for Microsoft

Installation & Configuration Manual
OnTime® for Microsoft version 6.1.x

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

© IntraVision ApS,

IntraVision

OnTime® for Microsoft

Installation Manual

The main audience for this manual is Microsoft administrators with proper experience in Windows Server and Exchange on-premises / Office 365 administration. It is therefore expected that the reader of this manual is no stranger to 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 Office 365 11
Ports for Exchange on-premises 11
The ports for the Exchange server must be open for port 443 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 18
Manual installation 20
Command-line scripts 20
Create the OnTime database at the SQL server 21
Pollarity 31
Catering 33
Visitor 35
OnTime Server 37
OnTime addon products 37

OnTime Configuration 38
Office 365 threads 38
OnTime Setup 39
Dashboard 40
Database 42
Local SQL server 42
External SQL server, same Windows domain 43
External SQL server, outside the Windows domain 43
License key 44
Domains 45
Authentication 45
Add Domain 46
Register OnTime in 'Microsoft Entra ID' 47

On-Premises configuration *50*
Source *53*
Source, LDAP *54*
Field Mapping *56*
Add/Edit Domain - Advanced *57*
Synchronisation settings *57*
Global Settings 58
Backend *58*
Frontend *60*
Name Formats *69*
Default Settings *71*
Roles *80*
Users 83
Members *83*
API Users *90*
Combined Rooms *91*
Groups 92
Directory Groups *92*
Static Groups *93*
Dynamic Groups *95*
Linked AD Groups *97*
Legend 99
Definition *101*
Appearance *102*
Importance *102*
Languages *102*
Pollarity 103
Configuration of Pollarity *104*
Catering 105
Administering Catering *106*
URLs for 'Catering Manager' *107*
Visitor 108

OnTime User – Calendar 110
OnTime client Web Desktop 110
OnTime client Web Mobile 111

Add-ins for OnTime 112
Add-in for OnTime in MS Teams 113
Teams config.html at your OnTime server *114*
User setup for MS Teams *115*
Add-in for OnTime in MS Teams Rail 116
User setup for MS Teams rail *116*
Add-ins for OnTime in Outlook 117
OnTime in Outlook *118*
OnTime Pollarity - add-in in Outlook *118*
Upload of add-ins for OnTime 120

Integrating OnTime Group Calendar with other systems 122
Integrating and launching OnTime from other solutions using custom URL´s *122*
Creating Integrations with OnTime Desktop *124*
Creating Integrations with OnTime Mobile *130*

Logfiles **133**
OnTime, Pollarity Catering, Visitor Logs *133*
Trace Communication **134**
Appendices **135**
OnTime server components and ports 135
Redirection whitelists 136
CORS 137
SSL certificates for the OnTime Tomcat Server 138
SSL certificates for the OnTime Auth Service 140
SSL root certificates for the OnTime server 142
OnTime Authentication Token 143
OnTime Domain Authentication (SSO) 144
Browser setup for SSO 146
ADFS login (SSO) 147
ADFS login (SSO) in Azure *147*
ADFS login (SSO) on-prem *148*
ADFS - at the OnTime server *150*
Whitelist 151
SQL Server network protocol setup 152
External access to OnTime 153
Reverse Proxy *154*
Access to OnTime - only through the reverse proxy *157*
Mapping of directory fields 158

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 you with a rich graphical interface and simple access.

OnTime presents other users calendar info 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 Outlook calendar.

We offer the following Clients and Interfaces:

- OnTime Web Desktop
- OnTime Add-in for MS Teams
- OnTime Add-in for 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 – Licenced 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 Teams, Outlook etc. We highly recommend running OnTime with secure communication.
Ref. to **SSL certificates for the OnTime Auth Service**

Note: Self-signed OnTime server certificates are not supported.

OnTime API

If you have developed calendar applications based on the OnTime API ver. 1, you must adapt the applications to API ver. 2.
OnTime API ver. 1 is no longer supported.

Pollarity

Pollarity is an optional module which supports voting for the best 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 timesaving 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 timesaving 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 install process.

We will then move on to the actual installation and configuration of your new OnTime environment.

The actual installation process may be done as a 'Quick installation' or as a 'Manual installation'.

Quick installation
- an MSSQL server 2019 Express database server is installed at the OnTime server

Manual installation
- more details are described, including the use of an MSSQL server installed externally to the OnTime server.

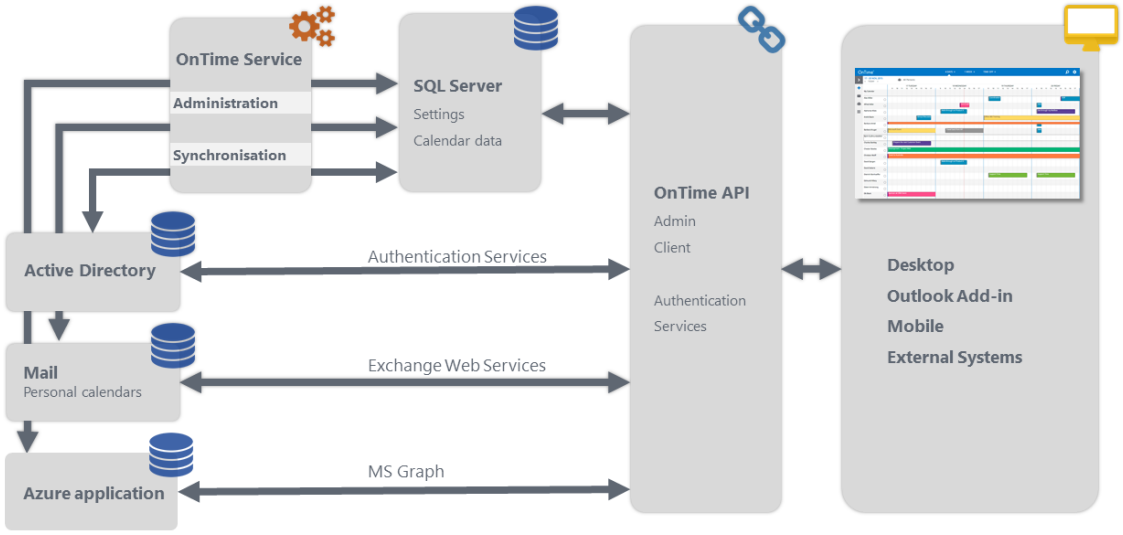
OnTime configuration
- the 'OnTime Admin Center' with the 'Dashboard' for stopping and starting the different processes in the backend
- configuration of user synchronisation
- different types of groups of users.

OnTime clients
- Web Desktop Client, MS Teams, Web Mobile Client and an add-in for 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 server requirements are based on our experience from several installations. Please bear in mind that in some cases other factors such as backup, anti-virus may affect the performance of the server and must be factored in.

OnTime must be installed running as a Windows administrator.

The OnTime installation is supported on
- Windows 2016 and 2019 with Microsoft SQL Server® 2019 Express
- Windows 2012 R2 and 2016 with Microsoft SQL Server® 2016 Express
- or Windows Server 2008 R2 with Microsoft SQL Server® 2014 Express
- we do not support Windows 2008 R2 running on Itanium CPUs

For small and medium-sized installations of OnTime, you can use Microsoft SQL Server® 2014, 2016, 2019 Express which are free. By default, 2019 is installed. We recommend using the full Microsoft SQL Server if your OnTime installation has more than 2.000 users. You can read about the limitations and requirements here https://www.microsoft.com/en-us/download/details.aspx?id=42299

Processor

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

RAM

Minimum of 4 GB Ram dedicated for the OnTime solution

If you are running OnTime on a Hyper V configuration, then you need to configure it to use static memory for the SQL Server to perform properly.

Hard Disk Space

Minimum of 20 GB hard drive dedicated to the OnTime solution

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 multipurpose 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 exclusive for OnTime and can serve no other applications.

Ports for the OnTime server

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

Ref. to **OnTime server components and ports.**

Ports for Office 365

If OnTime configuration for Office 365, please check ports outwards through the firewall (port 443) from the OnTime server:

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

Ports for Exchange on-premises

The ports for the Exchange server must be open for port 443

Prerequisites

AD domain

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

SQL Server 2014, 2016, 2019 Express or an existing MS SQL Server must be available.

The SQL Server Express may be downloaded from Microsoft. It is free.
Limitations: Microsoft SQL Server Express supports 1 physical processor, 1 GB memory, and 50 GB database storage

Create a user for OnTime in MS Exchange/Office 365

Mailbox user (minimum type 1, if in Office 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 user:
Refer to **OnTime client Web Desktop**
- the following browsers are supported:

	Chrome (Latest)	Safari (Latest)	Firefox (Latest)	Edge Chrominum (Latest)	Internet Explorer 11 (Latest)
Windows	Supported	N/A	Supported	Supported	Not Supported anymore
macOS	Supported	Supported	Supported	Supported	N/A

For the Catering and Visitor manager clients:
- the following browsers are supported:

	Chrome (Latest)	Safari (Latest)	Firefox (Latest)	Edge Chrominum (Latest)	Internet Explorer 11 (Latest)
Windows	Supported	N/A	Supported	Supported	**Not** supported
macOS	Supported	Supported	Supported	Supported	**N/A**

Note: The Catering Manager and the Visitor Manager are NOT supported in the Internet Explorer.

For the admin client
- the following browsers are supported:

	Chrome (Latest)	Safari (Latest)	Firefox (Latest)	Edge Chrominum (Latest)	Internet Explorer 11 (Latest)
Windows	Supported		Supported	Supported	**Not** supported

Only port 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 (8 and later)	Supported	
iOS (13.6 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

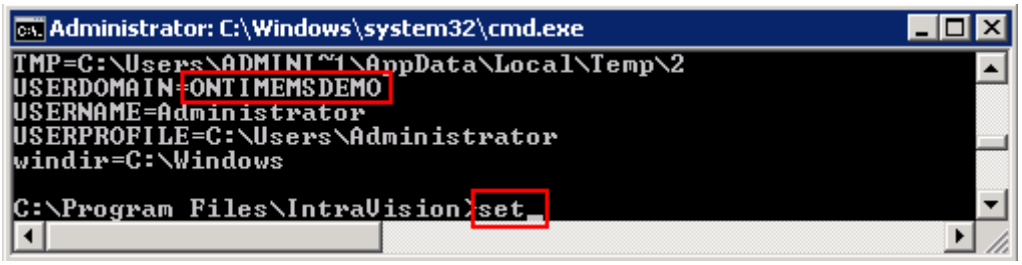
- OnTime requires a license key with the required number of users enabled to run.
- These keys are delivered directly by IntraVision or an OnTime Partner.
- A list of OnTime Partners is available at www.ontimesuite.com.

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 see your **'USERDOMAIN'**



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

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

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

OnTime Installation

We have two options for installing OnTime, quick or manual.

Quick installation

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

An MS SQL Server 2019 Express with scripts for a silent install may be downloaded from this download link:
http://file.ontimesuite.com/SQLExpress

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 get the proper permissions to run queries against the OnTime database.

Manual installation

Is 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 expects:

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

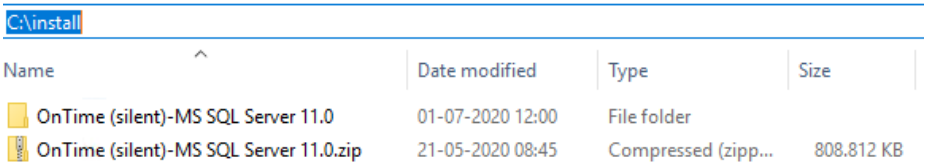
- Integrated Security is used, instead of SQL Server Security

- 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 http://file.ontimesuite.com/SQLExpress



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

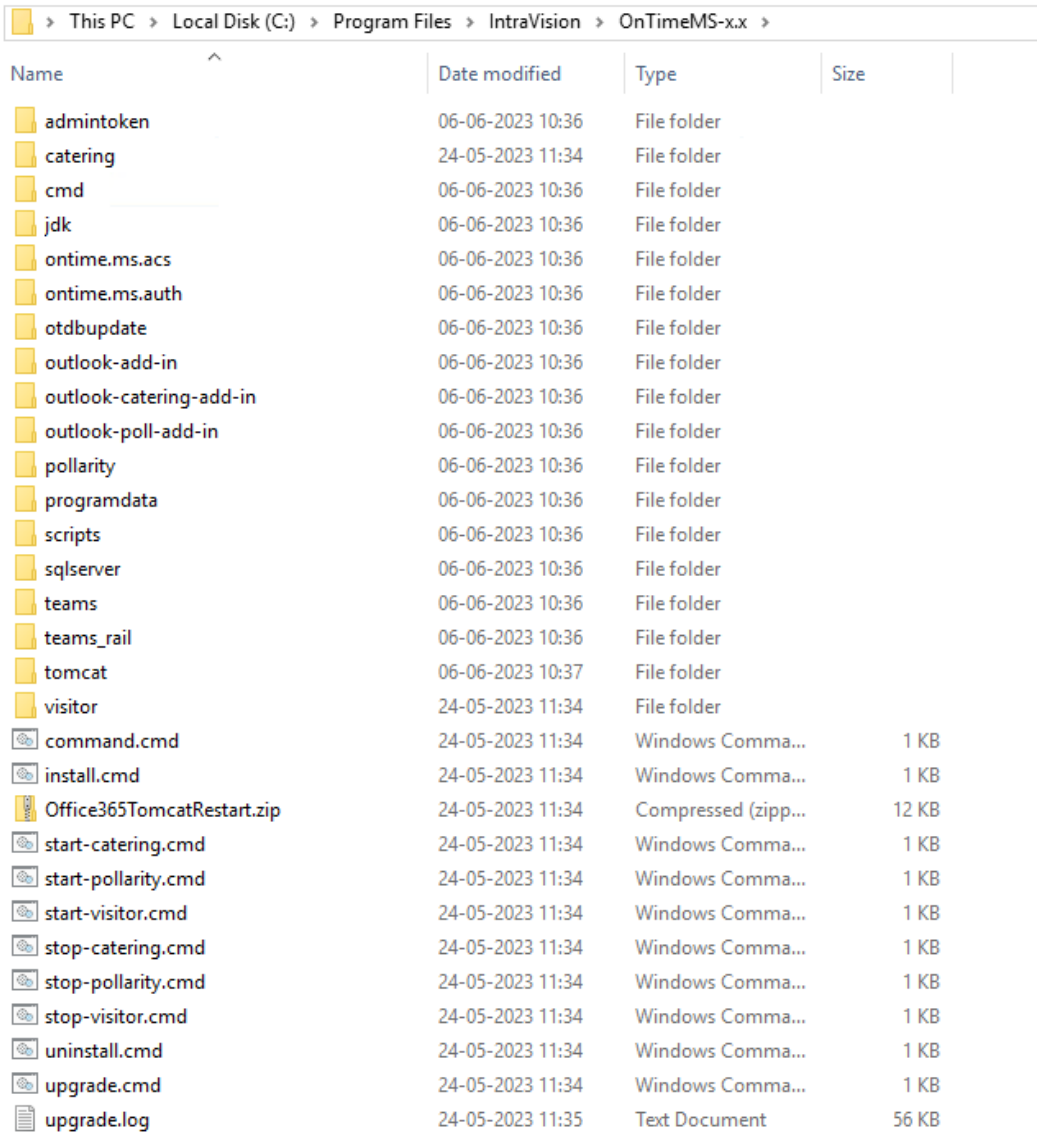
This command will silently install the SQL server.
A log file, 'installLog.txt' from the installation is created in the folder.

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

Result:
The SQL Server is installed in the 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 unwilling 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 licence.
8. It will create a database, 'catering' for Catering
9. It will create a database, 'visitor' for Visitor

Note: Pollarity, Catering, Visitor has each an optional licence.
Proceed to **OnTime Configuration.**

Manual installation

All the components may be configured after the usual Quick Installation completion. 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 SQLServer, the default port is 1433. If you want to use another port, remember to enter your chosen port in the OnTime Admin clients Database section.
Refer to the **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

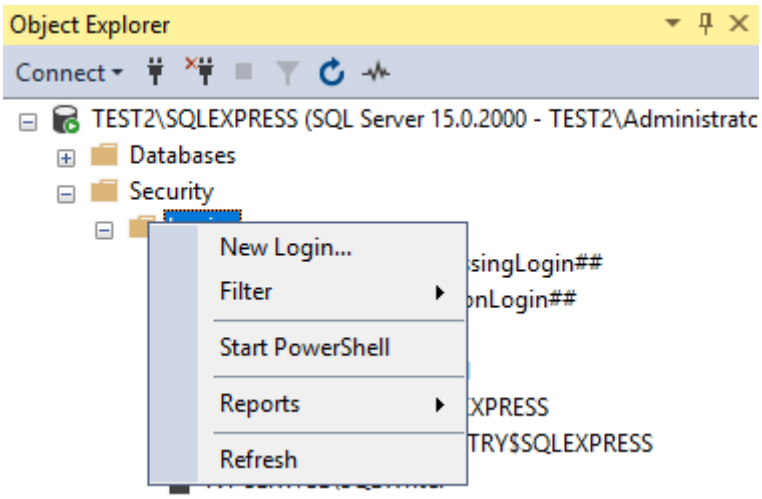
SQL Server network protocol setup.

'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, we need an administrative user, 'BUILTIN\Administrators' with the database role 'db_owner'.

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

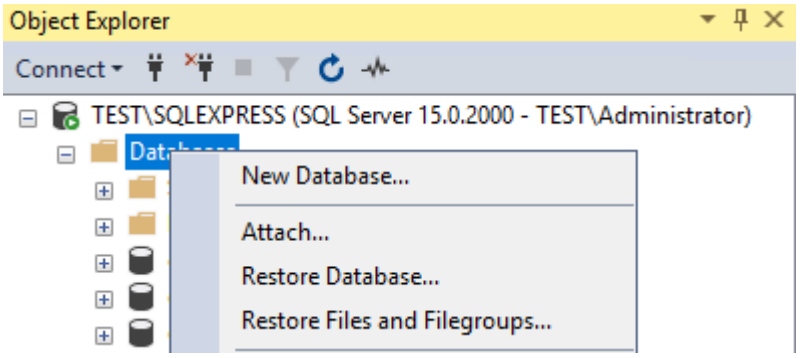


Enter the login name 'BUILTIN\Administrators'

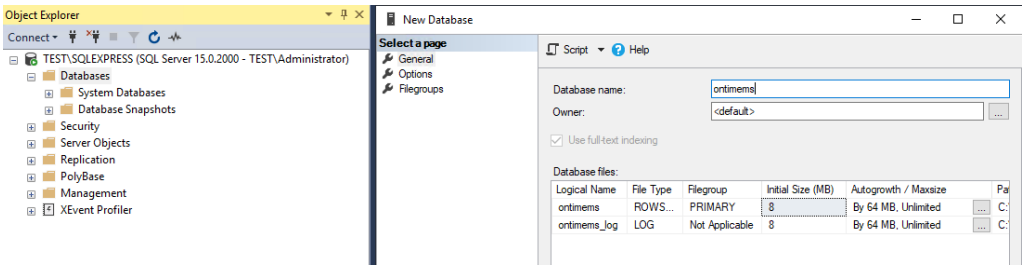
Click 'OK'

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'

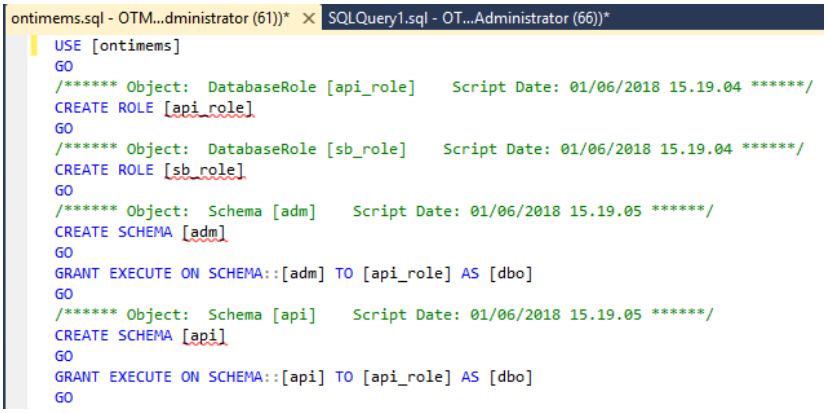


Click 'New database'. Enter the database name 'ontimems'. Click 'OK'



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 programmatical parameter for the database name.



Two methods are posssible 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
   ```

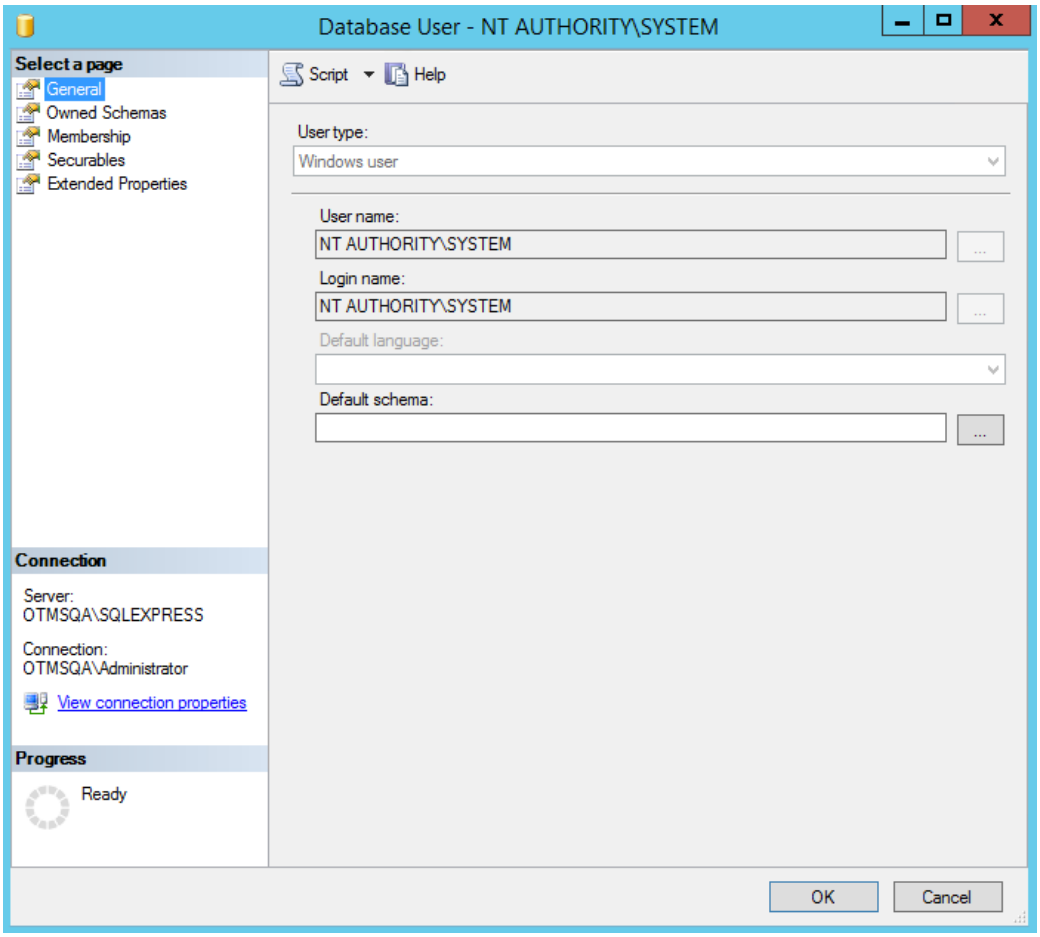
   - here SQLExpress is representing your SQL server's instance.

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

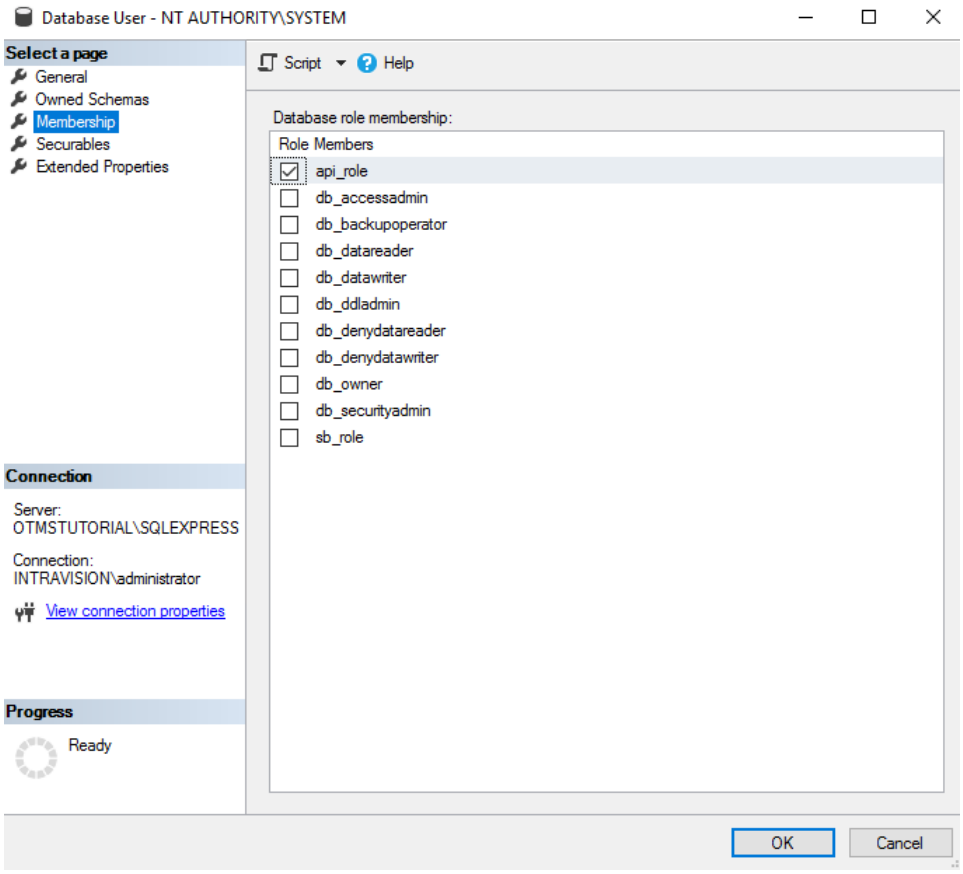
The OnTime application user, local SQL Server

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 'User name' field. Click 'OK'.



2. Click 'Membership' and select the 'api_role'. Click 'OK'.



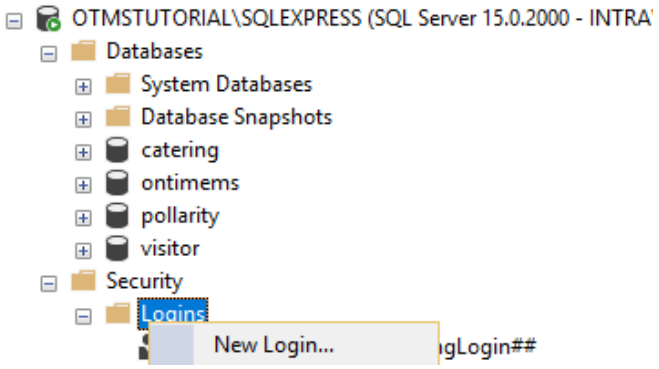
3. A configuration with the ‘NT AUTHORITY SYSTEM’ ensures that you may choose ‘integratedSecurity=yes’ in the database configuration.

   Please refer to **Database** in the 'OnTime Configuration' section.

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

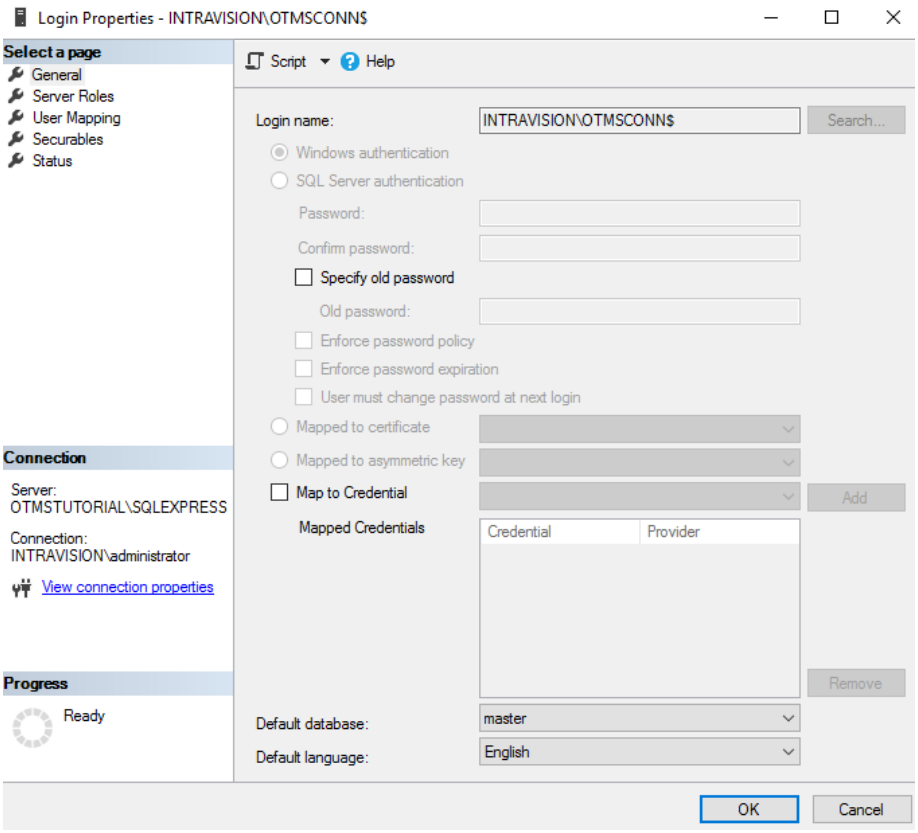
The OnTime application user, external SQL Server, same Windows Domain

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

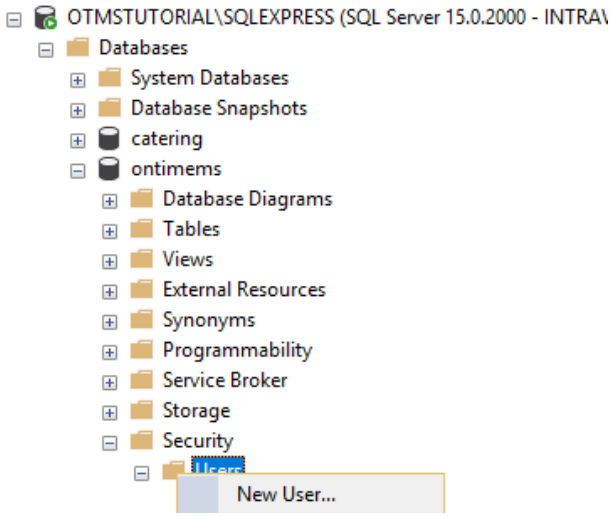


1. As 'Login name' you manually enter your OnTime servers hostname in the format: DOMAINNAME\HOSTNAME$
   - remember the '$' character at the end of the server's hostname.
   In the SQL server, this name is for authenticating your OnTime server.
   Note: Searching for the hostname is not possible – the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

   Example:



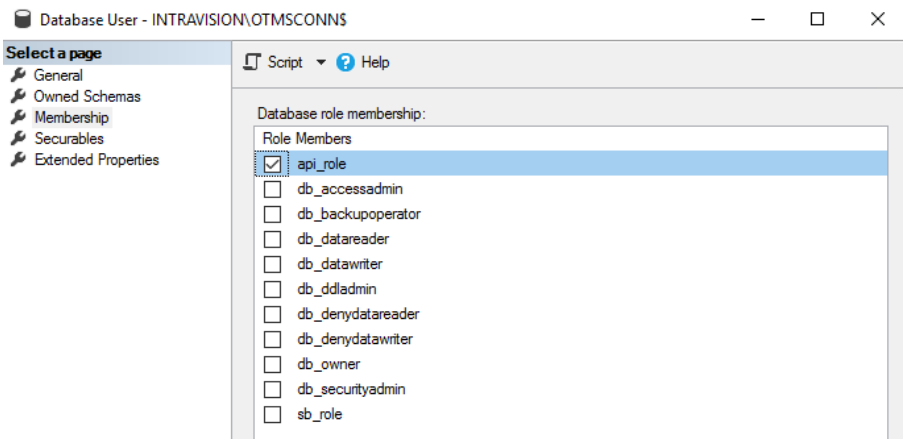
2. In the Security section of your new OnTime database, right-click Users, choose ‘New User’.



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

Copy the 'Login name' to the field 'User name'. Click OK

3. The server Login entry must have the role ''api_role'



Click 'OK'

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

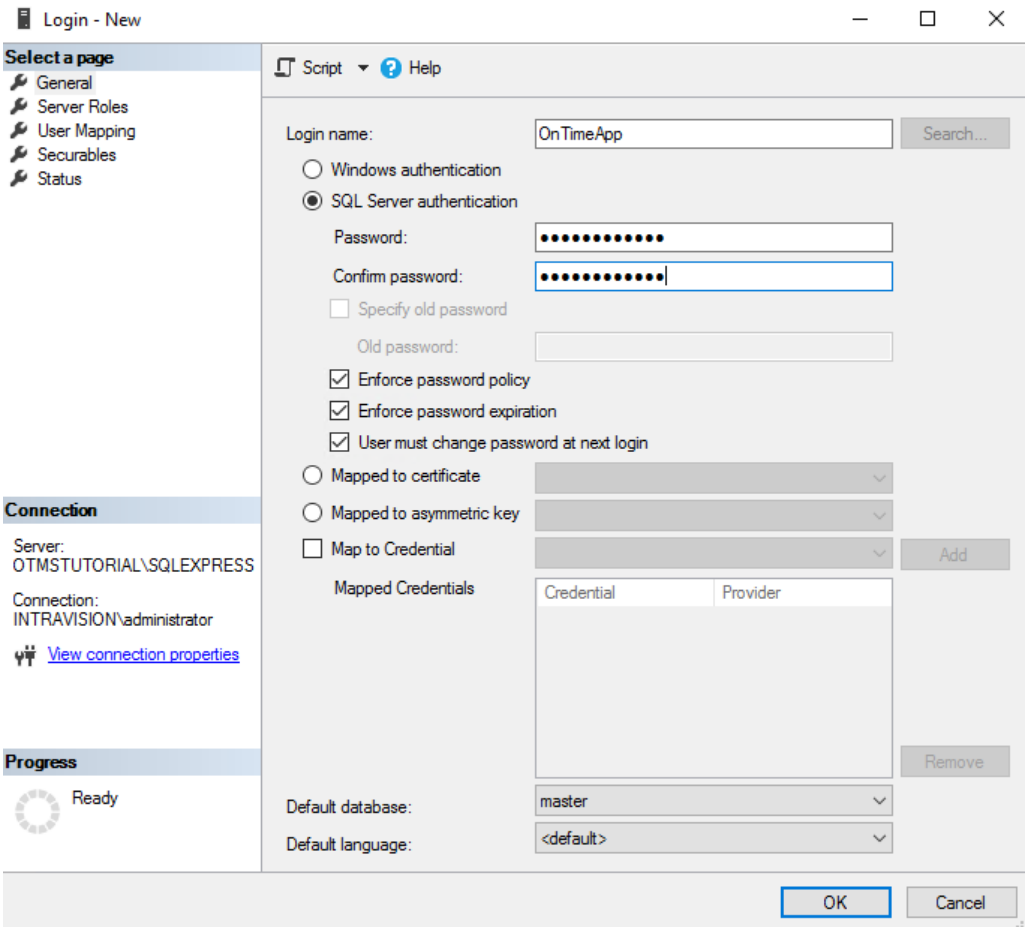
5. The database is now ready for access with 'Integrated Security' from the OnTime server within the same domain.
Please refer to **Database** in the 'OnTime Configuration' section.

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:

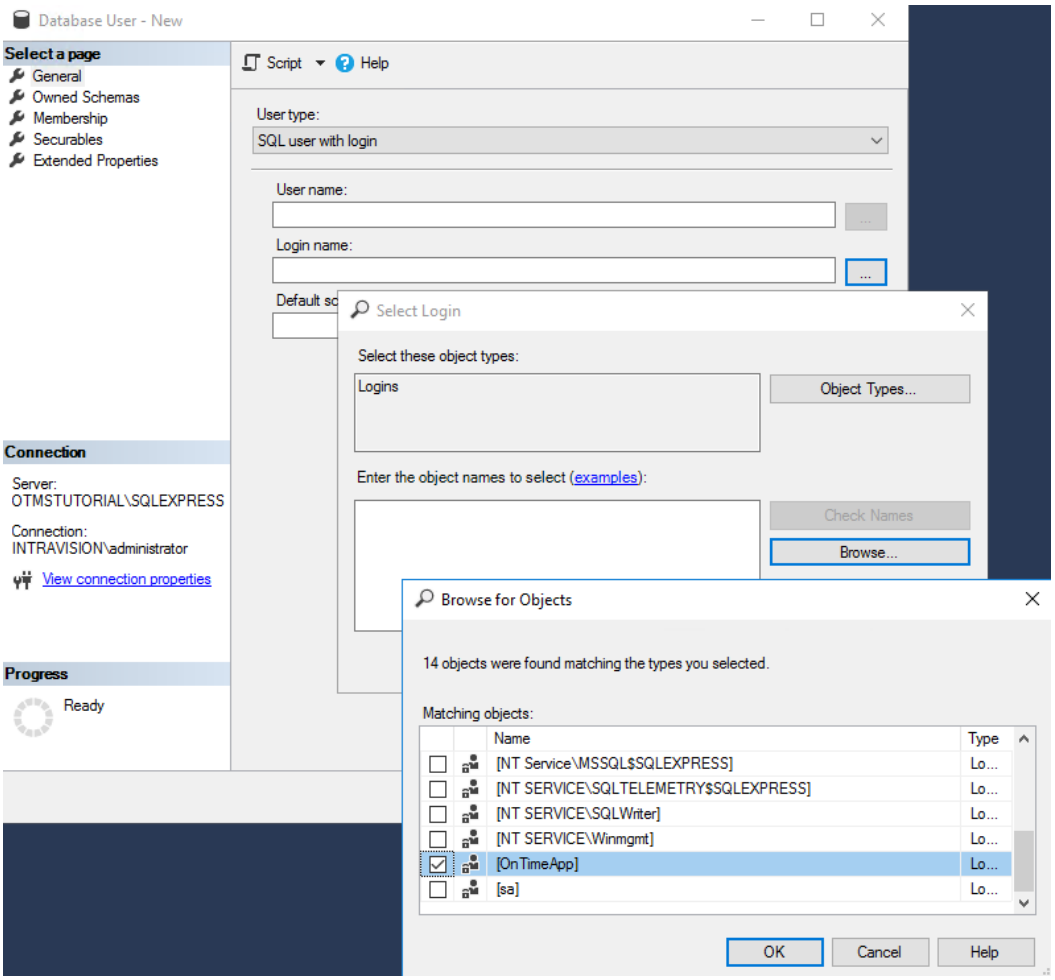
https://docs.microsoft.com/en-us/sql/database-engine/configure-windows/change-server-authentication-mode?view=sql-server-ver15

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. Take a note of the password. Click 'OK'

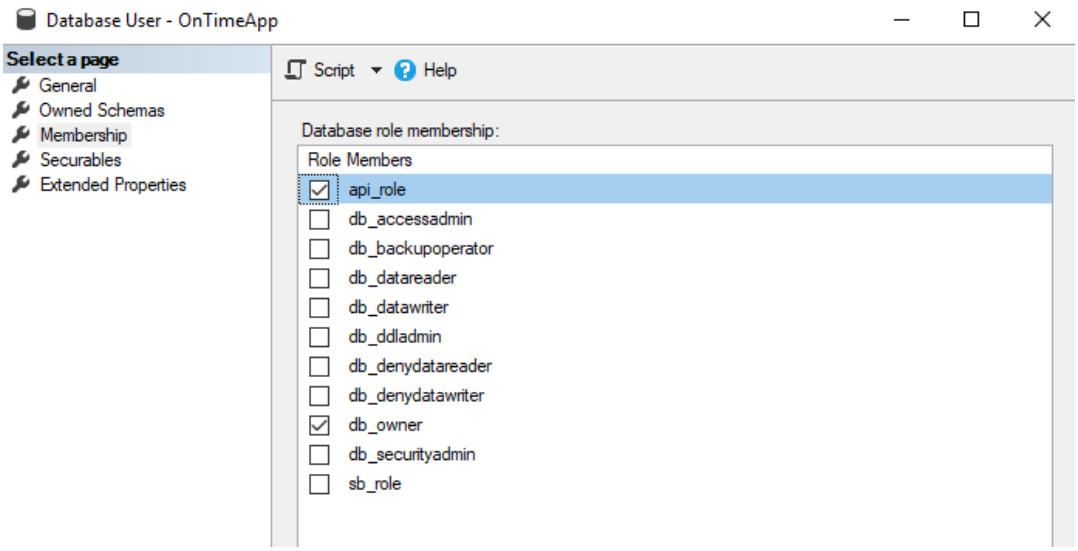


2. In the Security section of your new OnTime database, right-click Users, choose ‘New User’.

   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 'User name' field. Click 'OK'



3. Right-click your 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.

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 in one line!

This 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 in one line!

Pollarity

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

Pollarity database

Depending on you 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', tick 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 in one line!

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 in one line!

Pollarity application

1. Copy Pollarity files to the Tomcat server. This is 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 9.0 OnTimeTomcat'.

Catering

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

Catering database

Depending on you setup of the SQL server, local or external to the OnTime server the process is similar like 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 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\catering\otdbupdate`

Depending of 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 in 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 in 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 9.0 OnTimeTomcat'.

Visitor

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

Visitor database

Depending on you 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 in 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 in 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 9.0 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 9.0 OnTimeTomcat'.

The Auth service for OnTime is now running within Windows Services as 'OnTimeMS Auth'.

OnTime addon products

If you have licenses for the OnTime addon 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

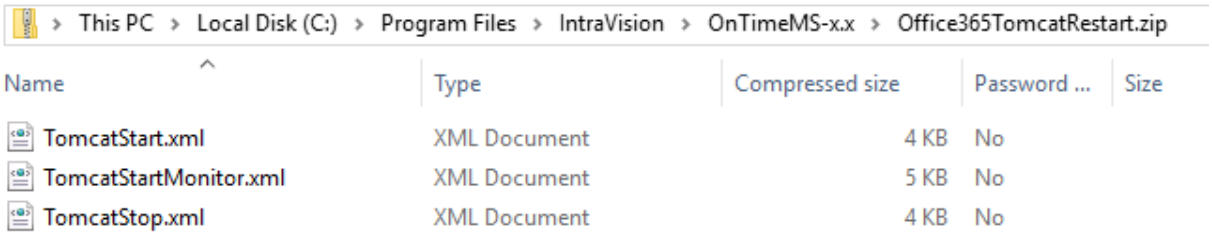
OnTime Configuration

Office 365 threads

If you are going to synchronise calendar information from “Office 365” it is recommended to restart the Tomcat webserver service regularly or even once every night. It helps to reduce the number of threads collected, referencing mailboxes that may be moved by Microsoft between different Exchange servers in the cloud.

Note - This is not necessary with Exchange servers “on-premises”.

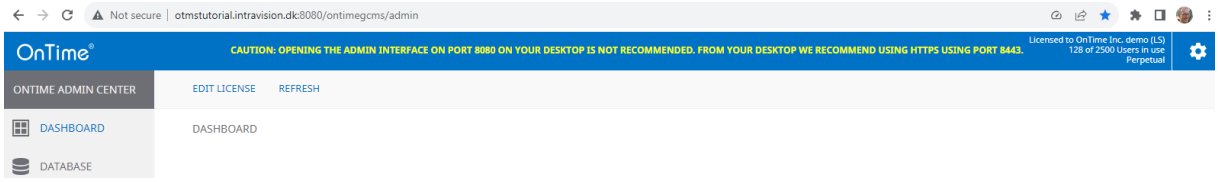
XML scripts for the Windows ‘Task Scheduler’ are included in the install package to help you with the scheduled restart.



OnTime Setup

From a browser - Open the administration URL –
https://ontime.example.com:8443/ontimegcms/admin
- or only on localhost, at the OnTime server!
http://127.0.0.1:8080/ontimegcms/admin

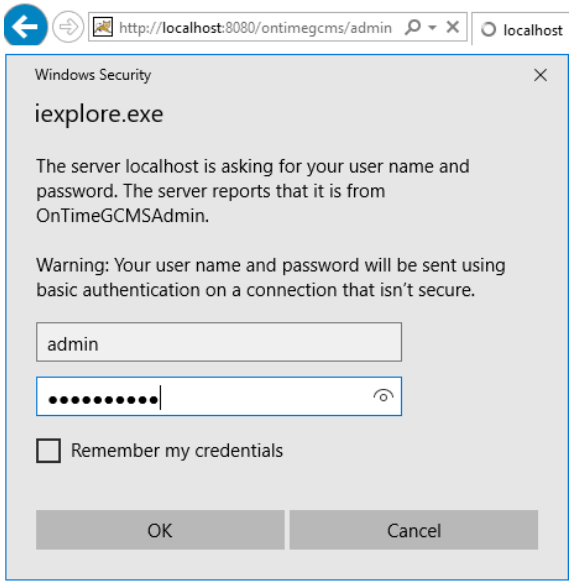
Note: Please insert your relevant URL instead of 'ontime.example.com'.
If you try administration remotely, http and port 8080, to the OnTime server you will get a yellow warning: 'Caution: Opening the admin interface on port 8080 is not recommended …'



Administrator: admin (beware of the casing, no capitals)

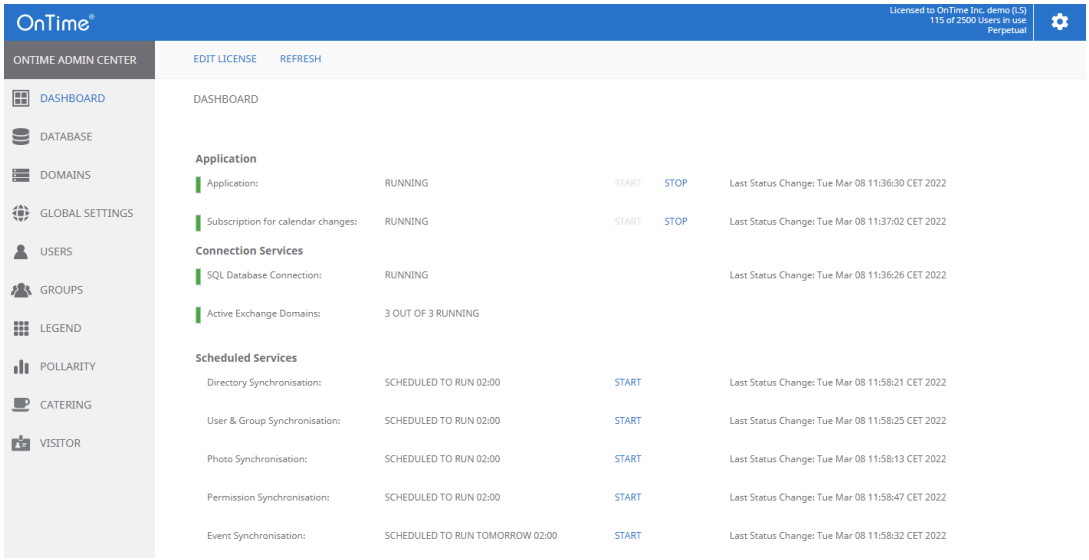
Password: ***** (your password from the OnTime installation phase)

Reset of 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 make the Tomcat service unwilling to start



Dashboard

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



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

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

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 on-demand to reflect changes at once.

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

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

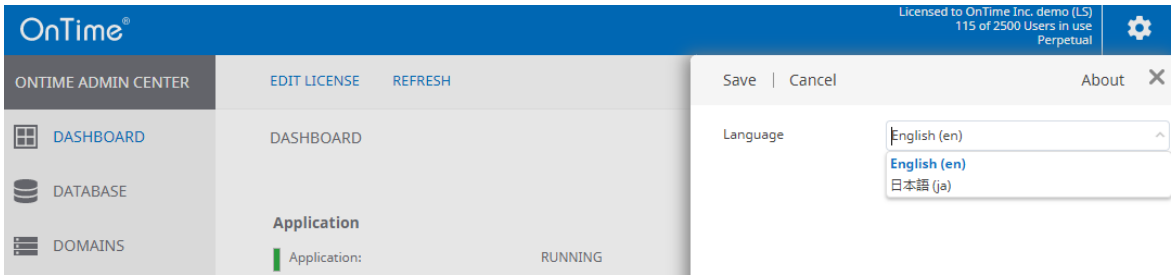
Photo Sync imports the users’ photos/avatars from the Exchange 2013 server

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

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

Administration of OnTime in Japanese is supported

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



Database

Local SQL server

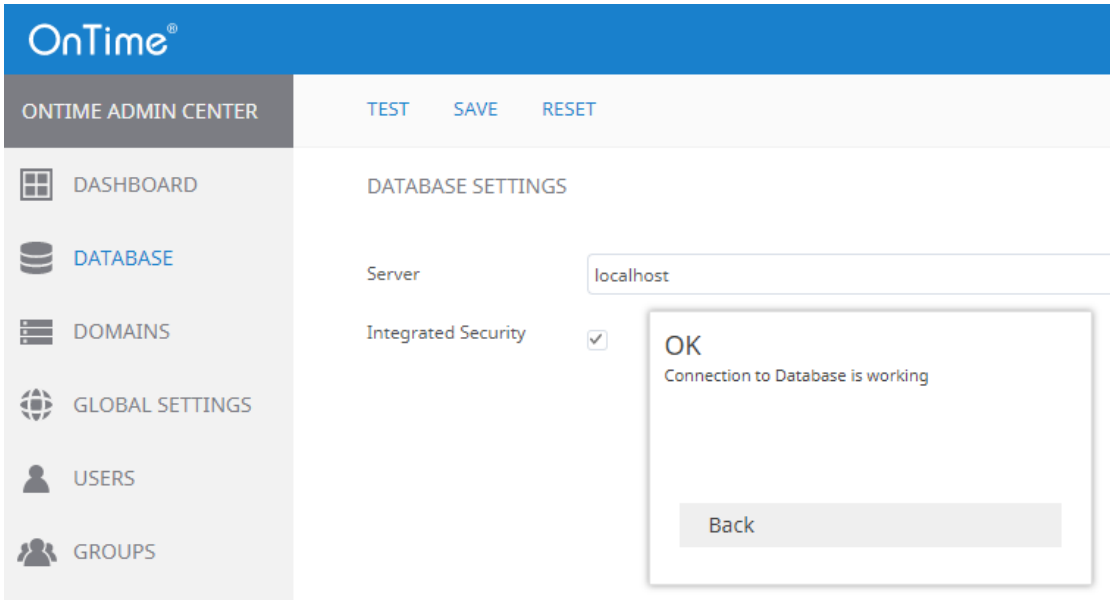
In the web admin interface, “OnTime Admin Center”, click “Database”.

If you have followed the ‘Quick installation path’ the fields are already populated with Server, ‘localhost’ and 'Integrated Security', ticked.

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

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

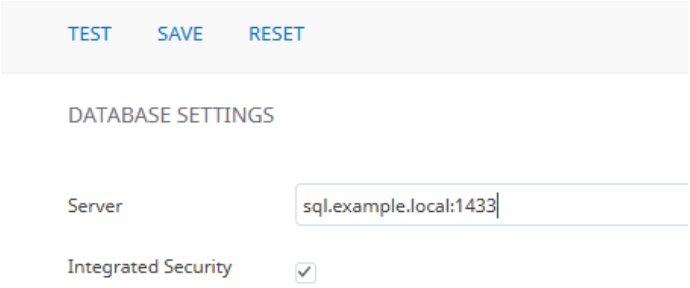
Click Save.



If you have the SQL server external to you OnTime server we have two cases:

External SQL server, same Windows domain

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



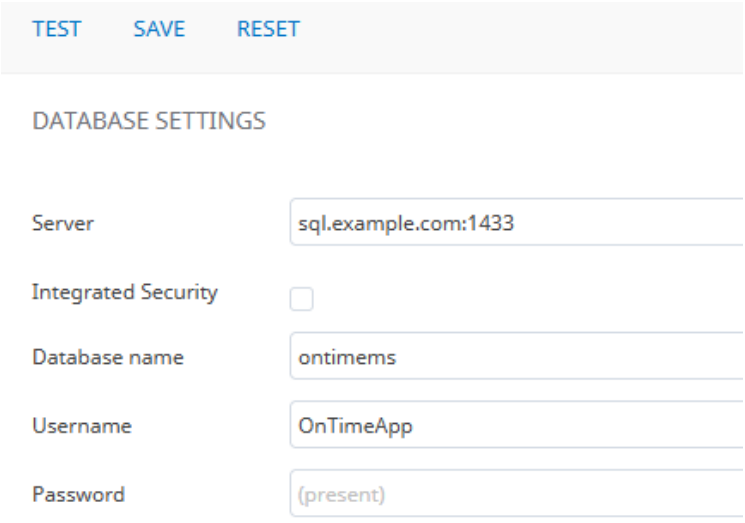
External SQL server, outside the Windows domain

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

Deselect the 'Integrated security' setting.

Enter the database name 'ontimems'

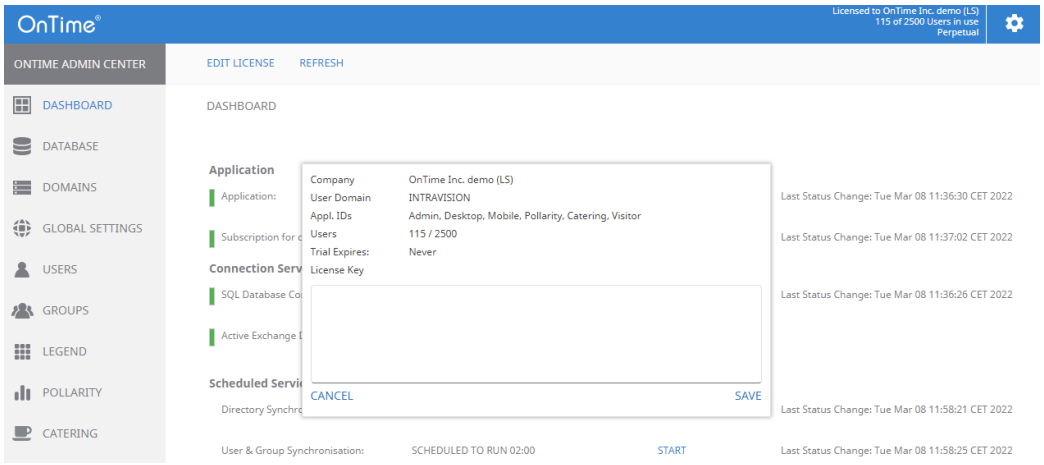
Enter username, OnTimeApp and the corresponding password



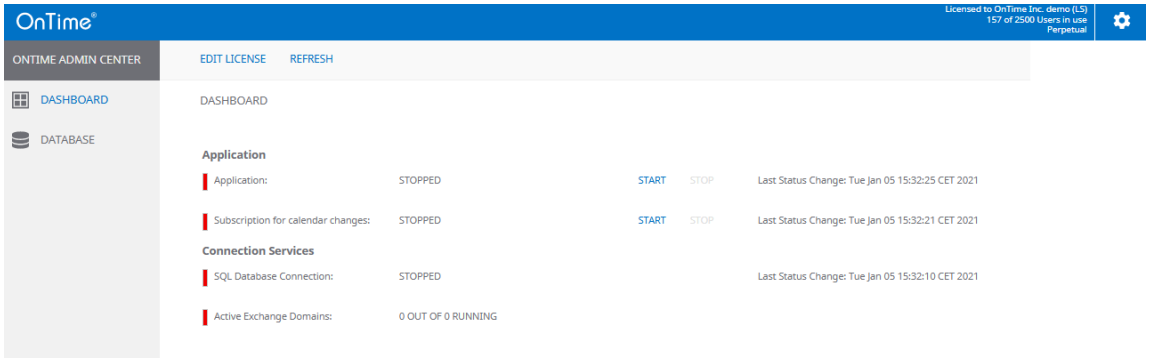
License key

Click ‘Dashboard’

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



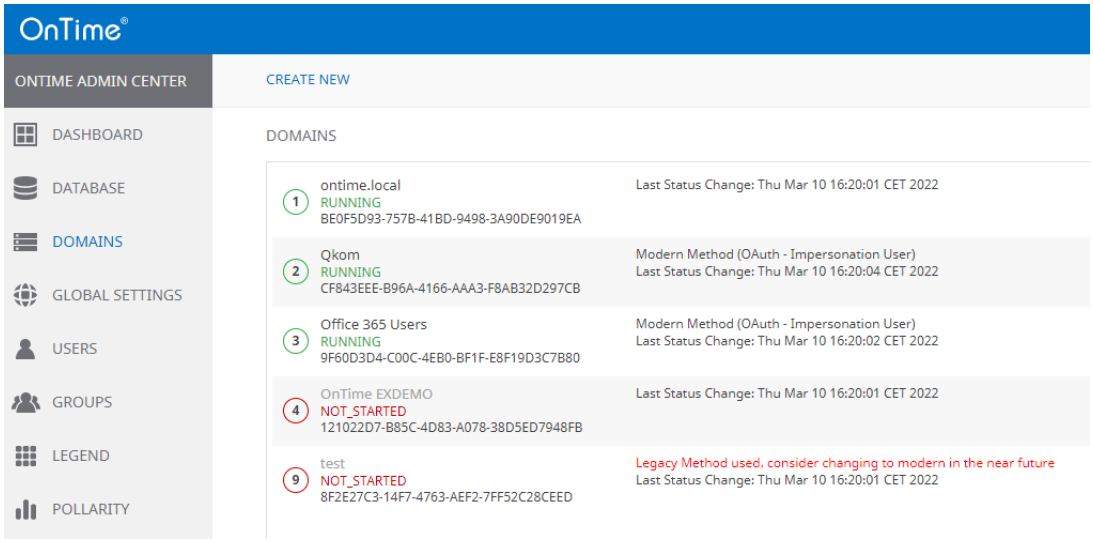
In the ‘Dashboard’ click ‘Start’ at ‘Subscription’ – the state colour should change into green.



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 from before 2.8 you will see an entry ‘Imported Domain’, it represents the single domain configuration from before the upgrade.

Authentication

OnTime supports three authentication method in Office 365:

1. OAuth – Client Credentials
2. Oauth – Impersonation User
3. Basic authentication.

If you connect to MS Exchange Online, Microsoft Office 365, you should choose OAuth, Microsoft recommends 'OAuth – Client Credentials' authentication – it supports multifactor authentication.

OnTime does not support multifactor authentication for the 'Oauth - Impersonation user', in Office 365.

Basic authentication is deprecated by Microsoft.

Note: Basic authentication/Form Based – Pass-through with multifactor authentication in Office 365 is not supported.

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

Note: If you choose Authentication type – Legacy Method (Basic) – you will miss details for rooms – like 'Capacity' and 'Floor' in OnTime.

Prerequisites

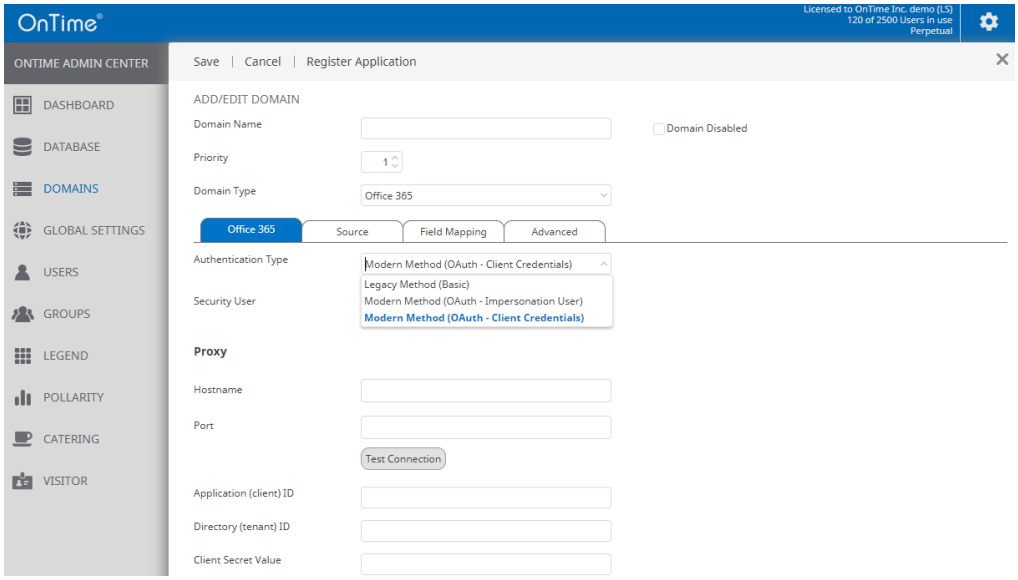
For getting data from Office 365, Azure, Graph we need access from the OnTime server to the internet - with the following url's:

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 – 'ticked' 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 'Office 365' or 'On-Premises'

Authentication Type: choose between ; Modern Method (Oauth – Client Credentials), Modern Method (Oauth – Impersonation User), Legacy Method (Basic) authentication.

Security User - This user is used by OnTime to read and edit all users calendars. Normally this username is written as an email address (UPN name). The user is created in MS Exchange/Office 365 as a mailbox user (minimum type 1, in Office 365)

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.

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 Azure Portal, look below.

Missing permissions in the Azure configuration, will be listed in red characters.

Register OnTime in 'Microsoft Entra ID'

The Oauth registering of the OnTime application in 'Microsoft Entra ID' is relevant for

Modern Method (Oauth – Client Credentials)
- and
Modern Method (Oauth – Impersonation User)

Note: We suggest Notepad as a media in-between for copying values to OnTime.

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

b) Click 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 URI', insert https://localhost: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] and [Directory (tenant) ID] into a text editor e.g. Notepad.

g) Click 'Add a certificate or secret'

h) Click '+ New client secret'

i) Add a description, such as 'OnTime Client Secret'

j) Choose expiration. Click Add

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

l) Click 'Authentication' tab. Tick 'Access Tokens'. Click 'Save'.

m) Copy the three values from 'Microsoft Entra ID' in the text editor into the page 'OnTime Admin Center' –
'Domains Add/Edit Domain/Authentication'.

n) Click 'API permissions' tab. Click 'Add a permission'.

o) Click 'Microsoft Graph'

p) Click 'Application permissions'

q) The following ‘API permissions’ have to be ticked, type a few letters in the Search field and tick the five permissions:
`Calendars.ReadWrite, Directory.Read.All, MailboxSettings.ReadWrite, People.Read.All, Place.Read.All, User.Read.All,`

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

r) Click 'Add a permission'.

s) Click 'Microsoft Graph'

t) Click 'Delegated permissions'

u) Search for EWS, tick:
`EWS.AccessAsUser.All`

v) Click 'Add a permission'

w) Click 'APIs my organization uses'

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

y) Click 'Office 365 Exchange Online

z) Click 'Application permissions'

aa) Tick 'full-access_as_app'

bb) Click 'Add permissions'

cc) Click 'Grant admin consent for "your company"
Click 'Yes' to answer the question ' Do you want to grant consent ...'

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

ee) All done ;-)

Description of OnTime functionality by 'Microsoft Entra ID' permissions

Calendars.ReadWrite - get Online Meeting event, build Online Meeting event or add to existing event.

Directory.Read.All - used for get members for MS Teams group, get Office Location for room, get and validate current application permissions.

MailboxSettings.ReadWrite - used for automaticRepliesSetting and make it possible to get and update AutoReply for mailboxes.

User.Read.All - translate event Ids between MS Graph and MS Outlook API’s.

Place.Read.All - get room extended information like capacity.

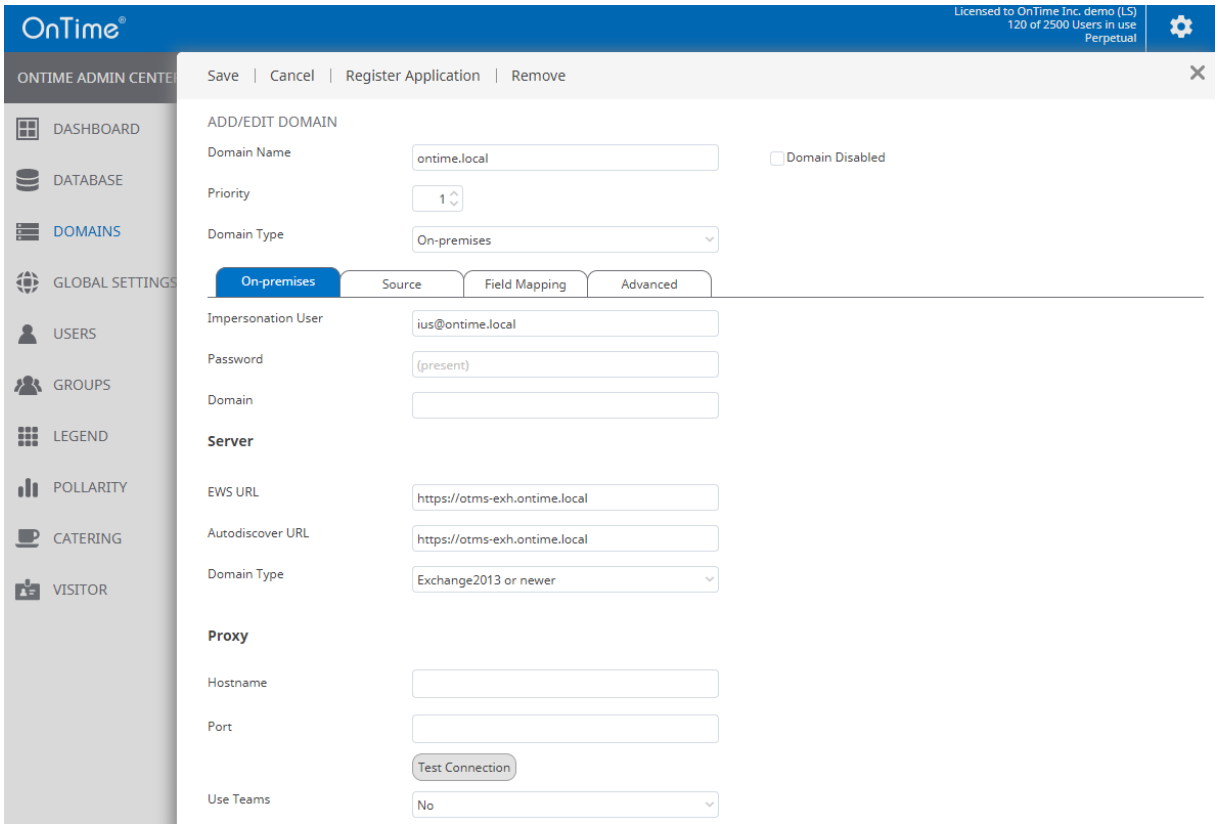
People.Read.All – used for Advanced Search.

EWS.AccessAsUser.All - Delegated permissions used for OAuth authentication functionality

On-Premises configuration

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

Note: The Exchange server has to be configured for 'Basic Authentication'.



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

Domain Disabled – ‘ticked’ 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 Office 365, the URLs must be changed accordingly, if the Exchange backend is ‘on-prem’.

‘Exchange Version’

- ‘Exchange2013 or newer’ is chosen for Exchange 2013 or newer, including Office 365
- ‘Exchange2010_SP2’ is chosen for Exchange 2010 SP2 or newer ServicePack.
    - limited support for avatars/pictures and description fields
    - no support for Show As “Working Elsewhere”.

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 – choose 'Yes' to configure Teams.
In this section it is possible to configure parameters for MS Teams

Get the values from the section below. I case you see a value in the field 'Missing parameters' you will have to recheck your parameters from 'Microsoft Entra ID' portal.

Teams registering the OnTime application in 'MS Entra ID' Portal

Note: We suggest Notepad as a media in-between for copying values to OnTime.

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'.
Populate 'Redirect URI', example https://localhost:8443/ontimegcms/code.html
Click 'Register'.

f) On next page (Overview) Copy the values [Application (client) ID] and [Directory (tenant) ID]

g) Click 'Authentication' tab. Tick 'Access Tokens'. Click 'Save'.

h) Click 'API permissions' tab. Click 'Add a permission'.

i) Click 'Microsoft Graph'

j) Click 'Application permissions'

k) The following API permission have to be ticked, type a few letters in the Search field and tick the permission
`Directory.Read.All`

l) At the bottom click 'Add permissions'.

m) Click 'Grant admin consent for "your company"

n) Click 'Yes' to answer the question ' Do you want to grant consent ...'

o) Click the 'Certificate & secrets' tab

p) Click 'New client secret'

q) Copy the value.

r) Copy the three values from 'Microsoft Entra ID' into the page 'OnTime Admin Center' –
'Domains Add/Edit Domain/Teams'.
Click Overview - in the Microsoft Entra ID portal,
Copy the values 'Application (client) ID' and Directory (tenant) ID to the according fields in 'Domains Add/Edit Domain/Authentication' page.

Click 'Save and Consent Domain'. You will get a list of the permissions accepted for your organization. Click 'Accept'.

Description of OnTime functionality by 'Microsoft Entra ID' permission

Directory.Read.All – is used to get members for MS Teams group, get Office Location for room, get and validate current application permissions.

Source

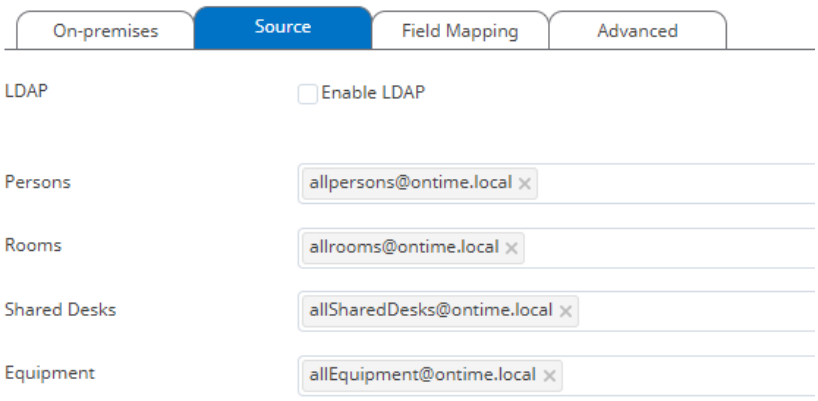
In this section, the users included in the OnTime Calendar are configured.

The users in the OnTime Calendar may be included in two ways

1. Distribution groups from the Exchange server (EWS, Exchange Web Services)
2. Via 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 calendar. The email addresses of these distribution groups are entered into the fields. More groups or individuals can be added, separated by commas.

The configuration for 'Exchange distribution groups' means that the lookup is done from the Exchange server using '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".

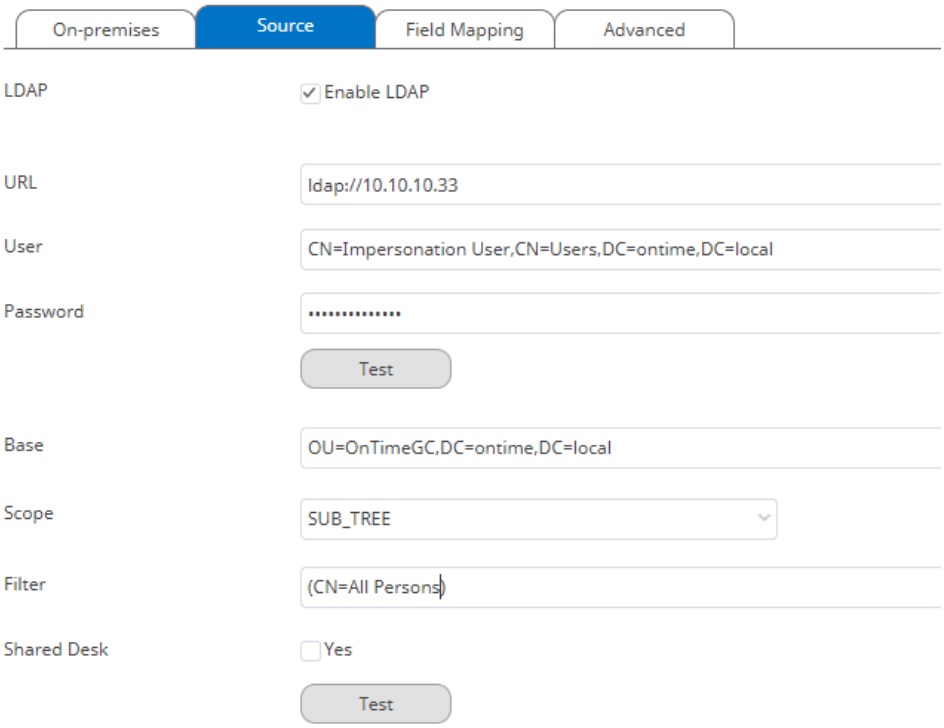
Source, LDAP

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 'LDAPS' to ensure a secure connection to Active Directory. This way you also support if the domain controller is setup 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. Press 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 Desk are included by including a Base reference to a group, like 'All Shared Desks' an 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)
```

Press 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.

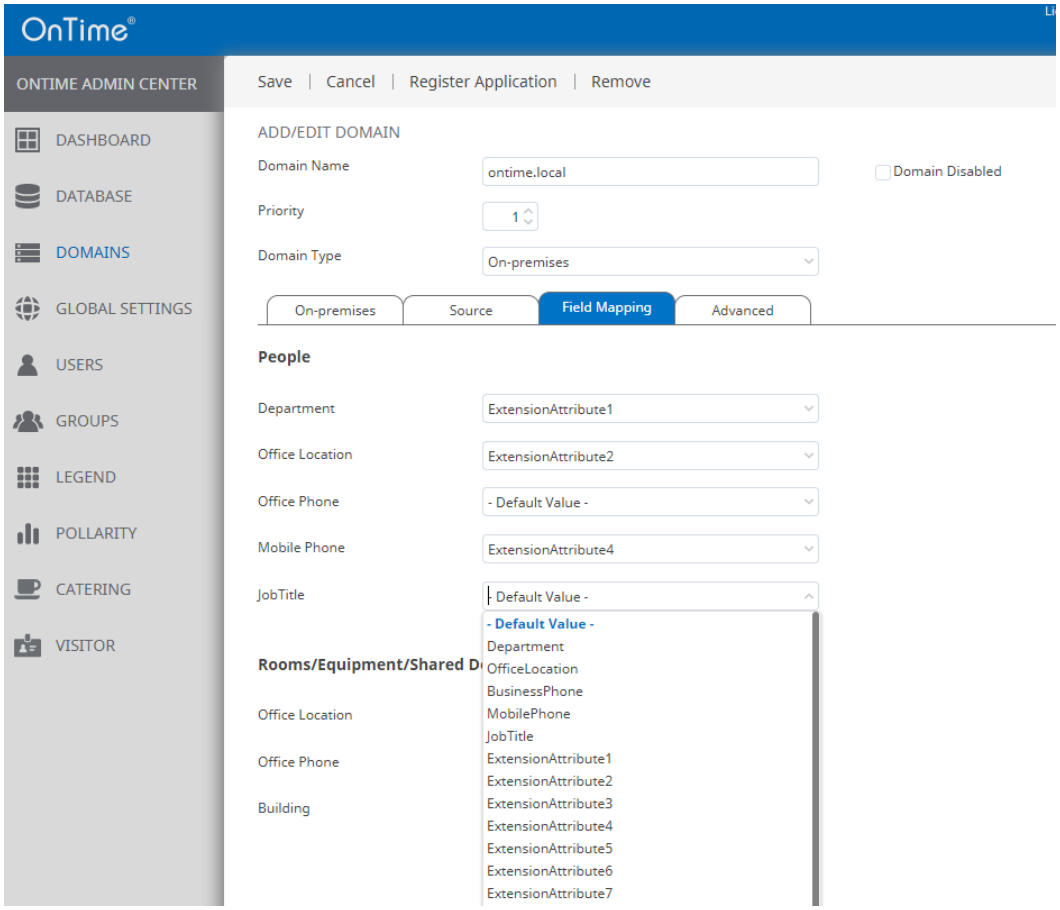
Click ‘Save’ to save your Domain settings.

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.



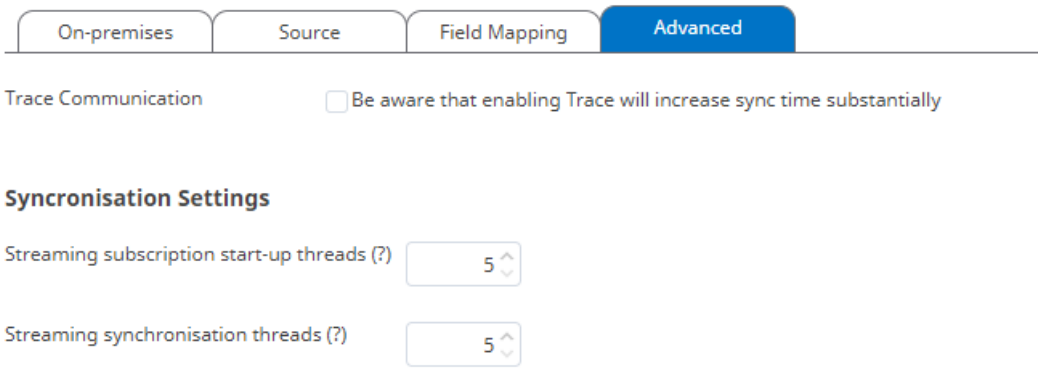
Parameters for the business card includes values from the AD like

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

Values may be fetched from AD Extension attributes.

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

Add/Edit Domain - Advanced



These default settings should not be changed normally.

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

Synchronisation settings

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

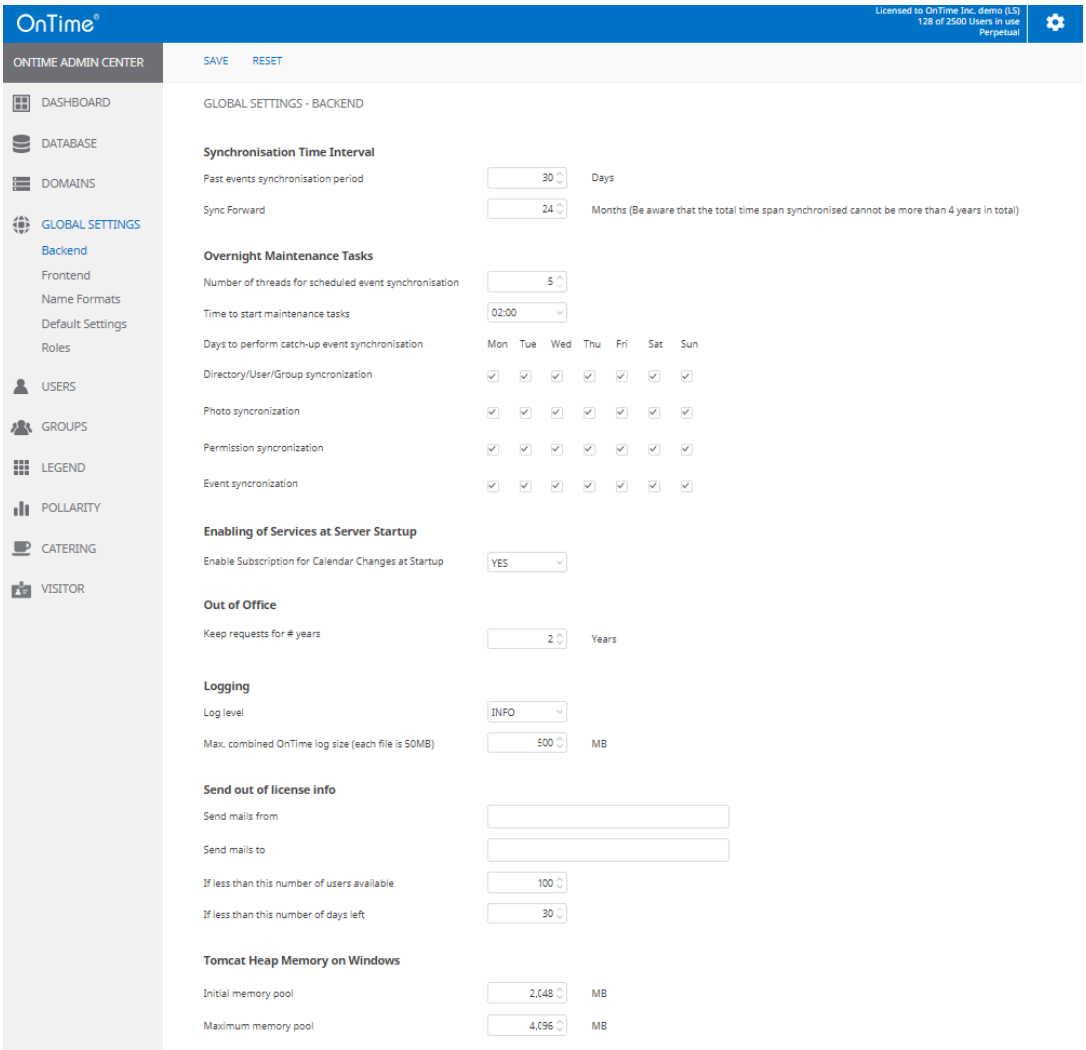
Streaming synchronisation threads – '5' is the minimum.
Recommendations are 5 threads for 1000 users, 25 threads for 8000 users.

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 4 years from your choice 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.

Time to start maintenance tasks – Specify time from 0 to 24 – server's time.

Weekdays to perform event synchronisation

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

Out of Office

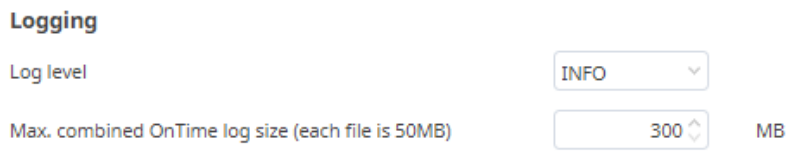
Time to keep requests in the OnTime database for # years – default is 2 years.

Enabling of Services

The setting 'ticked' loads the synchronisation service every time you start the Tomcat service. Normally you set it to "No" while you do your installation. When everything has been confirmed and OK, change it to 'ticked'.
Click **'Save'** and go to the **Dashboard**. Stop/Start the Application.

Logging

Here you can decide the level of logging for troubleshooting purposes and limiting of the log file size in MBs.



Refer to the **Logfiles** section for references to the log files.

Send out of license info

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

Send mail to – any internet mail user, eventually more addressees

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

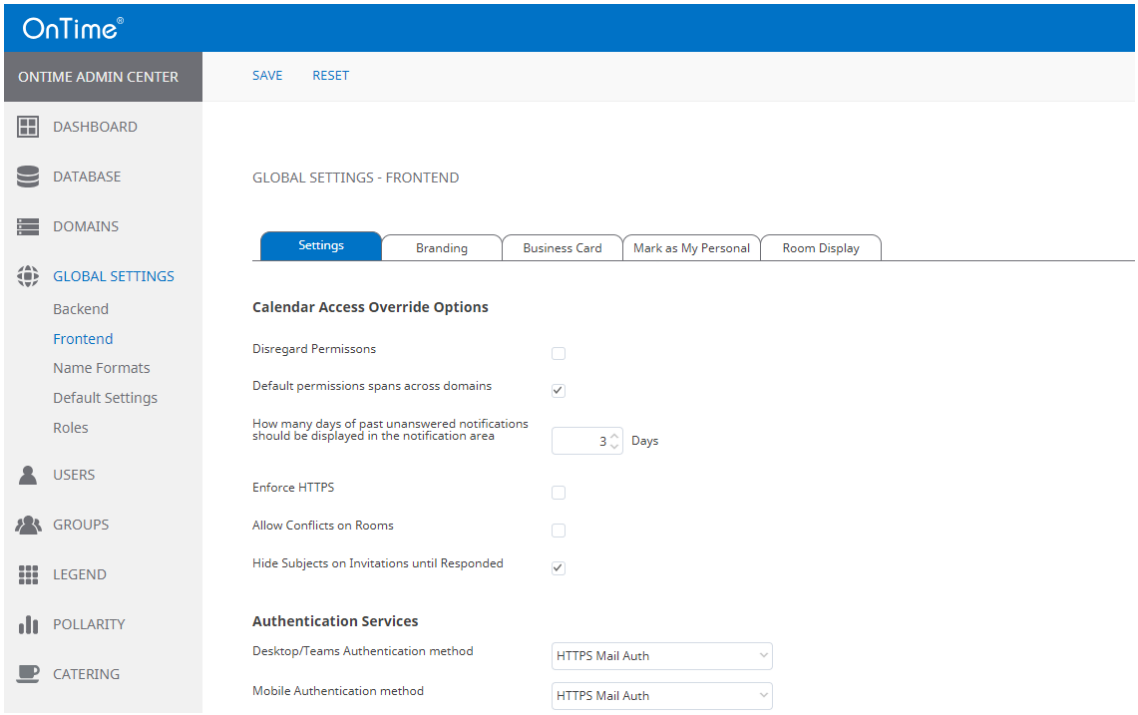
If less than this number of days left – warning threshold of days before the OnTime license expiry

Tomcat Heap Memory on Windows

Dependent on your setup and amount of users you may increase the memory for the Tomcat server.
When user installs/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 than 8Gb of RAM then the Initial Memory Pool will be 3 Gb and the Maximum Memory Pool of 6 Gb

Frontend

Click “Global Settings/Frontend” to enter the “Global Settings - Frontend” page.



Settings

In Exchange/Outlook, the default permissions granted by a user does not span to other domains. 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 = Unticked, default permissions set on users are ignored across domains.

Default permissions span across domains = Ticked, 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.

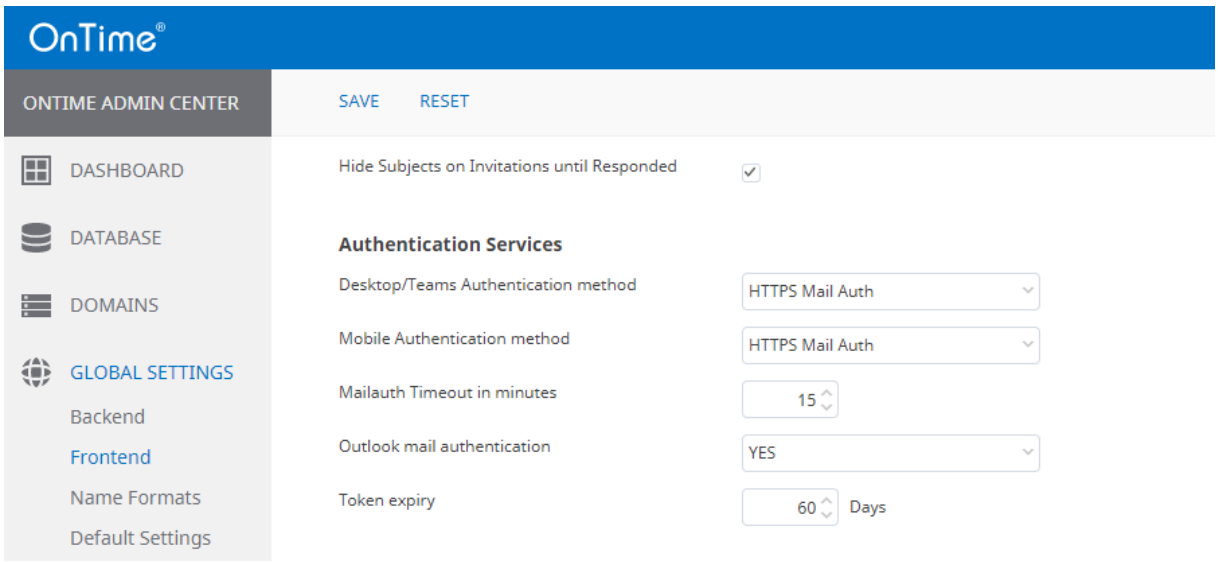
How many days of past unanswered notifications should be displayed in the notification area – Number of days unanswered invitations are kept in OnTime.

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 – tick to enable

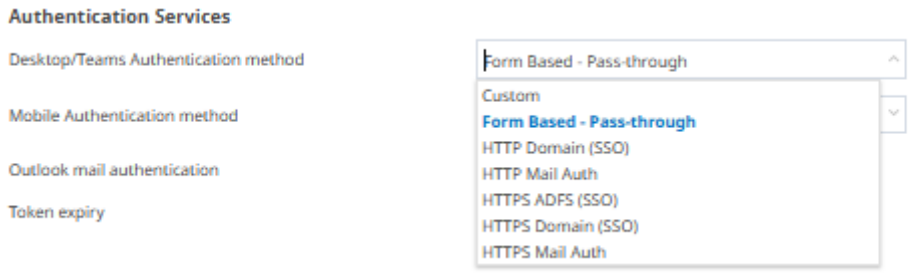
Authentication Services



This section describes different methods for users to obtain an OnTime authentication token for access to OnTime calendar data.

More details about the token in the section **OnTime Authentication Token.**

Desktop/Teams login methods in OnTime:



Note: Basic Authentication/Form Based – Pass-through with multifactor authentication in 'Office 365' is 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, to ensure secure connections to 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.

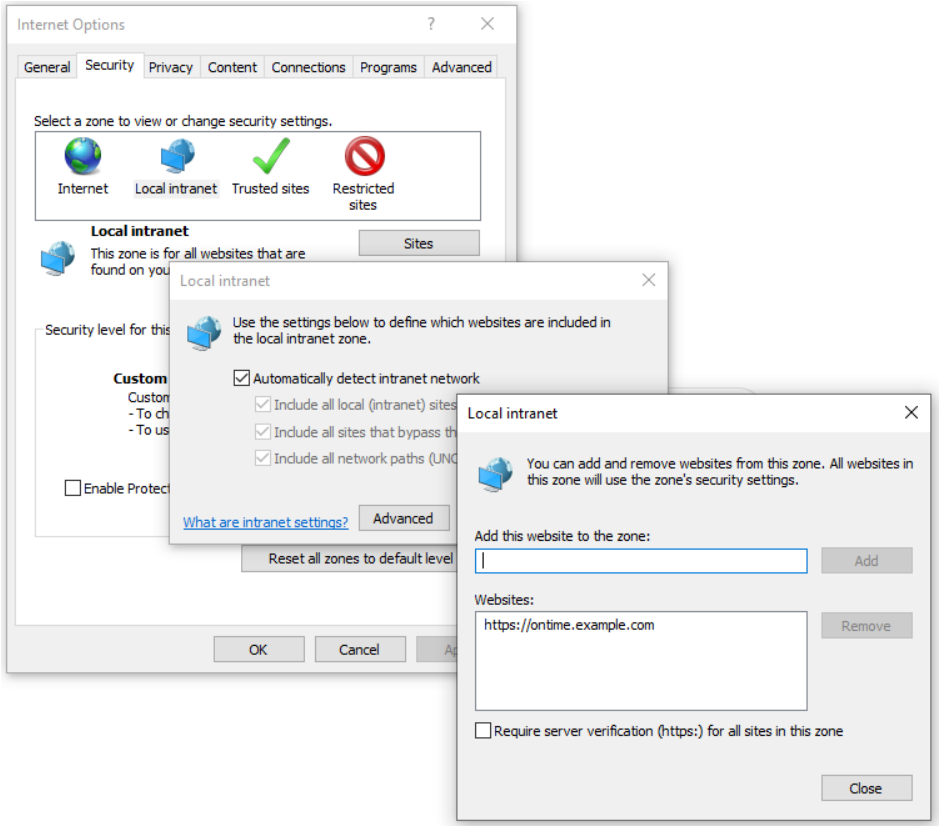
Ref. Browser setup for SSO for the browser to trust your OnTime server.

HTTPS ADFS (SSO) - is described further in the appendix **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:
For the Microsoft IE browser, go to Internet Options/Security/Local intranet.

Click “Sites” and “Advanced” to add your OnTime server.



The Chrome and Edge browsers trust your OnTime server because of the setup you made in Internet Explorer.

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**

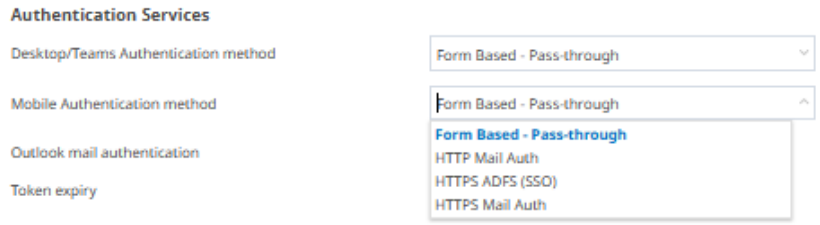
Click Edit and enter the name of your server – e.g. ‘ontime.example.com’

ADFS login (SSO)

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.

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)**

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 you are authenticating through ADFS, otherwise, it is 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.

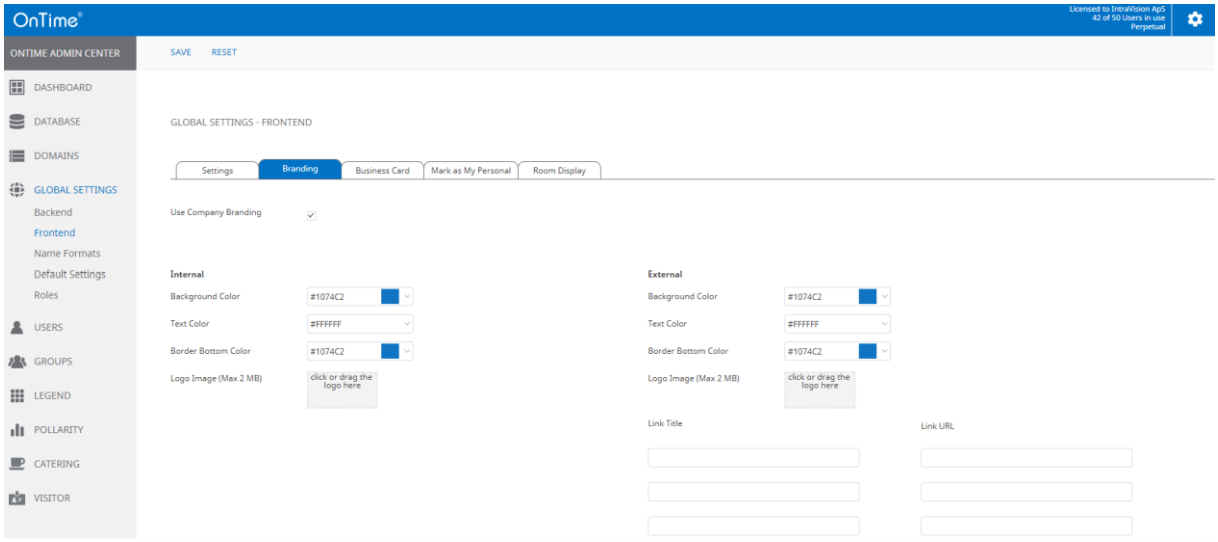
Default is 7 days. The minimum value is 1 day.

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’

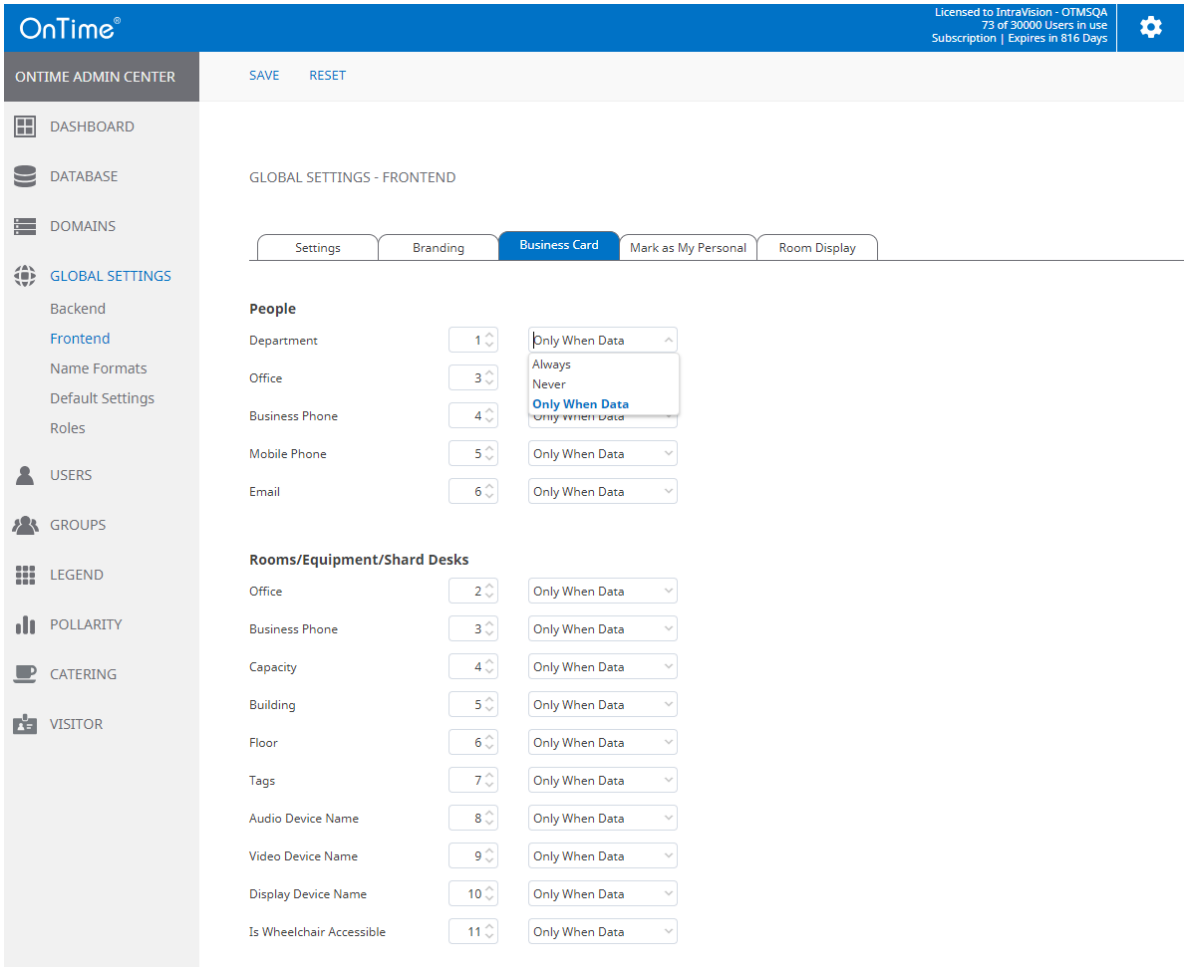
Use Company Branding – tick to enable.
Background Color – tick the arrow to choose the background color.
Text Color - tick the arrow to choose the background color.
Border Bottom Color - tick the arrow to choose the Border Bottom color.
Logo Image (Max 2 MB) – click or drag the logo to the field.

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 specifies individual data for People, Rooms, Equipment, Shared Desks.

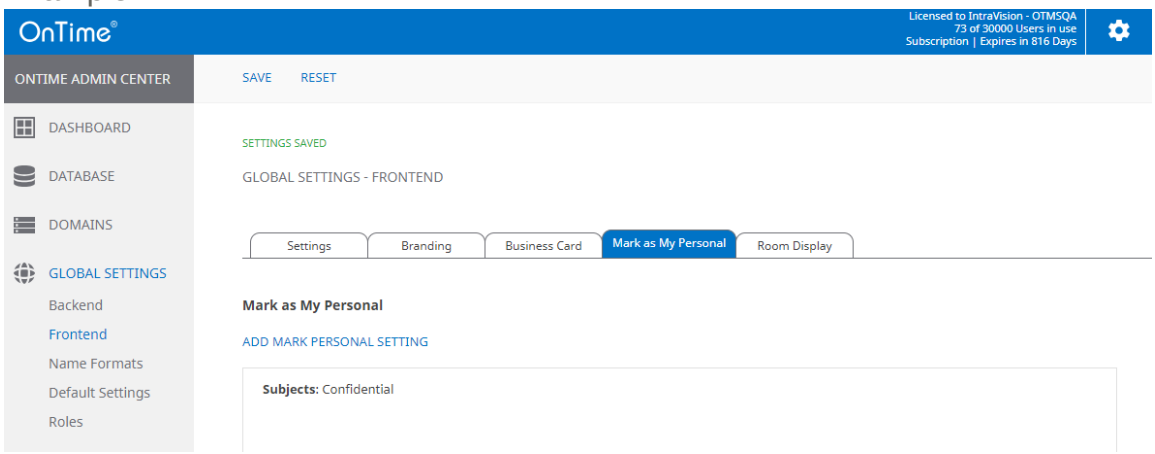
The column with numbers specifies the line numbers in the business card. In the righthand column you may specify if data is displayed.
Choice of 'Only When data', 'Always', 'Never'.



Mark as My Personal

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

Example:



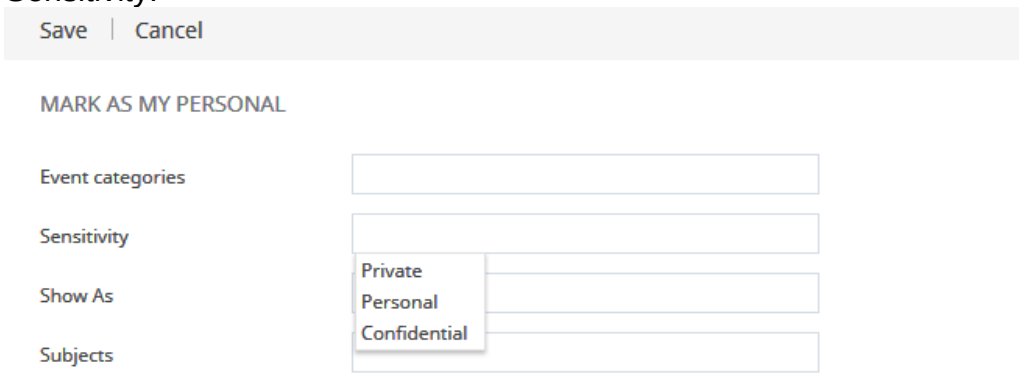
Click 'Add Mark Personal Setting' to setup.

Sensitivity is the levels as in Outlook.

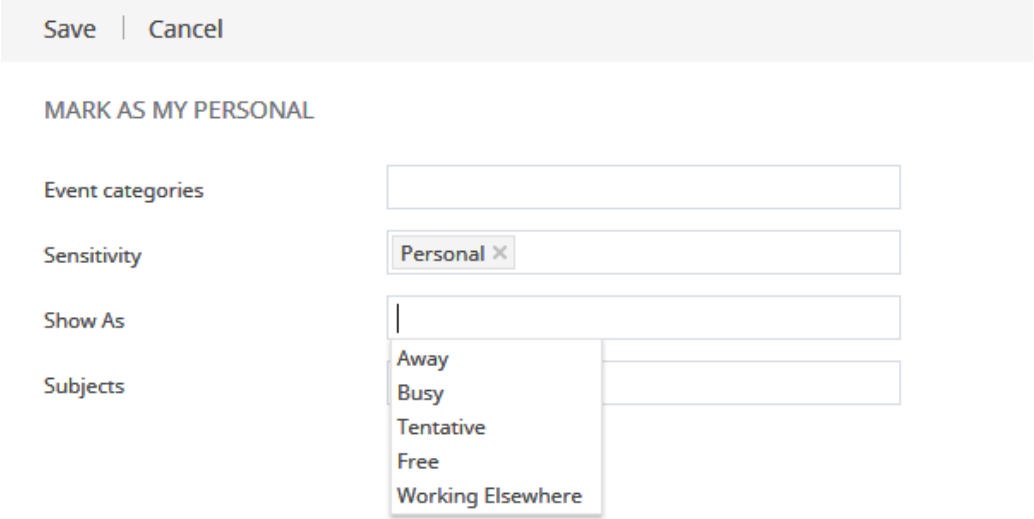
All the parameters in the 'Mark As My Personal' section have to be true to take effect.

The calendar 'Event categories' are configured within the Legend section.

Sensitivity:

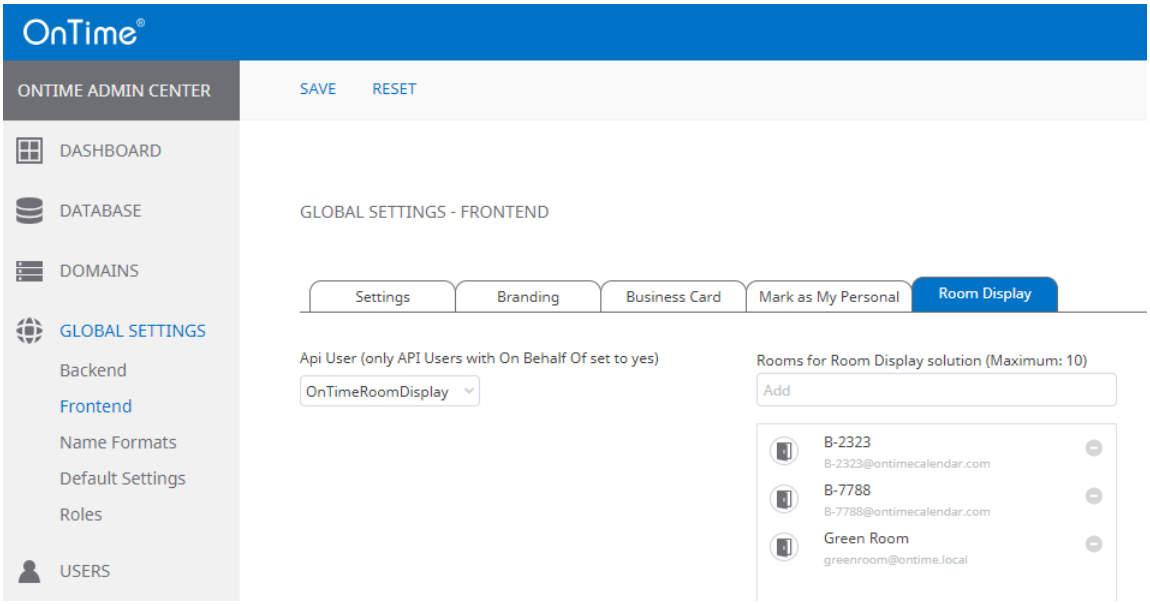


Show As:



Click '**Save'** and '**Save**'. Go to the **Dashboard**. Click Stop/Start the Application.

Room Display



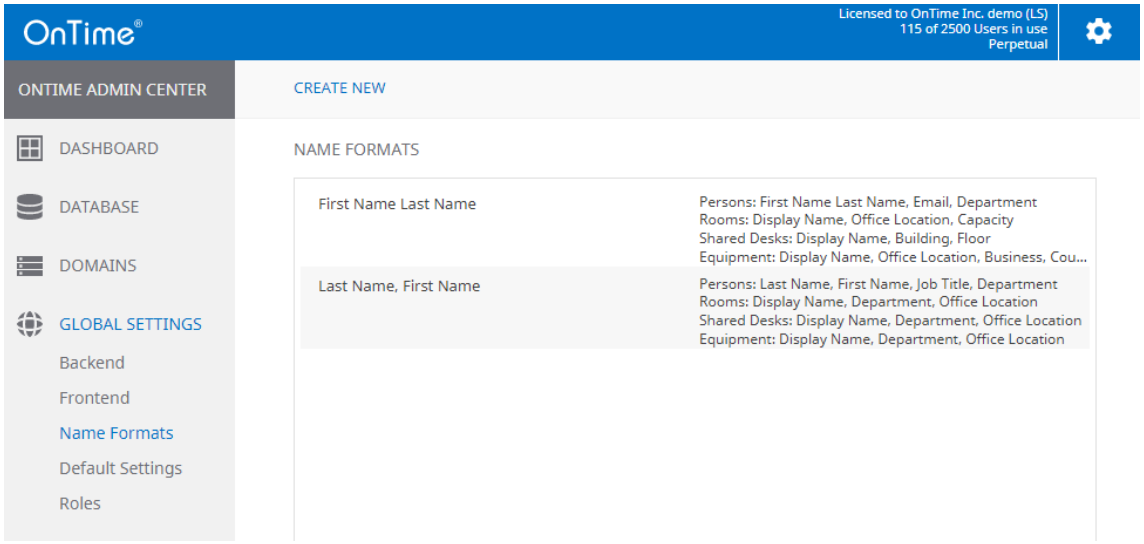
Choose an Api User, with 'On Behalf Of' set to yes.

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

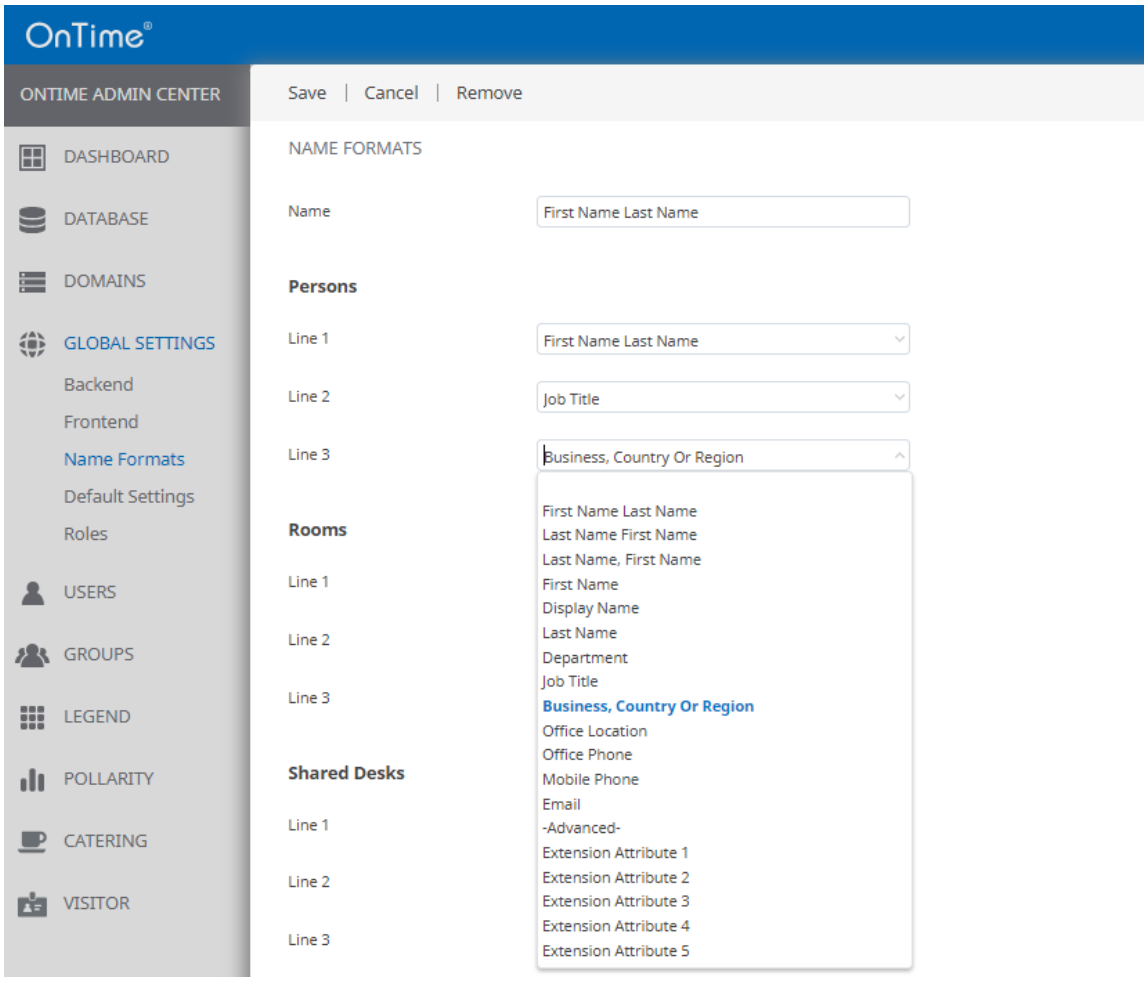
Click 'Save' – and restart the OnTime application in the Dashboard.

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

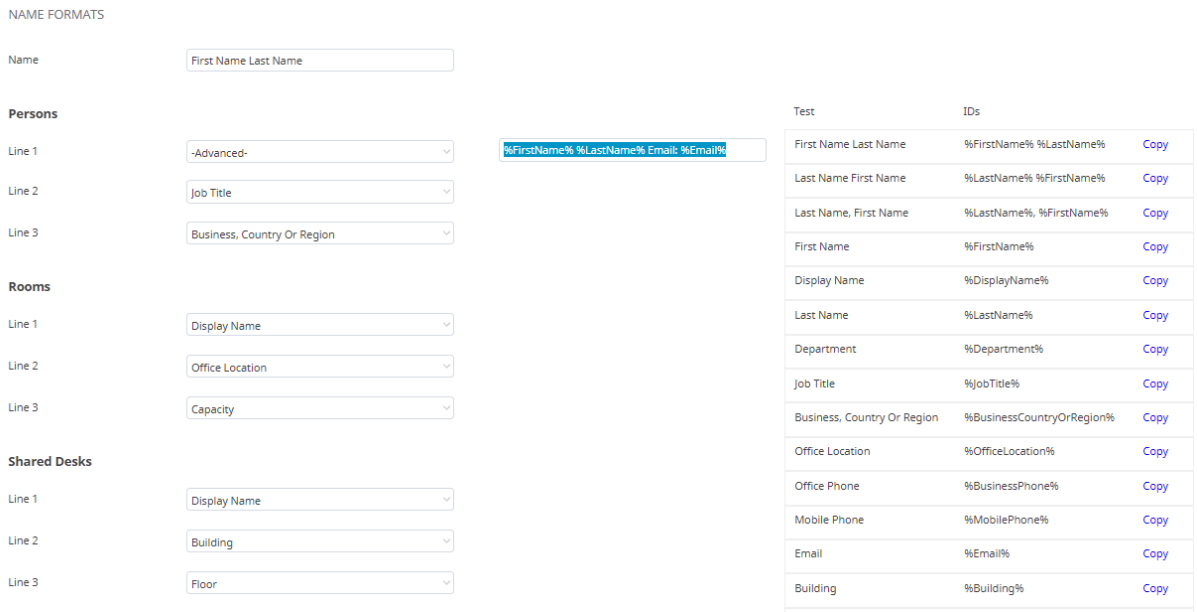
If you choose 'Advanced' in the dropdown menus you can have more information in each line. You may add more parameters to the field in the middle column. The parameters are enclosed with '%' characters. To avoid misspelling click 'Copy' and 'Paste' into the field in the middle column. You may add text/characters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

Example of field in the middle column:

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

Line 1 may display as:

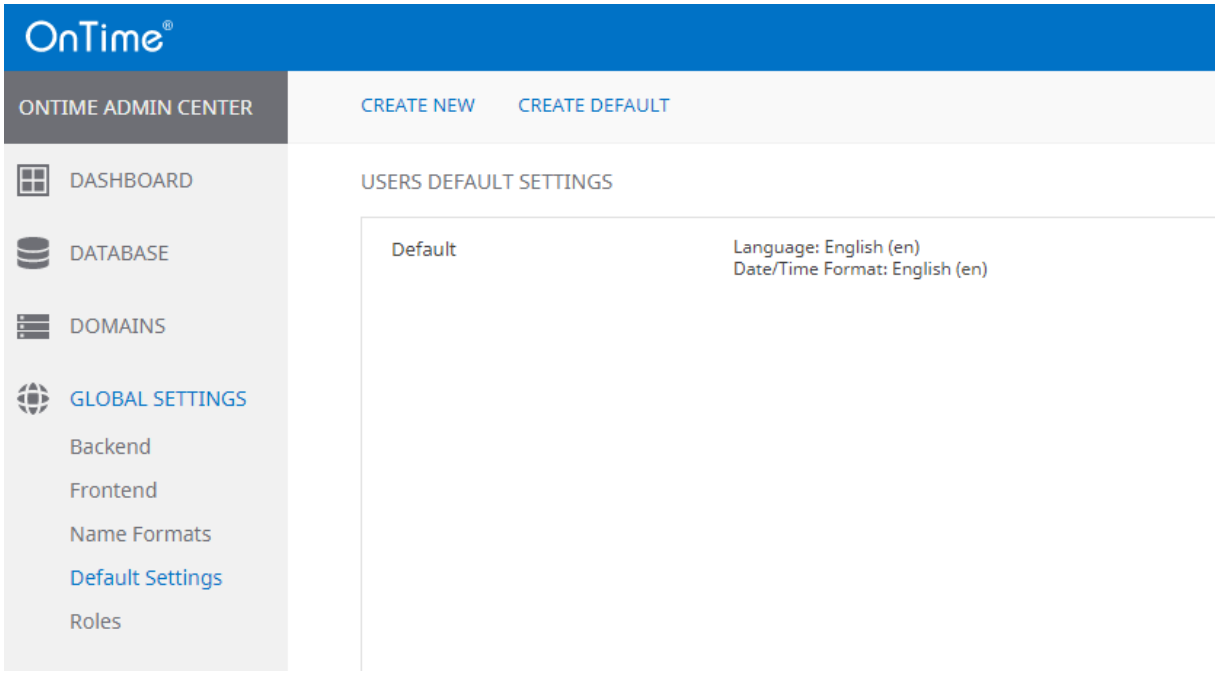
FirstName Lastname Email: email@example.com



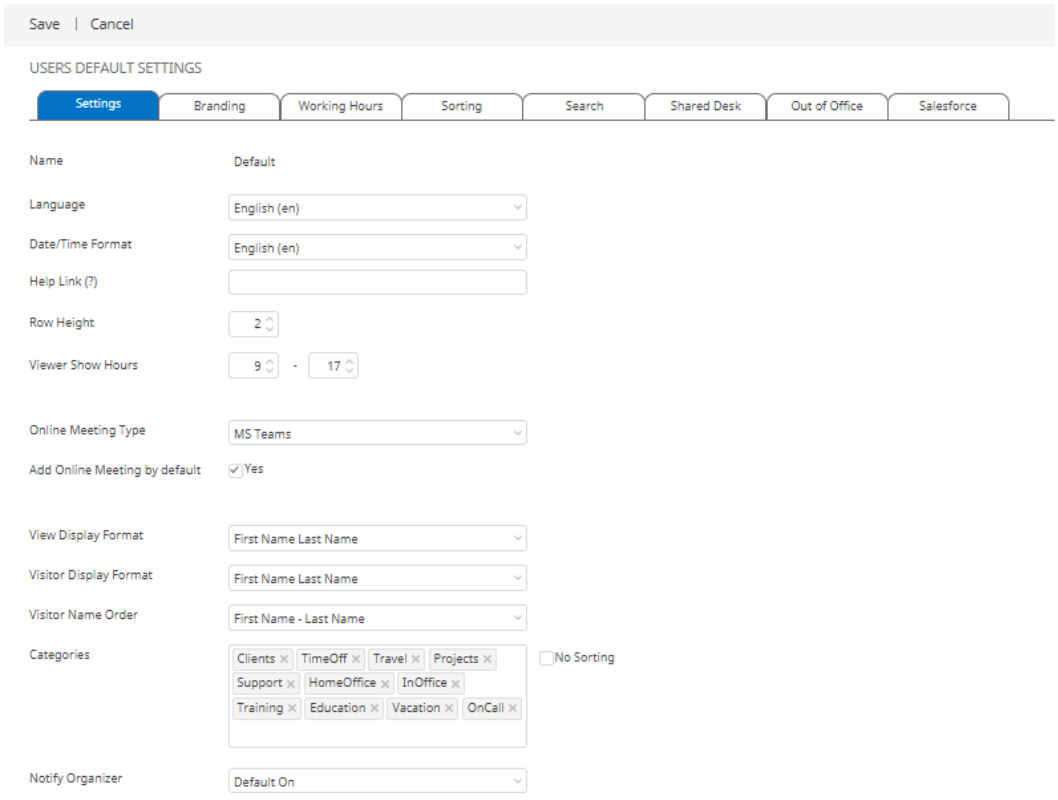
Click 'Save' to save your configuration

Default Settings

Click 'Default Settings'.



Click ‘Create New’, or chose 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 'MS Teams' or 'Skype for Business'.

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

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

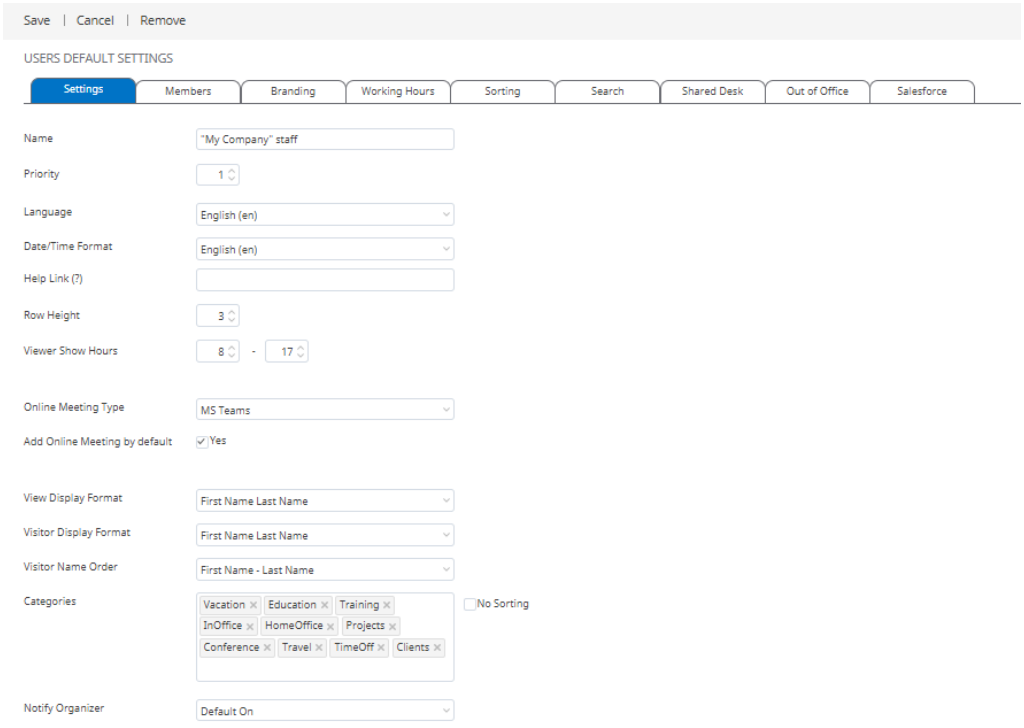
Visitor Display Format – order of 'First Name', 'Last Name'

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 origins from the Legends defined in the Legends section. Please refer to

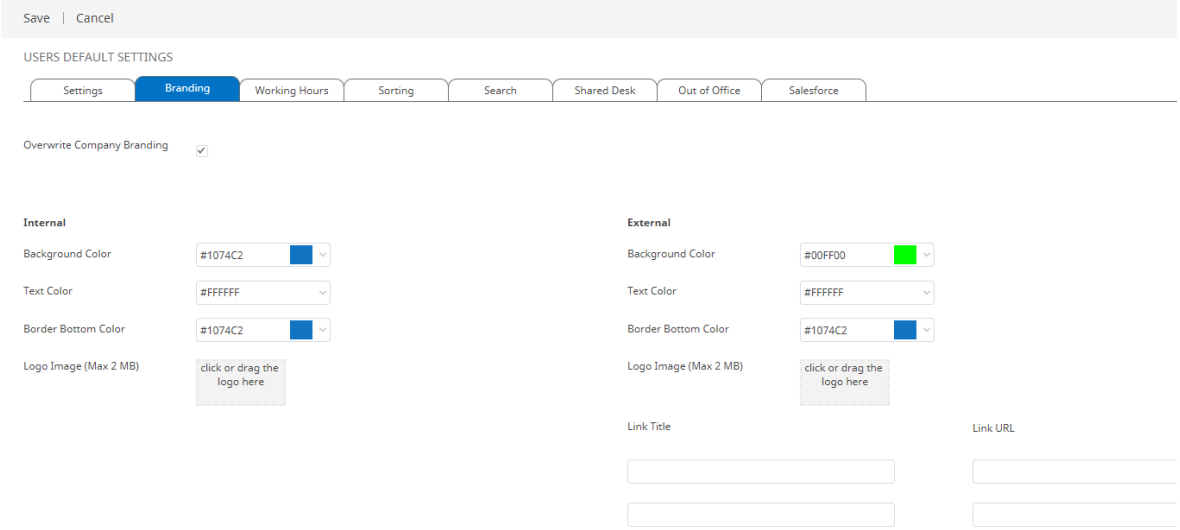
Members

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’.

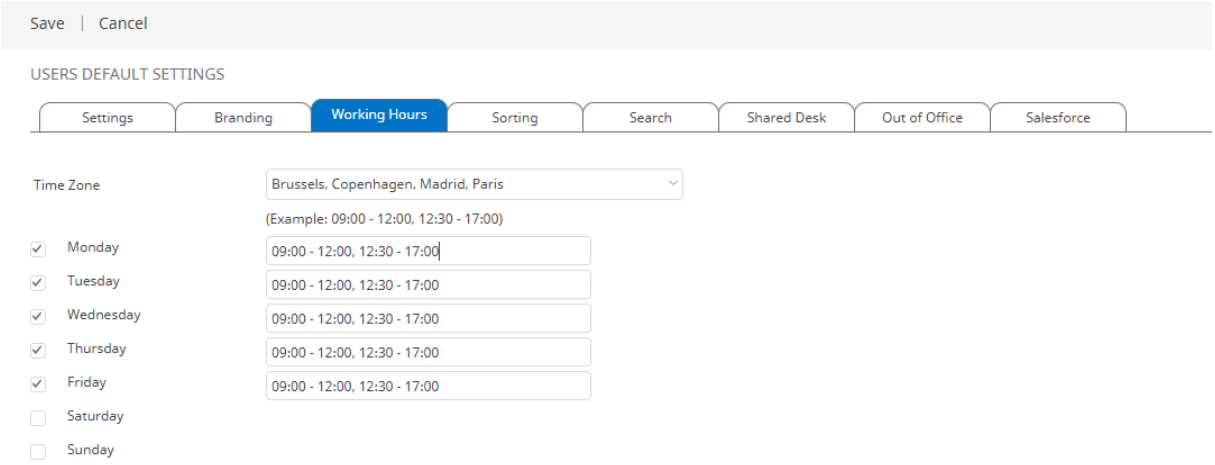
The lefthand column ‘Internal’ is for the Desktop.
The righthand column ‘External’ is for applications like ‘Pollarity’

Overwrite Company Branding – tick to overwrite
Background Color – tick the arrow to choose the background 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’.

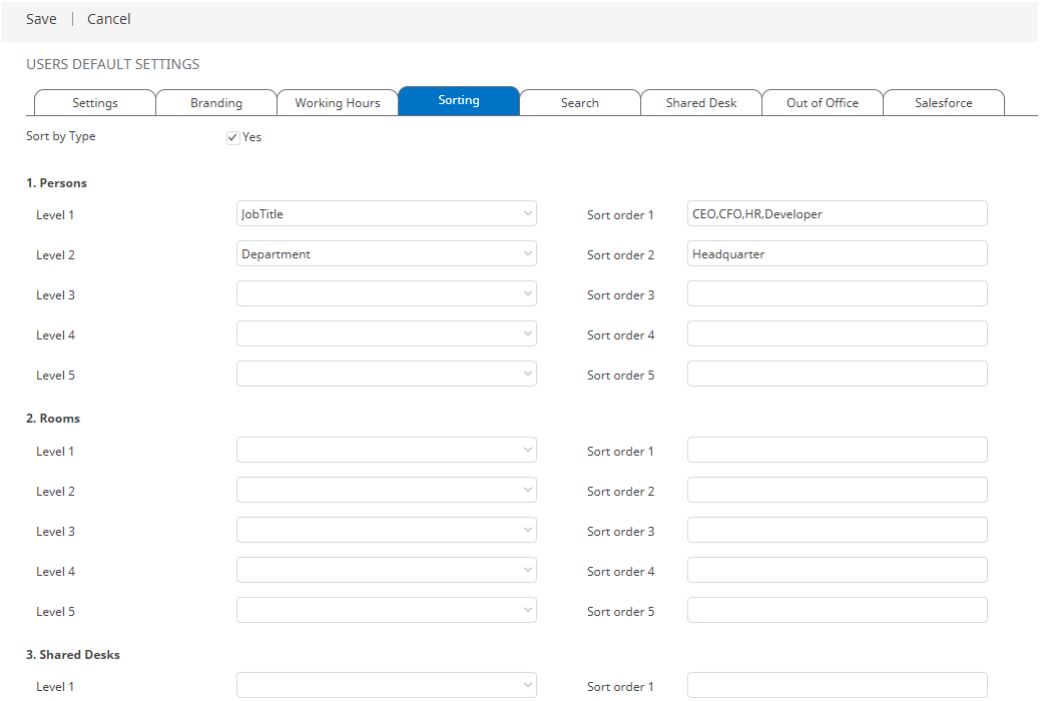
Working Hours

– 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 upon their names.

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: JobTitle

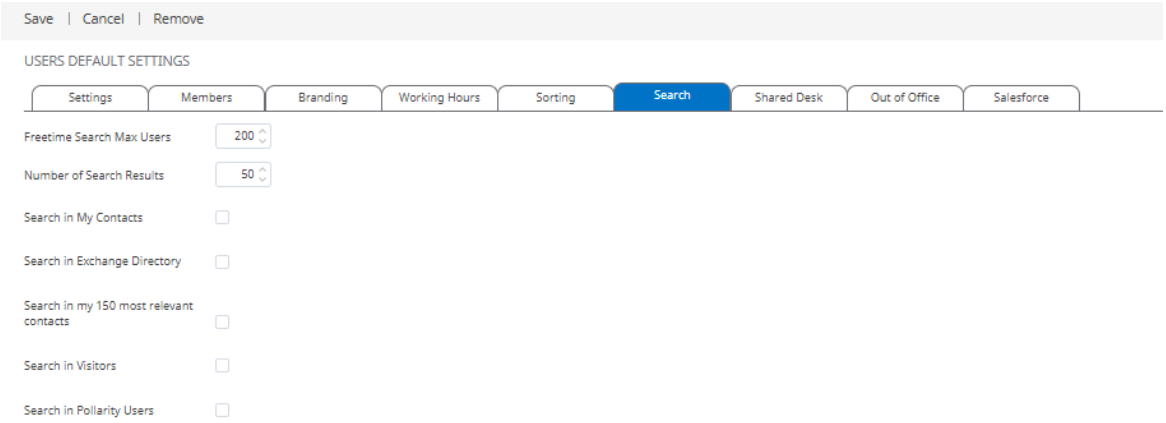
Sort order 1: CEO, CFO, HR, Developer

Level 2: Department

Sort order 2: Headquarter

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 avoid search in the private Contacts.

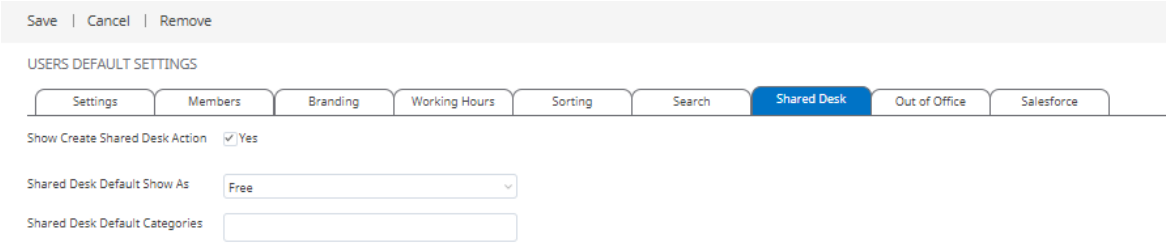
Search in Exchange Directory – tick to enable

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

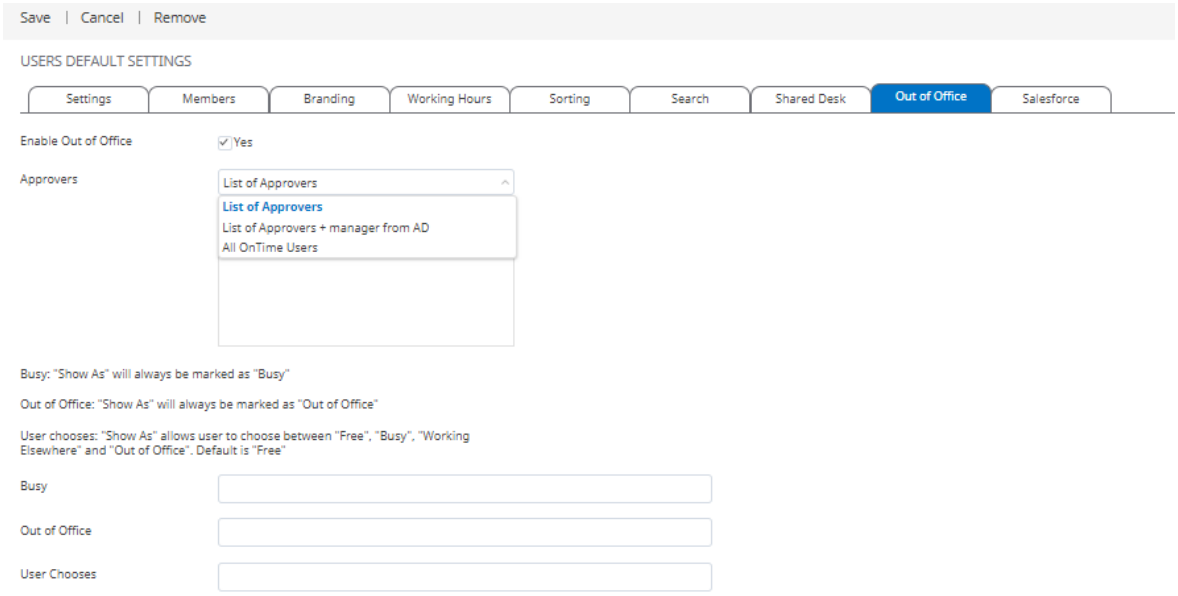


Show Create Shared Desk Action – tick 'Yes' to show the action button in the user's desktop

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

Shared Desk Default Categories – The legend (color) shown for the user 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 colored according to the legends in the user interface.

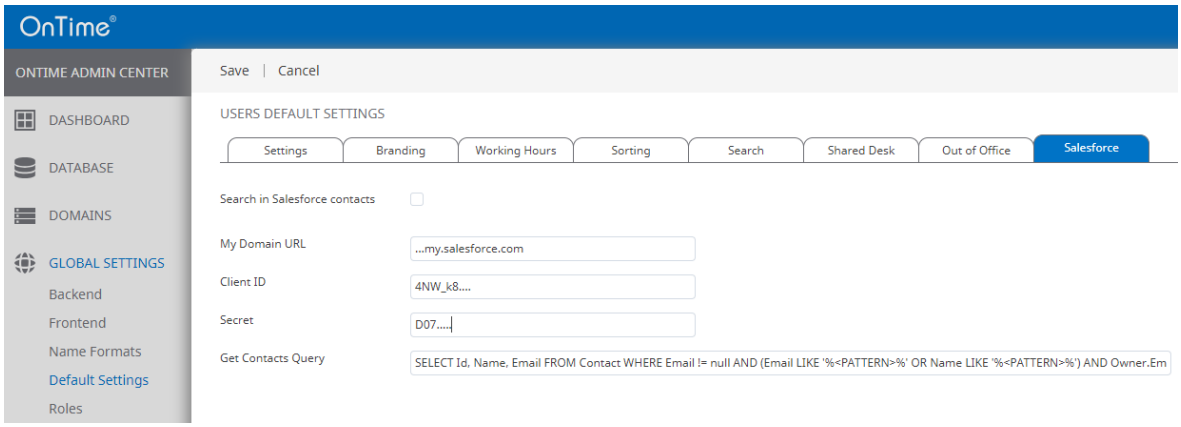
Busy: 'Show As' will be marked as 'Busy'

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’

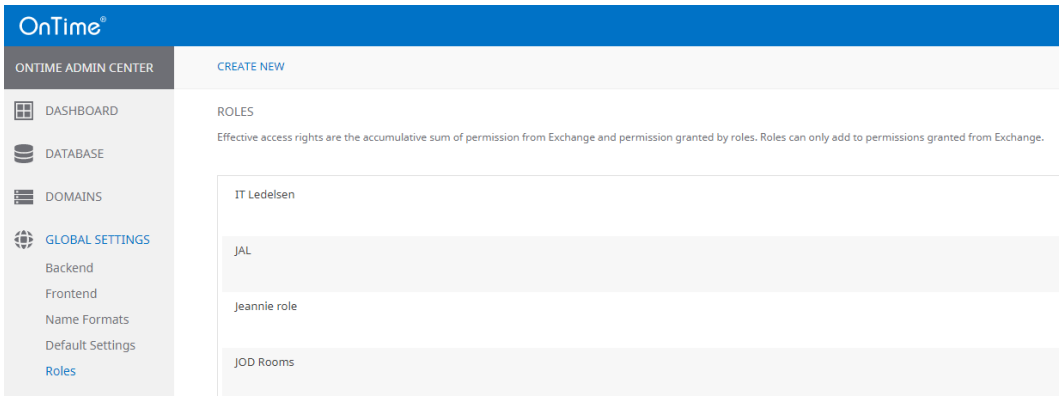
Roles

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.

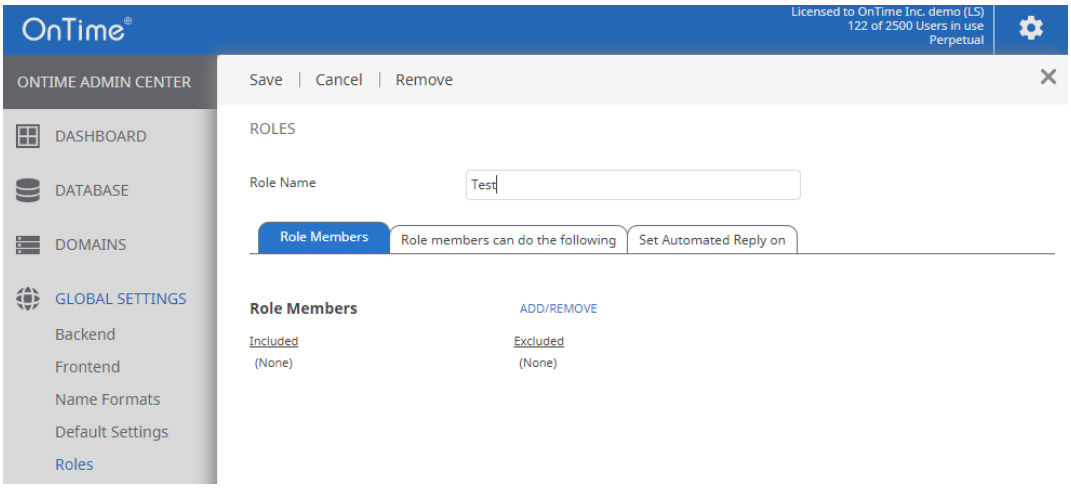
Dynamic Distribution Groups from Office 365 are supported.

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

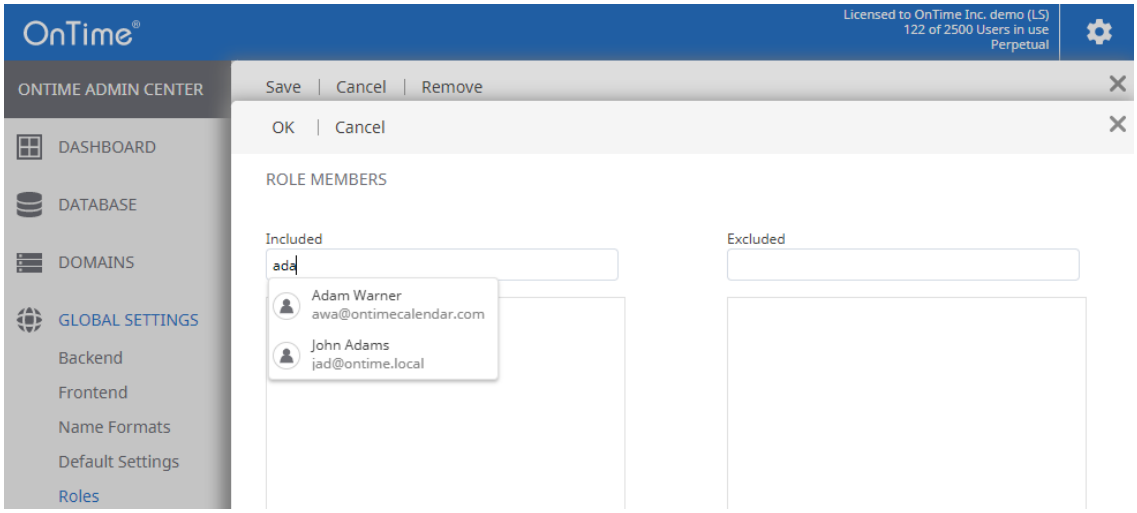


Click 'Create New' to create a role.

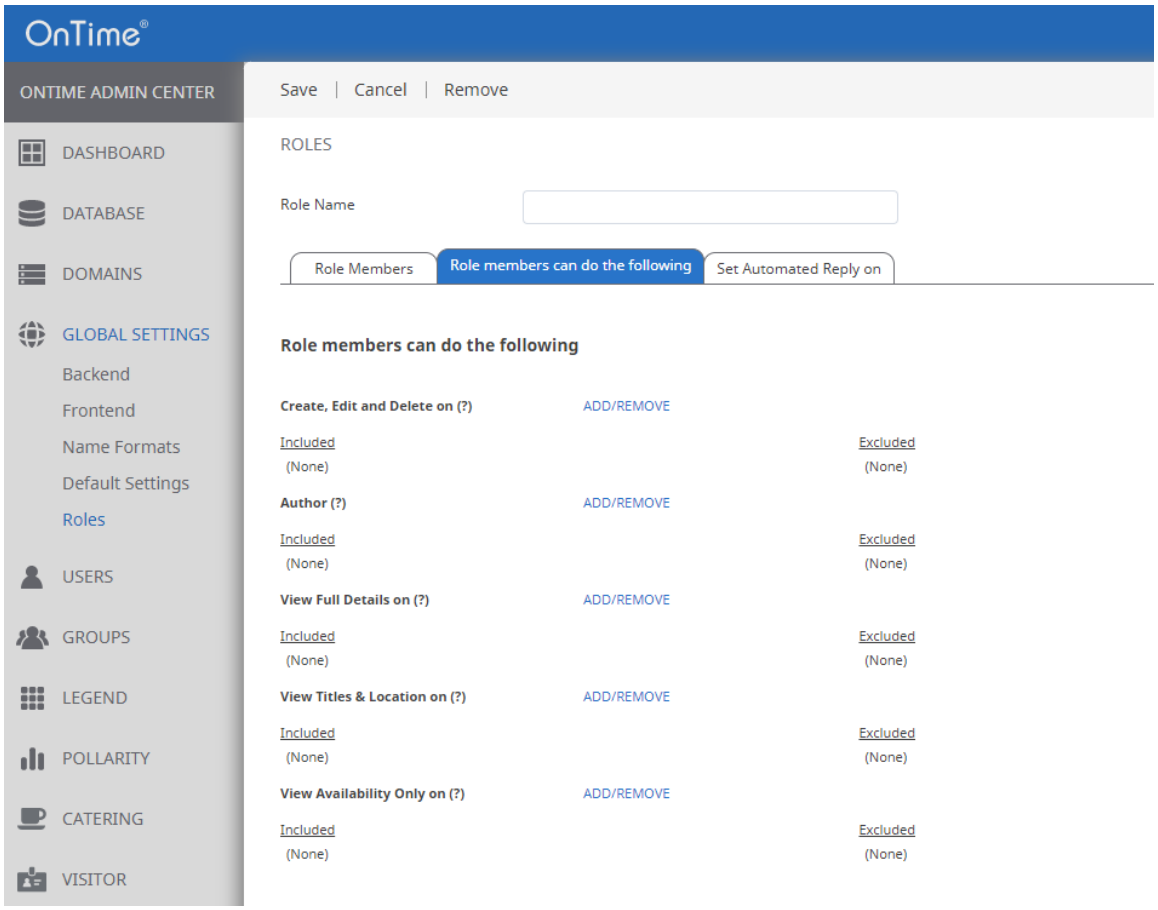
Enter a 'Role Name'.



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.

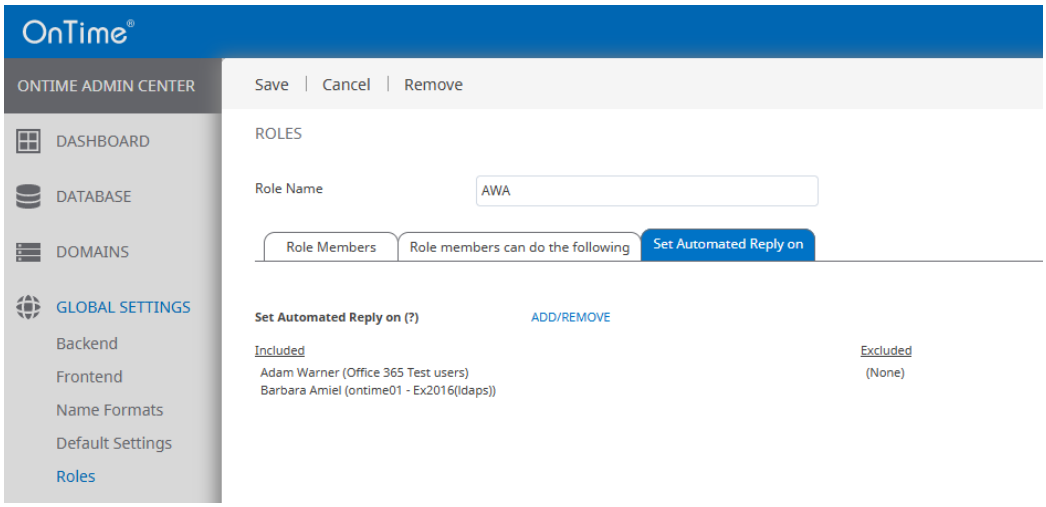


There are five different levels of what Role menbers can do to Calendar entries in OnTime.

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/Busytime 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.



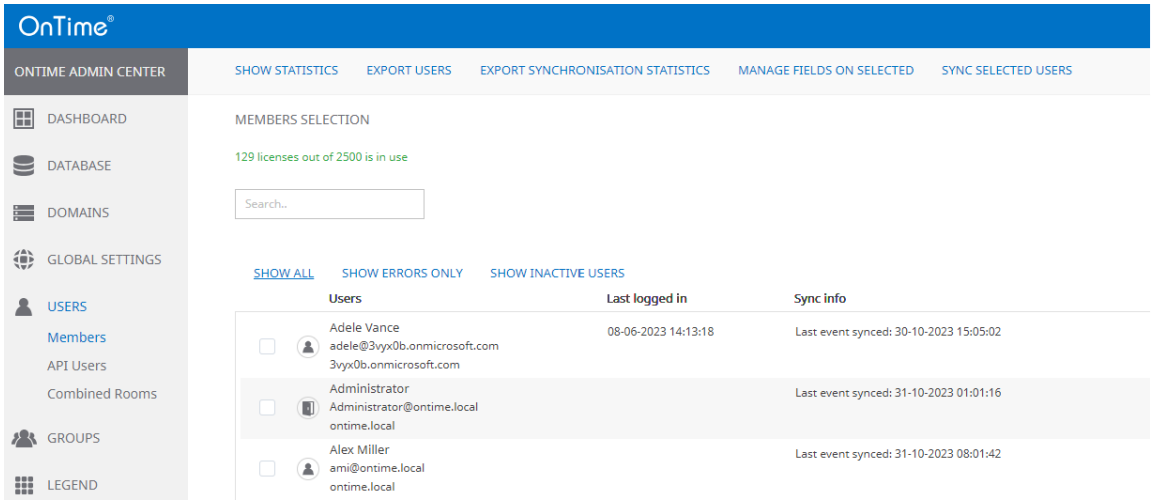
When done editing permissions, click ‘Save’ on the roles document.

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

Users

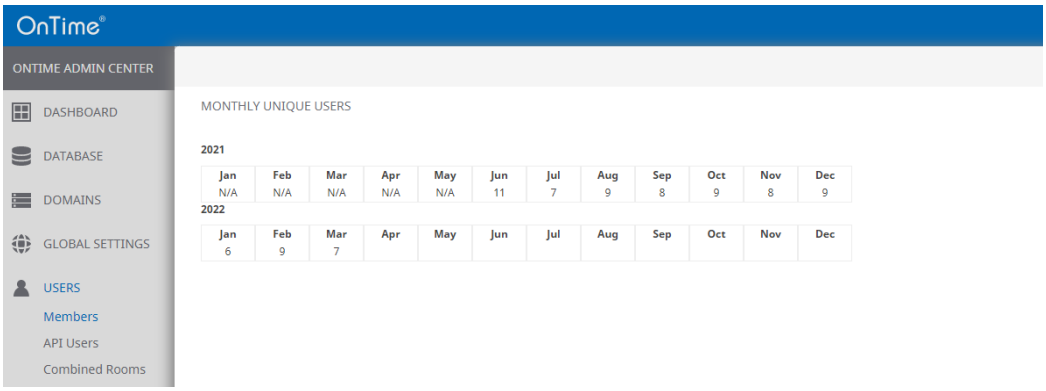
Members

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'



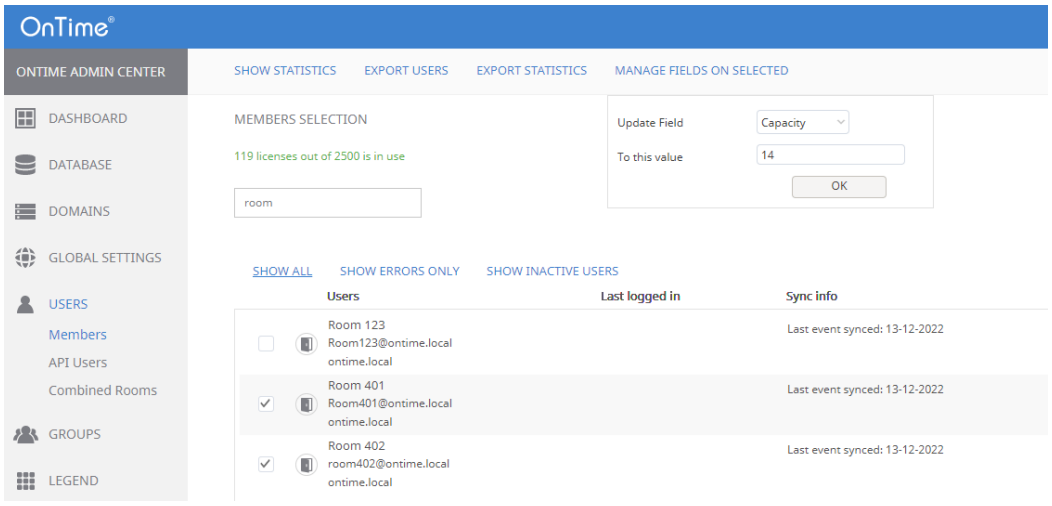
The N/A – not applicable, means no data available for the month.

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'.

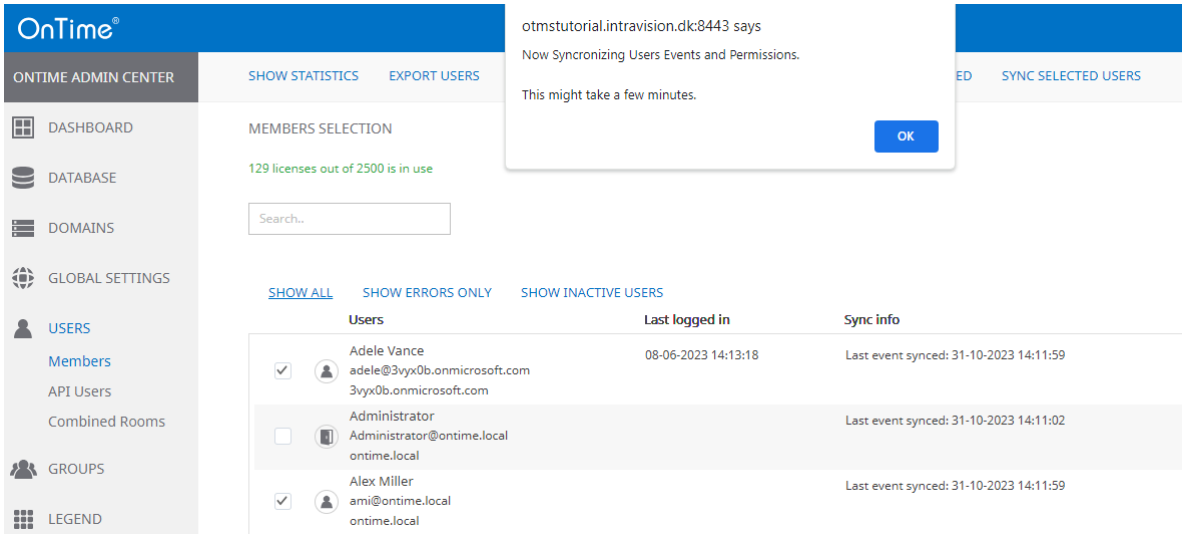
You may export statistics from OnTime in a comma-separated file by clicking 'Export Statistics'.

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

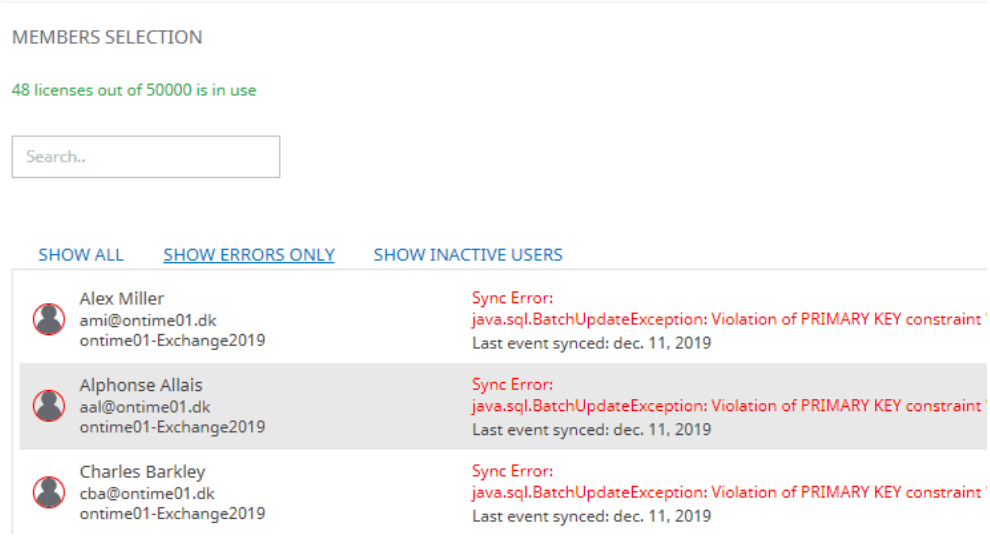


If the result box shows fewer updates than you expected – some of the resources do not have editable fields in their ‘Business Card’.

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.



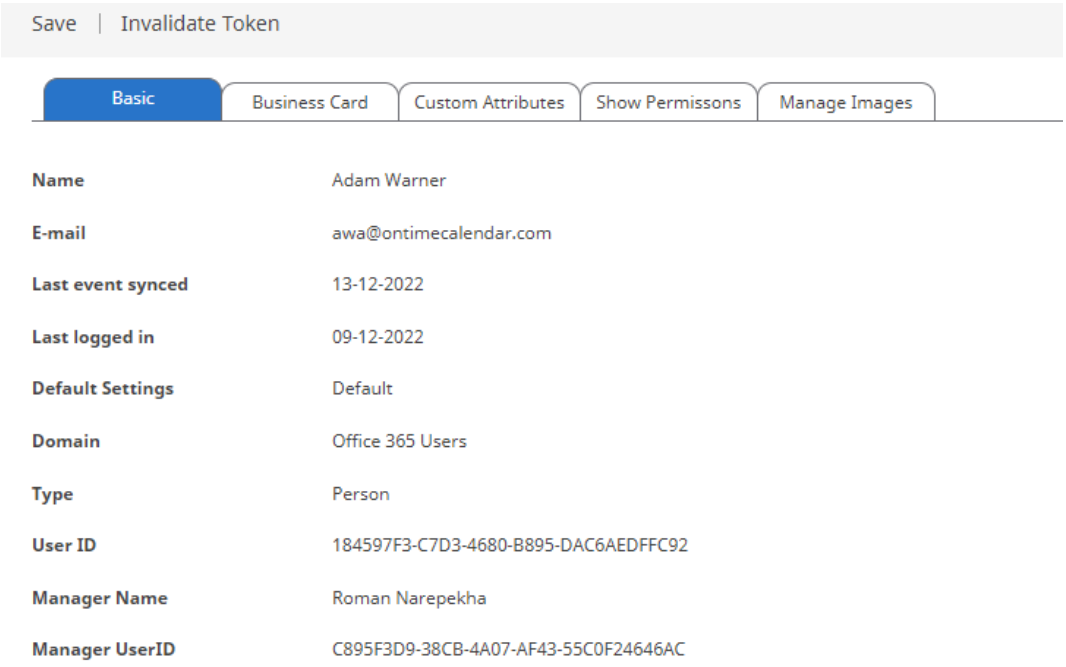
“Show Inactive Users” tab shows information about the users who are currently not active in the system. These users can be permanently removed by clicking on them and invoking action “Purge User”

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 Center’.

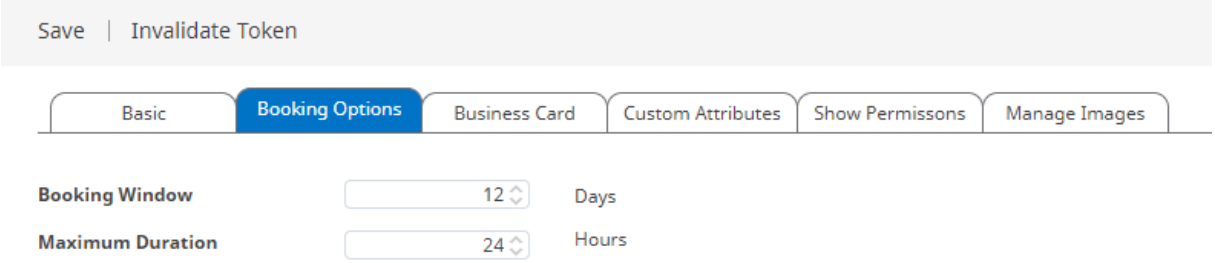
Basic



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

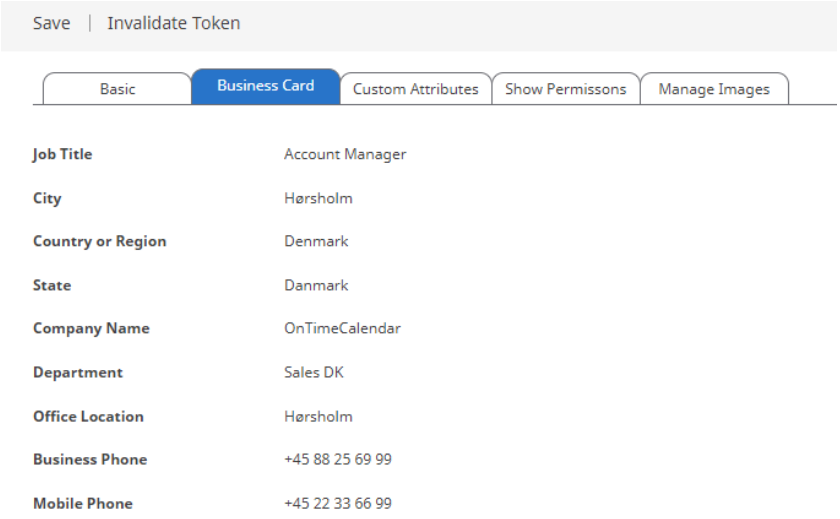
This tab is only relevant for the three user types – Room, Equipment, SharedDesk – not for the user type, person.



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.

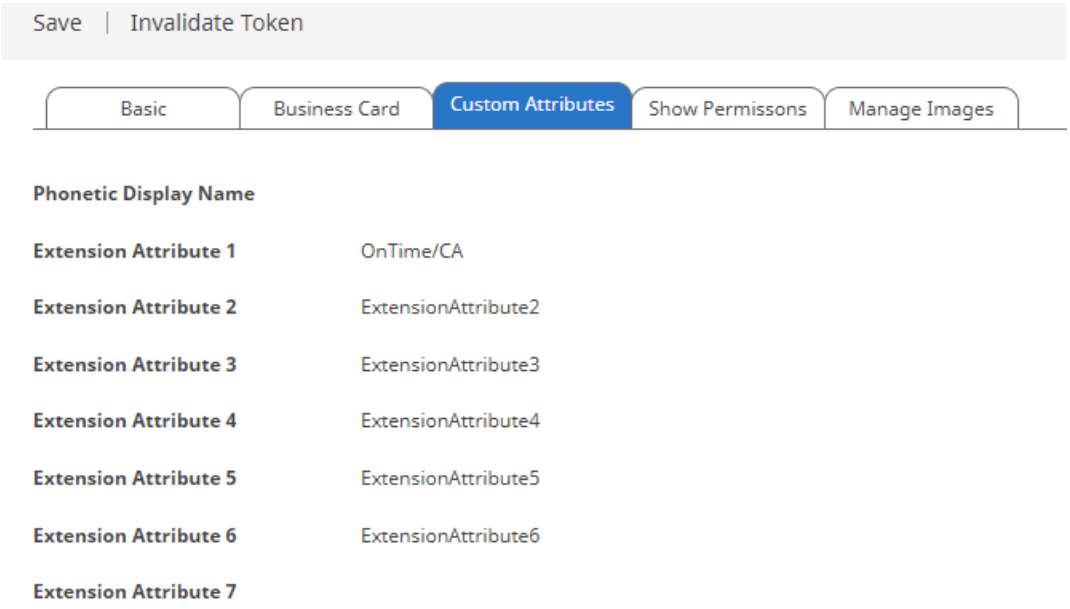
Business Card

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



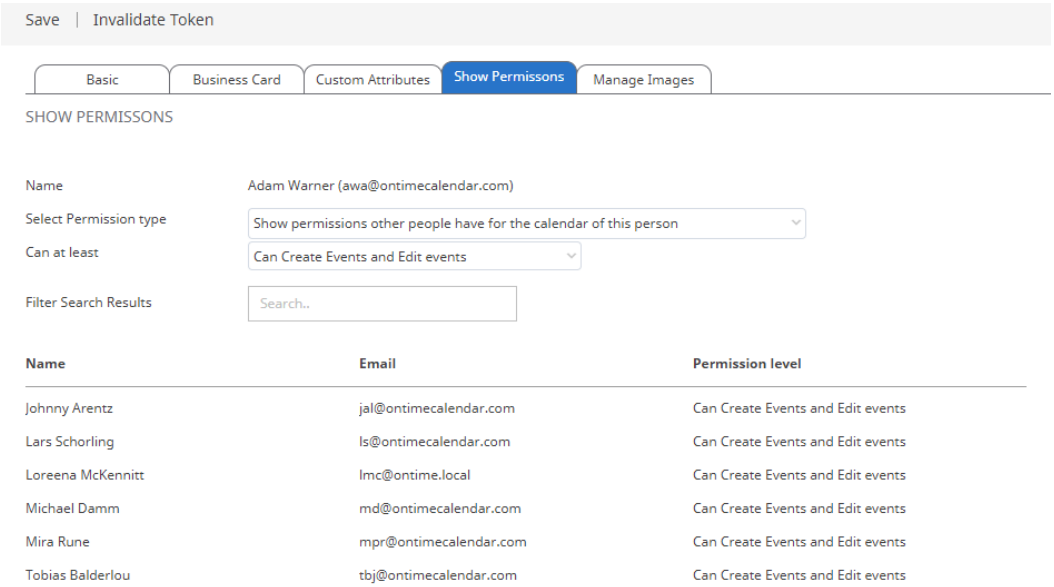
Custom Attributes

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



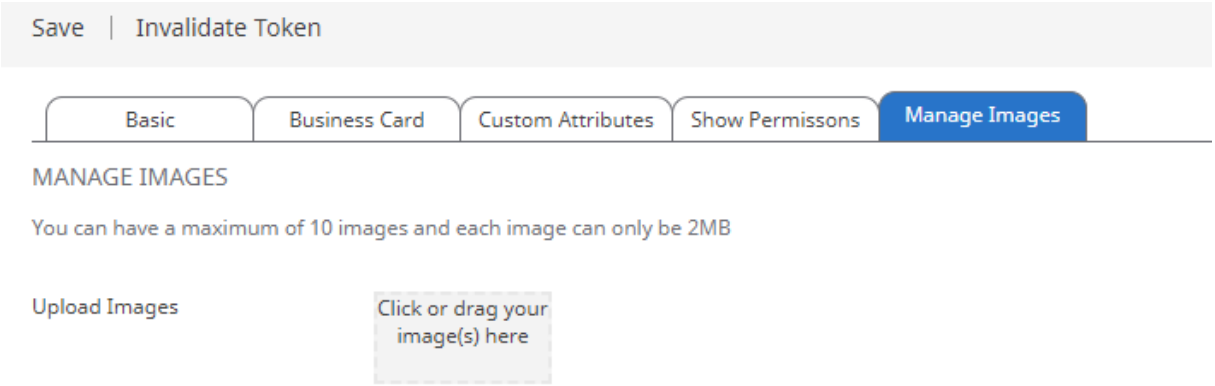
'Show Permissions' is used to get an overview of the calendar permissions for the specific user. Two selections of permission types are possible, permissions for other users to this person's calendar, and permissions that this user has to other user's calendars.

‘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:

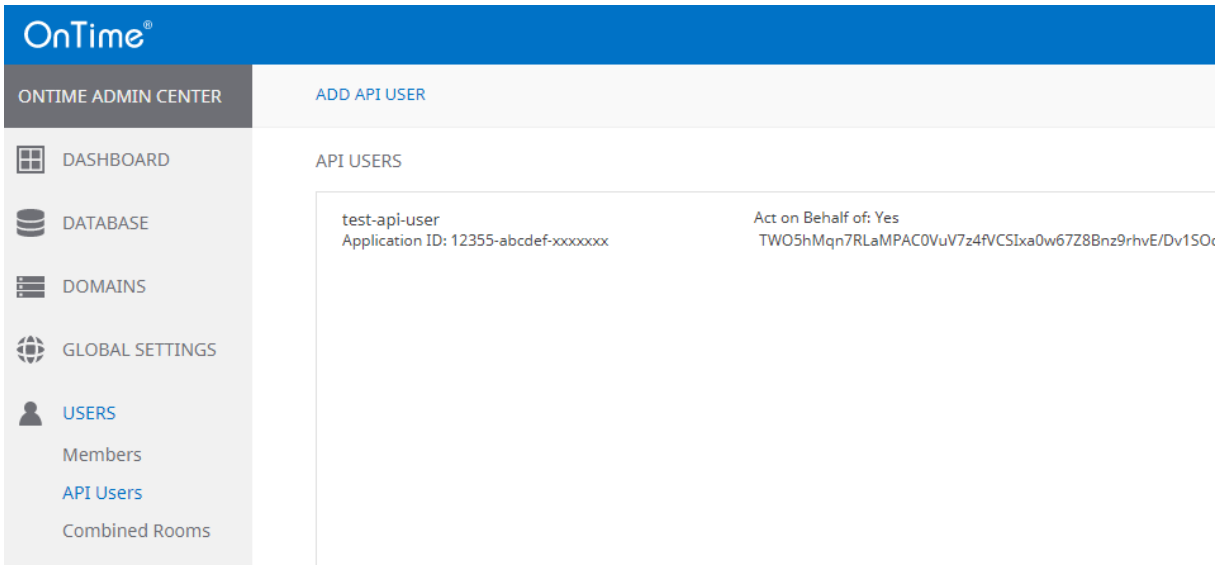


API Users

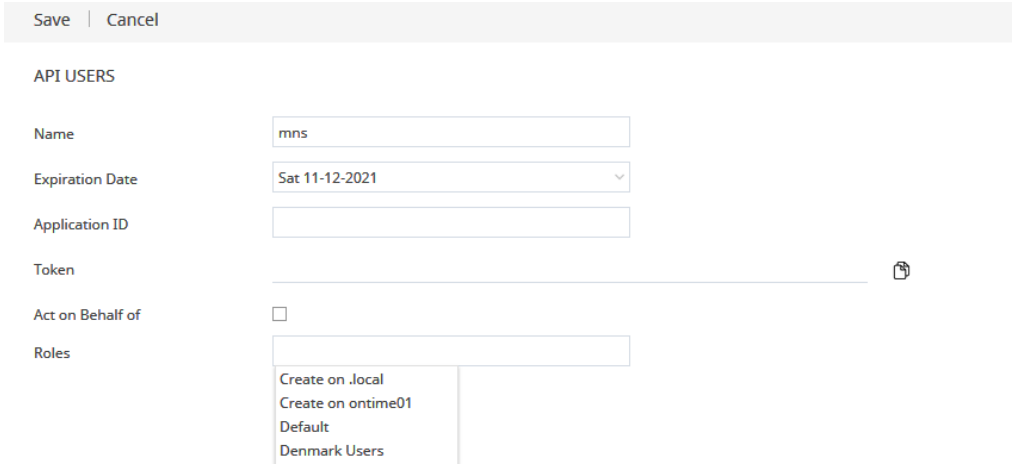
The API user is used for developing your own external applications using the OnTime API.

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

Click 'Users/API Users'



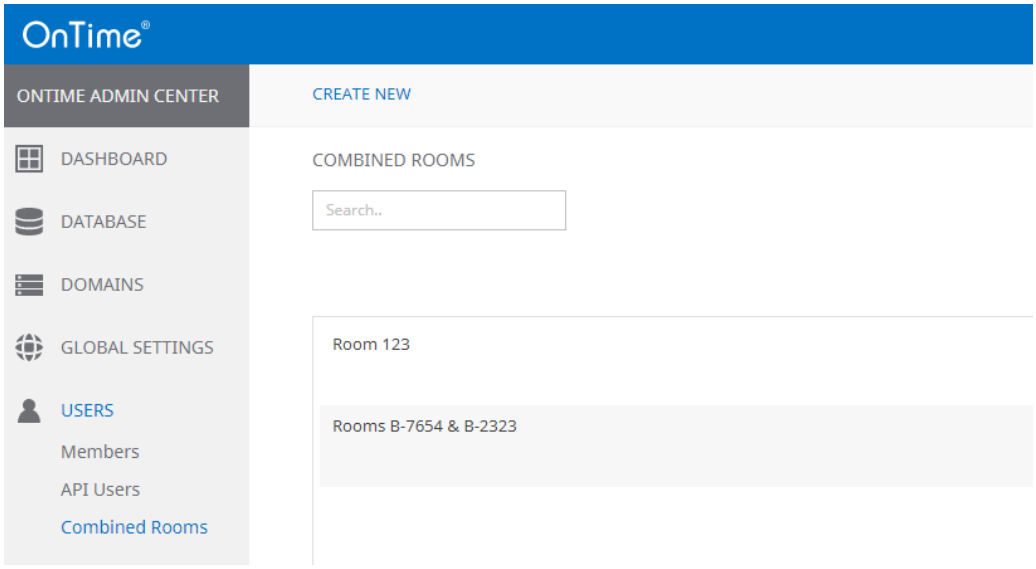
Click 'Add API User' to create a new OnTime API User.



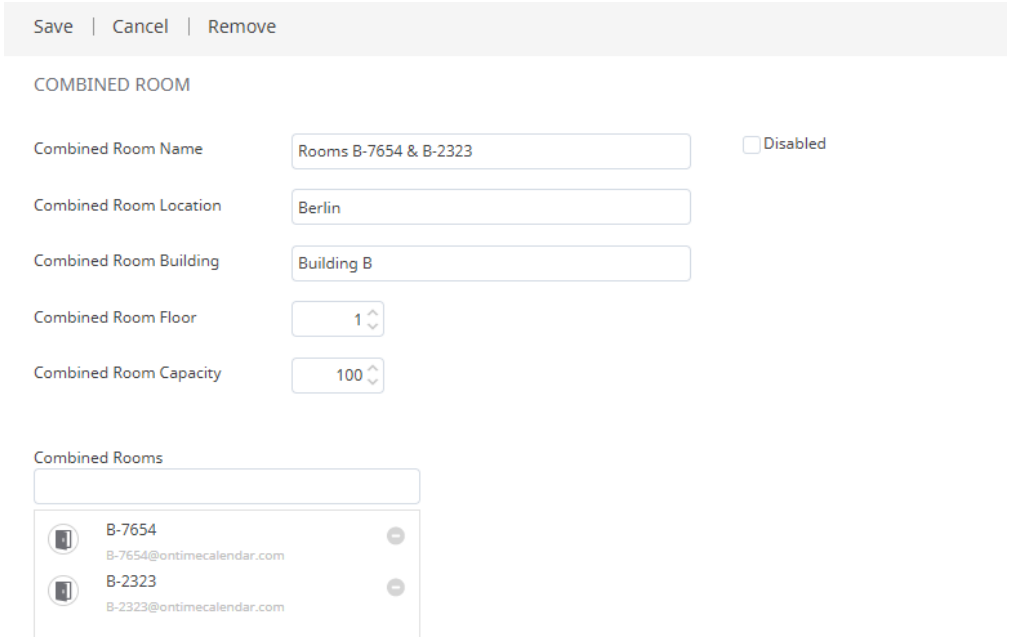
Name – enter a name of the API User.
Expiration Date – enter the expiration date for this API User
Application ID – license acquired
Token – when you click 'Save' a token is generated in the OnTime back-end.
Act on Behalf of – ticked, means that the API User acts with the individual rights of all users (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':

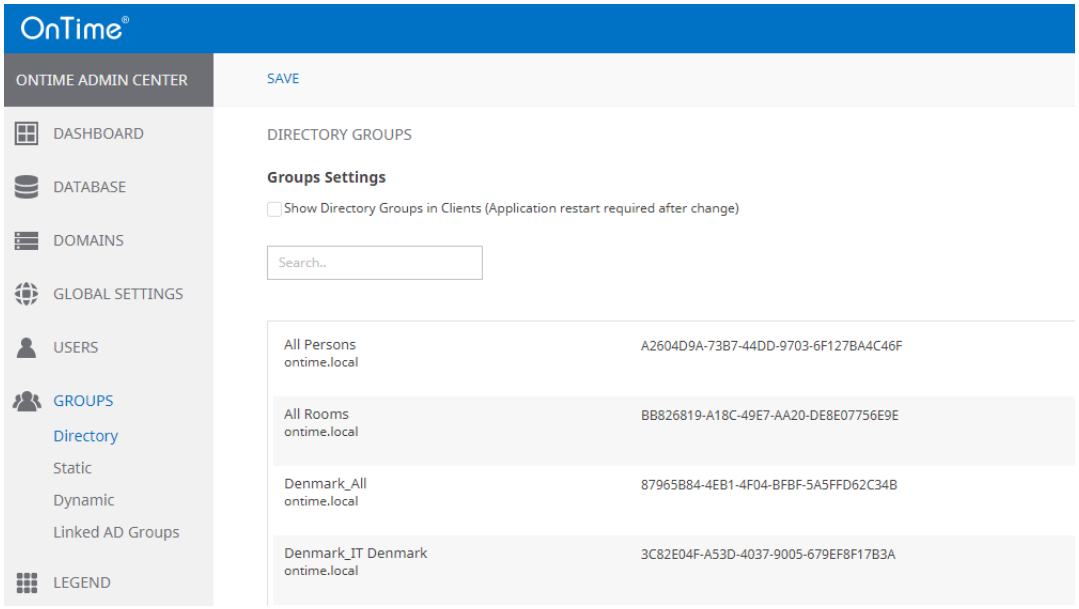


Groups

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.



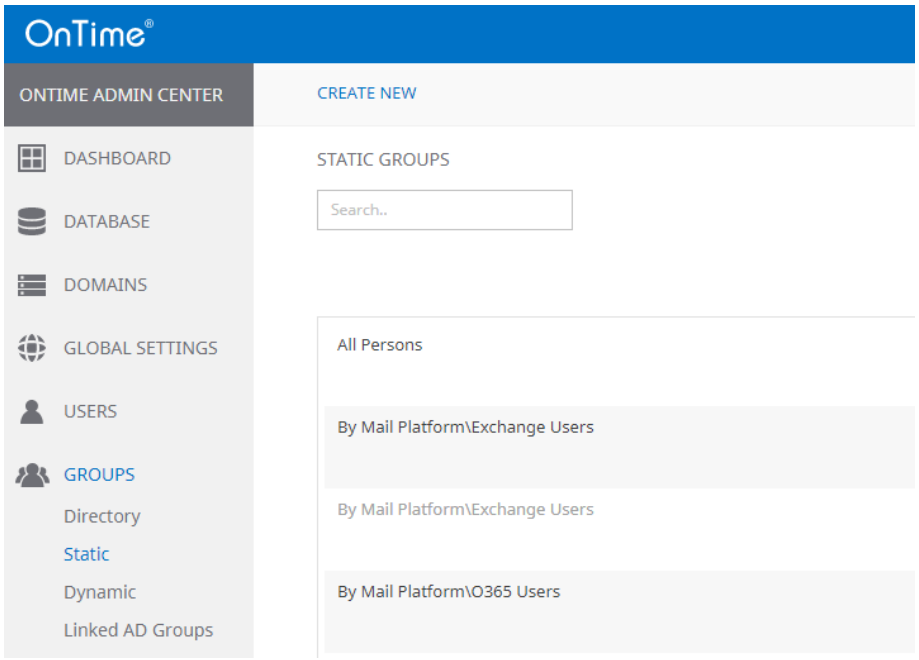
To show these groups in the OnTime client, tick 'Show Directory Groups in Clients' and ”Save”.

If you change your groups in Active Directory

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

Static Groups

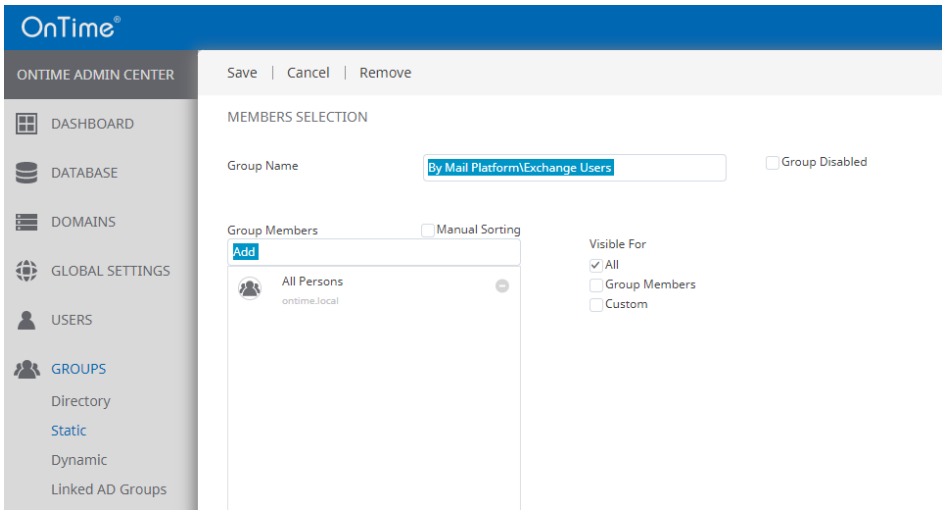
Click 'Groups/Static' and 'Create New' for groups within OnTime.



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.



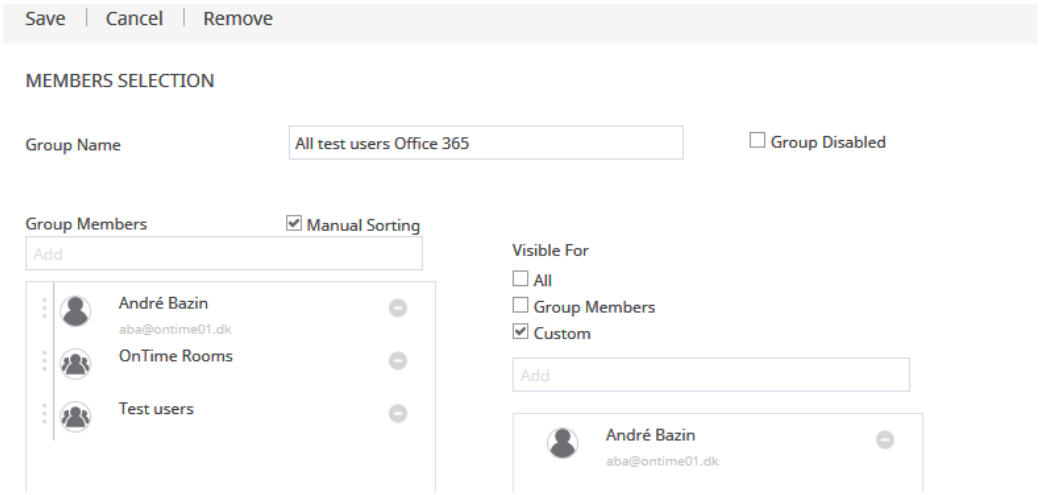
Group Name – Enter a name for the group

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.

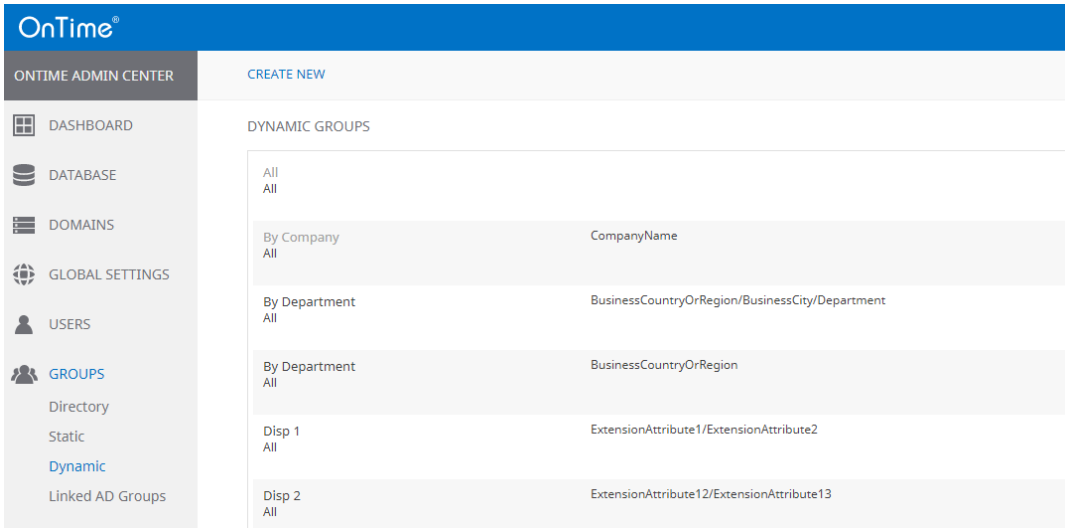
Changes in the static groups must be followed by clicking 'Start' at 'User & Group Sync' in the **Dashboard.**

Dynamic Groups

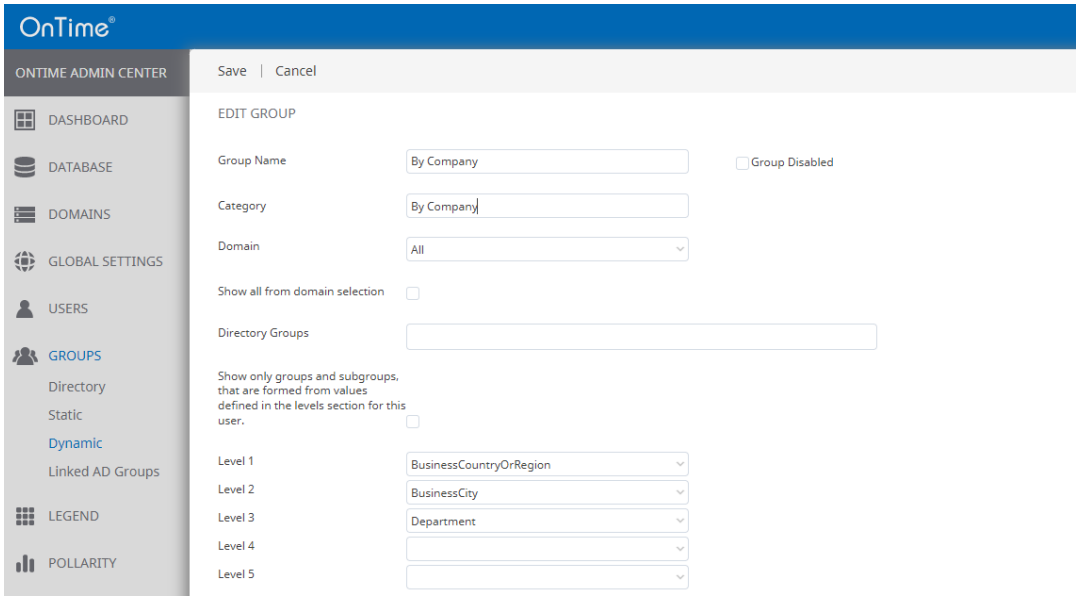
Click Groups/Dynamic to configure your dynamic groups. These groups depend on the users' attributes in 'Active Directory/Exchange'.

Dynamic Distribution Groups from Office 365 are supported.

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.**

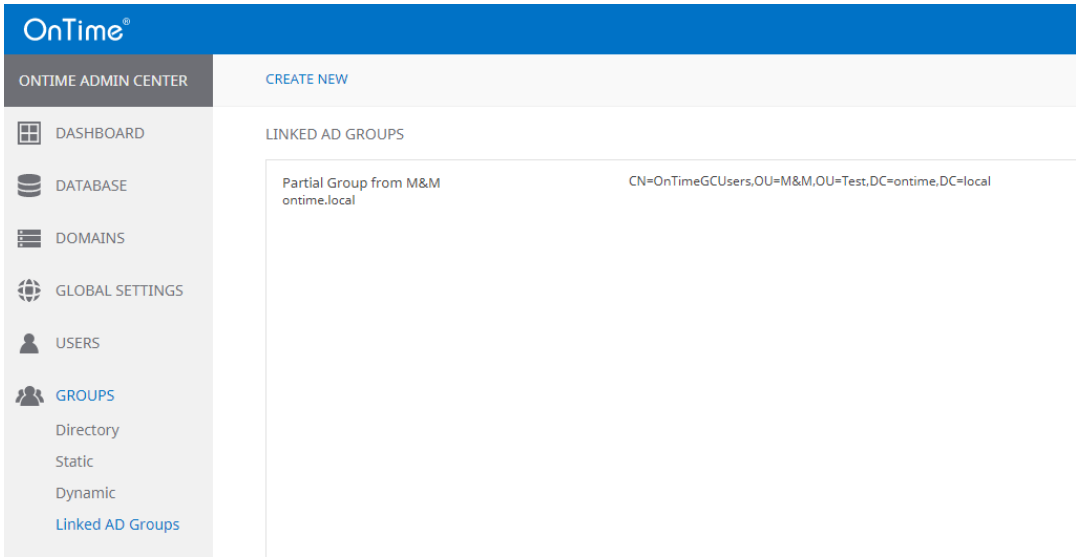
It is possible to add a “Show All” group for the OnTime clients, by adding a group and tick “Show All”. This group will contain all members in OnTime.

Linked AD Groups

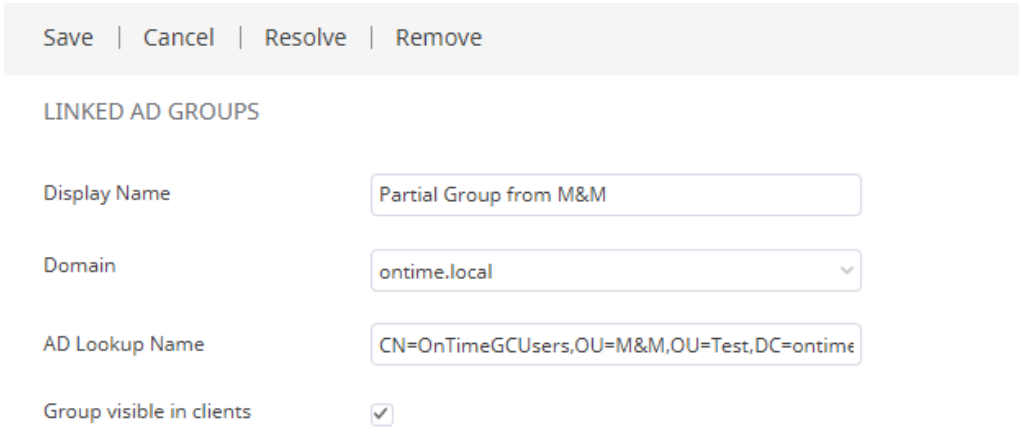
This is only possible if Domain configuration is using ldap.

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.

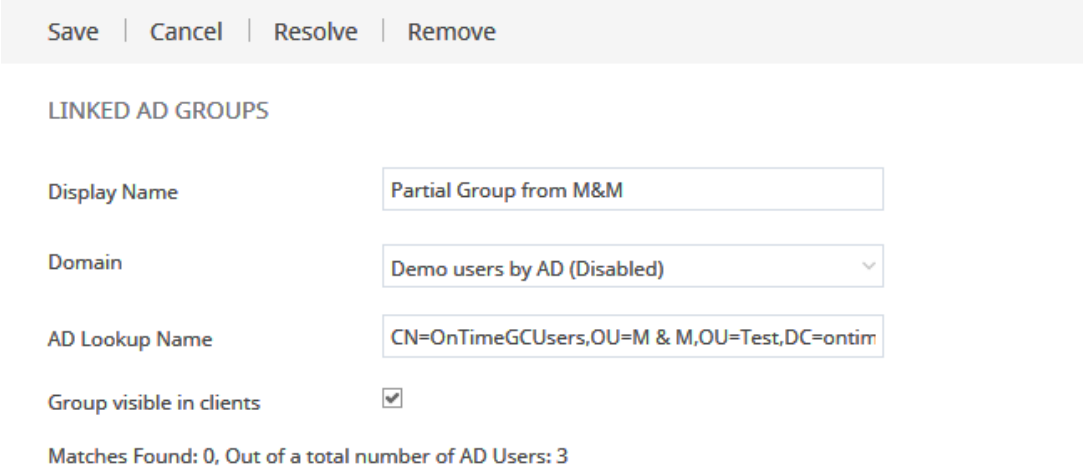
Click Groups/Linked AD Groups to configure your Linked AD Group, click ‘Create New’ or choose a group to edit.



An example:



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

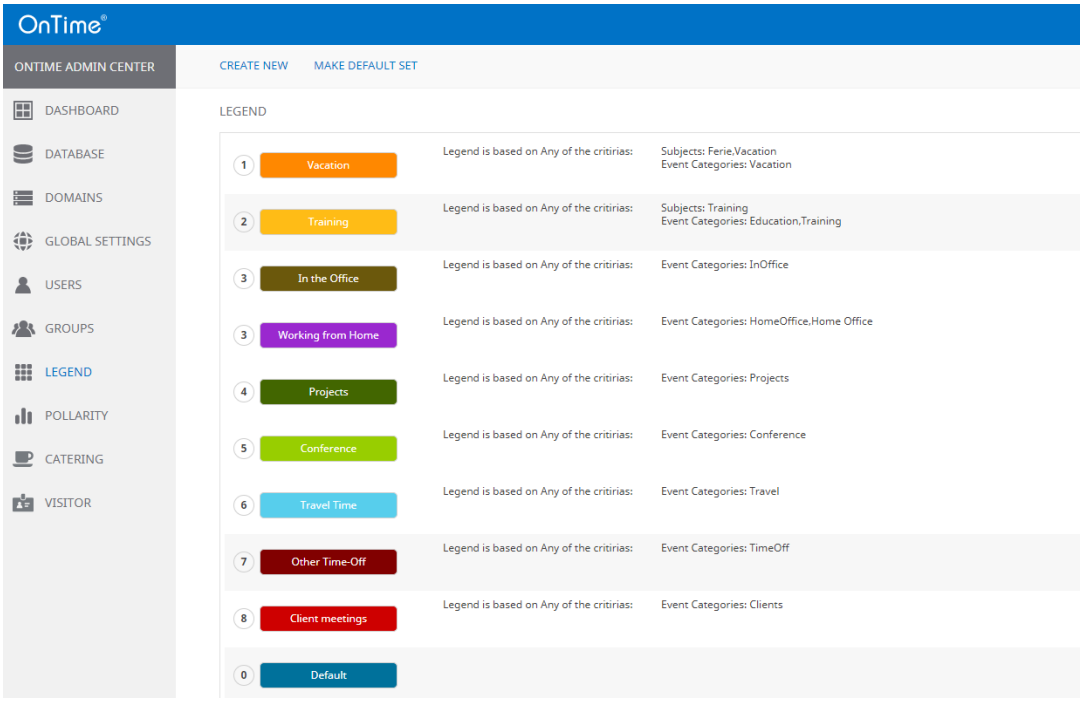


Legend

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.

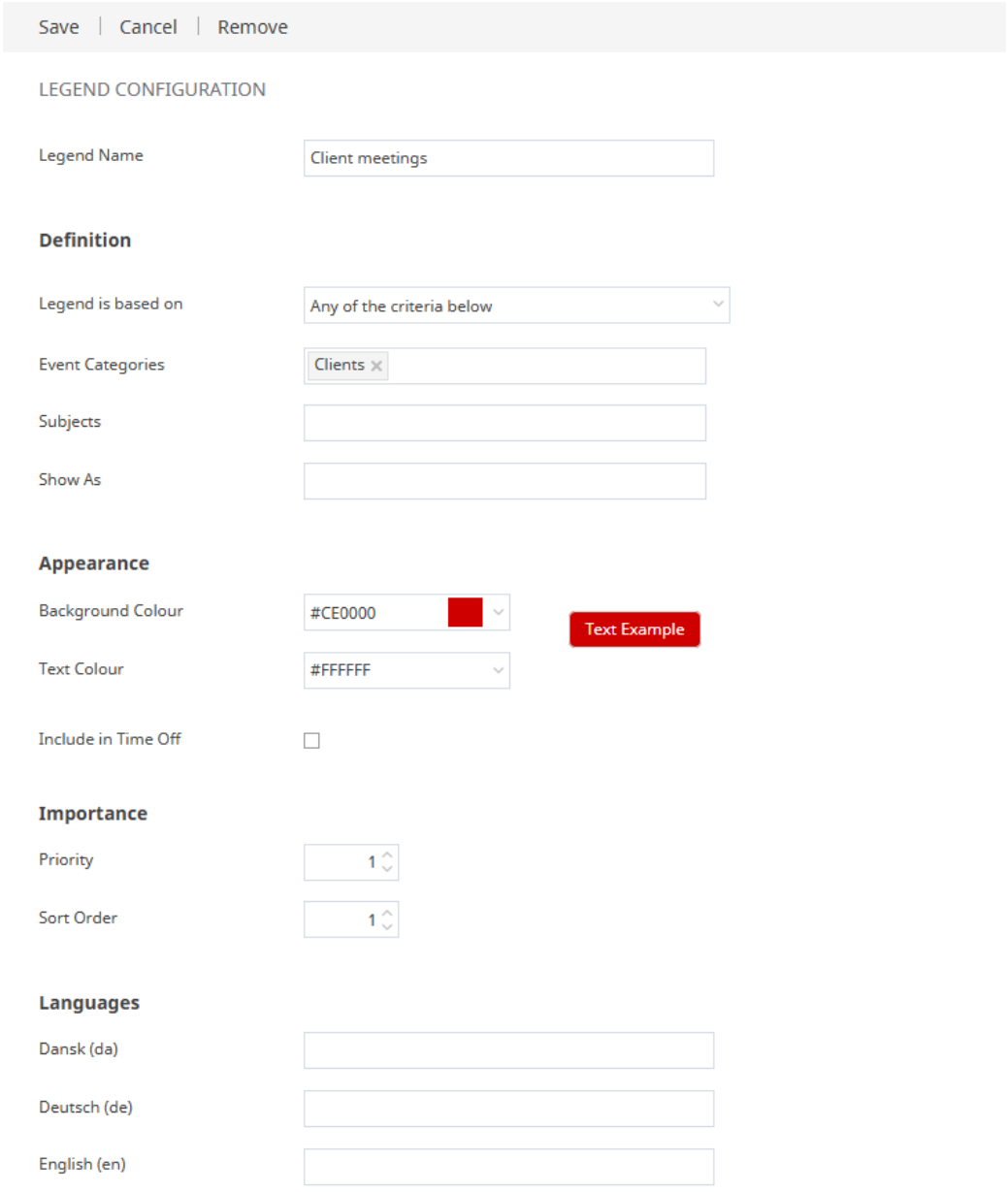
The color coding of the categories will show in the user’s calendar overview.



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.

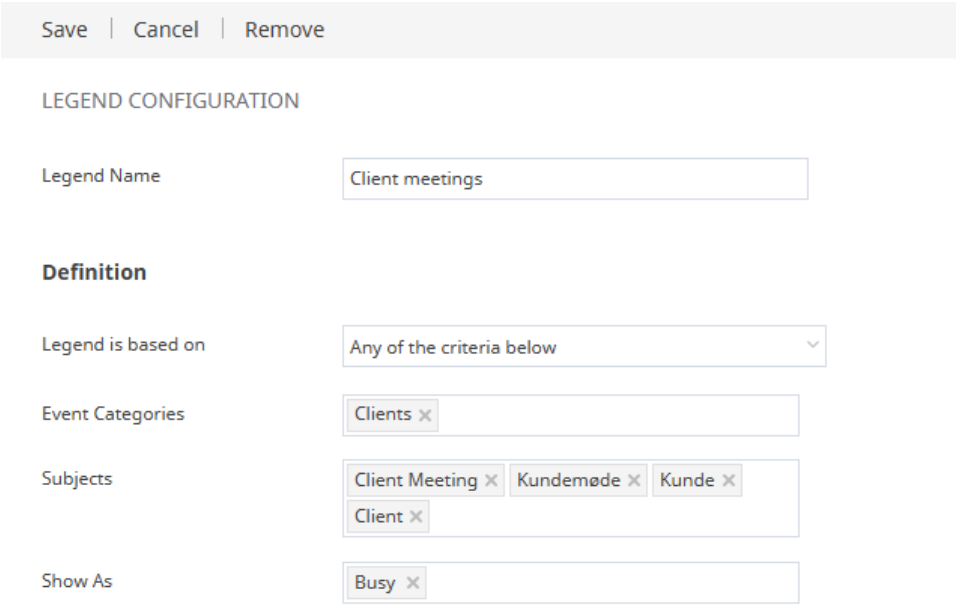
The button “Make Default Set” creates eight standard legends, as shown above.

Click the Legend name to see the details:

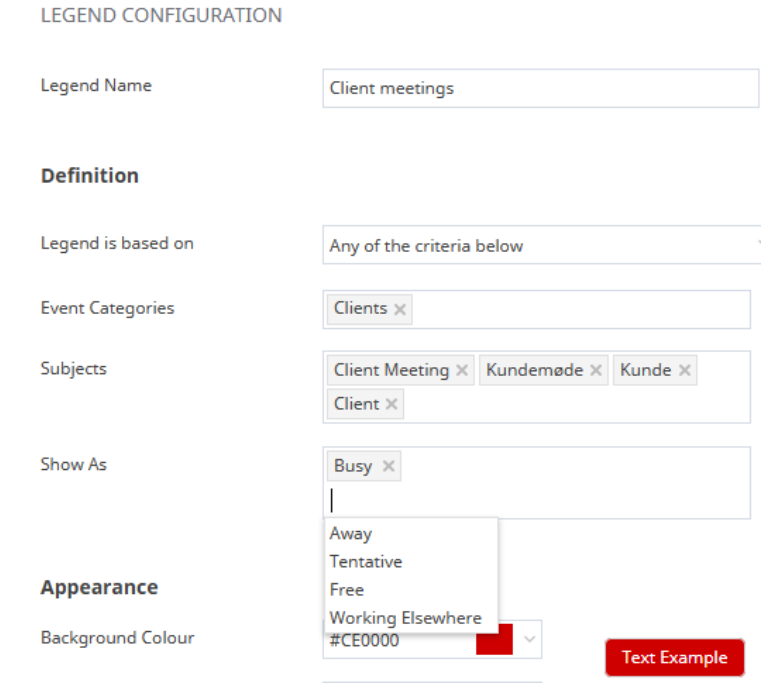


Definition

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** is 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.

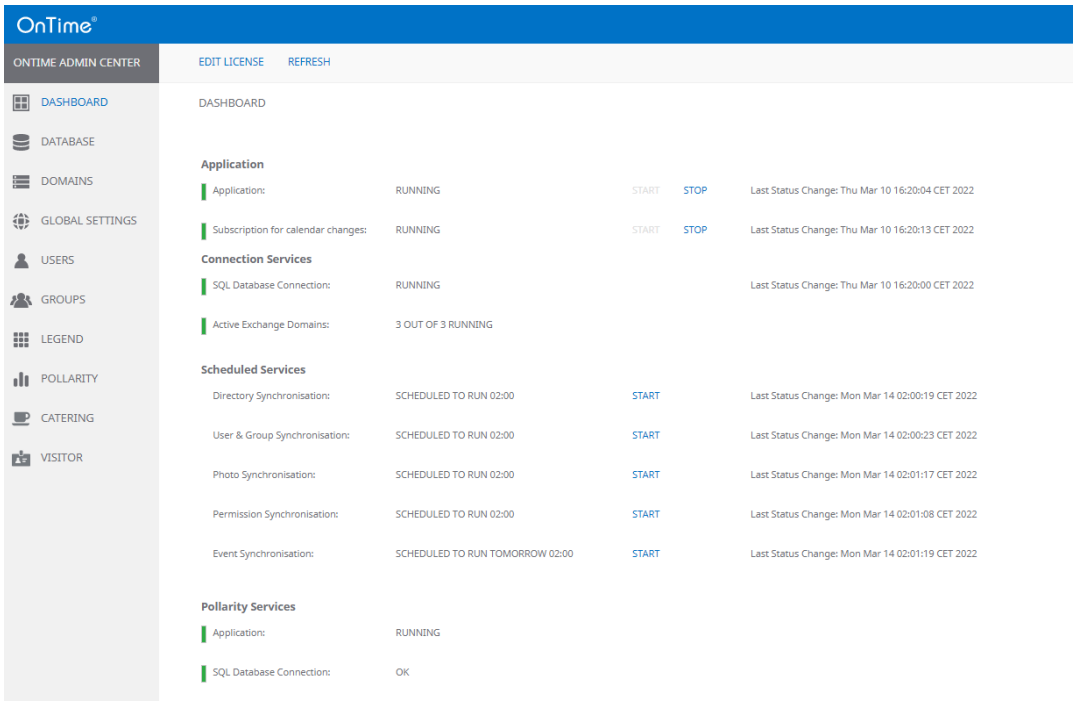
Changes in the "Legend Configuration" only requires clicking "Save", no further actions in the Dashboard are necessary.

Pollarity

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

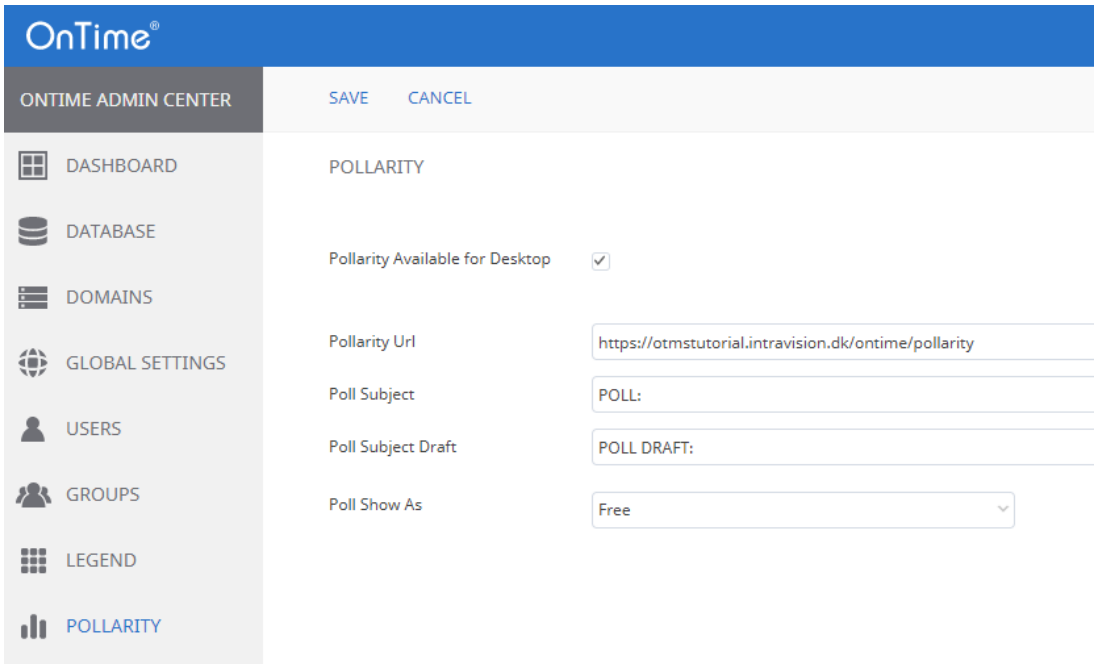
If Pollarity is used in OnTime with users external to the environment, a reverse proxy solution in the DMZ is required.
Ref. to **Reverse Proxy.**

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



Configuration of Pollarity

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



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

Pollarity 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’.

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

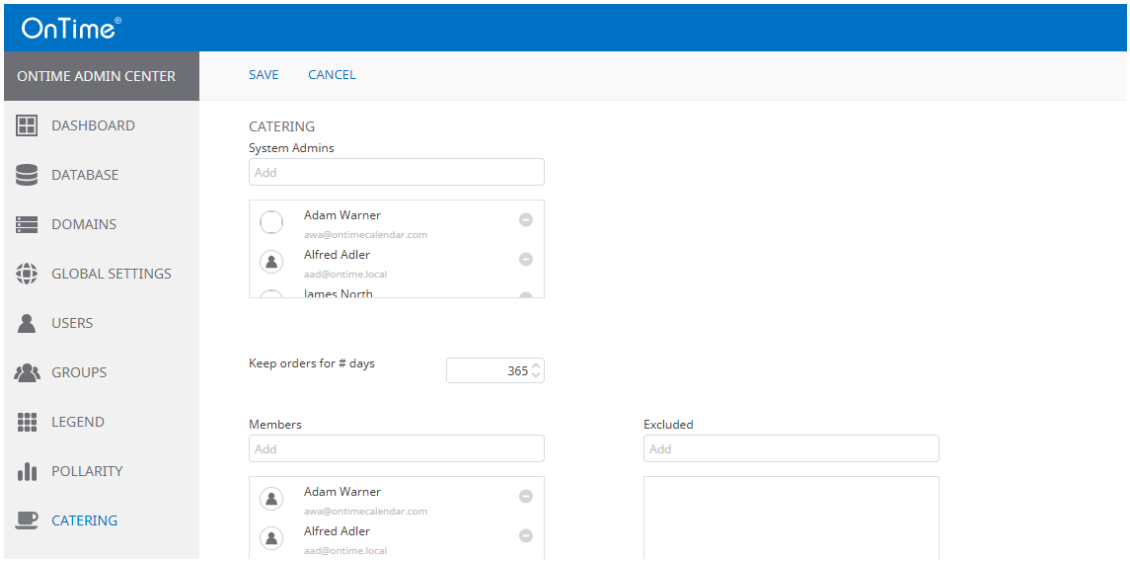
The role **'System Admin'** is to create/remove/edit canteens in the 'Catering Manager'.

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 Center' 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'.

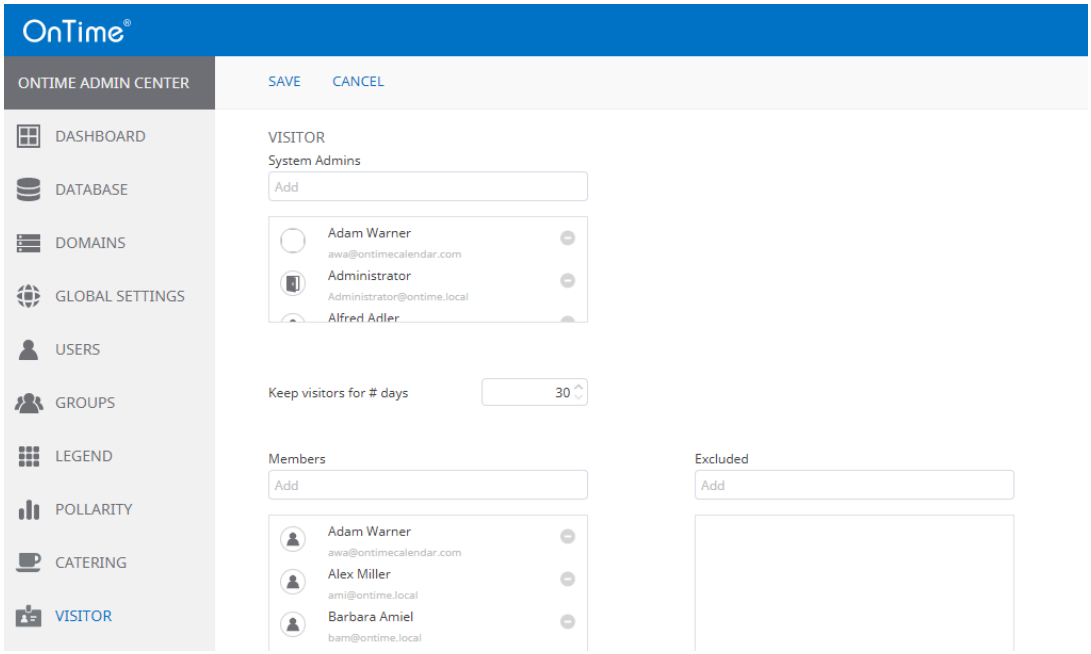
The role **'Visitor Manager'** is to edit locations - and administer visitors.

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

The 'Visitor Manager' is accessed by the URL:
https://ontime.example.com/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 Center' to administer the persons 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.

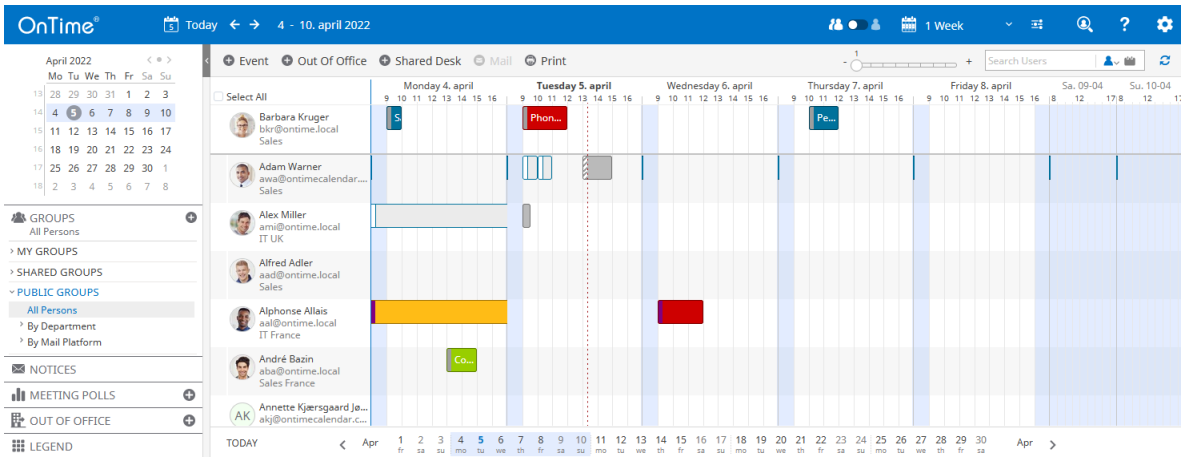
Visitor 'Members'
Add Visitor 'Members' by entering characters and selecting persons or OnTime 'Directory Groups' in the 'Add' box.
The members in the list are dedicated to the two roles 'Visitor Managers' and 'Visitor Staff' in the 'Visitor Manager':
https://ontime.example.com/ontimegcms/visitormanger
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 a button for 'Visitor registration' when creating a meeting in Ontime.

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’.

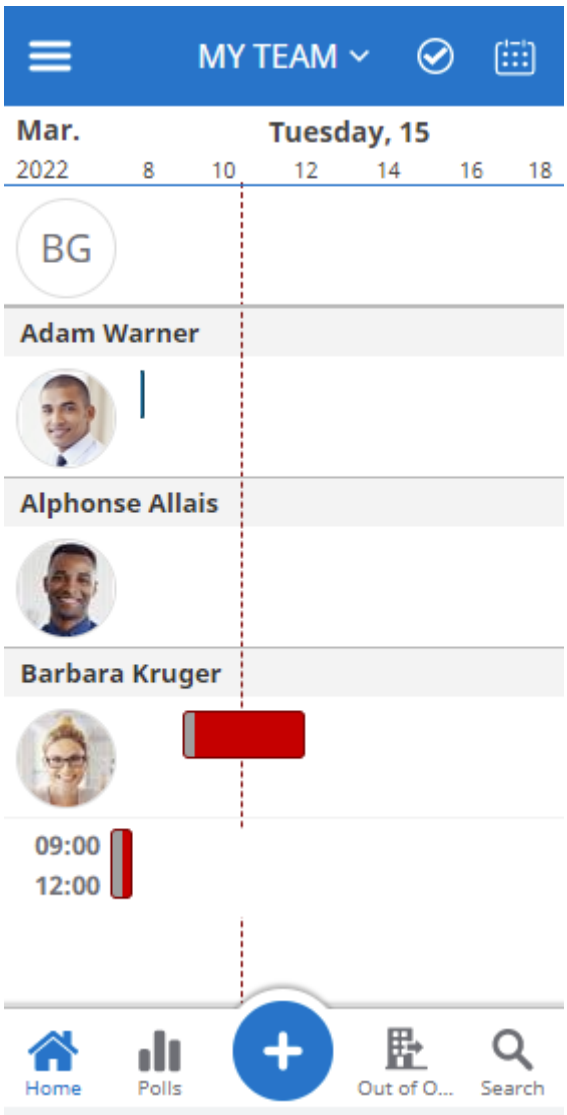


OnTime client Web Mobile

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 MS Teams and MS Outlook.

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

If you are using multiple domains, you need to register an OnTime application for each of the domains you want to use in MS 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: MS Teams, and 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 Office 365 is described in the section **Upload of add-ins for OnTime**

Add-in for OnTime in MS Teams

Note: MS 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 MS 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\teams.

Edit the **manifest.json** file and change the following to fit your setup.

In the bottom of the file, look for:

```
"validDomains": [
    "*.ontimecalendar.com",
    "*.ontimesuite.com",
    "*.intravision.dk"
  ],
  "configurableTabs": [
    {
      "configurationUrl": "https://ontime.example.com/teams/config.html",
      "scopes": ["team"]
    }
  ]
```

In the 'validDomains' area, replace the existing with your domains in the same manner.

In the 'configurableTabs' area, replace 'ontime.example.com' with your DNS name for the OnTime server.

Save the json file and zip it together with the **img** folder. The name of the zip file is for you to decide.

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

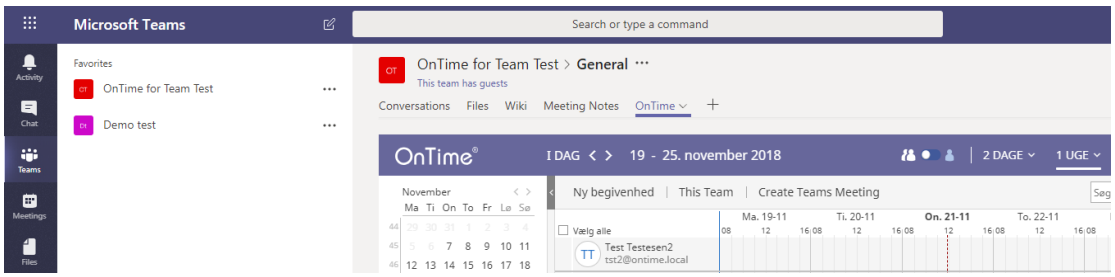
Teams config.html at your OnTime server

In your OnTime installation files you will find a .cmd file ‘add-url-config.cmd’ in the folder \teams
- Run it as ‘Administrator’
- you will be asked to enter the name (URL) of your OnTime server
- in the resulting config.html file you see your resulting server name as example: https://ontime.example.com/ontimegcms/teams
- the .cmd file also copies config.html to the webservers teams folder: C:\Program Files\Intravision\OnTimeMS-x.x\tomcat\webapps\teams

User setup for MS Teams

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 app.
Click 'Use these settings' and 'Save'.

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



Add-in for OnTime in MS Teams Rail

In MS Teams it is possible to add OnTime to the lefthand navigation in MS Teams – **the Rail**

To create the OnTime rail-application that can be used in MS Teams, go to the OnTime servers install files C:\Program Files\IntraVision\OnTimeMS-x.x\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_rail.zip'

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

User setup for MS Teams rail

On the Notification Rail sidebar, you will see a new OnTime add-in tab, move it up to make it more useful.

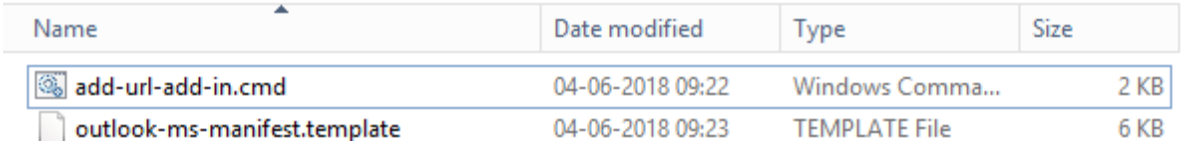
* If you want only to check how it is working, it is easy to uninstall after, right-click - uninstall.

Add-ins for OnTime in Outlook

Installation

Note: MS Outlook 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 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/outlook-add-in folder.



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

Here you type in your OnTime server name (DNS Name – with https!) and the manifest file will be created.

The generated file ‘ontime-outlook-manifest.xml’ lets you deploy on the admin Office 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**

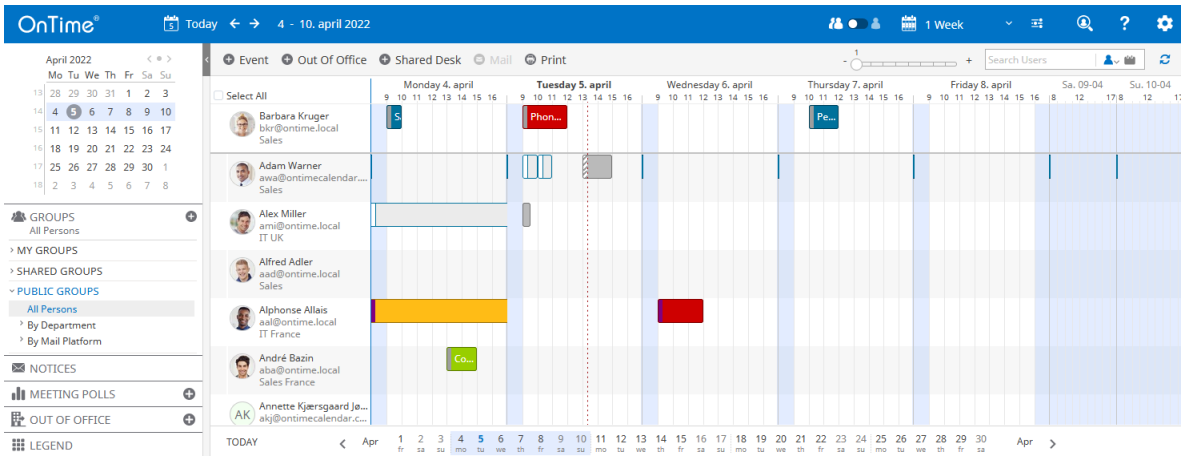
For more information:

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

OnTime in Outlook

In Outlook click “OnTime” to see your OnTime Calendar.

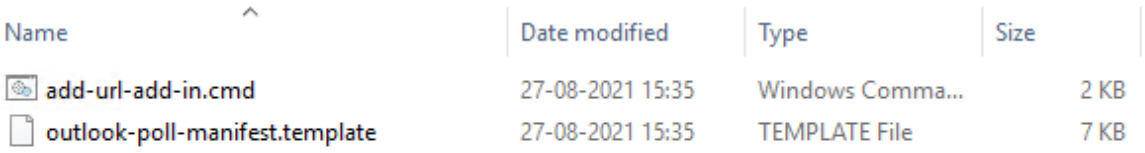
If you do not see the OnTime button, you might have to adjust your settings for the bottom menu line, click the three dots - default is only four items in the menu.



OnTime Pollarity - add-in in 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/outlook-poll-add-in' folder.



Name	Date modified	Type	Size
add-url-add-in.cmd	27-08-2021 15:35	Windows Comma...	2 KB
outlook-poll-manifest.template	27-08-2021 15:35	TEMPLATE File	7 KB

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

Here you type in 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 Office 365 account. Remember to choose “add from file” in the selection, when adding.

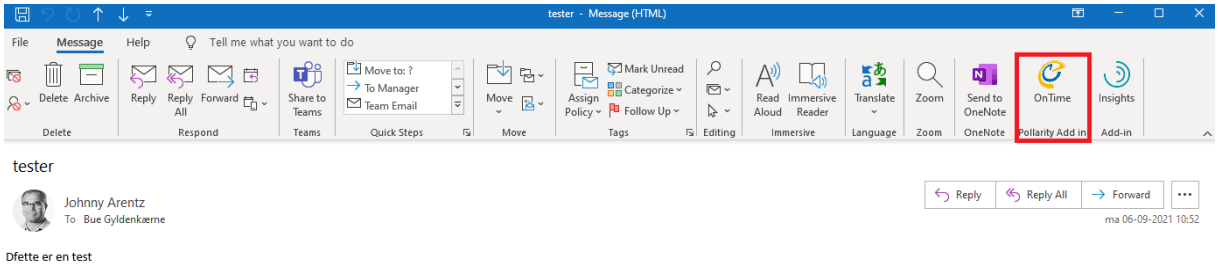
Note:
Upload of the zip-file is described in the section **Upload of add-ins for OnTime**

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 Outlook, with OnTime Poll-add-in

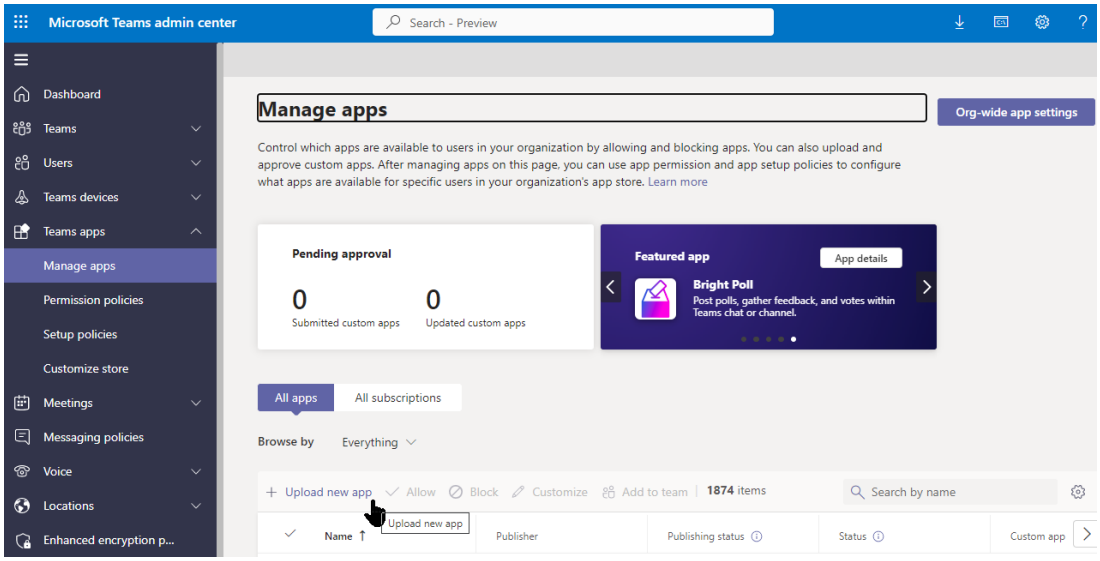
- visible when you open an incoming mail



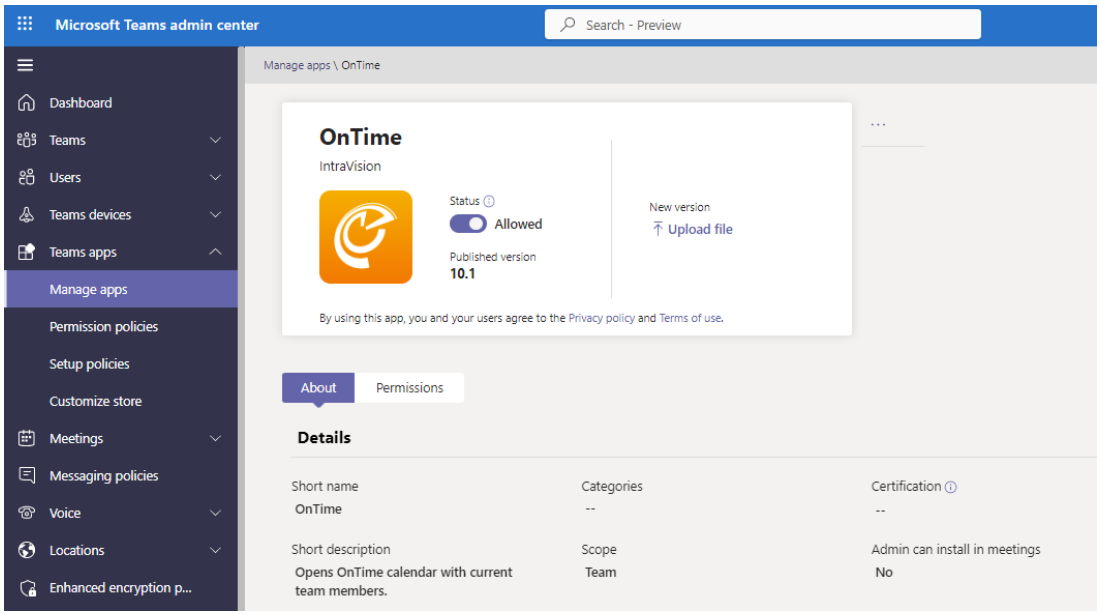
Upload of add-ins for OnTime

To add the OnTime add-in to MS Teams or Outlook, 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:



Click ‘Upload new app’ and click ‘Upload’
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 OnTime in Teams and Outlook, please refer to:
https://www.youtube.com/watch?v=CI2vHsN5XPk

- and of course the official Microsoft documentation:
https://learn.microsoft.com/en-us/microsoftteams/teams-overview

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 URL´s

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 url´s. 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"	Open existing item
"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}

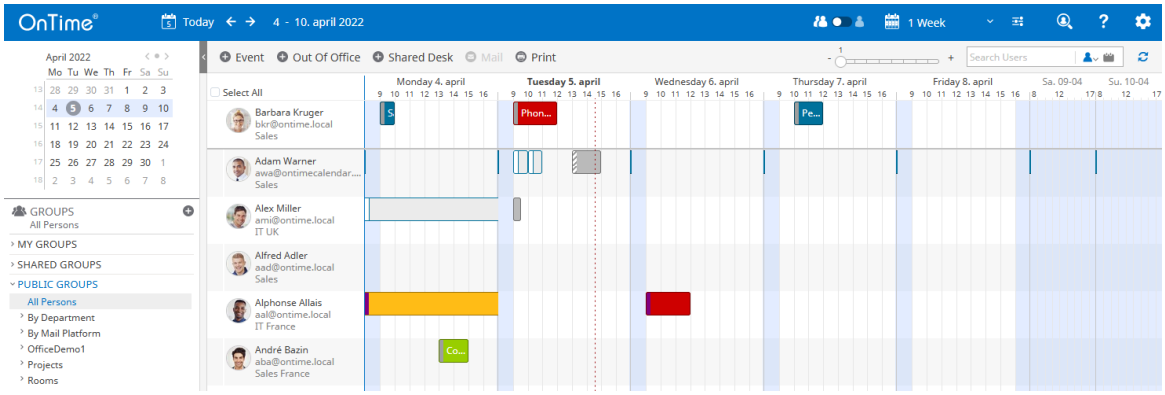
Key	Value	Description
"view"	"days" "weeks" “ooo” “list” “day” “week”	Group view Group view Time off view List view Person view Person view
"starthour"	0 – 23	
"endhour"	1 – 24	
"units"	1 – 9 weeks, 1 – 14 days	
"offhours"	true/false	
"weekends"	true/false	
"rowheight"	1 – 9	

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

Creating Integrations with OnTime Desktop

Open the desktop client with a specified user selected.

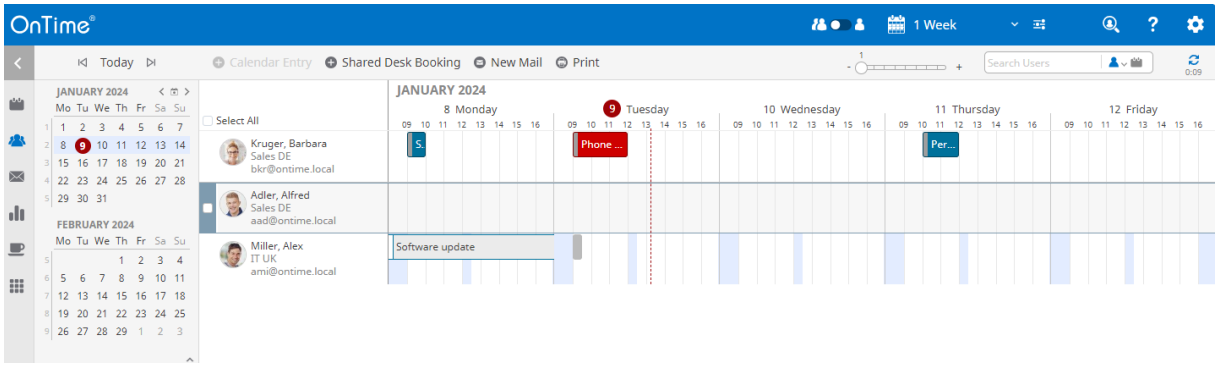
https://otmsdemo.intravision.dk/ontimegcms/desktop?user=”bkr@ontime.local"



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

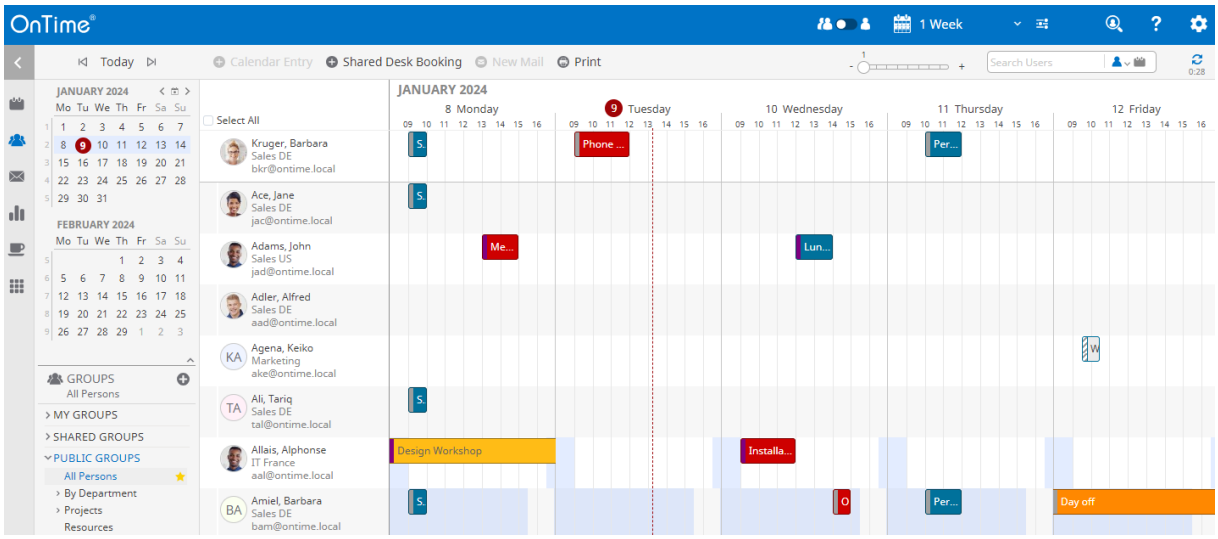
https://otmsdemo.intravision.dk/ontimegcms/desktop?users=["ami@ontime.local","aad@ontime.local"]

List of ‘users’ mail addresses.



Open the desktop client with a public group selected

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



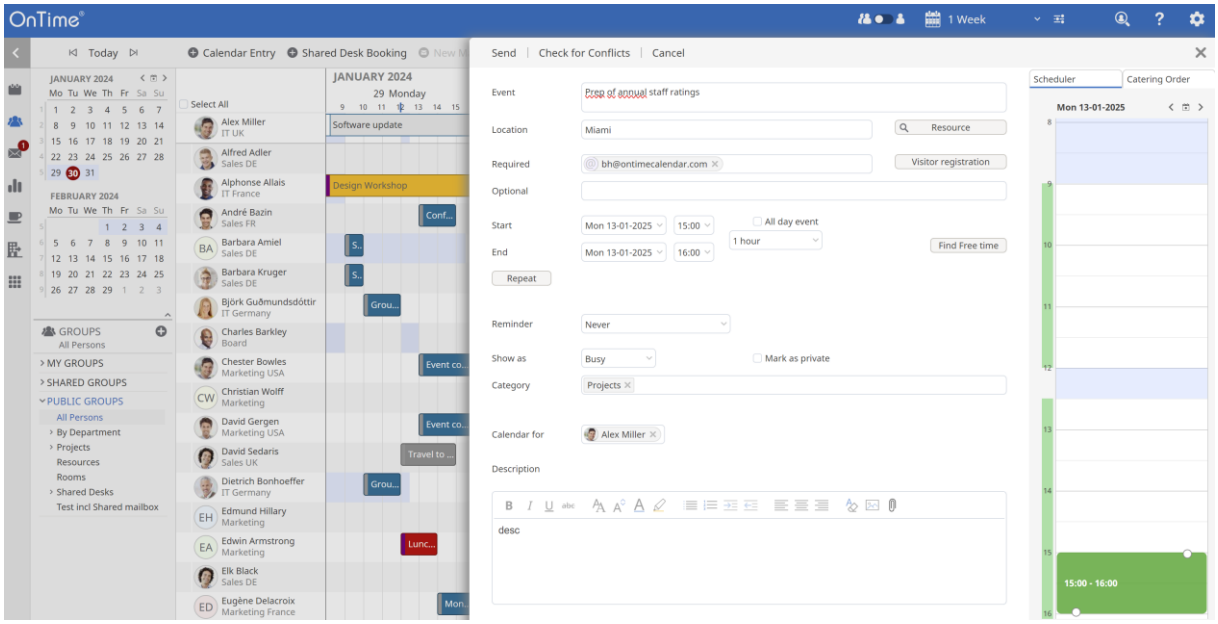
Open the desktop client with an existing Entry Selected

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

Open the desktop client creating a new entry

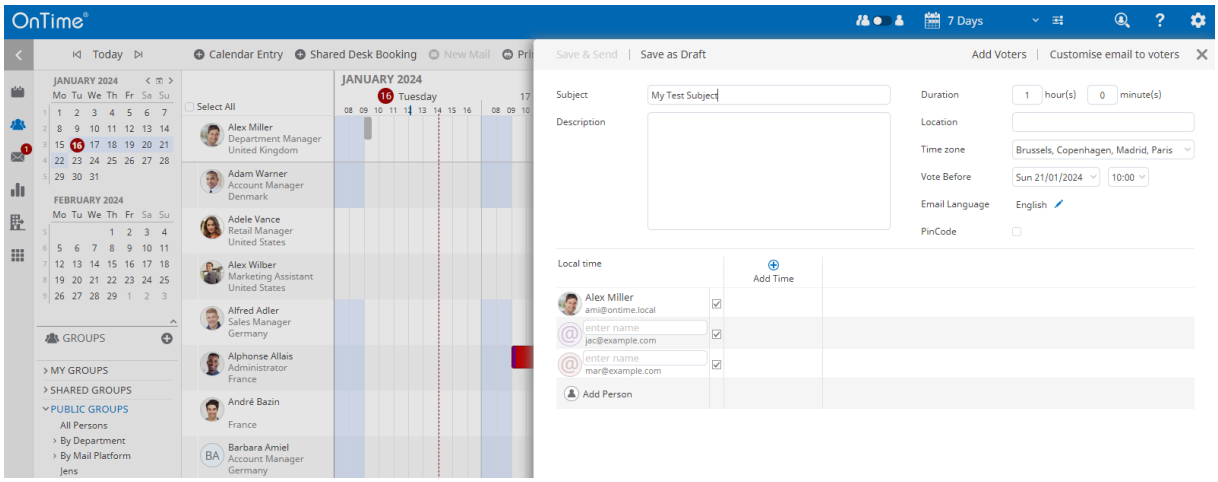
Example:

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

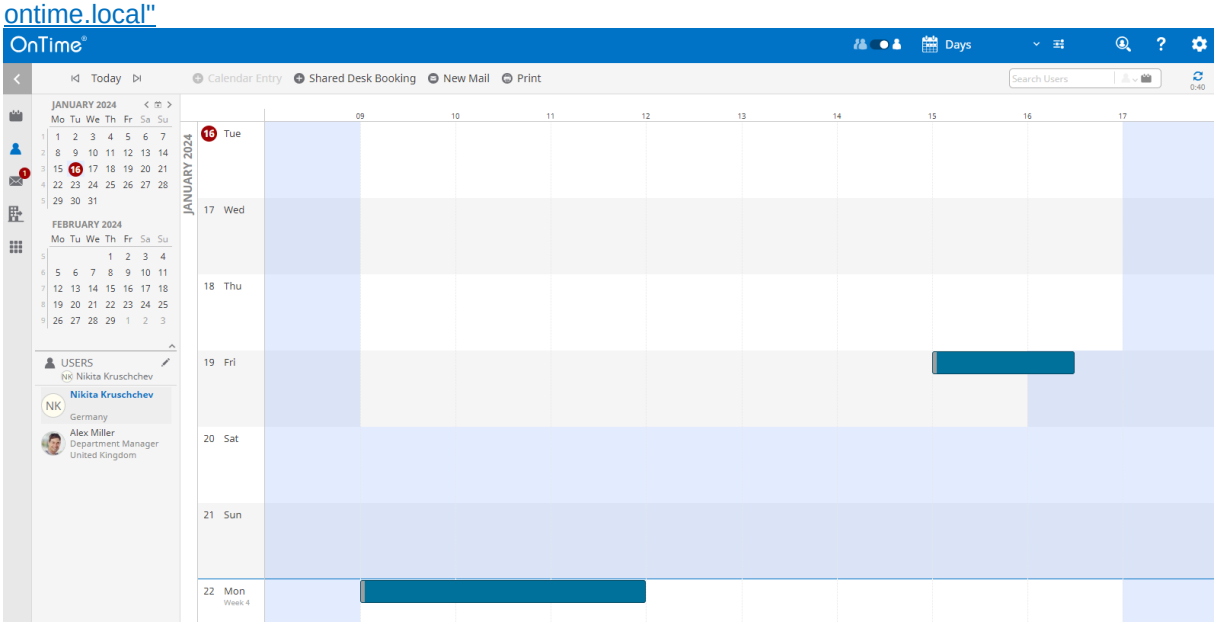
https://otmsdemo.intravision.dk/ontimegcms/desktop?newpoll={"emails":["mar@example.com","jac@example.com"],"subject":"My Test Subject"}



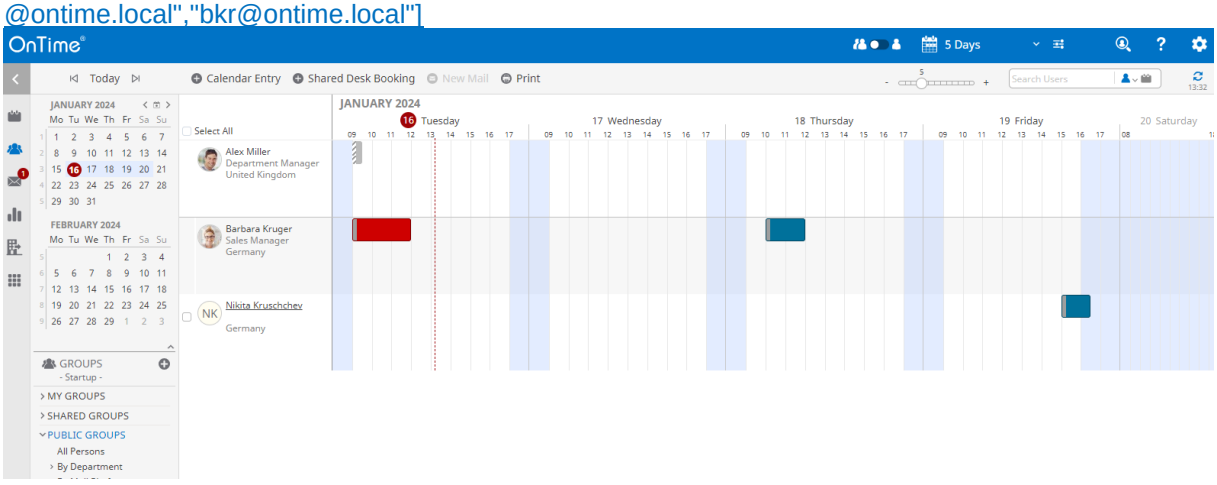
Open the desktop client in a view

Examples:

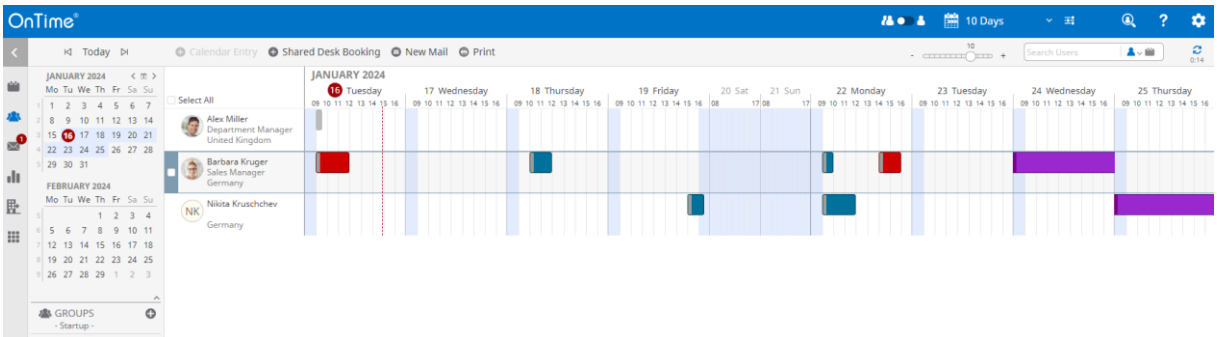
Person view:
https://otmstutorial.intravision.dk/ontimegcms/desktop?view={"view":"day","rowheight":5}&user="nkr@ontime.local"



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"]

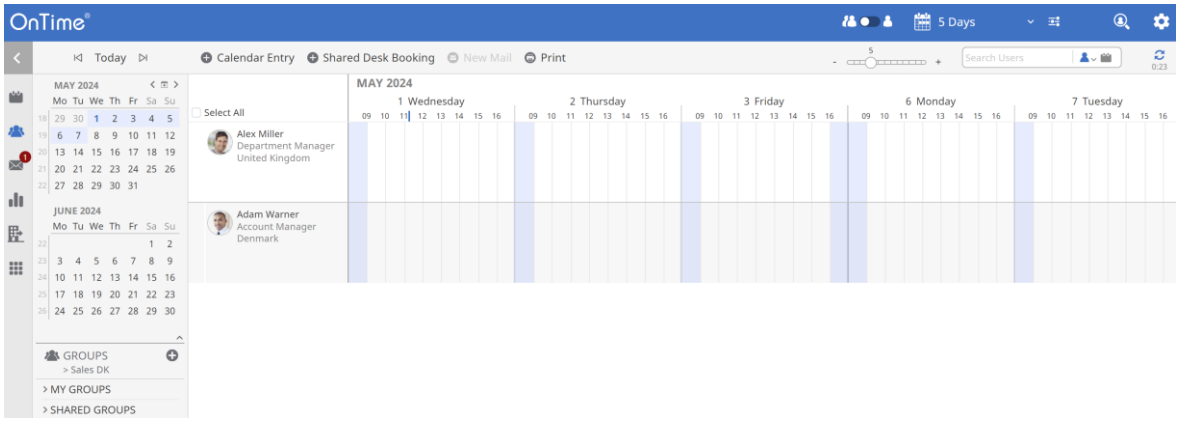


Open the desktop client a certain date with 'viewstart'

Example:

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

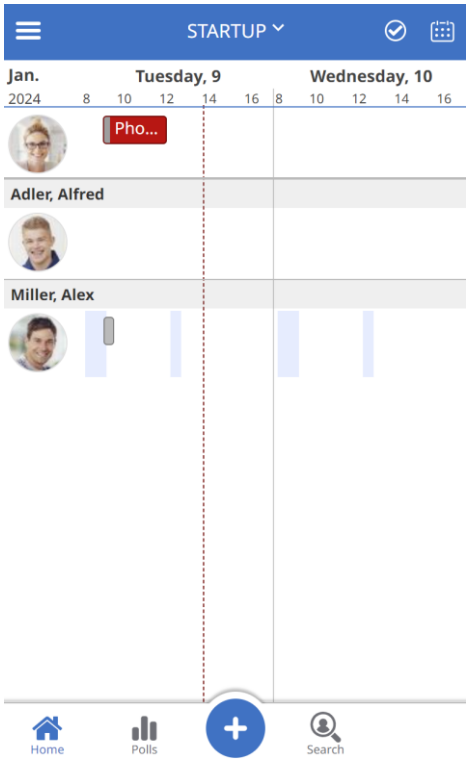
The view opens with the group recently viewed.



Creating Integrations with OnTime Mobile

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

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



Open the mobile client with a selected group

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

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

Open the mobile client with an existing Entry Selected

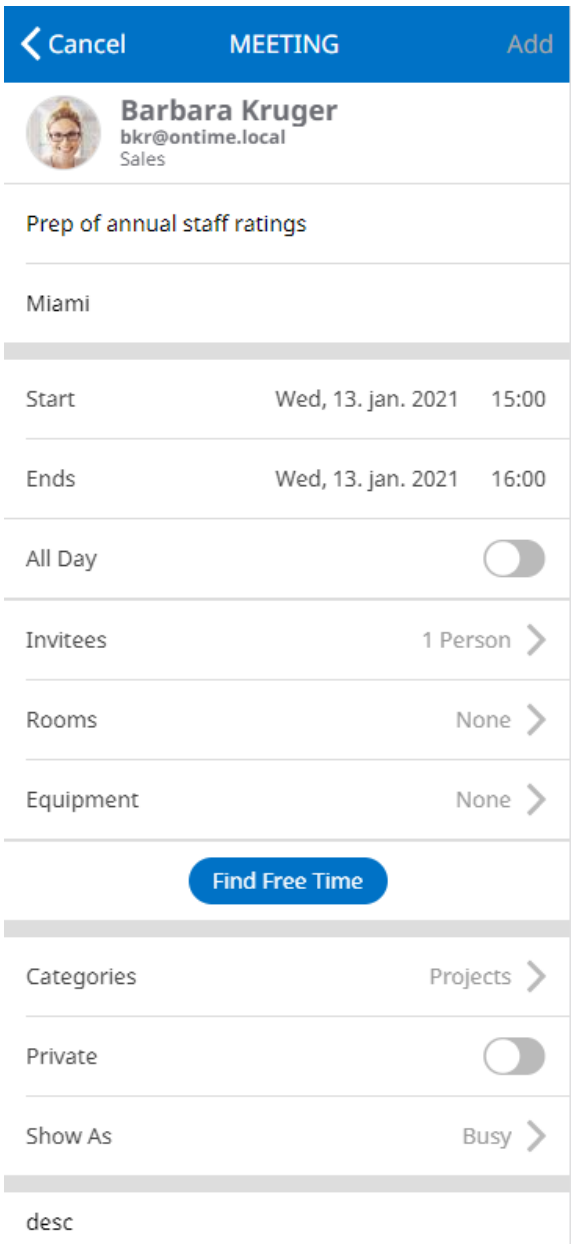
Example:
https://otmsdemo.intravision.dk/ontimegcms/mobile? openitem={"Email": "user@user.dk", "EventID" : "<EventID>"}

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)



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 opened 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 specially 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

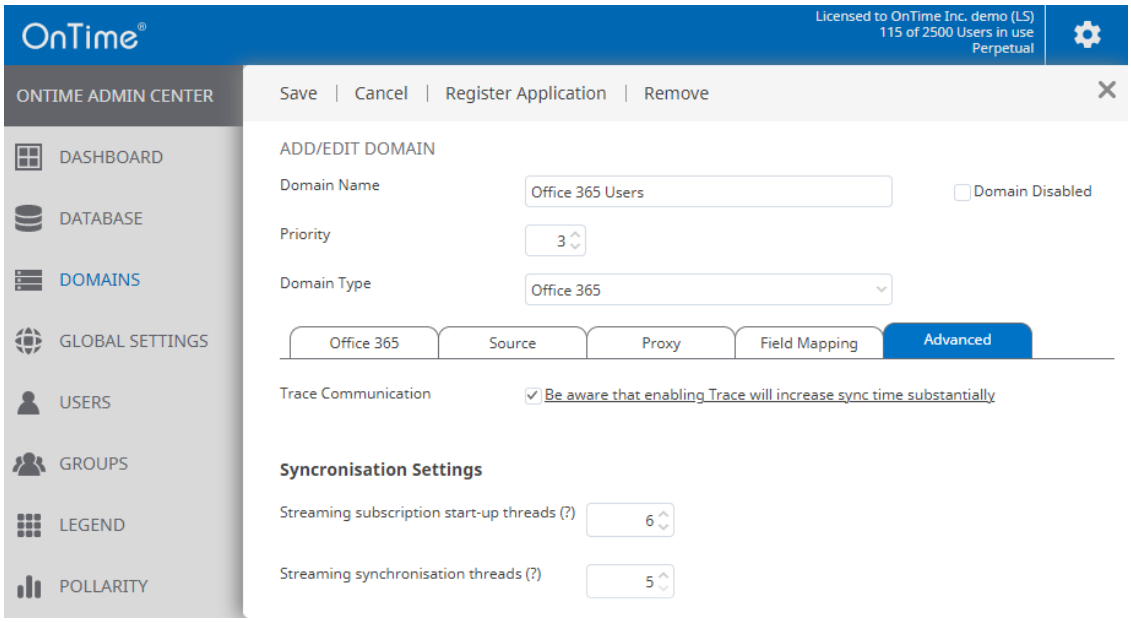
`manager` - Log for the `manager` application which is shipped with Tomcat by default

`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 Center” – 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.

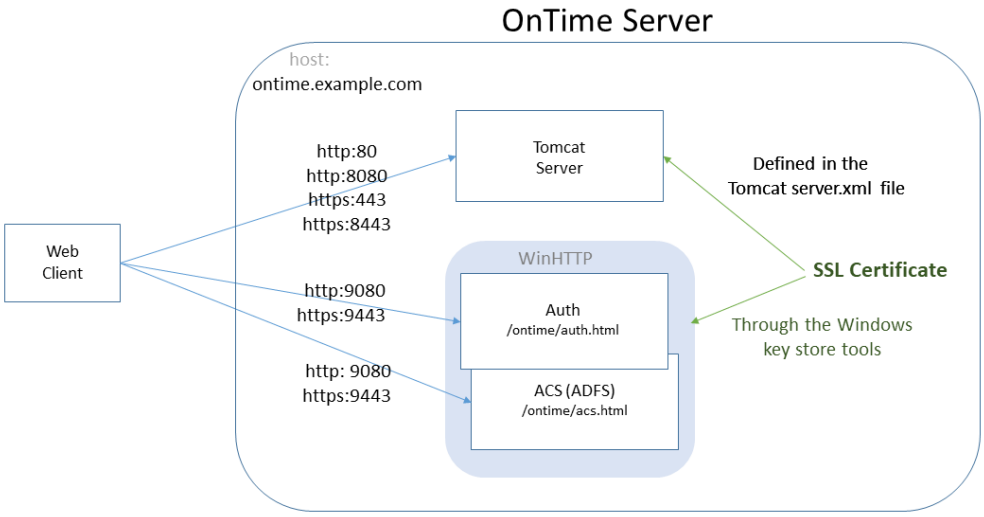
In the C:\Program Files\IntraVision\OnTimeMS-x.x\tomcat\logs directory the trace log is found as the filename starting with ontimetomcat-stdout (current date).

- like

ontimetomcat-stdout.2021-xx-xx.log

Appendices

OnTime server components and ports

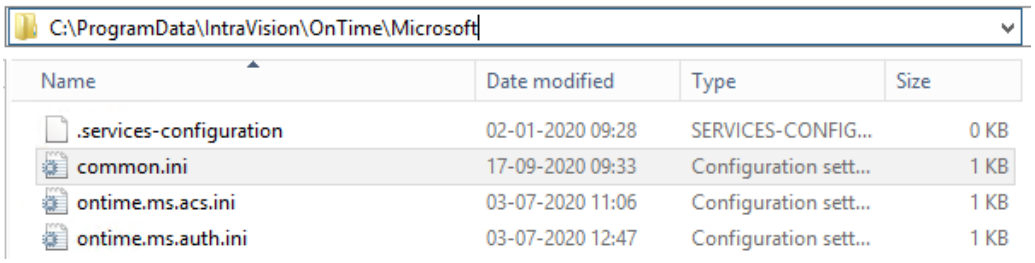


Redirection whitelists

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

Retrieve the private key:

```
C:\OpenSSL-Win32\bin\temp>
```

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

If you have not made an openssl.cfg file, you will see a warning, not important.
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:

```
C:\OpenSSL-Win32\bin\temp>
..\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
```

Retrieve the server's certificate:

```
C:\OpenSSL-Win32\bin\temp>
..\openssl pkcs12 -in certs.pfx -clcerts -nokeys -out ontime-rsa-cert.pem
```

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
```

2. Extract the certificate chain, in the command prompt:

```
C:\OpenSSL-Win32\bin\temp>
..\openssl pkcs12 -nokeys -in certs.pfx -out ontime-rsa-chain.pem
```

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'.

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

   C:\ProgramData\IntraVision\OnTimeGCMS\keys\

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

SSL certificates for the OnTime Auth Service

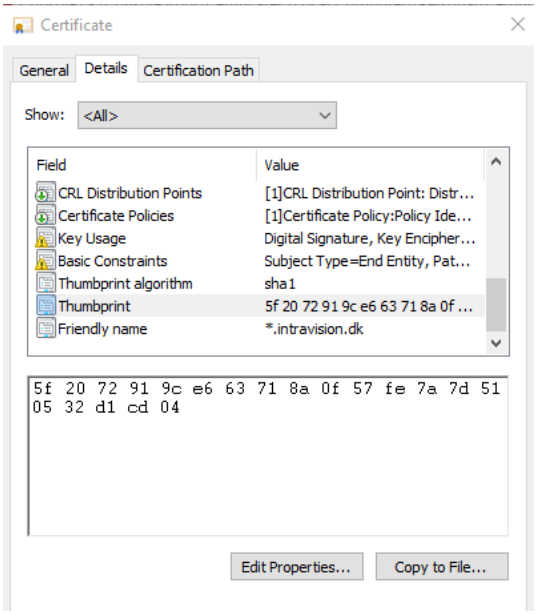
If SSL (https) communication is required for the OnTimeMS Auth service, you must install a certificate at the Windows server. Acquire an SSL certificate pfx or p12 (pkcs12 format) file for the OnTime server.

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).

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.

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

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

SSL root certificates for the OnTime server

One 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.

In your current OnTime installation open a command prompt as administrator in the directory
C:\Program Files\Intravision\OnTimeMS-x.x\jdk\lib\security.
Adapt the following command to your requirement, all in one line:

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

List the entries of the certificate store:

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

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 (multifactor 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.

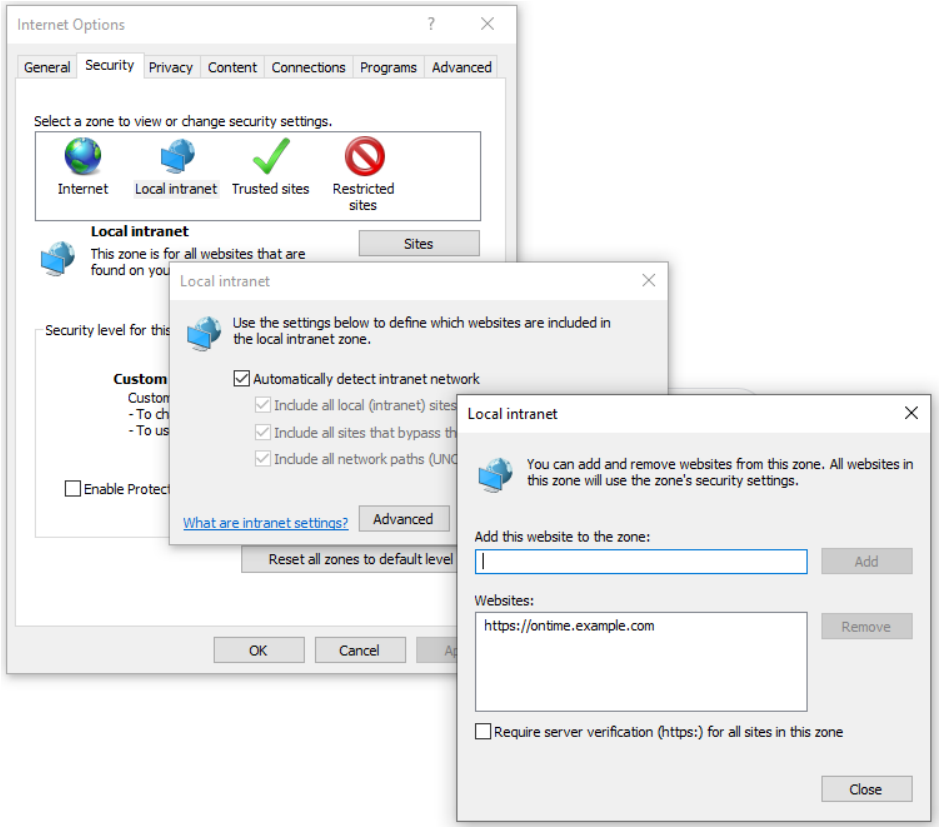
The parameter ‘LDAP_URL’ may be used to address a certain LDAP server and eventually a certain ‘OU’ in your AD domain.
For authentication, you remove the ‘;=’ characters in front of LDAP_USER and LDAP_PWD and adapt the parameters to your environment.

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:
For the Microsoft IE browser, go to Internet Options/Security/Local intranet.

Click “Sites” and “Advanced” to add your OnTime server.



The Chrome and Edge browsers trust your OnTime server because of the setup you made in Internet Explorer.

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 Azure

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.

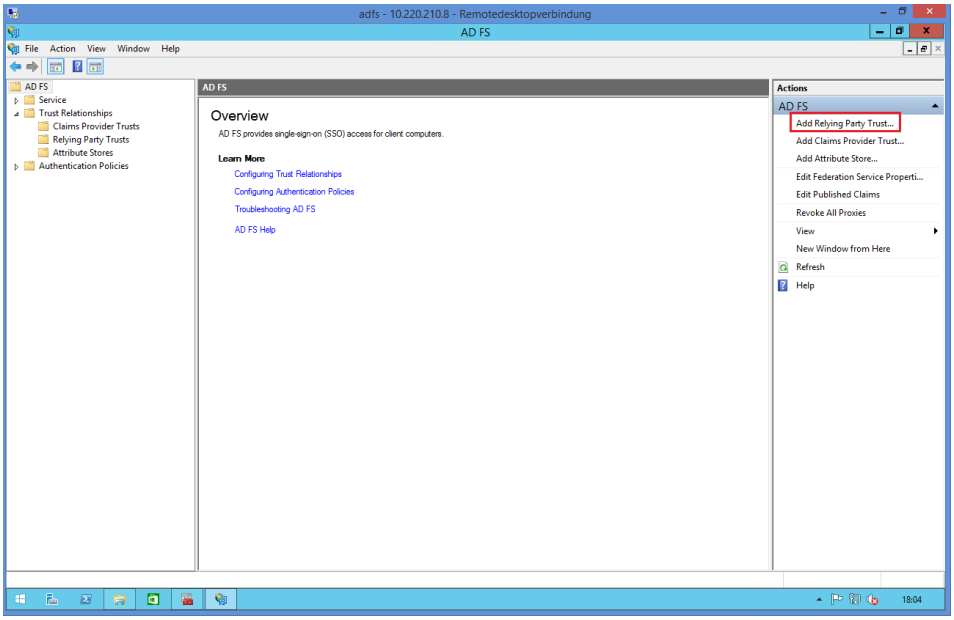
ADFS login (SSO) on-prem

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”.

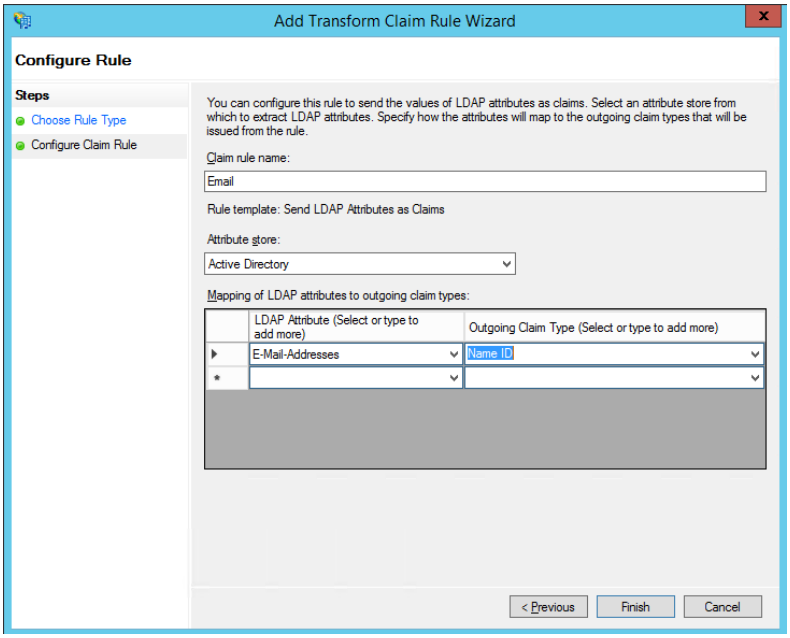
1.5 Choose “Permit all users to access this relying party”.

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

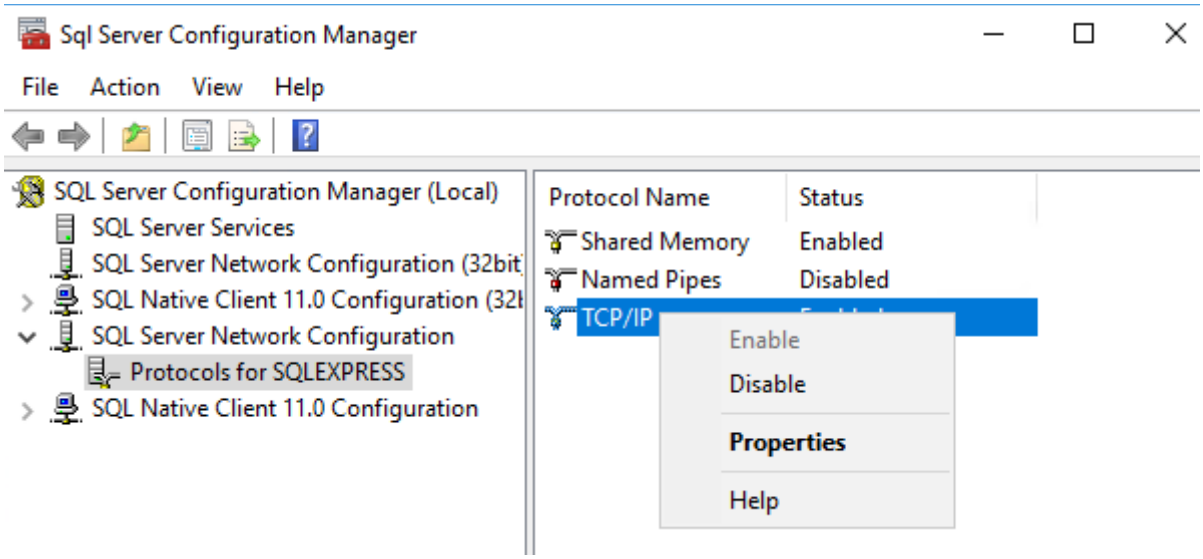
More entries require more lines like

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’.



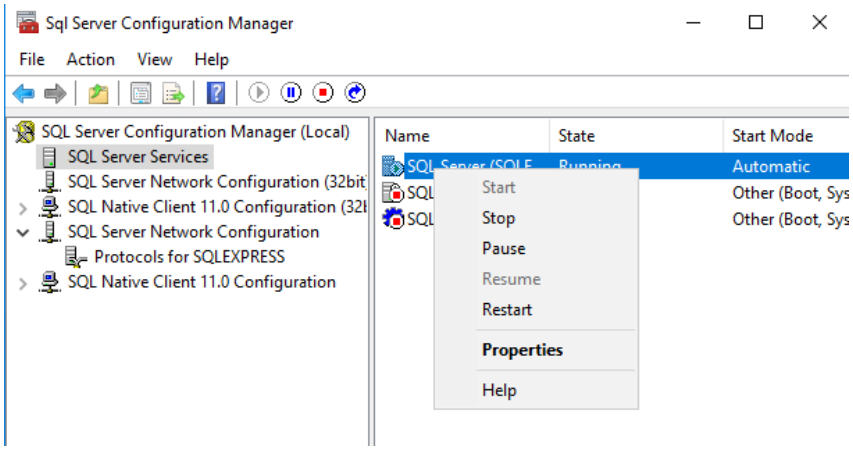
Right-click TCP/IP and choose properties.

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.

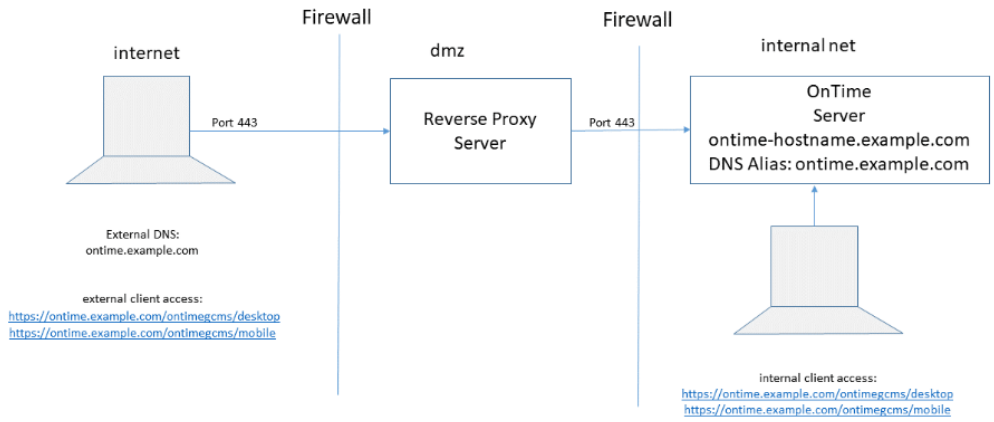
Note: The OnTime authentication method 'HTTP(S) Domain (SSO)' is not supported through a reverse proxy.

OnTime desktop and mobile clients require the following two URL's 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 is not able to 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