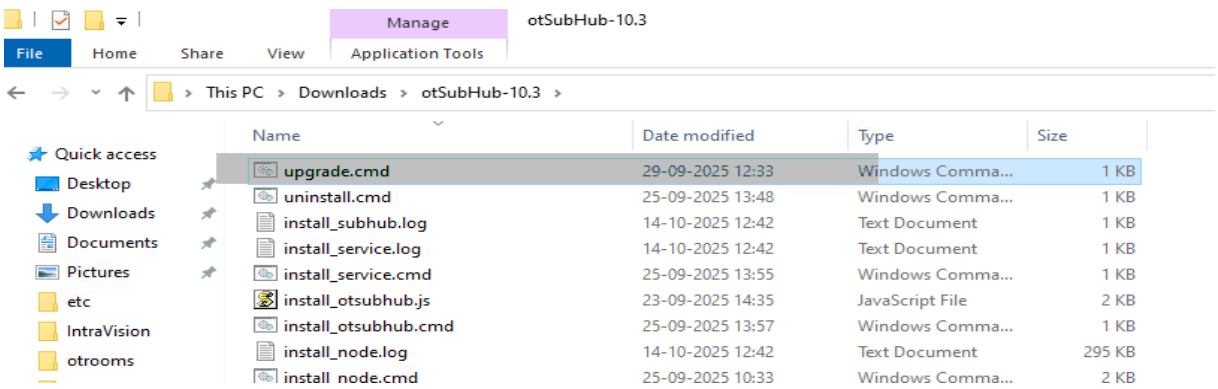
See the section *Microsoft Graph Change Notifications* for more information

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)

4. 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 can simply unzip the file locally on that machine.
5. 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)
6. Finally, make sure that 'otSubHub' service listed under Windows Services after the upgrade assignment.



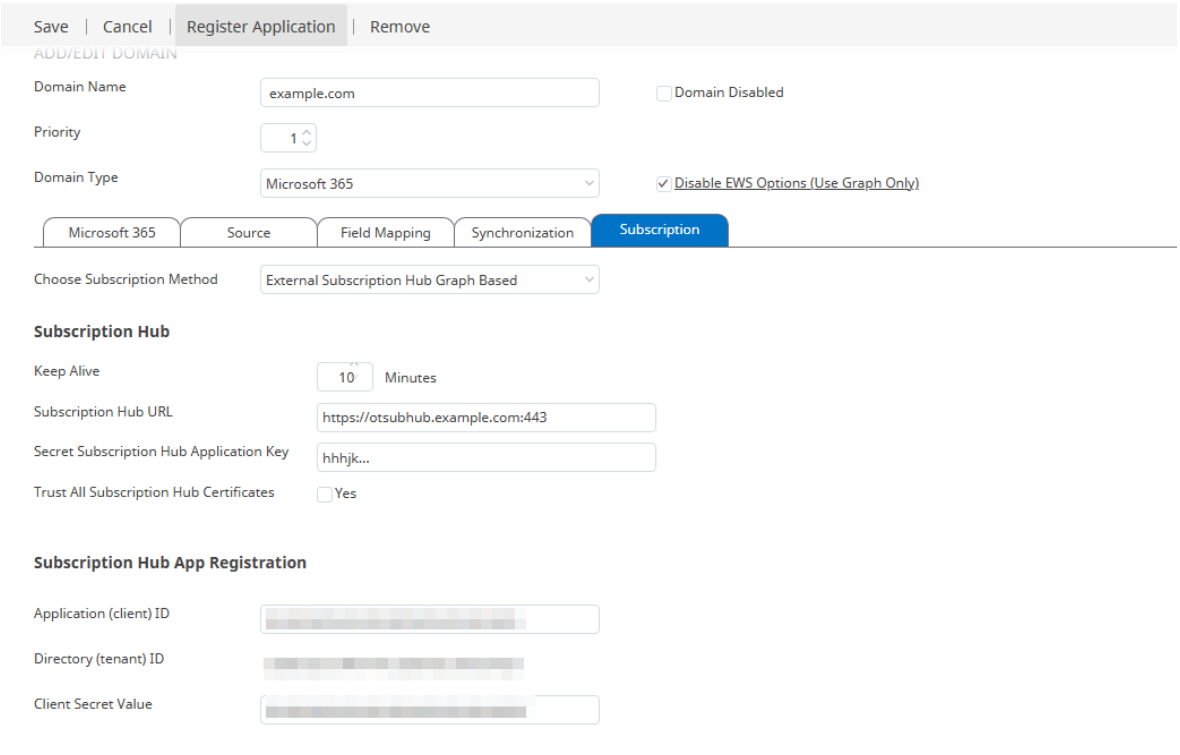
Configuring the Subscription Hub in OnTime Admin

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).

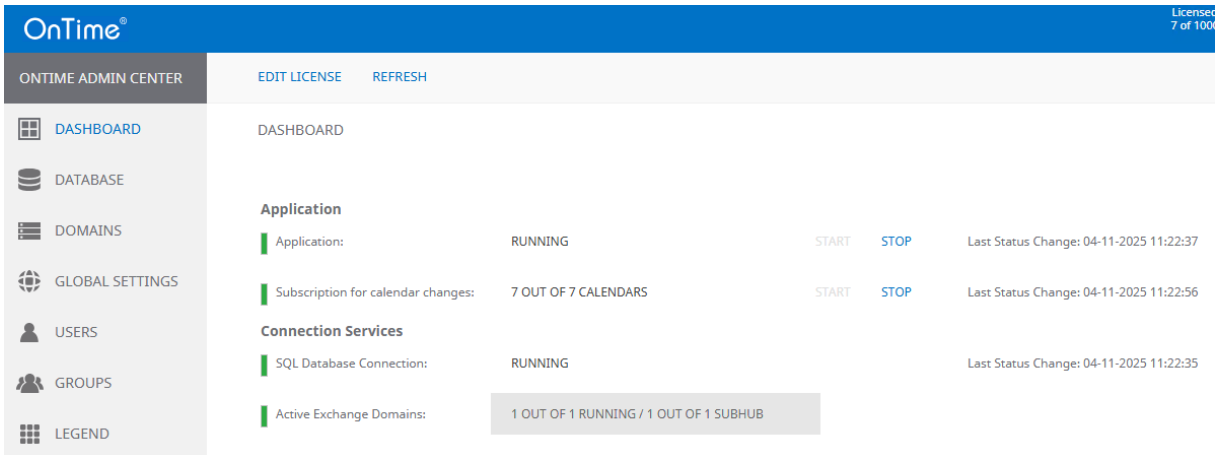
5. Set Subscription Hub URL
   Open the 'otSubHub.json' file located in 'C:\node\otsubhub' in a text editor, copy the Subscription Hub URL (including the port number) values, and paste it into the 'Subscription Hub URL' field (see example below).
6. Insert Secret Key
   Open the 'otSubHub.json' file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



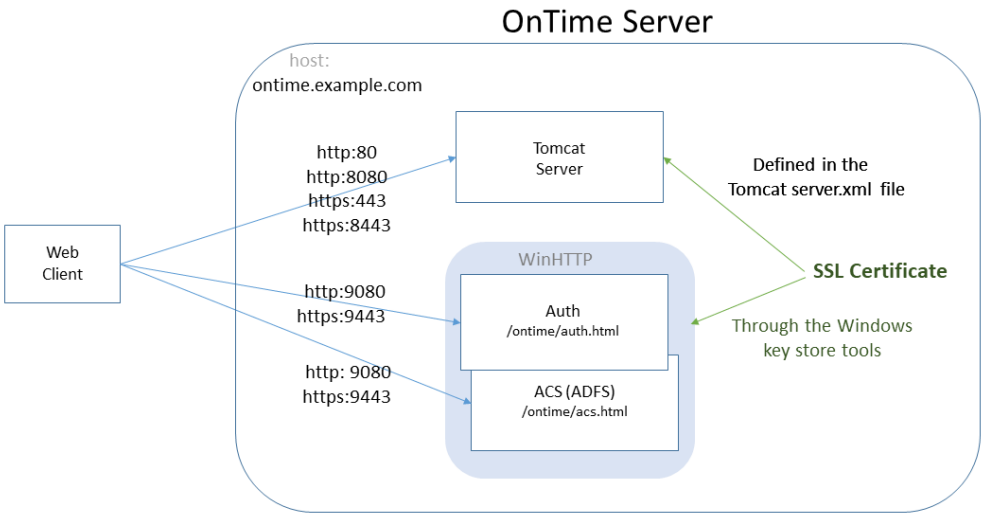
An example of the ‘otSubHub.json’ file is shown below.

```
{
        "noticeServer": {
                "protocol": "https",
                "port": 443,
                "key": "c:/node/certs/key.pem",
                "cert": "c:/node/certs/cert.pem",
                "payload": {
                        'URL': "https://otsubhub.example.com",
                        "clientState": " o5vy+WNM2JurnOc/HuEFg+tsVco= "
                }
        },
        "backendServer": {
                "protocol": "http",
                "port": 8443,
                "secretKey": " kH7KoGfI42Wqp5f/fIKrCBJnB2I "
        },
        "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 can view the status of ‘SUBHUB’* when it is running (see example below)



OnTime server components and ports



Integrating OnTime Group Calendar with other systems

OnTime provides two different ways of integrating with your business solutions.

1. Launching the OnTime interface from your business solution using custom URLs
2. Integration on the data level by using the OnTime Open Api (add-on module)

Integrating and launching OnTime from other solutions using custom URLs

A powerful way to use the graphical interfaces of the OnTime Desktop and Mobile client for integration with other systems like CRM, HRM or other solutions, is to use custom URLs. In the following sections we will show examples from the OnTime Desktop and Mobile client.
Note: Some systems require the parameters as 'URL encoded'.

Parameters:
user = " < value> "
value:email
example: user="abc@example.com"

users = [<value>]
value:email
example: users=["abc@example.com","def@example.com"]

group = " <value> "
value:groupname
example: group="Copenhagen"

openitem = {key:value, key2:value2}

Key	Value	Description
"Email"	"Email"	Organizer E-mail
"EventID"	"EventID"	The EventID may be obtained from an API call (an APIUser license key is required)

newitem = {key:value, keyN:valueN}

Key	Value	Description
"required"	"Email"	Persons required
"subject"	"Subject"	Text
"location"	"Location"	Text
"categories"	"Categories"	Text
"start"	"Start time"	Coded in ISO 8601 format, (UTC–GMT)
"end"	"End time"	Coded in ISO 8601 format, (UTC–GMT)
"body"	"Body"	Text
"showas"	"Busy" "Free"	

newpoll = {"emails":["Email1","Email2","EmailN"],"subject"}

view = {key1:value,keyN:valueN}

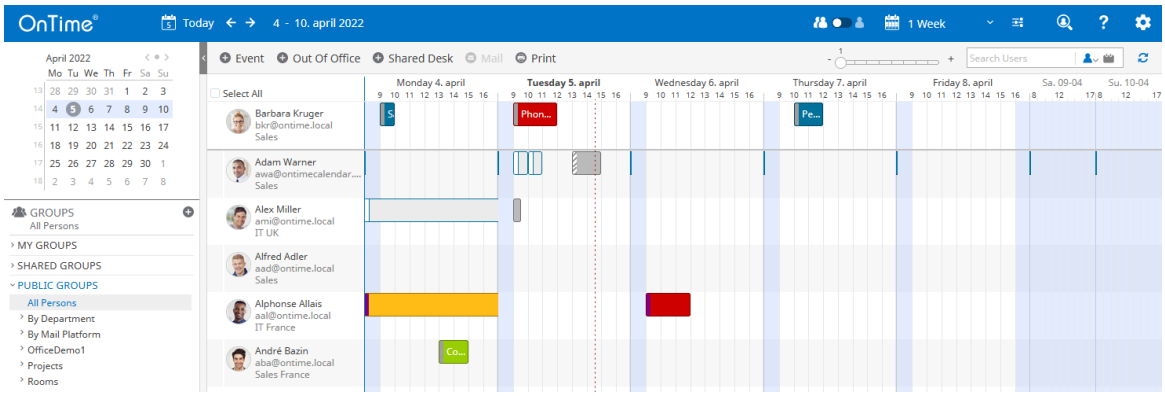
Key	Value	Description
"view"	"days" "weeks" “ooo” “list” “day” “week”	Group view Group view Time off view List view Person view Person view
"starthour"	0 – 23	
"endhour"	1 – 24	
"units"	1 – 9 weeks, 1 – 14 days	
"offhours"	true/false	
"weekends"	true/false	
"rowheight"	1 – 9	

viewstart = " <value> "
  value:date (yyyymmdd)
example: viewstart="20240501"

Creating Integrations with OnTime Desktop

Open the desktop client with a specified user selected.

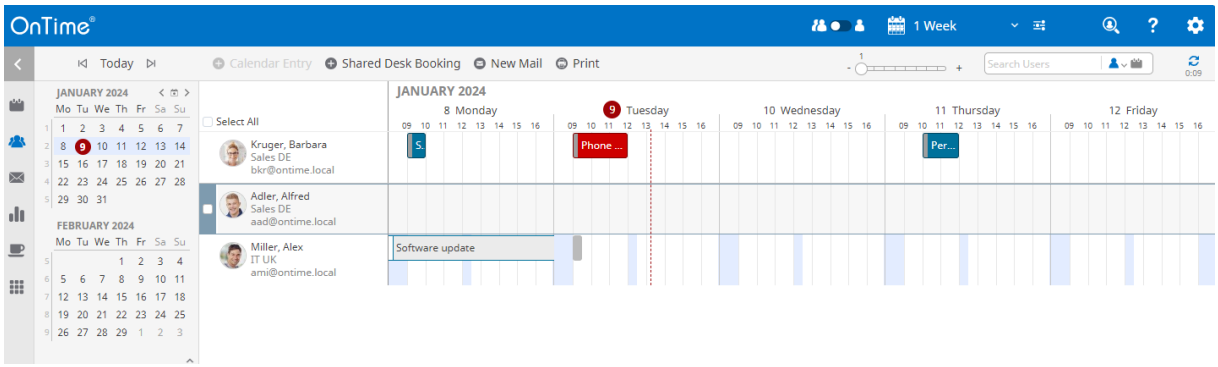
https://otmsdemo.intravision.dk/ontimegcms/desktop?user=”bkr@ontime.local"



Open the desktop client with a set of users selected in a temporary group

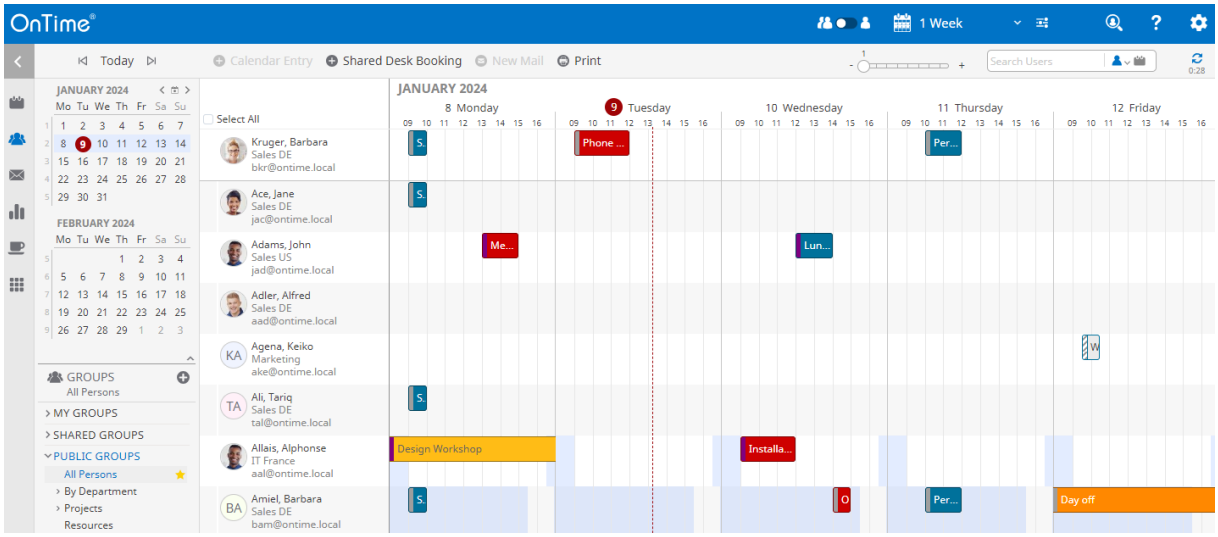
https://otmsdemo.intravision.dk/ontimegcms/desktop?users=["ami@ontime.local","aad@ontime.local"]

List of ‘users’ mail addresses.



Open the desktop client with a public group selected

https://otmsdemo.intravision.dk/ontimegcms/desktop?group="All Persons"



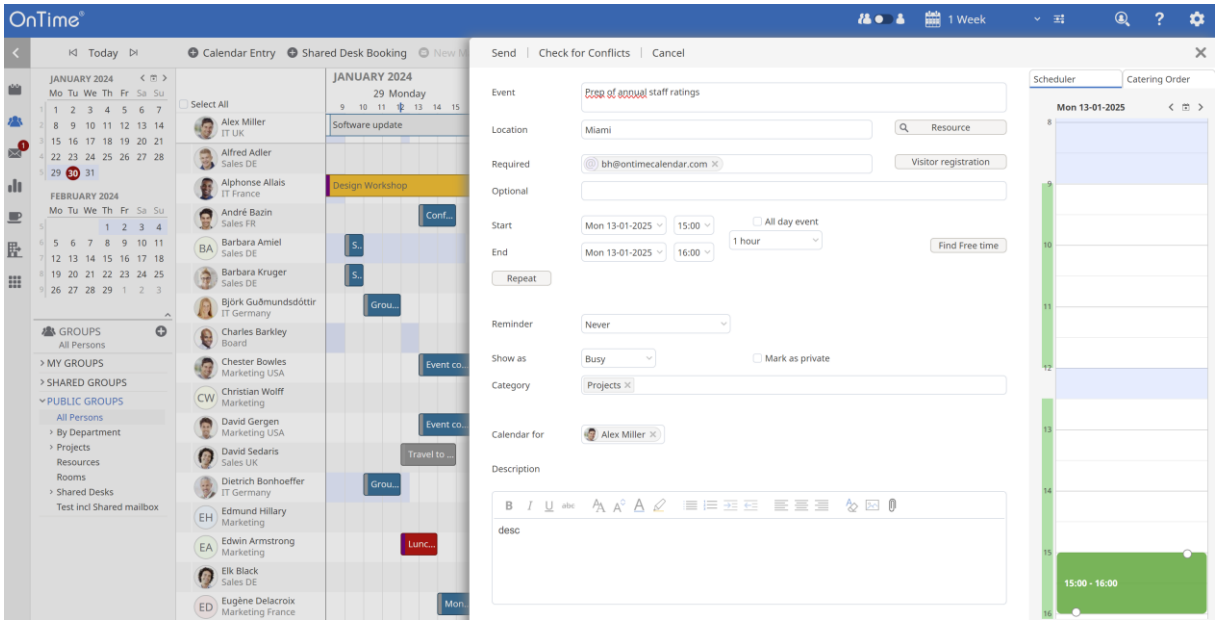
Open the desktop client with an existing Entry Selected

Example:
https://otmsdemo.intravision.dk/ontimegcms/desktop?openitem={"Email": "user@user.dk", "EventID" : "<EventID>"}

Open the desktop client creating a new entry

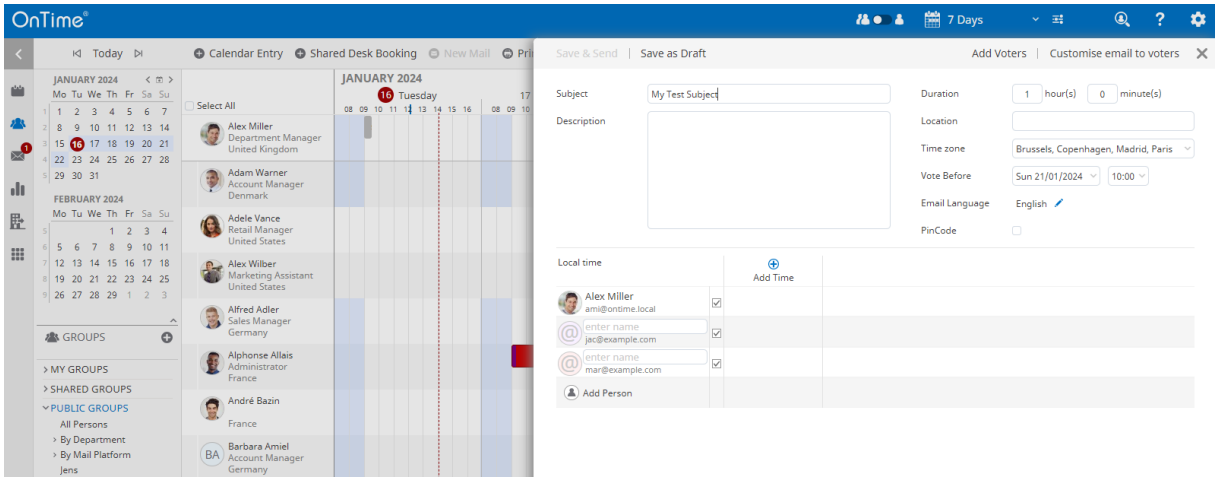
Example:

https://otmsdemo.intravision.dk/ontimegcms/desktop?newitem={"required":["bh@ontimecalendar.com"], "subject":"Prep of annual staff ratings", "location":"Miami", "categories":["Projects"], "start":"2025-01-13T14:00:00Z", "end":"2025-01-13T15:00:00Z", "body":"desc","showas":"Busy"}



Open the desktop client creating a poll

https://otmsdemo.intravision.dk/ontimegcms/desktop?newpoll={"emails":["mar@example.com","jac@example.com"],"subject":"My Test Subject"}

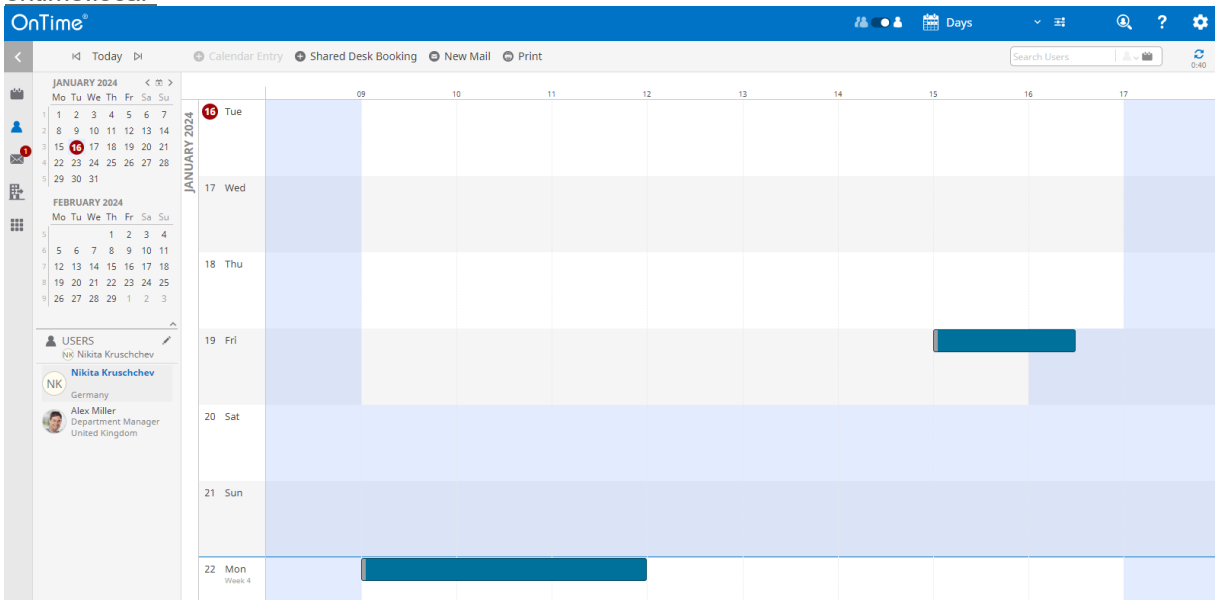


Open the desktop client in a view

Examples:

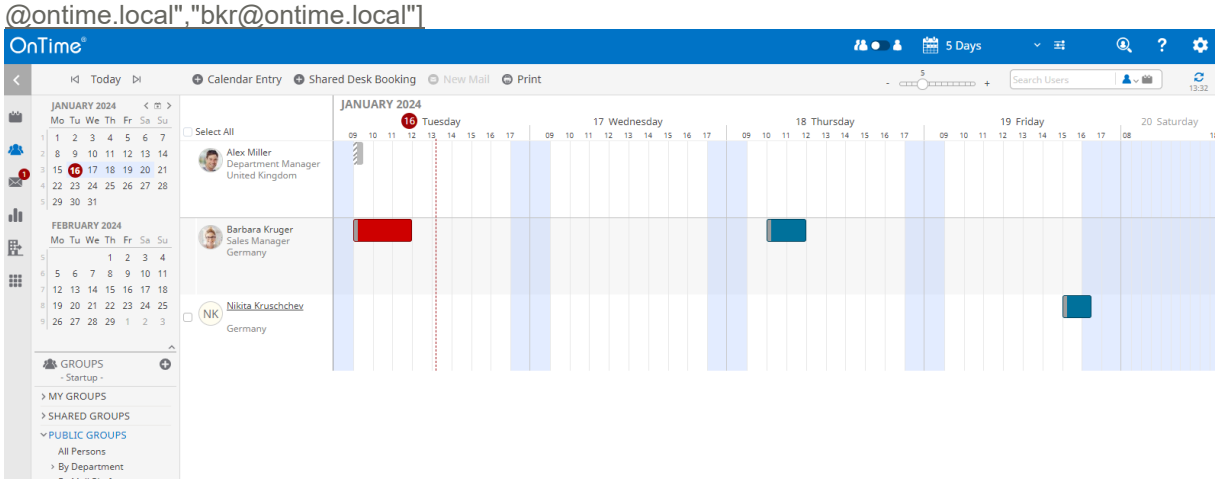
Person view:

https://otmstutorial.intravision.dk/ontimegcms/desktop?view={"view":"day","rowheight":5}&user="nkr@ontime.local"

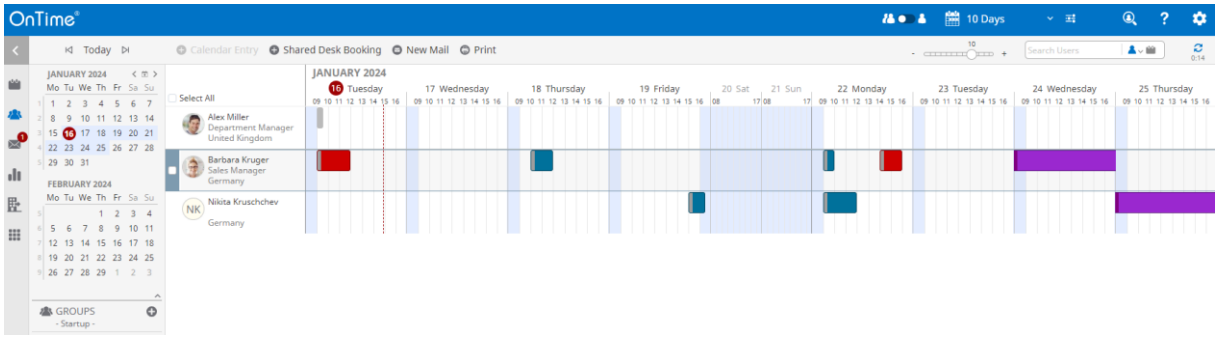


Group view:

https://otmstutorial.intravision.dk/ontimegcms/desktop?view={"view":"days","rowheight":5}&users=["nkr@ontime.local","bkr@ontime.local"]



https://otmstutorial.intravision.dk/ontimegcms/desktop?view={"view":"days","rowheight":3,"units":10,"weekends":true}&users=["nkr@ontime.local","bkr@ontime.local"]

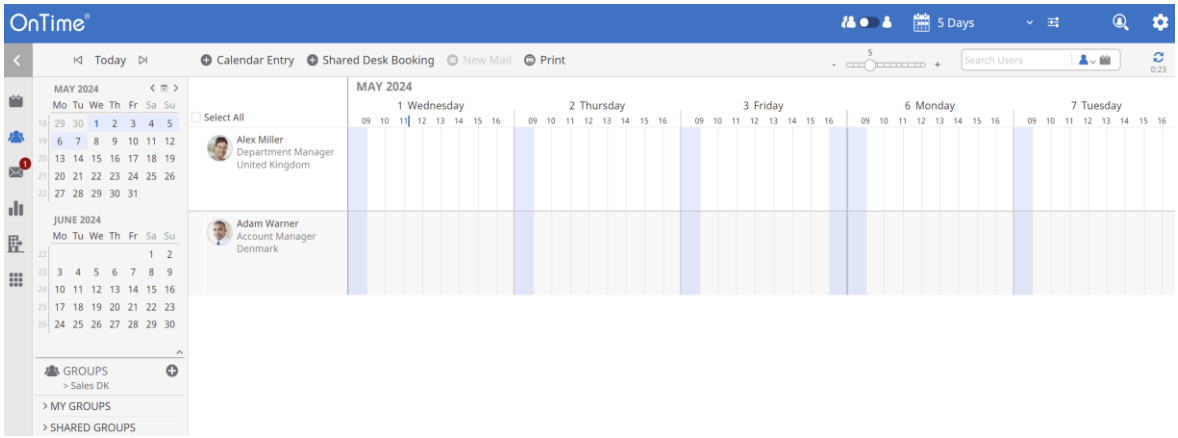


Open the desktop client a certain date with 'View start'

Example:

https://otmstutorial.intravision.dk/ontimegcms/desktop?viewstart="20240501"

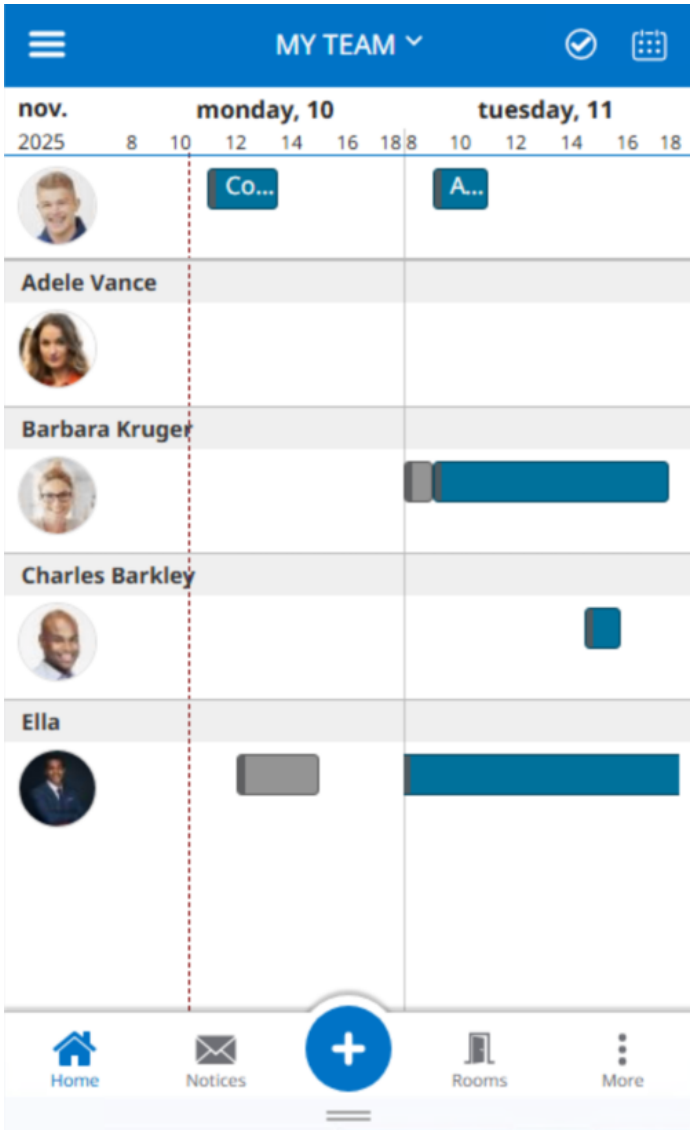
The view opens with the group recently viewed.



Open the mobile client with a selected group

https://otmsdemo.intravision.dk/ontimegcms/mobile?group="By Department\\France\\Paris\\Sales Fr"

Note: The backslashes must be preceded by another backslash as an 'escape' character.



Open the mobile client with an existing Entry Selected

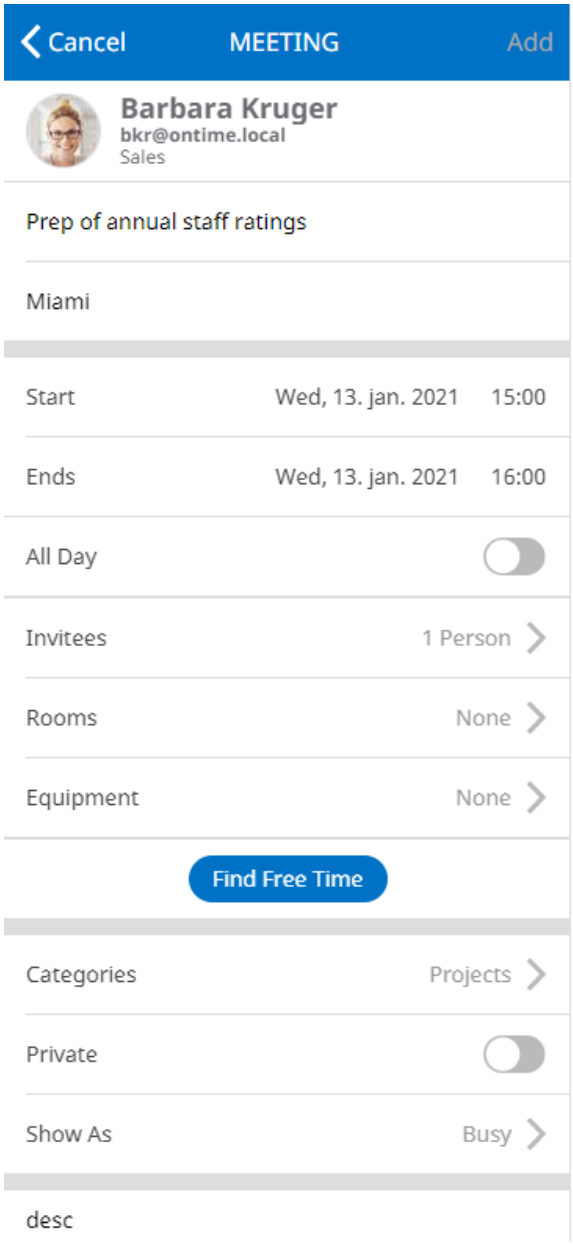
Example:
https://otmsdemo.intravision.dk/ontimegcms/mobile? openitem={"Email": "user@user.dk", "EventID" : "<EventID>"}

Open the mobile client creating a new entry

Example:

https://otmsdemo.intravision.dk/ontimegcms/mobile?newitem={"required":["bh@ontimecalendar.com"], "subject":"Prep of annual staff ratings", "location":"Miami", "categories":["Projects"], "start":"2025-01-13T14:00:00Z", "end":"2025-01-13T15:00:00Z", "body":"desc","showas":"Busy"

Times are coded in ISO 8601 format, UTC (GMT)

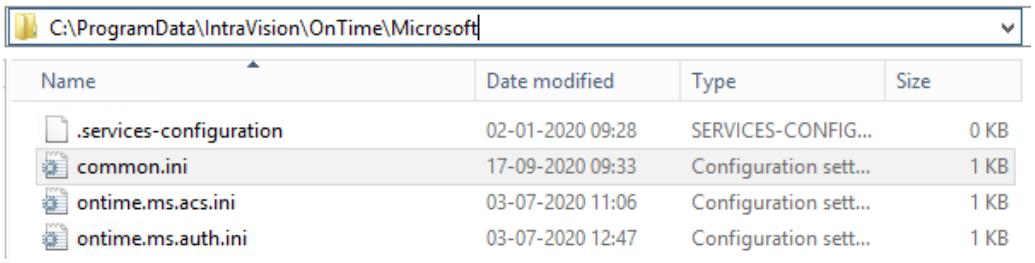


Redirection whitelists

Configure the whitelist to prevent malicious URL redirection

Using malicious redirects is a risk that we recommend organisations take very seriously. OnTime for Microsoft normally only needs to allow for redirection to a very limited number of URLs.

If whitelist is configured, the authentication token will be passed only to the URLs which match the whitelist. If any other redirect URL is passed to the authentication service, the token will not be issued.
In the folder “Programdata\Intravision\OnTime\Microsoft” you create a file called ‘common.ini’ and enter your whitelist configuration.



The REDIRECT_WHITELIST is used as a prefix. If a redirection starts with a URL from REDIRECT_WHITELIST, then it is allowed.

It means that if common.ini has a single property like this:

REDIRECT_WHITELIST=
- it means that all URLs are allowed.

REDIRECT_WHITELIST=https://
- this will allow all https redirects:

If no REDIRECT_WHITELIST is provided in the .ini files, then the Auth services behave exactly as they do now - allow any redirect to happen.

However, these are the misconfigurations.

A correct configuration example could be:
REDIRECT_WHITELIST=https://ontime.example.com/
Note: Please insert your relevant URL instead of ‘ontime.example.com’

You may add multiple lines with REDIRECT_WHITELIST=

CORS

In case an external application is accessing the OnTime server from a browser, standard CORS (Cross-Origin Resource Sharing) rules will apply. To allow these ‘third party’ requests at the OnTime server a change in the configuration of the Tomcat server is required.

In the folder C:\Program Files\IntraVision\OnTimeMS-x.x/tomcat/conf
the configuration is made in the file ‘web.xml’.

In the filter section add a ‘CorsFilter’. The example below is wide open, should only be used in a development scenario:

```
<filter>
        <filter-name>CorsFilter</filter-name>
        <filter-class>org.apache.catalina.filters.CorsFilter</filter-class>
        <init-param>
                <param-name>cors.allowed.origins</param-name>
                <param-value>*</param-value>
        </init-param>
</filter>
<filter-mapping>
        <filter-name>CorsFilter</filter-name>
        <url-pattern>/*</url-pattern>
</filter-mapping>
```

Further information:
https://tomcat.apache.org/tomcat-10.0-doc/config/filter.html#CORS_Filter

SSL certificates for the OnTime Tomcat Server

If the OnTimeTomcat server is required to run on SSL then three certificate files are needed for the Tomcat server.

1. ontime-rsa-key.pem
2. ontime-rsa-cert.pem
3. ontime-rsa-chain.pem

The three files mentioned are in '.pem' format (base64 encoded). The first file contains the server's private key. The second file contains the servers ssl-certificate. The third file contains the signing chain certificates from the 'Root CA' and the 'Intermediate CA'.

In the OnTime installation the three files are mentioned in the server.xml file, placed in: C:\Program Files\IntraVision\Ontime.x.x\tomcat\conf\

Depending on the system where you obtained the SSLcertificate you might get the SSL certificate as a .pfx or. p12 (pkcs12 format) file for the OnTime server.

Generating the OnTime .pem files from the certificate file:

Install the OpenSSL 'command line' tool
- may be found from https://wiki.openssl.org/index.php/Binaries

In a command prompt ensure that OpenSSL is working with your certicate file:
C:\test>
```
openssl pkcs12 certs.pfx
```
- Enter passwords and you should see a list of certificates on the screen.

Retrieve the private key to a file:

```
openssl pkcs12 -in certs.pfx -out private.pem –nocerts -noenc
```

Enter Import Password: ***** (Enter)
A private password protected .pem file is generated with the private key.

1. **Remove the password from the private.pem file and generate the first file for OnTime:**

   ```
   openssl rsa -in private.pem -out ontime-rsa-key.pem
   ```

   The OnTime-rsa-key.pem file contains the private key without a password.

Example:

```
-----BEGIN RSA PRIVATE KEY-----
MIIEowIBAAKCAQEAi45lsXhcxMMBUf96S5kS9ZHHLmMECAzkOJtTK14o3FnbMWMz
RlunTVL0VibOxdBraVfyEY2DbiBnwamHtBx6PEXVmk48AtohoMUWRajW6xQXZ/xa
7oGd6zwnkau9ns04AFXPKfLf2YfD/MbevtU6xhbXKWsjq6kAeQSMF6BbrumJ5uTx
6XTZSnS+z2NL+FmFuwdjnjAlJRbTFgYSIIlO94K2pleY3XAz5HUbxK9QsvPmfi9I
D/NRmM4sdFYVUxqJxgUju6vY9XRqGids3KcpenQ4R++AJwn5yckIyQAp32ern5vn
HDVuqvYnxeV0n4hEe9o2267RhS4NKkQHjsd8/wIDAQABAoIBAH2650XwjoOmvHXH
```

2. **Retrieve the server's certificate, generate the second file for OnTime:**

```
openssl pkcs12 -in certs.pfx -out ontime-rsa-cert.pem -clcerts -nokeys
```

Option:
Depending on the certificate supplier you may get this file as 'ssl_certificate.crt'. Rename it to 'ontime-rsa-cert.pem'

Example:

```
-----BEGIN CERTIFICATE-----
MIIGLzCCBRegAwIBAgIQCEyplwG8D7vWyBkyjLso6DANBgkqhkiG9w0BAQsFADBe
MQswCQYDVQQGEwJVUzEVMBMGA1UEChMMRGlnaUNlcnQgSW5jMRkwFwYDVQQLExB3
d3cuZGlnaWNlcnQuY29tMR0wGwYDVQQDExRSYXBpZFNTTCBSU0EgQ0EgMjAxODAe
Fw0xOTA0MDEwMDAwMDBaFw0yMTAzMzExMjAwMDBaMBgxFjAUBgNVBAMMDSoub250
aWllMDEuZGswggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQCLjnWxeFzE
```

3. **Extract the certificate chain, generate the third file for OnTime:**

```
openssl pkcs12 -in certs.pfx -out ontime-rsa-chain.pem -nokeys
```

An ontime-rsa-chain.pem file is generated with the certificate chain, Root CA and Intermediate CA, base64 encoded.

Option:
If you copy this file into a .crt extension - you may double-click/Open the file to check your 'Certification Path'.

4. The three OnTime .pem files are placed in the folder as referenced in the server.xml file:

   C:\ProgramData\IntraVision\OnTimeGCMS\keys\

5. After the update of the key files, restart the Apache Tomcat service

SSL certificates for the OnTime Auth Service

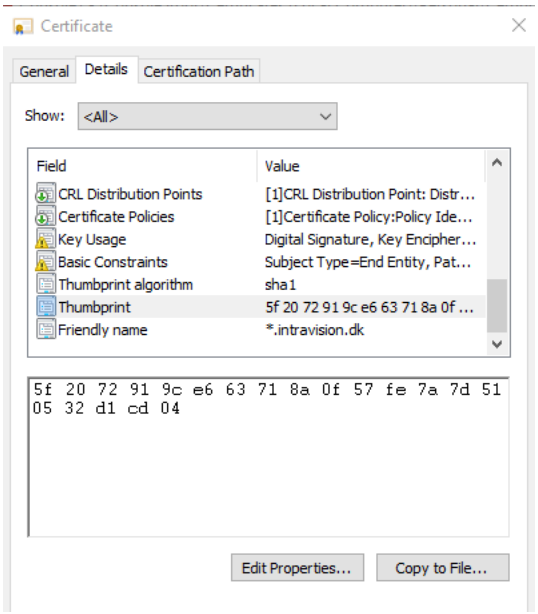
If HTTPS Domain (SSO) authentication is configured – please check the OnTime setup in the 'OnTime Admin Centre/Global Settings>Frontend' – a certificate is required for the OnTimeMS Auth service.
You must install a certificate at the Windows server. Acquire an SSL certificate pfx or p12 (pkcs12 format) file for the OnTime server.

1. Open a command prompt in administrator mode:
   Run >certlm
   - to open the Microsoft Certificates application for 'Local Computer'.

   Right-click 'Personal', choose 'All Tasks/Import'.
   Click 'Next'.
   Browse for your SSL certificate file, searching in – Personal Information Exchange (*.pfx,*.p12) files – click 'Open' – click 'Next'.
   Enter the password for your SSL certificate file, click 'Next' and click 'Finish'.
   Upon the message 'The Import was successful' – click 'OK'.

   Check the imported certificates – click 'Personal/Certificates' in the Certificates application.

2. Acquire the thumbprint of the certificate.
   Expand 'Certificates' – 'Personal' – 'Certificates'.
   Open the certificate for your server.
   Choose details – and thumbprint.



Copy the thumbprint characters into a text editor fx. Notepad.
Remove the spaces in between the characters.
Copy the characters to the clipboard for use as 'certhash' in the next section.

4. Open a command prompt in administrator mode:

Run 'netsh' with parameters, substitute the value of 'certhash' with your own value. The 'appid' is just a dummy value (needed).

In case you want to change the certificate – delete the old, run:

```
netsh http delete sslcert ipport=0.0.0.0:9443
```

- and rerun the 'netsh http add' command above with new parameters.

In case you want to show (list) the certificate(s), run:

```
netsh http show sslcert ipport=0.0.0.0:9443
```

In case you want to add the certificate, run:
Note: Run the following three lines as one line in the command prompt:

```
netsh http add sslcert ipport=0.0.0.0:9443
certhash=5f2072919ce663718a0f57fe7a7d510532d1cd04
appid={00112233-4455-6677-8899-AABBCCDDEEFF}
```

The response text should show:

```
SSL Certificate successfully added.
```

At this stage, you have enabled the SSL communication for all Windows web services that need it.

SSL root certificates for the OnTime server

A customer has reported issues with the secure connection from the OnTime server to the Microsoft sites that provide access to the cloud:

https://login.microsoftonline.com
https://graph.microsoft.com
https://portal.azure.com

The issue turned out to be a missing trusted root certificate in common between the Microsoft site and the Apache Tomcat server used in OnTime.

Example with https://graph.microsoft.com

Obtain the root certificate
Open the site https://graph.microsoft.com
in a web browser
In the URL bar, click the padlock to display the SSL certificate information.
Check the root certificate in the 'Certification path' – 'Digicert Baltimore Root'
Export the root certificate into a file, C:\tmp\baltimoreca.cer in 'Base-64 encoded X.509' format.
In a text editor check the content of the file – should include 'BEGIN CERTIFICATE' and 'END CERTIFICATE' at the top and bottom.

Import the root certificate
In OnTime's Apache Tomcat server import the root certificate to the java root certificate store, the file 'cacerts'. The tool 'keytool.exe' is used for the import.

The tool to change the 'cacerts' file is 'keytool.exe' it is found in the directory:
C:\Program Files\Intravision\OnTimeMS-x.x\jdk\lib\bin

The 'cacerts' file is found in the directory:
C:\Program Files\Intravision\OnTimeMS-x.x\jdk\lib\security

Open a command prompt in administrative mode at:
C:\Program Files\Intravision\OnTimeMS-x.x\jdk\lib\security

To check the path and functioning of ‘keytool.exe’ described, try the following command:

List the entries of the certificate store:

```
..\..\bin\keytool.exe -list -cacerts
```

The fingerprints of the supported root certificates will be listed.

In case you want a further inspection, redirect to a file:

```
..\..\bin\keytool.exe -list -cacerts > c:\tmp\cacerts.txt
```

Add the new root certificate authority:
Adapt the following command to your requirement, **All parameters must be entered on one line.**

the example input file here mentioned is ‘baltimoreca.crt’:

```
..\..\bin\keytool.exe -import -keystore cacerts -noprompt -storepass
‘changeit’ -trustcacerts -alias ‘baltimoretrustedca’ -file
C:\tmp\baltimoreca.crt
```

The password to the file ‘cacerts’ is by default ‘changeit’.

OnTime Authentication Token

OnTime uses a token system for authentication.
There are no special OnTime username/password as OnTime relies on Authentication Services to verify the users' identity.

Currently there are the following methods for authentication:
- Domain SSO, which uses identity of a user logged into the Windows domain
- ADFS SSO
- Form based authentication, which passes the credentials to the Exchange server, and checks for the response (multi-factor authentication is not supported)
- Mail based authentication, which sends an email to the user's inbox and waits for the user's confirmation

In all cases after the user successfully completes the login procedure (which in SSO solutions may be automated), a Temporary Login Token is generated by the authentication service. Temporary Login Token has a short timespan (30 seconds by default) and is then passed to OnTime which generates the User Token.
The User Token can now be used for further interaction with the system. The User Token has a longer expiration time (1 week by default, it can be configured in the Admin UI) and is renewed every time it is used, so users do not have to login again if they are continuously using OnTime. The User Token is saved in a cookie, so users can continue using OnTime after the browser is reopened.
There is one exception to the above flow: Form based authentication creates a User Token immediately.

The API User can also be used to create a User Token if the Login method is called with the OnBehalfOf rights. The User Token created by the API User is not renewable and should be created again after expiration.

In case the User Token is compromised, then all the currently issued User Tokens for a particular user can be invalidated through the Invalidate Token functionality on the Admin UI.

OnTime Domain Authentication (SSO)

When Windows users have authenticated with the MS AD domain they may access the OnTime web application easily without a login box with password for OnTime.
A Windows service “OnTimeMS Auth” is used to authenticate the Windows users access to OnTime.
This domain (SSO) authentication is configured in Global/Backend - Authentication Services.
When the service is installed, it is seen in the list of Windows services with the name ‘OnTimeMS Auth’.

Installation of the service:

In the folder C:\Program Files\IntraVision\OnTimeMS-x.x\cmd
you will find the command ‘ontime.ms.auth-install.cmd’.
Run it as an administrator to install the OnTimeMS Auth service.

The OnTimeMS Auth service offers Windows domain logon authentication in the browser. To have SSO, your browser has to trust the OnTime server.
For details please have a look at Browser setup for SSO.

Customisation of the “OnTimeMS Auth” service

In the folder C:\Program Files\IntraVision\OnTimeMS-x.x\ontime.ms.auth, look for the file ‘ontime.ms.auth.ini’. Make a copy of the file to the folder C:\ProgramData\IntraVision\OnTime\Microsoft. In the default setup of a Windows server, the folder ‘ProgramData’ is normally a ‘hidden item’.

The default version of ‘ontime.ms.auth.ini’ reflects the default parameters in the service:

```
;=THIS IS A COMMENT prepended by ;=
;=VERSION=12.1.0.0multifactor
;=Default settings sample ini file
;=%ProgramData%\IntraVision\OnTime\Microsoft\ontime.ms.auth.ini
;=Multiple values are represented by new lines
;=URL=http://+:9080/ontime/auth.html
;=URL=https://+:9443/ontime/auth.html
;=MAIL_ATTRIBUTE=mail
;=AUTH_SCHEME implementations Negotiate, Basic, and NTLM
;=AUTH_SCHEME=Negotiate
;=AUTH_SCHEME=NTLM
;=AUTH_SCHEME=Basic
;==============================
;=Below are optional parameters
;=Note: LDAP_URL is the ldap binding url
;=LDAP_URL=LDAP://SERVER:PORT/DC=acme,DC=inc
;=Note: Authentication is ADS_SECURE_AUTHENTICATION thus omitting credentials
implies using calling thread security context
;=LDAP_USR=USER_NAME
;=LDAP_PWD=PASSWORD_IN_CLEAR_TEXT
```

The ‘URL’ parameters are interrelated. To disable http (port 9080), remove the ‘;=‘ characters in front of ‘URL=https’ to enable ‘https’, this setting will disable ‘http’. Save the file and restart the service.

The three ‘AUTH_SCHEME implementations’ are enabled by default.
To disable for example ‘NTLM’ you remove the ‘;=‘ characters in front of ‘Negotiate’ and ‘Basic’. Save the file and restart the service.

If your OnTime server is not part of the AD (untrusted), you might need the LDAP settings.

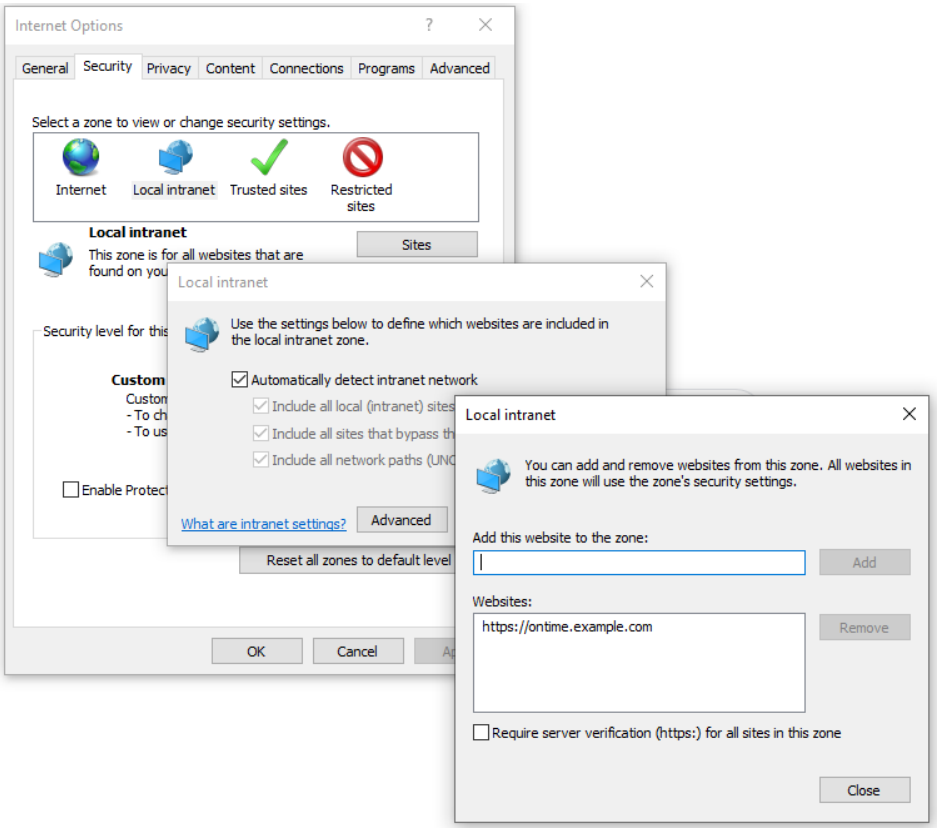
The parameter ‘LDAP_URL’ may be used to address a certain LDAP server and eventually a certain ‘OU’ in your AD domain.
For authentication, you remove the ‘;=‘ characters in front of LDAP_USER and LDAP_PWD and adapt the parameters to your environment.

Browser setup for SSO

In organizations a trusted OnTime server in the ‘Local intranet’ is configured by a ‘Group Policy’ at the domain level.

Individual user configuration:

The Chrome and Edge browsers trust your OnTime server due to the configuration you applied in the Internet Options settings via the Windows Control Panel. Click “Sites” and “Advanced” to add your OnTime server.



The Firefox browser is treated differently. In an empty tab of Firefox enter ‘about:config’ as the URL.
Accept the risk and continue.

In the search field, enter **network.negotiate-auth.trusted-uris**

Click Edit and enter the name of your server – e.g. ‘ontime.example.com’

ADFS login (SSO)

ADFS login (SSO) in Microsoft Entra ID

1. Login to https://portal.azure.com
2. Click for 'Microsoft Entra ID'
3. Click 'Add/Enterprise Application'
4. Click 'Create your own application'
5. Enter a name for your application
6. Choose 'Integrate any other application you don't find in the gallery (Non-gallery)'
7. Click 'Create'
8. Click on 'Properties' in the created Enterprise application
9. Check that 'Enabled for users to sign-in', 'Assignment required', 'Visible to users' are set to 'Yes'
10. Click on 'Single sign-on' and then 'SAML'
11. Click 'Edit' "Basic SAML Configuration"
    Identifier (Entity ID): https://ontime.example.com/unique_identifier (mark as Default/copy value for later)
    The unique identifier can be created from
    https://www.uuidgenerator.net/version1
    Reply URL: https://ontime.example.com/ontime/acs.html
    Sign on URL: https://ontime.example.com/ontimegcms/desktop
    Click 'Save', click the 'X' in the upper right corner.
12. Click 'Users and Groups
    Click 'Add users/group.' The group has to be a Security group
    Click 'none selected', add users and then click 'Select'
    Click 'Assign'
13. If your UserPrincipalName differs from your email addresses, click on edit 'Attributes & Claims'
    click on 'Unique User Identifier (Name-ID)'
    Select 'user.mail' in 'Source attribute'
    Click 'Save', click the 'X' in the upper right corner.

14. Copy "App Federation Metadata Url" in the "SAML Signing Certificate" area
15. Go to the section - ADFS - at the OnTime server

Note: Only one tenant configuration for ADFS is supported in OnTime.

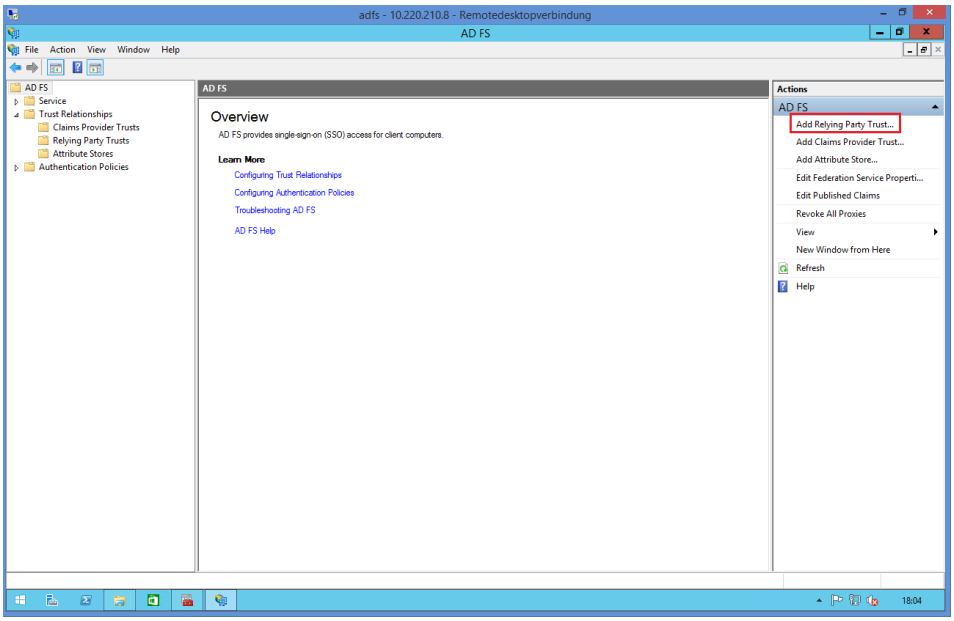
ADFS login (SSO) on-prem

The OnTime backend software was changed from OnTime ver. 4.1.7 onwards.
If you migrate from an earlier version of OnTime, please review the steps below.

Single-sign-on (SSO) for the users of OnTime may be configured through ADFS (Active Directory Federation Services). SSL must be enabled at the OnTime server.

Configuration steps:

1. Creation of RPT, ‘Relying Party Trusts’ in AD FS Management.
   Open ‘AD FS Management’.
   Click ‘Add Relying Party Trust’ in the right-hand navigation



   Enter data about the relying party:

1.1 Display Name: OnTime GC
   AD FS profile
   Skip ‘Optional token encryption certificate’.

1.2 Check ‘Enable support for the SAML 2.0 WebSSO protocol’
   ‘Relying party SAML 2.0 SSO service URL’ (Endpoint).
   Example:
   https://ontime.example.com/ontime/acs.html

1.3 Add the „Relying party trust identifier“ (Identifier).
Example:
https://ontime.example.com/ontime/acs.html

1.4 Choose “I do not want to configure multi-factor authentication settings for this relying party trust at this time”.

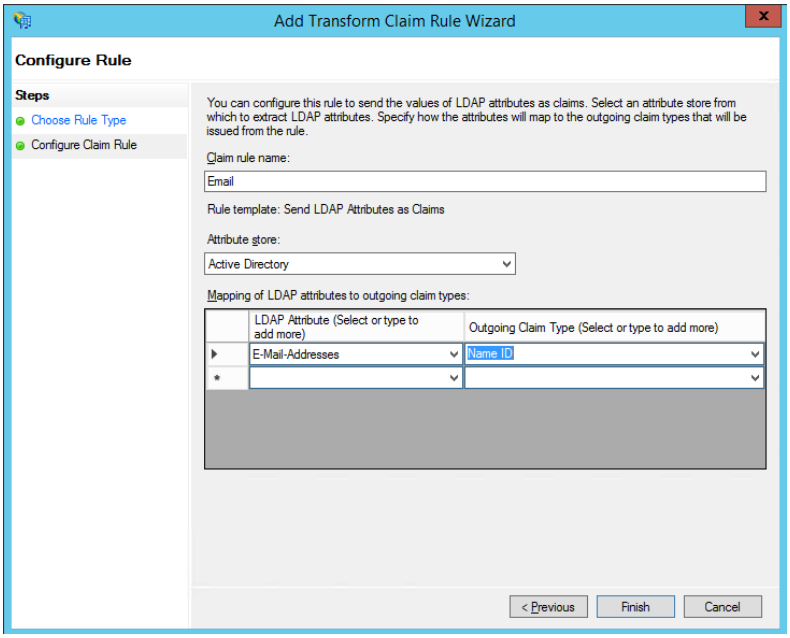
1.5 Choose “Permit all users to access this relying party”.

1.6 Check “Open the Edit Claim Rules dialogue …”.

1.7 Close

1.8 Take a note of the Identifier

1.9 Edit Claim Rules
Add Rule…
Claim rule template: Send LDAP Attributes as Claims
Claim rule name, e.g., Email
Attribute store: Active Directory
Mapping of LDAP attributes to outgoing claim types
LDAP Attribute: E-Mail-Addresses
Outgoing Claim Type: Name ID



ADFS - at the OnTime server

Customisation of 'OnTime ACS' is done by copying the file 'ontime.ms.acs.ini' from the folder:
C:\Program Files\Intravision\OnTime-x.x\ontime.ms.acs

to the folder C:\ProgramData\IntraVision\OnTime\Microsoft.

The folder 'ProgramData' is by default a hidden item in 'Windows Explorer'.

The default version of 'ontime.ms.acs.ini' reflects the default parameters in the service code, replace with your own IDs:

Cloud setup:

```
;=THIS IS A COMMENT prepended by ;=
;=VERSION 13.0.0.0
;=Default settings sample ini file
;=%ProgramData%\IntraVision\OnTime\Microsoft\ontime.ms.acs.ini
APP_ID_URI=https://ontime.example.com
;=Enter link here or download the file manually, name it FederationMetadata.xml and
place it in this folder
FEDERATION_METADATA_URL=https://login.microsoftonline.com/b24bc1f9-4f5b-4959-87d6-
43b68225381d/FederationMetadata/2007-06/FederationMetadata.xml?appid=667cdd71-cde5-
4c36-9e9e-25918aa22574
;=In case you use proxy, uncomment following lines and provide the correct values:
;=PROXY_HOST=proxy.mydomain.dk
;=PROXY_PORT=1256
```

If you are running on-prem, you need to change it to:

```
;=THIS IS A COMMENT prepended by ;=
;=VERSION 13.0.0.0
;=Default settings sample ini file
;=%ProgramData%\IntraVision\OnTime\Microsoft\ontime.ms.acs.ini
APP_ID_URI=https://ontime.example.com
;=Enter link here or download the file manually, name it FederationMetadata.xml and
place it in this folder
FEDERATION_METADATA_URL=https://fs.example.com/FederationMetadata/2007-
06/FederationMetadata.xml
;=In case you use proxy, uncomment following lines and provide the correct values:
;=PROXY_HOST=proxy.mydomain.dk
;=PROXY_PORT=1256
```

From your note of the Identifier, adapt the ini file accordingly:

The parameter 'APP_ID_URI' should reflect your OnTime application Identifier.

Note: Using the 'OnTimeMS ACS' service requires an SSL certificate for the OnTime server from a publicly trusted certification authority. Establishing an SSL certificate for the OnTime Server is described in the Appendix SSL certificates for the OnTime Tomcat Server.

Whitelist

In the folder C:\ProgramData\Intravision\OnTime\Microsoft\ - you may add a text file 'common.ini' to control redirection from the OnTime server. A missing file allows any redirection.
The common.ini file controls redirection for all auth-methods.

Entries in the common.ini file can be:

REDIRECT_WHITELIST=https://example1.com
or
REDIRECT_WHITELIST=https://ontime.example1.com

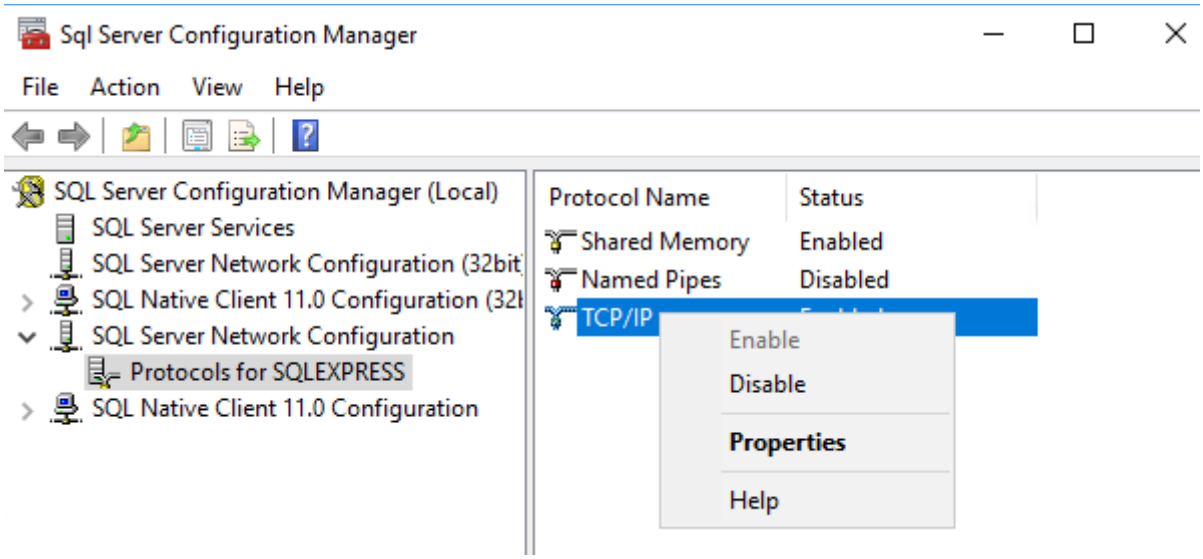
More entries require more lines like

REDIRECT_WHITELIST=https://example2.com

SQL Server network protocol setup

At the SQL Server open the ‘SQL Server 201X Configuration Manager’.

In the ‘Network Configuration’ section, choose ‘Protocols’, right-click TCP/IP and choose ‘Enable’. Click ‘OK’.



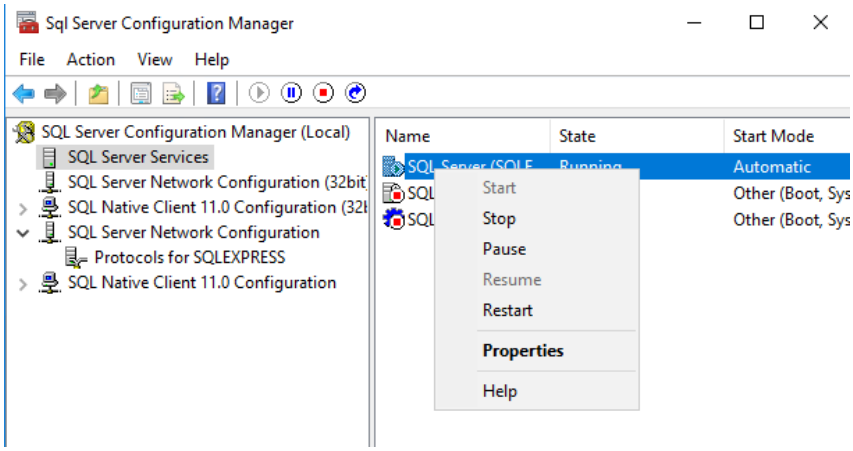
Right-click TCP/IP and choose properties.

Click ‘IP Addresses’.

Scroll down to the bottom and enter the value 1433 in the field ‘TCP Port’.

Click ‘OK’.

Restart the SQL Server Service!



External access to OnTime

In the following scenarios, OnTime is installed on a server in the internal network.

Scenario 1
If there already is a working VPN solution with reference to the internal DNS, access to OnTime will work right away.

Scenario 2
A reverse proxy server may be installed in the DMZ and configured for access to the internal OnTime server.

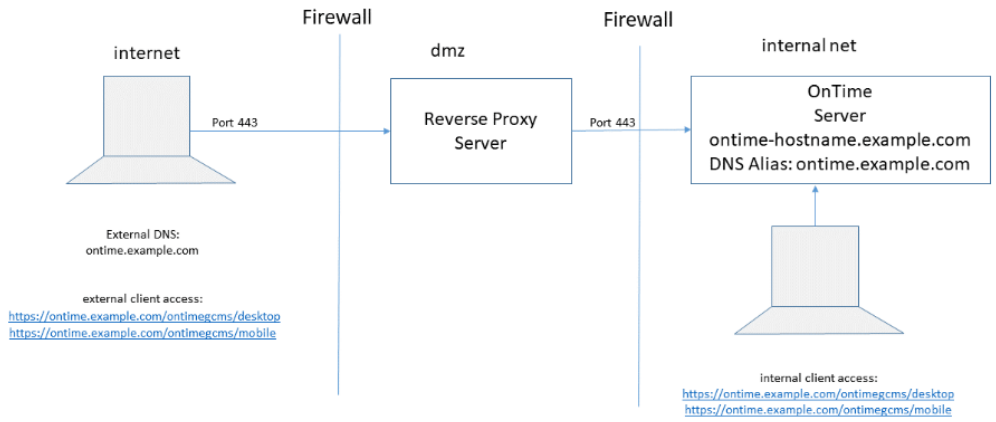
Note: The 'HTTP(S) Domain (SSO)' authentication method is not supported through a reverse proxy.

OnTime desktop and mobile clients require the following two URLs working both from the internal net and externally from the internet:
https://ontime.example.com/ontimegcms/desktop
https://ontime.example.com/ontimegcms/mobile

Note: Please insert your relevant URL instead of 'ontime.example.com'.

The external URL should be registered in your external DNS.
In your internal DNS, the OnTime server should be added as an alias for the ontime-hostname of your internal DNS reference.

Example of configuration:



In the example, the proxy server has the virtual server definition – 'ontime.example.com'
- the OnTime server has the hostname – 'ontime-hostname.example.com'

The hostname ‘ontime.example.com’ is a virtual hostname that the clients reference both externally and internally.

The port 443 is open from the proxy server to the internal OnTime server in the firewall.

Note: It is a requirement that the internal OnTime server has an SSL certificate installed – refer to the section **SSL certificates for the OnTime Tomcat Server**

Note: After the installation of the SSL certificate, it is required to change the authentication of clients to https – refer to the section Authentication.

Reverse Proxy

In this example, an Apache 2.4 HTTP server is used as a proxy server in the DMZ.

The package ‘httpd-2.4.58-win64-VS17.zip’ – with OpenSSL version 3.1.3 - may be downloaded from:

https://www.apachelounge.com/download/#google_vignette

Extract the zipped package to C:\
The Apache server files are extracted to the folder C:\Apache24

To enable the Apache server as a Windows service:

Open a command prompt as the administrator:

cd C:\Apache24\bin

> httpd.exe -k install

Running this command might request you to install ‘Visual C++ Redistributable’ from Microsoft.

Among the Windows ‘Services’ you will see a new service ‘Apache2.4’.

The configuration is done in the file C:\Apache24\conf\httpd.conf

In the example below:
- the Apache modules should be enabled by removing the hash characters
- the Server name (FQDN) is ‘ontime.example.com’, the external virtual website.
- the generation of the two certificate files referenced are described in more detail in SSL certificates for the OnTime Tomcat Server

- the ProxyPass statements include the FQDN of the internal OnTime server.

Virtual server configurations are added at the end of the file C:\Apache24\conf\httpd.conf.
Adjust the settings to your server environment:

```
###### Enable the following modules by removing the leading hash characters
#LoadModule rewrite_module modules/mod_rewrite.so
#LoadModule proxy_module modules/mod_proxy.so
#LoadModule proxy_http_module modules/mod_proxy_http.so
#LoadModule ssl_module modules/mod_ssl.so
#LoadModule http2_module modules/mod_http2.so

### Enable the following http/https ports if not already enabled above, by removing the leading hash
character
#Listen 80 http
#Listen 443 https


### Handle OnTime Group Calendar request from incoming host "ontime.example.com" to "ontime-
hostname.example.com"

<VirtualHost *:80>
### This virtual server is redirecting from http to https
        ServerName ontime.example.com
        ProxyPreserveHost on
        ProxyRequests Off
        RewriteEngine on
        RewriteCond %{HTTPS} !=on
        RewriteRule ^/?(.*) https://%{SERVER_NAME}/$1 [R,L]
</VirtualHost>


<VirtualHost *:443>
### This virtual server is mapping request for the main OnTime web applications to the OnTime Tomcat
server
### Authentication ‘Form-Based – Pass-through’
### Authentication ‘HTTP(S) Mail Auth’
### Authentication ‘HTTP(S) ADFS (SSO)’
### Authentication.’HTTP(S) Domain (SSO)’ is not supported through the proxy!!!
        ServerName ontime.example.com
        Protocols h2 http/1.1
        ProxyPreserveHost on
        ProxyRequests Off
        SSLEngine on
        SSLProxyEngine on
        SSLCertificateFile "C:\Apache24\keys\ontime-rsa-chain.pem"
        SSLCertificateKeyFile "C:\Apache24\keys\ontime-rsa-key.pem"
        SSLProtocol -all +TLSv1.2 +TLSv1.3
        <Location "/">
                ProxyPass https://ontime-hostname.example.com/
                ProxyPassReverse https://ontime-hostname.example.com/
        </Location>
        #ErrorLog logs/ontime443_error.log
        #CustomLog logs/ontime443_access.log common
</VirtualHost>
```

If you want to use the proxy server for other purposes than OnTime you may add other virtual host definitions with their own DNS names, registered in the external DNS service. But beware that the Apache HTTP server defaults to the first listed virtual server definition - if it cannot parse the URL.

The line ‘ProxyPassReverse’ preserves the URL seen in the browser.

An SSL certificate has been added to the proxy server. In this setup, a star certificate was chosen, for both the proxy server and the internal OnTime server.

An ip reference to the internal OnTime server, ‘ontime-hostname.example.com’ has been added to the ‘hosts’ file at C:\Windows\System32\drivers\etc of the proxy server (no DNS in the DMZ).

Access to OnTime - only through the reverse proxy

In case OnTime is deployed in a way that it can only be accessed through the reverse proxy, then the setup can be simplified.

It may be decided that the reverse proxy does the SSL offloading. Then the internal OnTime Tomcat server does not need to have the .pem files installed.

Note: The authentication choice of 'HTTP(S) Domain (SSO)' is not supported with the reverse proxy server for external access.

The reverse proxy needs to proxy one to two addresses, depending on which authentication method is used.

The OnTime Tomcat server by default runs on ports 80, 8080, 8443, 443 (if .pem files are present). The reverse proxy can be configured to proxy the calls to port 8443 – recommended, or 8080.

Example configuration:

```
<VirtualHost *:443>
### This virtual server is addressing the main OnTime application on Tomcat
### Authentication 'Form-Based – Pass-through'
### Authentication 'HTTP(S) Mail Auth'
### Authentication 'HTTP(S) ADFS (SSO)'
        ServerName ontime.example.com
        ProxyPreserveHost on
        ProxyRequests Off
        SSLEngine on
        SSLProxyEngine on
        SSLCertificateFile "C:\Apache24\keys\ontime-rsa-chain.pem"
        SSLCertificateKeyFile "C:\Apache24\keys\ontime-rsa-key.pem"
        SSLProtocol -all +TLSv1.2 +TLSv1.3
        <Location "/">
                ProxyPass https://ontime-hostname.example.com:8443/
                ProxyPassReverse https://ontime-hostname.example.com:8443/
        </Location>
        #ErrorLog logs/ontime443_error.log
        #CustomLog logs/ontime443_access.log common
</VirtualHost>
```

Mapping of directory fields

*The OnTime application looks for the UPN in the AD for the presence of 'mail OR email OR emailaddress' in this order.

OnTime Admin	EWS	AD
Upn *	EmailAddress.Address	mail OR email OR emailaddress
DisplayName	EmailAddress.Name	displayName
CompanyName	CompanyName	company
BusinessCity	PhysicalAddressDictionary[Business].City	l
BusinessState	St	st
BusinessCountryOrRegion	PhysicalAddressDictionary[Business].CountryOrRegion	co
BusinessPhone	PhoneNumberDictionary[BusinessPhone]	telephoneNumber
MobilePhone	PhoneNumberDictionary[MobilePhone]	mobile
Department	Department	Department
JobTitle	JobTitle	title
OfficeLocation	OfficeLocation	physicalDeliveryOfficeName
PhoneticDisplayName		msds-phoneticdisplayname
Capacity	(Graph call /places/microsoft.graph.room) capacity	msExchResourceCapacity
Building	(Graph call /places/microsoft.graph.room) building	
Floor	(Graph call /places/microsoft.graph.room) floorNumber	
ExtensionAttribute1		ExtensionAttribute1
ExtensionAttribute2		ExtensionAttribute2
ExtensionAttribute3		ExtensionAttribute3
ExtensionAttribute4		ExtensionAttribute4
ExtensionAttribute5		ExtensionAttribute5
ExtensionAttribute6		ExtensionAttribute6
ExtensionAttribute7		ExtensionAttribute7
ExtensionAttribute8		ExtensionAttribute8
ExtensionAttribute9		ExtensionAttribute9
ExtensionAttribute10		ExtensionAttribute10
ExtensionAttribute11		ExtensionAttribute11
ExtensionAttribute12		ExtensionAttribute12
ExtensionAttribute13		ExtensionAttribute13
ExtensionAttribute14		ExtensionAttribute14
ExtensionAttribute15		ExtensionAttribute15

Configuring private settings for Rooms

Overview

In response to feedback regarding the visibility of meeting subjects in rooms designated for private meetings, OnTime developers recommend a specific configuration to ensure the privacy of such meetings. By default, the privacy setting of incoming meeting requests for a room is deactivated upon booking, making the meeting visible to others. This section provides guidance on how to maintain the privacy of meetings within OnTime.

Procedure

To uphold the privacy settings of a room, ensuring that meetings designated as private remain private, administrators should execute a PowerShell command. This command explicitly retains the private status of meetings, preventing unauthorized visibility of the meeting's subject to other users.

Required Command

Utilize the following PowerShell command to preserve the privacy settings of a room:

```
Set-CalendarProcessing -Identity "Room" -RemovePrivateProperty $False
```

Replace "Room" with the actual name of the resource (room) you intend to configure. This command prevents the clearing of the private flag on incoming meeting requests for the specified room, thereby ensuring the meetings stay private as intended.

Important Notes

Execution Rights: Ensure you have the appropriate administrative rights to execute PowerShell commands within your OnTime environment.

Identity Parameter: The Identity parameter uniquely identifies the room whose settings you wish to configure. It should be replaced with the name of the room as recognized by OnTime.

Impact of the Command: This configuration affects all future meeting requests for the specified room, ensuring their private status is maintained upon booking.

Reference

For further details on the Set-CalendarProcessing command and its parameters, please consult the Microsoft PowerShell documentation:
Ref: https://learn.microsoft.com/en-us/powershell/module/exchange/set-calendarprocessing?view=exchange-ps