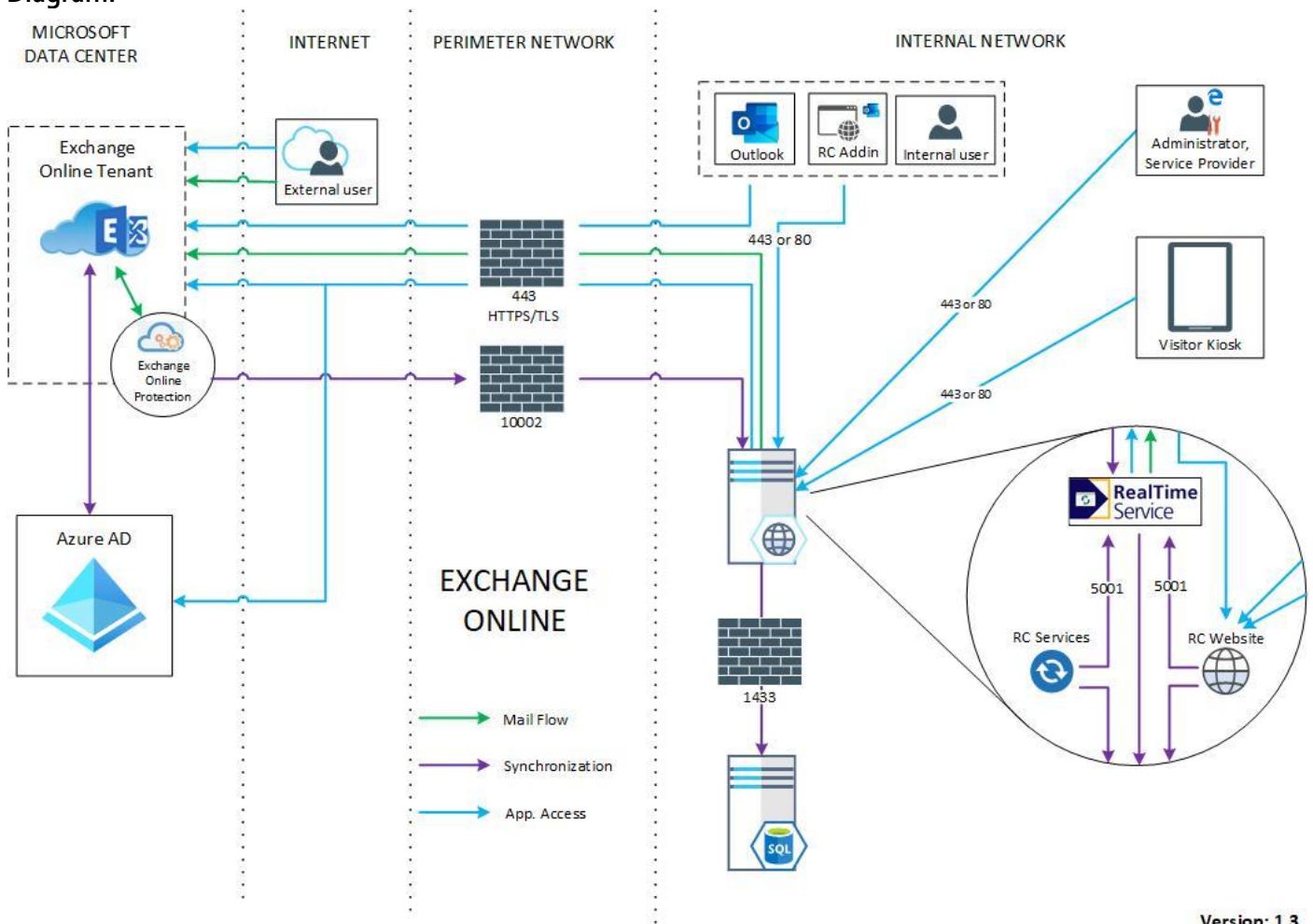


# O365 Resource Central requirements

## Application server system requirements.

[System requirements for Resource Central 4.3 - Add-On Products](#)

### Diagram.



## Pre-installation steps.

The configuration detailed in this section must be carried out before Resource Central SAAS can be installed.

### SQL server.

The SQL server must allow SQL authentication, and we need a login during installation that allows us to create the 2 databases. Once databases are created DB\_Owner rights suffice.

Further requirements:

- **"Full-Text and Semantic Extraction for Search"** feature must be installed. (Check with query `"SELECT FULLTEXTSERVICEPROPERTY('IsFullTextInstalled')"`)

## Application server.

We have the following requirements for the Windows Web server.

- English GUI language.
- .NET 4.8
- IIS and asp.net – see detailed list in box below.

```
NetFx4Extended-ASPNET45", "IIS-WebServerRole", "IIS-WebServer", "IIS-CommonHttpFeatures", "IIS-HttpErrors", "IIS-HttpRedirect", "IIS-ApplicationDevelopment", "IIS-NetFxExtensibility45", "IIS-HealthAndDiagnostics", "IIS-HttpLogging", "IIS-LoggingLibraries", "IIS-RequestMonitor", "IIS-Security", "IIS-RequestFiltering", "IIS-Performance", "IIS-WebServerManagementTools", "IIS-ManagementConsole", "IIS-StaticContent", "IIS-DefaultDocument", "IIS-ISAPIExtensions", "IIS-ISAPIFilter", "IIS-HttpCompressionStatic", "IIS-HttpCompressionDynamic", "IIS-ASPNET45", "IIS-ApplicationInit"
```

Furthermore, these are strong recommendations:

- Assign a DNS A record (or a cname).
- We recommend using an SSL certificate for the website.
- Exclude services and folders as exemplified with Defender exclusions in box below.

```
Add-MpPreference -ExclusionProcess "C:\Program Files (x86)\Add-On Products\RealTime Service 6\RealTimeService.exe"  
Add-MpPreference -ExclusionPath "%programdata%\Add-On Products"  
Add-MpPreference -ExclusionProcess "C:\Program Files (x86)\Add-On Products\RC Synchronize Service\RCSynchronize.exe"  
Add-MpPreference -ExclusionProcess "C:\Program Files (x86)\Add-On Products\RC Permission Service\RCSettingPermissionServices.exe"  
Add-MpPreference -ExclusionProcess "C:\Program Files (x86)\Add-On Products\RCMaintenanceService\RCMaintenanceService.exe"  
Add-MpPreference -ExclusionProcess "C:\Program Files (x86)\Add-On Products\RC Tracking Service\RCTrackingService.exe"  
Add-MpPreference -ExclusionPath "C:\inetpub\wwwroot\ResourceCentral"
```

## O365 service account.

We need a service account in O365 with the following:

- It must have a mailbox.
- Cannot be hidden in GAL.
- Modern authentication is supported.
- Must be configured with "Application Impersonation Role" as described here:  
<https://docs.microsoft.com/en-us/exchange/client-developer/exchange-web-services/how-to-configure-impersonation> (From Microsoft)  
<https://support.add-on.com/article/273-steps-to-configure-application-impersonation-rights-in-exchange-servers>  
(Our KB with some explanations)
- Features that cannot be used when scope is applied to impersonation.  
[Impact of impersonation rights on some Resource Central features - Add-On Products](#)
- A conditional access rule can be applied to the service account access to your tenant.  
[Block external access for O365 Service Accounts using Conditional Access in Azure AD - Add-On Products](#)

## Optional requirements for use of Resource Finder permissions and Resource Data Sync.

Resource Central has some features that can collect information from Mailbox settings, Calendar settings etc. with the purpose of synchronizing values from Resources and to effective booking permissions for the individual user based on group memberships and booking policies applied to resources. The use of these features requires furthermore that:

- Basic authentication with remote PowerShell must be allowed.
- MFA is not supported.
- Must be member of "View-Only Organization Management" Exchange role.

## Azure AD access with modern authentication.

Resource Central needs a connection to AD to look up people, locate mailboxes and read basic information, and in O365 this information resides in Azure.

When modern authentication is enforced this Azure app is not only used for AD access, but also to provide the service account authentication endpoint for Realtime Service. Follow the instruction in this knowledgebase article to create the app:

<https://support.add-on.com/article/505-how-to-set-up-realtime-service-with-modern-authentication>

We will need the following information to configure this connection:

- Tenant name in O365. (xxx.onmicrosoft.com)
- Application ID
- Secret Key
- Scope URI

## Resource mailboxes.

Resource mailboxes must be created for rooms and equipment that should be part of Resource Central, and we recommend that the following is prepared.

- Add all rooms intended for Resource Central to a security group (or distribution list) for management purposes.
- Ensure that resource scheduling is correctly set up.
- We recommend that you take steps to preserve the subject of meetings. Below sample script does this for all resources in your organization.

```
Get-MailBox -Filter {(ResourceType -eq "Room") -or (ResourceType -eq "Equipment")} | Set-CalendarProcessing -AutomateProcessing AutoAccept -AddOrganizerToSubject $False -DeleteSubject $False
```

- Use policies in Exchange to control who can book or request a room.

<https://docs.microsoft.com/en-us/powershell/module/exchange/mailboxes/set-calendarprocessing?view=exchange-ps>

## Firewall requirements.

The Exchange connection method we use requires that traffic from Exchange EWS (in this case Exchange online) which is TCP port 10002 is allowed inbound through the firewall and subsequently NAT redirected to the server where Resource Central is running. Microsoft has a web service that can deliver updated information about the IP pool they use.

<https://docs.microsoft.com/en-us/office365/enterprise/urls-and-ip-address-ranges?redirectSourcePath=%252farticle%252fOffice-365-URLs-and-IP-address-ranges-8548a211-3fe7-47cb-abb1-355ea5aa88a2>

A complete list of all the communication ports we use with our Exchange connection tool (Realtime Service) can be found here (focus should be on push notification on port 10002 since the other inbound are used locally on the server):

<https://support.add-on.com/article/204-inbound-and-outbound-realtime-service-rtts-ports-and-needed-ip-addresses>

## Post-installation steps.

The points below cannot be implemented until the Resource Central environment is running.

### Office add-in deployment.

We always recommend implementing FQDN for the Resource Central web site to get a nice name for the users that will connect to the backend, but also to allow for easy replacement in case a server dies.

In this case where the Office add-in is a topic, the following is required for the Resource Central web site:

- Must have a DNS A record (or a cname).
- The site must have a valid public SSL certificate.
- The site must be accessible to the public. (Implementation of the Office add-in involves importing a manifest that points back the Resource Central website, and O365 must be able to make the connection and requires a valid SSL certificate.

Here is some additional information surrounding the Office add-in from our knowledgebase.

User guide: <https://support.add-on.com/article/446-resource-central-outlook-add-in-user-guide>

Implementation: <https://support.add-on.com/article/445-resource-central-outlook-add-in-installation-guide>

### Outlook COM add-in deployment.

This is the full com Outlook add-in which must be deployed to the client computers.

User guide: <https://support.add-on.com/article/442-resource-central-user-guide>

Below you will find links to a set of knowledge-based articles on the subject.

It is highly recommended that you do a test deployment first to verify the method.

We have several Knowledgebase articles on this subject, and you will find some basic information in the guide associated with the add-in.

Installation guide:

<https://support.add-on.com/article/432-resource-central-com-add-in-4-o-installation-guide>

Deployment guides:

<https://support.add-on.com/article/370-how-to-perform-add-in-4-o-deployment-using-command-line>

Additional topics:

<https://support.add-on.com/article/343-outlook-2013-and-2016-may-disable-or-load-resource-finder-com-add-in-slowly>

<https://support.add-on.com/article/469-alerts-on-add-in-produced-by-outlook>

### External authentication - SSO.

Resource Central supports several SSO methods that can be tied to O365.

We do not recommend the use of SAML as Microsoft Teams lacks support for it.

The methods are described in this support article:

<https://support.add-on.com/article/605-external-authentication-details-for-oauth2-open-id-connect-in-azure>