ManageEngine
M365 Security Plus

M365 Security Plus

# Installation Guide

# Table of Contents

# System requirements

This section lists all the hardware and software requirements for your environment.

## Hardware requirements

The table below lists the hardware and respective specifications required by ManageEngine M365 Security Plus.

| Hardware | Minimum | Recommended |
|---|---|---|
| Processor | 2.4GHz | 3GHz |
| Number of cores | 4 | 6 or more |
| RAM | 8GB | 16GB |
| Disk space Disk | 100GB (SSD preferred) | 200GB (SSD preferred) |
| throughput | 5MB per second | 20MB per second |

**Note:**

- The values above are subject to change based on customer requirements.
- Choose the required disk space based on usage and future requirements.

## Software requirements

This section lists the platforms and browsers supported by M365 Security Plus.

### Supported platforms

- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2
- Windows Server 2012
- Windows Server 2008 R2 SP1
- Windows 10
- Windows 8.1
- Windows 8
- Windows 7 SP1

### Supported browsers

- Internet Explorer 9.0 and above
- Firefox 45.0 and above
- Chrome 45.0 and above

## Supported databases

### PostgreSQL

| M365 Security Plus build number | Supported database versions |
|---|---|
| 4400 and above | PostgreSQL 9.4-9.6 and 10.12 |
| 4000-4400 | PostgreSQL 9.2-9.6 |

Table 1: Supported PosgreSQL versions

### MS SQL

| M365 Security Plus build number | Supported database versions |
|---|---|
| 4000 and above | Microsoft SQL Server 2005 and above |

Table 2: Supported MS SQL versions

## Port requirements

M365 Manager Plus uses port 80 for HTTP and port 443 for HTTPS communications.

# Other prerequisites

Before you configure a Microsoft 365 tenant, make sure these prerequisites are satisfied:

- You have a working internet connection and the required domains are not blocked by your firewall. Please refer to this table to review the entire list of domains that should be allowed by your firewall.

- If you plan to install the product in a system running Windows 7 SP1 or Windows 2008 R2 SP1, make sure that you have Microsoft .NET version 4 and PowerShell version 5.1 installed in your system.

  a. To check if Microsoft .NET Framework is installed, open **Command Prompt** from Run. Enter the following command reg query: "HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\NET Framework Setup\NDP\v4\full" /v version
  Check the displayed version. If the version 4 is not installed, install Microsoft .NET Framework 4 from here.

  b. To check if PowerShell is installed, type **PowerShell** from Run. If PowerShell is installed, check for its version number by running the command $PSVersionTable. If the version is below 5.1 or if PowerShell is not installed, install PowerShell V 5.1 from here.

# Installing M365 Security Plus

M365 Security Plus is distributed in the EXE format and is available in a 64-bit version for Windows that can be installed in any machine that meets the system requirements.

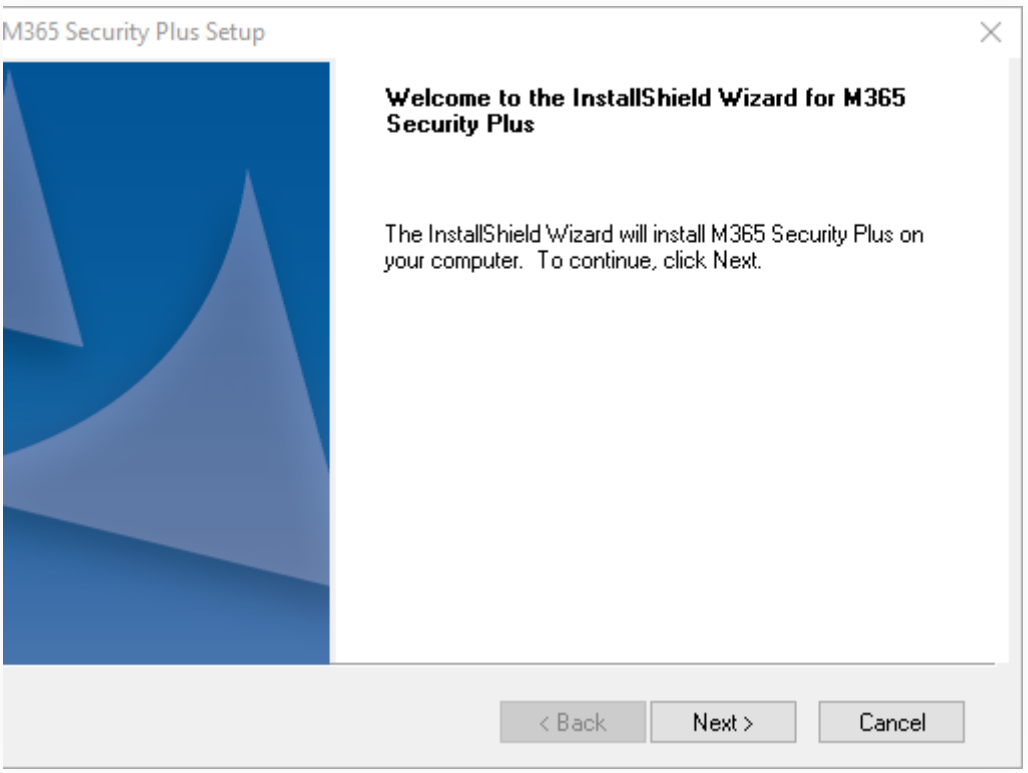
You can install M365 Security Plus as:

- An application
- A Windows service

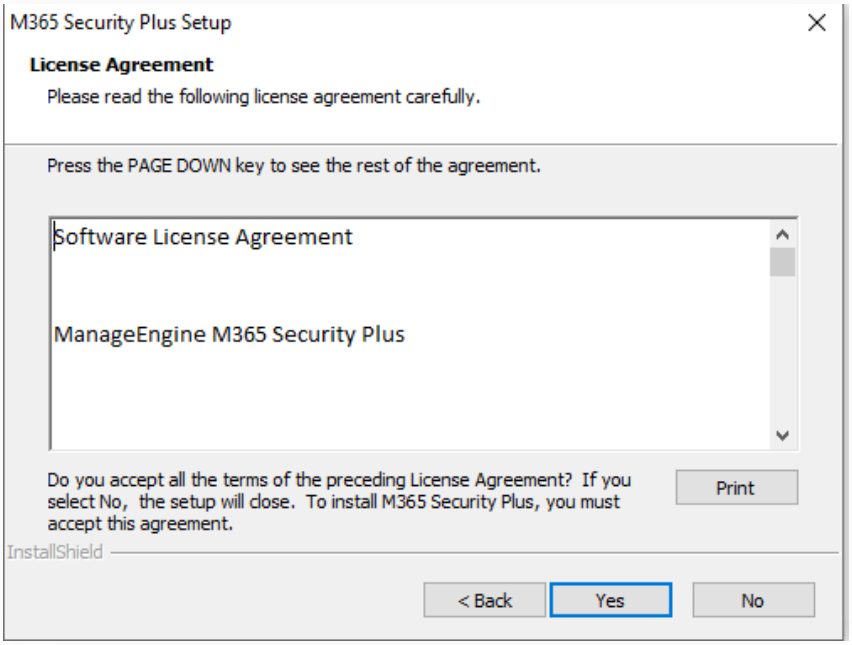
## Installing M365 Security Plus as an application

By default, M365 Security Plus will be installed as an application. You can download M365 Security Plus from www.m365securityplus.com

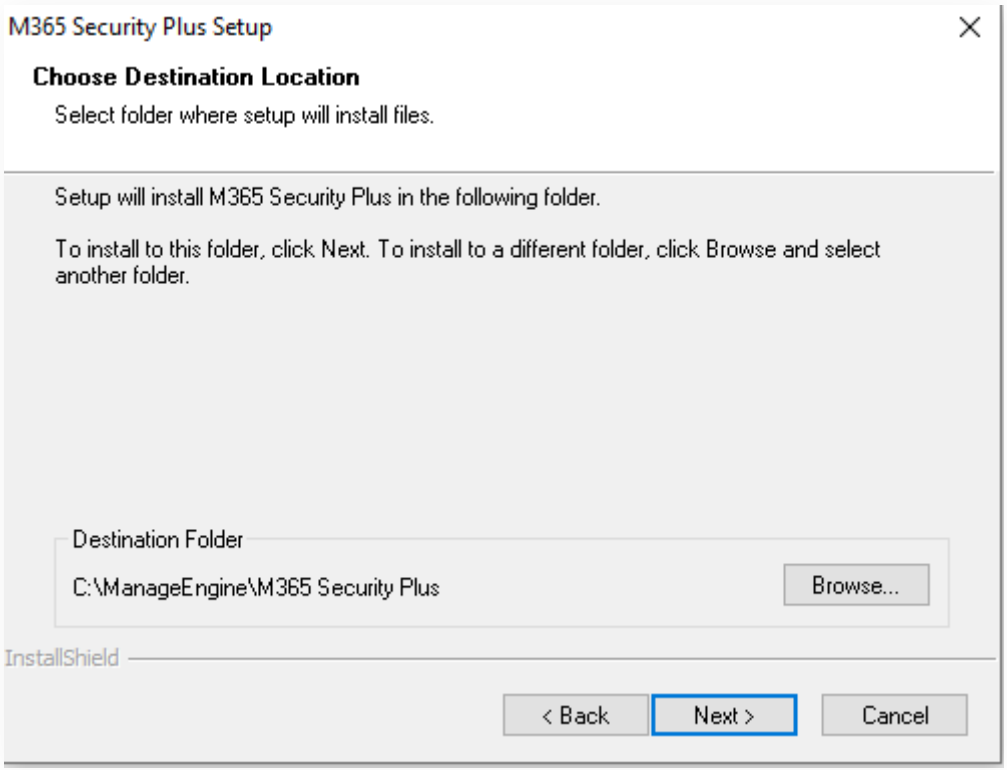
1. Download M365 Security Plus.
2. Right-click on the downloaded file and select **Run as Administrator.**
3. The M365 Security Plus Install Shield window opens. Click on **Yes** to continue.



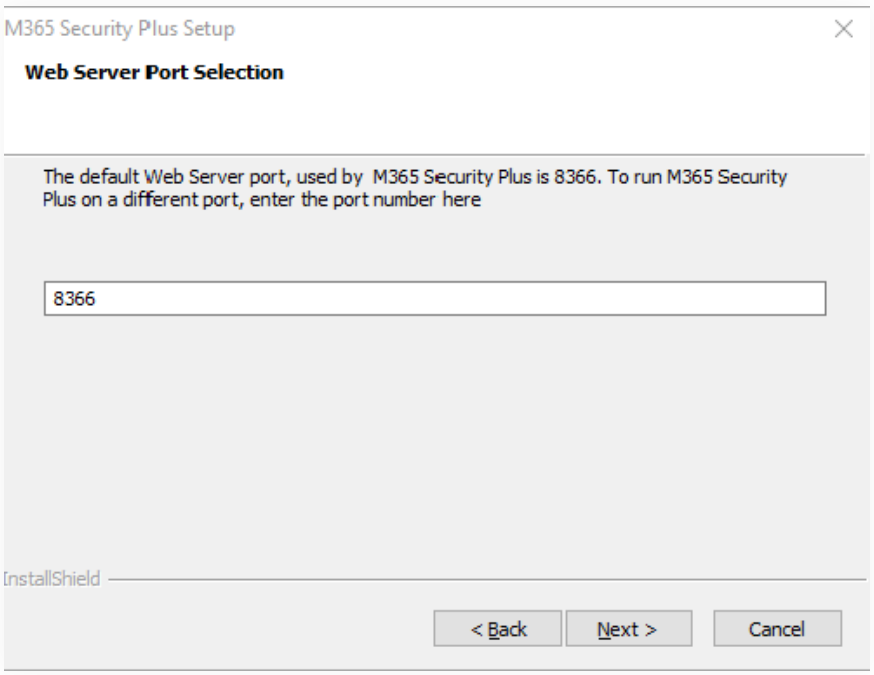

4. Click on **Yes** to accept the LIcense Agreement.



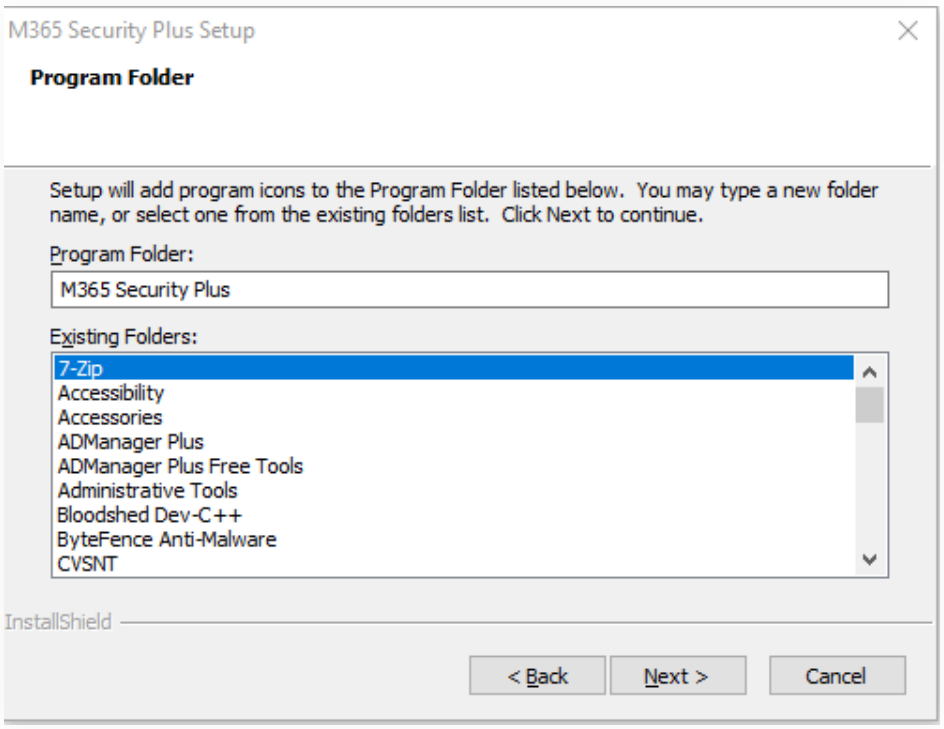

5. The default destination folder for M365 Security Plus is C:\ManageEngine\M365 Security Plus. If you want to modify the installation folder, use the **Browse** option to do so. Click on **Next.**



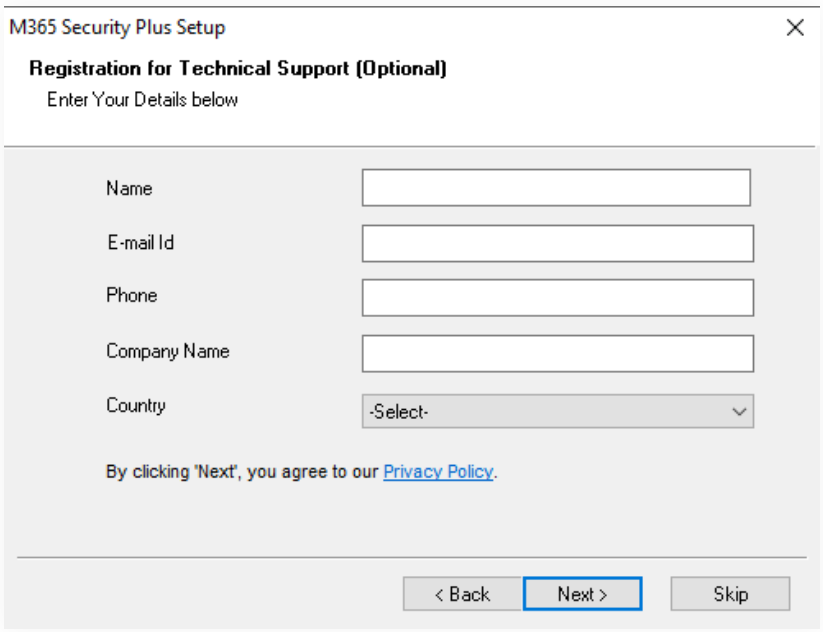

6. The default port used by M365 Security Plus is **8365**. You can change the port number if you want. Click on **Next**.



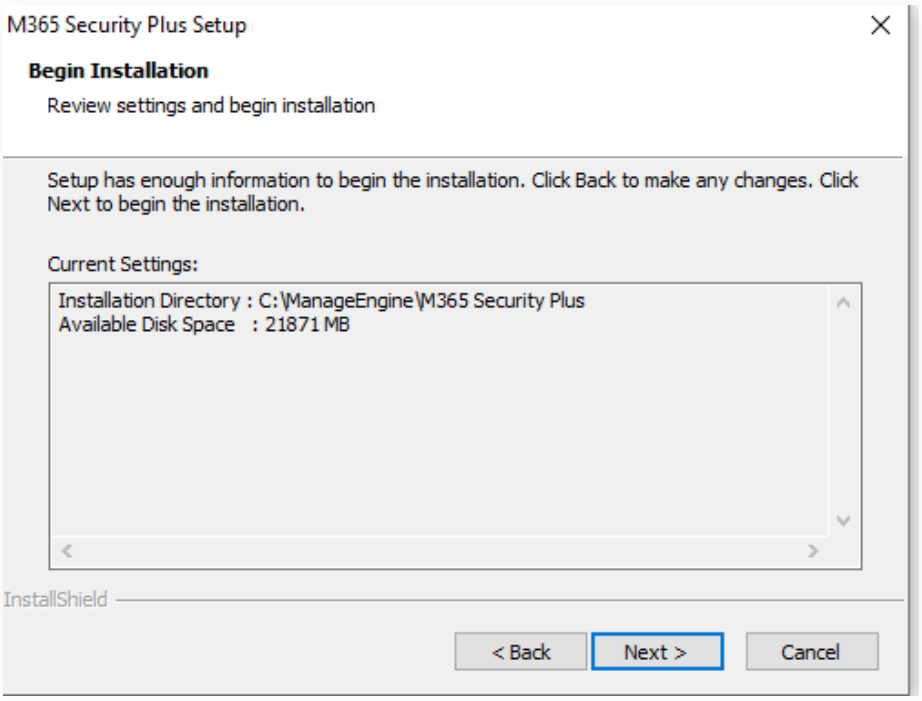

7. The default folder name is M365 Security Plus. You can change the name if required. Click on **Next**.



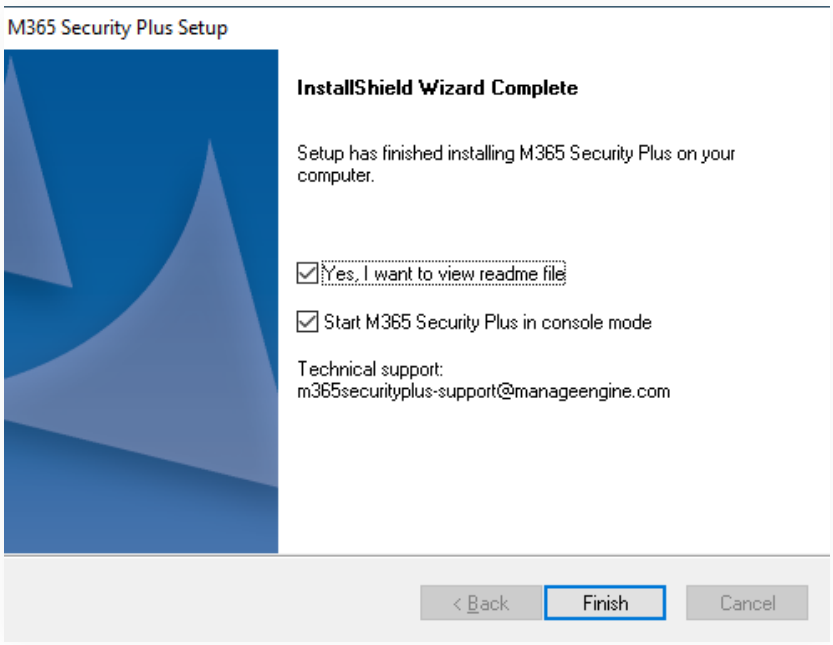

8. Fill in the **Registration for Technical Support** form if you need assistance in configuring or using the tool or, you can click on **Skip.**




9. Review the installation directory and available free disk space details, and click on **Next** to begin installation.




10. To start M365 Security Plus as an application, select the **Start M365** Security **Plus in console mode** option and click on **Finish.**




## Install M365 Security Plus as a Windows service

M365 Security Plus can installed as a Windows service using either the Start menu or command prompt.

**Installing M365 Security Plus as a service from the Start Menu**

To install M365 Manager Plus as a service, perform the following steps after installing M365 Security Plus.

1. Click **Start → All Programs**
2. Select **M365 Security Plus**
3. Select **NT Service**
4. Select **Install M365 Security Plus as a service**
5. When M365 Security Plus is installed as a service, M365 Security Plus runs with the privileges of the system account.

**Installing M365 Security Plus as a service from the Command Prompt**

To install M365 MSecurity Plus as a service from the command prompt, perform the following steps after installing M365 Security Plus.

1. Go to **Start → Run → Type cmd**
2. Go to M365 Security Plus_installation_directory\bin folder on the command prompt.
3. Type InstallAsService.bat
4. This will install M365 Security Plus as a service.

# Starting M365 Security Plus

M365 Security Plus can be started in either of the following ways:

1. Double-click the **ManageEngine M365 Security Plus** icon from the desktop.
2. Select **Start → All Programs → M365 Security Plus → Start M365 Security Plus.**

Starting the M365 Security Plus automatically launches the client in the default browser.

1. On the login page, enter a valid user name and password.
2. By default, the **User name** and **Password** are "admin" and "admin" respectively.
3. Click on **Login.**

# Tenant configuration

When you login for the first time, you will be automatically redirected to the tenant configuration page.

1. Click on the **Configure using Microsoft 365 Login** option.
2. Click on **Proceed** in the pop-up that appears.
3. You will now be redirected to the Microsoft login page where you must enter your **Global Administrator** credentials. You have to pass through multiple authentication methods, if your account is multi-factor authentication-enabled.

**Note:**

M365 Security Plus will not store your Global Administrator credentials.

4. Click on **Accept** in the pop-up that displays to allow M365 Security Plus to:

- Create a service account with the Global Administrator credentials provided by you. It will be created with the Exchange Administrator and View-Only Organization Management roles.
- Create an Azure AD application to fetch Microsoft 365 data using Microsoft Graph API.

5. You will be now redirected to the Microsoft 365 portal. Select the Global Administrator account you had provided in Step 3, and click on **Accept** to provide consent for the application created for M365 Security Plus.

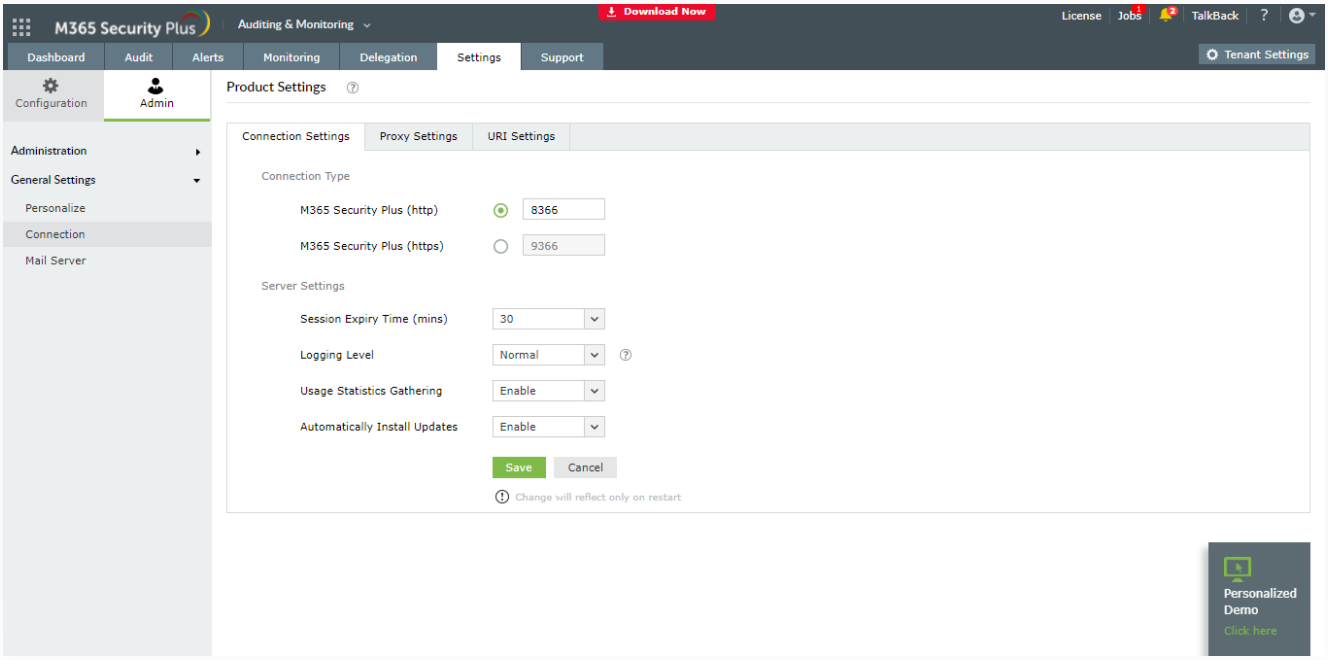
If the tenant configuration was successful, you can see your tenant listed in the **Configured Microsoft 365 Tenants** page.

**Note:**

In the above tenant configuration method, Azure AD application creation and permission assignment is done automatically. If the tenant configuration is not successful, refer to this guide to learn how to configure the tenant manually.

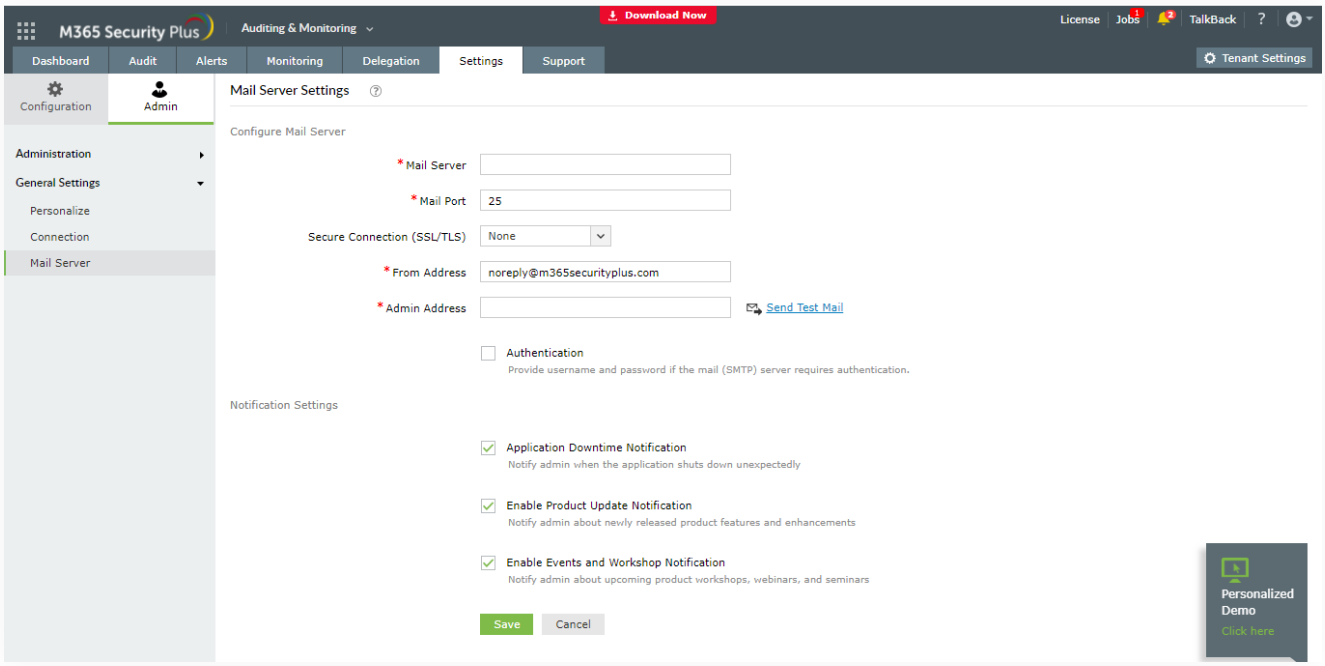
# Connection settings

You can configure port number, proxy server and URI in **Settings>Admin>General Settings>Connection**




# Server settings

You can configure mail server and product notifications in **Settings>Admin>General Settings>Mail Server**



# Installing service packs

- Shut down M365 Security Plus
  - If the product runs as an application, click on **Start** → **All Programs** → **M365 Security Plus** → **Stop M365 Security Plus.**
  - If the product runs as a Windows service, click on **Start** → **Run** → type services.msc → Right click on **ManageEngine M365 Security Plus ->Stop**
- Execute the stopDB.bat file under M365 Security Plus_installation_directory\bin folder.
- Backup M365 Security Plus by zipping the contents of M365 Security Plus installation directory.
- In case of MS SQL Database Server, take a backup of the database also.
- Open a Command Prompt as an administrator and execute the UpdateManager.bat file under M365 Security Plus_installation_directory\bin.
- Click **Browse** and select the .ppm file that you have downloaded.
- Click on **Install**. Depending on the amount of data to be migrated, the installation procedure may take a few minutes. Please do not terminate the procedure prematurely.
- Click **Close** and then **Exit** to quit Update Manager tool.
- Start M365 Security Plus.
  - If the product runs as an application, click on **Start** → **All Programs** → **M365 Security Plus** → **Start M365 Security Plus**
  - If the product runs as a Windows service, click on **Start** → **Run** → type services.msc → right-click **ManageEngine M365 Security Plus** →**Start**

# Uninstalling M365 Security Plus

To uninstall M365 Security Plus, stop M365 Security Plus before uninstalling the product.

**To Stop the Application**

Select **Start** → **Programs** → **M365 Security Plus** →**Stop M365 Security Plus Server**

**To Uninstall the Application**

Select **Start** → **Programs** → **M365 Security Plus** →**Uninstall M365 Security Plus**

# Appendix

## Minimum scope

The roles and permissions (minimum scope) required by a service account to be configured in M365 Security Plus are listed below.

| Module | Role Name | Scope |
|---|---|---|
| Management | User Administrator | Manage users, contacts, and groups. |
| | Privileged Authentication Administrator | Reset password, block, or unblock administrators. |
| | Privileged Role Admin | Manage role assignments in Azure Active Directory (AD). |
| | Exchange Administrator | Update mailbox properties. |
| | Teams Service Admin | Manage Microsoft Teams. |
| Reporting | Global Reader | Get reports on all Microsoft 365 services. |
| | Security Reader | Get mailbox reports. |
| Auditing and Alerting | Security Reader | Get audit logs and sign-in reports. |
| Monitoring | - | - |
| Content Search | - | - |

Table 3: Roles and permissions required by the service account.

**Note:**

- If an Azure AD Application is not configured for M365 Security Plus, the Service Admin role is required for the Monitoring feature.
- An Azure AD Application needs to be configured for M365 Security Plus to use the Content Search feature.

The roles and permissions (minimum scope) required by an Azure AD application configured for M365 Security Plus are listed below.

| Module | API Name | Permission | Scope |
|---|---|---|---|
| Management | Microsoft Graph | User.ReadWrite.All | User creation, modification, deletion and restoration. |
| | | Group.ReadWrite.All | Group creation, modification, deletion, restoration, add or remove members and owners. |
| Reporting | Microsoft Graph | User.Read.All | Users and group members report. |
| | | Group.Read.All | Group reports. |
| | | Contacts.Read | Contact reports. |
| | | Files.Read.All | OneDrive for Business reports. |
| | | Reports.Read.All | Usage reports. |
| | | Organization.Read.All | License details reports. |
| | | AuditLog.Read.All | Audit log-based reports |
| | Azure Active Directory Graph | Domain.Read.All | Domain-based reports. |
| Auditing and Alerting | Microsoft Graph | AuditLog.Read.All | Audit reports and alerts. |
| Monitoring | Office 365 Management APIs | ServiceHealth.Read | Health and performance reports. |
| Content Search | Microsoft Graph | Mail.Read | Content search reports. |

Table 4: Roles and permissions required by the Azure AD application.

# Firewall settings

The following endpoints must be allowed by the firewall for the seamless functioning of the tool.

### General domains

The general domains that must be allowed through the firewall are as follows:

1. microsoft365securityplus.com
2. *.zoho.com
3. *.manageengine.com
4. *.zohocorp.com
5. api.bcti.brightcloud.com
6. *.manageengine.jp (Only Japanese build users)
7. *.manageengine.cn (Only Chinese build users)

### Azure AD general cloud

The Azure general cloud users must ensure that the following domains are allowed by their firewall.

Azure Germany, China and US cloud users refer to the respective tables

| Module | Endpoint |
|---|---|
| REST API | login.microsoftonline.com |
| | graph.windows.net |
| | graph.microsoft.com |
| | manage.office.com |
| | portal.office.com |
| | login.windows.net/common/oauth2/token |
| | admin.microsoft.com/fd/CommerceAPI/my-org |
| Exchange Online | outlook.office.com |
| | outlook.office365.com/powershell-liveid |

Table 5: Domains to be allowed by Azure AD general cloud users.

### Azure Germany

The Azure Germany cloud users must ensure that the following domains are allowed by their firewall.

| Module | Endpoint |
|---|---|
| REST API | login.microsoftonline.de |
| | graph.cloudapi.de |
| | graph.microsoft.de |
| | portal.office.de |
| | manage.office.de |
| | login.microsoftonline.de/common/oauth2/token |
| Exchange Online | outlook.office.de |
| | outlook.office.de/powershell-liveid |

Table 6: Domains to be allowed by Azure AD Germany cloud users.

### Azure China

The Azure China cloud users must ensure that the following domains are allowed by their firewall.

| Module | Endpoint |
|---|---|
| REST API | login.partner.microsoftonline.cn |
| | graph.chinacloudapi.cn |
| | microsoftgraph.chinacloudapi.cn |
| | manage.office.cn |
| | portal.azure.cn |
| | login.partner.microsoftonline.cn/common/oauth2/token |
| Exchange Online | partner.outlook.cn |
| | partner.outlook.cn/PowerShell |

Table 7: Domains to be allowed by Azure AD China cloud users.

### Azure US

The Azure US cloud users must ensure that the following domains are allowed by their firewall.

| Module | Endpoint |
|---|---|
| REST API | login.microsoftonline.us |
| | graph.windows.net |
| | graph.microsoft.us |
| | manage.office.us |
| | portal.azure.us |
| | login.microsoftonline.us/common/oauth2/token |
| Exchange Online | outlook.office365.us |
| | outlook.office365.us/powershell-liveid |

Table 8: Domains to be allowed by Azure AD US cloud users.

## Other useful documents

1. Guide to secure M365 Security Plus installation
2. Guide to install SSL certificate in M365 Security Plus
3. Tenant configuration guide
4. Guide to setup M365 Security Plus in Azure
5. Guide to host M365 Security Plus on the internet