2023-02-17

HORNETSECURITY

365 TOTAL PROTECTION

www.hornetsecurity.com

THE CLOUD SECURITY PIONEER

Contents

Language and Icons Used in the Documentation

Gender Equality

For better readability, the generic masculine form is used in this documentation. Nevertheless, the information refers to members of all genders.

Used symbols

The following symbols are used to improve the recognizability of relevant steps within instructional chapters:

Symbol	Description	Explanation
	Prerequisites	Condition that must be fulfilled before performing the next step
	Interim result	Result that is reached after executing a step
	Final result	Result that is reached after the described order of steps

Safety instructions and warnings

Warnings and safety instructions are used to inform the user about residual risks and dangers and how to avoid them with the recommended procedure. Following safety instructions and warnings are used in this documentation:

Symbol	Description	Explanation
	NOTE	Further information within a given paragraph that is relevant for the execution of later steps.
	TIP	Note about configuration options.
	IMPORTANT	Warning containing information about restrictions or important configuration options of a service.

Symbol	Description	Explanation
	ATTENTION	Warning about additional costs that may be incurred depending on the booked services.
	WARNING	Warning about a potential loss of data.
	DANGER	Warning about a potential system infection with malware.

About 365 Total Protection

Our 365 Total Protection service is intended for Microsoft 365 customers and protects their emails and data in Microsoft 365. 365 Total Protection is specifically designed for and seamlessly integrated with Microsoft 365.

365 Total Protection is available in a Business, Enterprise and Enterprise Backup version. These versions have different functionalities:

- All versions protect emails and data by filtering attachments (see About Content Control), with custom rules for email filtering (see About the Compliance Filter) and with settings for email encryption (see Email Encryption).
- The Enterprise and Enterprise Backup versions additionally support legally compliant archiving of emails (see Archiving), provide analysis mechanisms for detecting complex threats (see Structure and Functions of ATP) and maintain email traffic in the event of an email server failure (see About the Continuity Service). In addition, with these versions, administrators have the option of deleting emails (see Ex Post Deletion) that have already been delivered from their users' Microsoft 365 mailboxes (see Mailbox Types) if, for example, an email is subsequently found to be a threat.
- With the Enterprise Backup version, data from a customer's Microsoft 365 tenant and Windows-based endpoints can additionally be backed up and restored (see About 365 Total Backup).

Once 365 Total Protection is set up for a customer, the customer's domains, groups and users in the Control Panel are synchronized with their Microsoft 365 organization. Later, the domains, groups and users in the Control Panel are regularly synchronized with Microsoft 365.

Partner-level administrators can configure 365 Total Protection for a new customer directly during the onboarding (see Onboarding of a New Customer as a Partner on page 8). Existing customers can upgrade to 365 Total Protection at any time (see Upgrade to 365 Total Protection as a Customer on page 25).

Notice:

Existing customers who upgrade to the Enterprise or Enterprise Backup version and have used an on-premises Exchange server in the past, can migrate mailbox data from their on-premises Exchange server to their Microsoft 365 tenant during the upgrade (see About Mailbox Migration on page 43). This makes it easier for customers to switch to Microsoft 365.

After the setup of 365 Total Protection, a 14-day trial period starts. In order to continue using 365 Total Protection after the trial period, the customer must purchase the service (see Ordering 365 Total Protection on page 109).

Onboarding of a New Customer as a Partner

365 Total Protection (see About 365 Total Protection on page 6) allows partners to perform the setup in the Control Panel automatically for customers with a Microsoft 365 account. All the customer's domains and users created in Microsoft 365 are automatically transferred and displayed in the Control Panel.

Notice:

Group members from Microsoft 365 can also be synchronized in the Control Panel. To synchronize group members, customer-level administrators must create groups with the same names in the Control Panel. For more information, see Group Management in the Control Panel on page 112.

Partner-level administrators can set up customers in two ways: Either a partner-level administrator sends the customer an onboarding link (see Creating an Onboarding Link on page 8) that allows the customer to perform the setup themselves, or a partner-level administrator logs in to Microsoft with the customer's administrative credentials and performs the onboarding process (see Adding a 365 Total Protection Customer to the Control Panel on page 9). Once a partner-level administrator has initiated the onboarding for a customer, the administrator can configure 365 Total Protection for the customer (see Setting up 365 Total Protection on page 10). If the 365 Total Protection Enterprise Backup version has been selected, the partner-level administrator can also configure 365 Total Backup for the customer to back up data from their Microsoft 365 tenant.

Afterwards, some DNS settings must be configured in order for the domains to redirect the email traffic.

Creating an Onboarding Link

You can create an onboarding link for your customers so they can set up our services themselves. The link will take them to the 365 Total Protection onboarding form. You can share this link with your customers so they can set up 365 Total Protection themselves (see Setting up 365 Total Protection on page 10). The link can be used multiple times.

1. Log in to the Control Panel with your administrative credentials.
2. In the scope selection, select the partner under which you would like to create the new customer.
3. Navigate to **365 Total Protection** > **365 Total Protection**.

4. Select a version of 365 Total Protection for your customers under **Your onboarding address**. You have the following options:
   - **Leave selection open**
   - **Business**
   - **Enterprise**
   - **Enterprise Backup**

   A unique link is generated.
5. Click on to copy the link to the clipboard.

An onboarding link for 365 Total Protection has been created.

Adding a 365 Total Protection Customer to the Control Panel

You can add a new 365 Total Protection customer (see About 365 Total Protection on page 6) to the Control Panel if you have administrative credentials for the Microsoft 365 environment of that customer.

1. Log in to the Control Panel with your administrative credentials.
2. In the scope selection, select the partner under which a new 365 Total Protection customer is to be created.

Figure 1: Select partner in the scope selection

3. Navigate to **365 Total Protection** > **365 Total Protection**.

4. Select a 365 Total Protection version for the new customer.

Figure 2: Select version

The onboarding form is displayed.

The onboarding of a new 365 Total Protection customer has been initiated.

Next, you can set up 365 Total Protection for the customer (see Setting up 365 Total Protection on page 10).

Setting up 365 Total Protection

You can set up 365 Total Protection.

You have opened the onboarding form for 365 Total Protection (see Adding a 365 Total Protection Customer to the Control Panel on page 9).

Once you have opened the onboarding form for 365 Total Protection, you can set up 365 Total Protection (see About 365 Total Protection on page 6).

1.

> **Important:**
>
> The **Display name (domain) in the Control Panel** field is for the customer's primary domain, not their .onmicrosoft domain. This domain is displayed in the Control Panel.

Enter your contact data in the onboarding form

> **Notice:**
>
> The contact data will allow us to contact you in case of problems or queries.

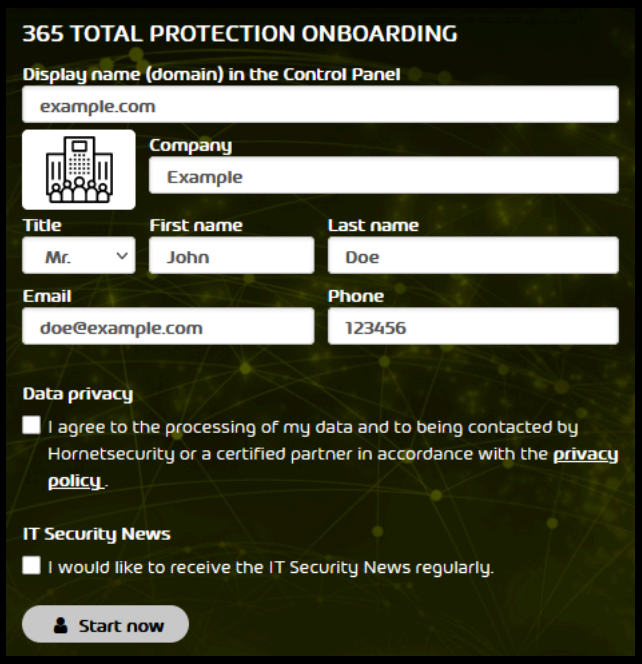

Figure 3: Enter contact data

2. Tick the checkbox under **Data privacy**.
3. Optional: If you would like to receive our IT Security News, tick the checkbox **I would like to receive the IT Security News regularly.**.

4.

Attention:

Once 365 Total Protection is activated, a 14-day free trial period starts. In order for a customer to continue using the service after the trial period, the customer must purchase the service (see Ordering 365 Total Protection on page 109).

Click on **Start now** to start the setup process.

The Microsoft login page is displayed.

5. Log in to Microsoft 365 with your administrative credentials.

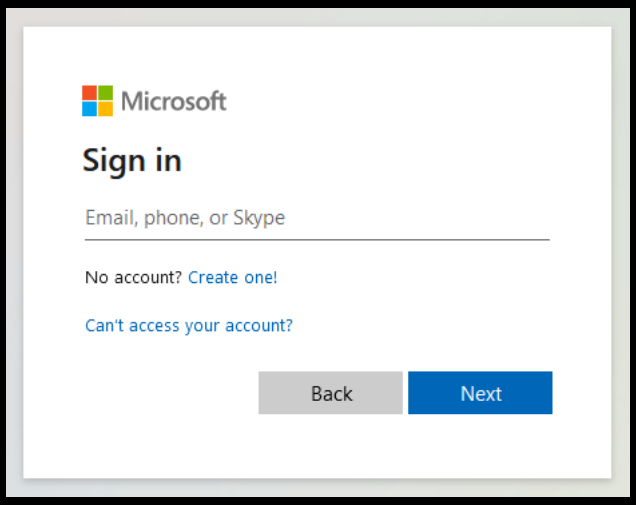

Figure 4: Enter Microsoft credentials

Notice:

During the ensuing synchronization, only domains and mailboxes are transferred. The configuration settings from Microsoft are not modified. Groups are also synchronized with Microsoft 365 if a customer has manually created groups with the same names in the Control Panel (see Group Management in the Control Panel on page 112).

6. Accept the requested permissions to connect our services to Microsoft.

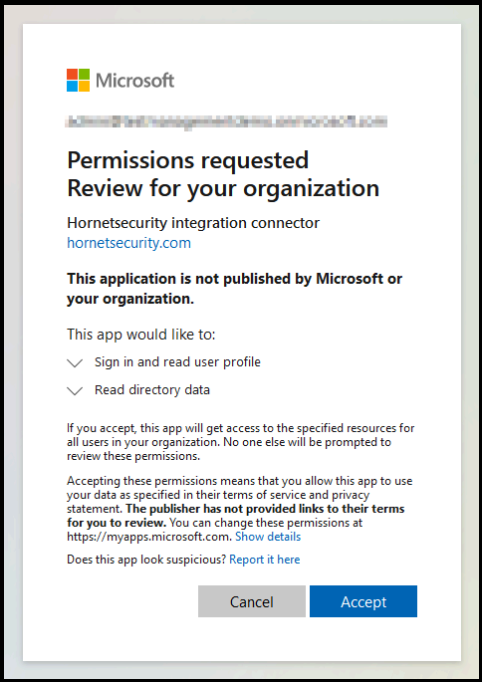

Figure 5: Accept permissions

The domains and mailboxes from Microsoft 365 are created in the Control Panel. The domains are added to the **Customer Settings** > **Domains** module (see Domains). The domains are first assigned the state **Not verified** in the column **Verified**. After a few minutes, we check whether the domains can be verified (see Domain Verification).

The customer's domains and mailboxes have been created in the Control Panel. Now, the administrator of the customer's Microsoft 365 organization can log in to the Control Panel with their credentials from Microsoft 365 and configure the services.

After the synchronization, you need to configure the services from Microsoft (see Configuration of Microsoft Services on page 94) so you can fully use our services.

If you have selected 365 Total Protection Enterprise Backup, you must also configure 365 Total Backup(see Configuring 365 Total Backup on page 14) to back up data from the customer's Microsoft 365 tenant.

Configuring 365 Total Backup

You have configured 365 Total Protection Enterprise Backup for a customer (see Setting up 365 Total Protection on page 10).

The 365 Total Protection Enterprise Backup service combines the 365 Total Protection Enterprise and 365 Total Backup services (see About 365 Total Protection on page 6). Once you have configured 365 Total Protection Enterprise Backup for a customer, you can configure 365 Total Backup for the customer. Using this procedure, you will configure 365 Total Backup according to the default settings. In that case, all Microsoft 365 mailboxes, files stored in OneDrive for Business accounts and SharePoint document libraries, as well as Teams chats for users and groups from the customer's tenant are backed up.

Notice:

Customer-level or partner-level administrators can configure 365 Total Backup with other settings by opening 365 Total Backup via the **Backup** > **365 Total Backup** module (see Launching 365 Total Backup).

With 365 Total Backup, data from Windows-based endpoints can also be backed up. However, endpoints are not included in the default configuration. Only partner-level administrators can configure backups of endpoints. To do so, partner-level administrators can open 365 Total Backup via the **Backup** > **365 Total Backup** module.

1. Log in to the Control Panel with your administrative credentials.
2. Select the customer's domain from the scope selection.

3. Navigate to **365 Total Protection** > **365 Total Protection**.

The setup status of 365 Total Protection Enterprise Backup is displayed.

Figure 6: Setup status

4. Click on **Configure now** under **Configure 365 Total Backup**.

A page for configuring 365 Total Backup opens in a new tab. The customer's data is predefined.

> **Notice:**
>
> The page uses the language that is set for the customer's parent partner in the Control Panel (see Setting Default Values for Timezone and Language).

5. Click on **Next**.

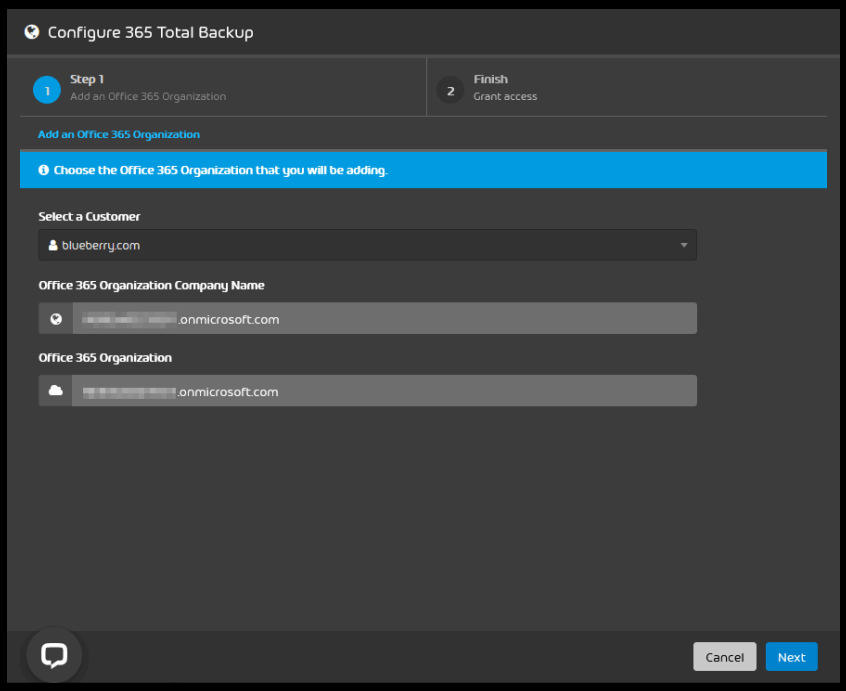

Figure 7: Check data

A window with an overview of the configuration steps opens.

6. Click on step 1.

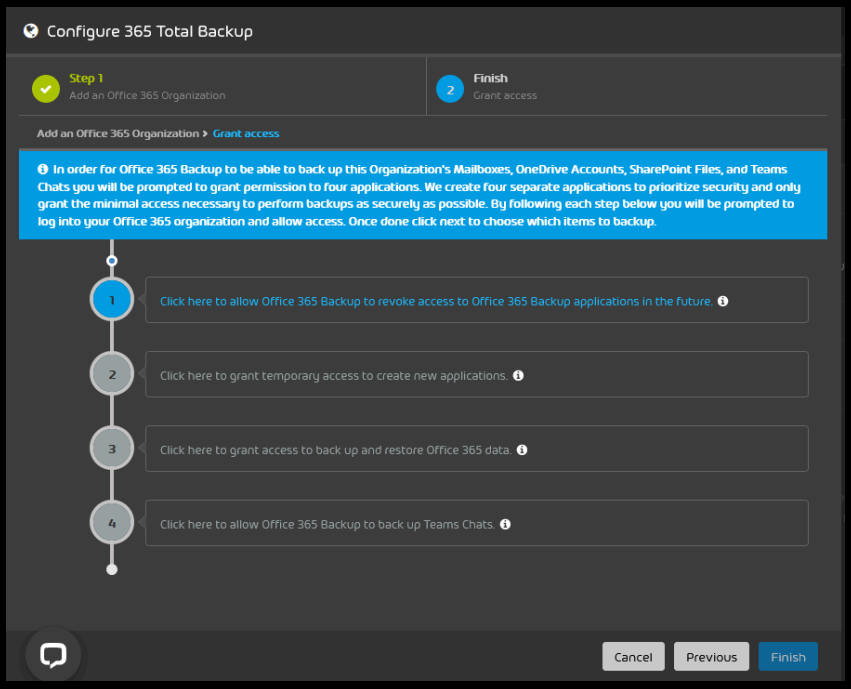

Figure 8: Perform step 1

The Microsoft 365 login page opens in a new tab.

7. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

8. Grant the requested permissions.

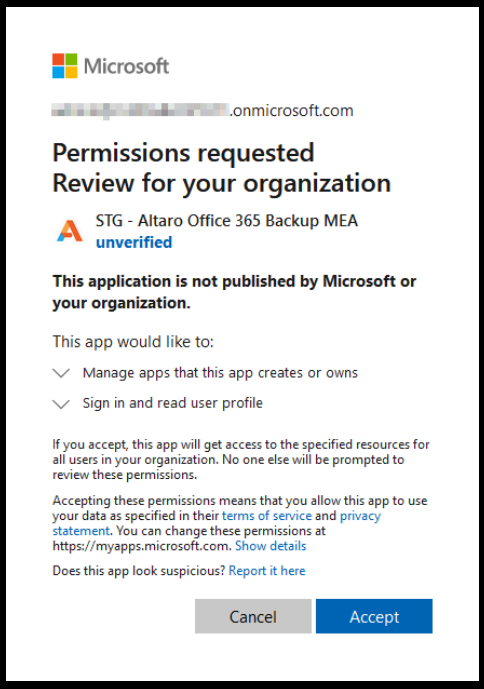

Figure 9: Grant permissions

The permissions are granted. A confirmation message is displayed.

Figure 10: Confirmation window

9. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

10. Click on step 2.

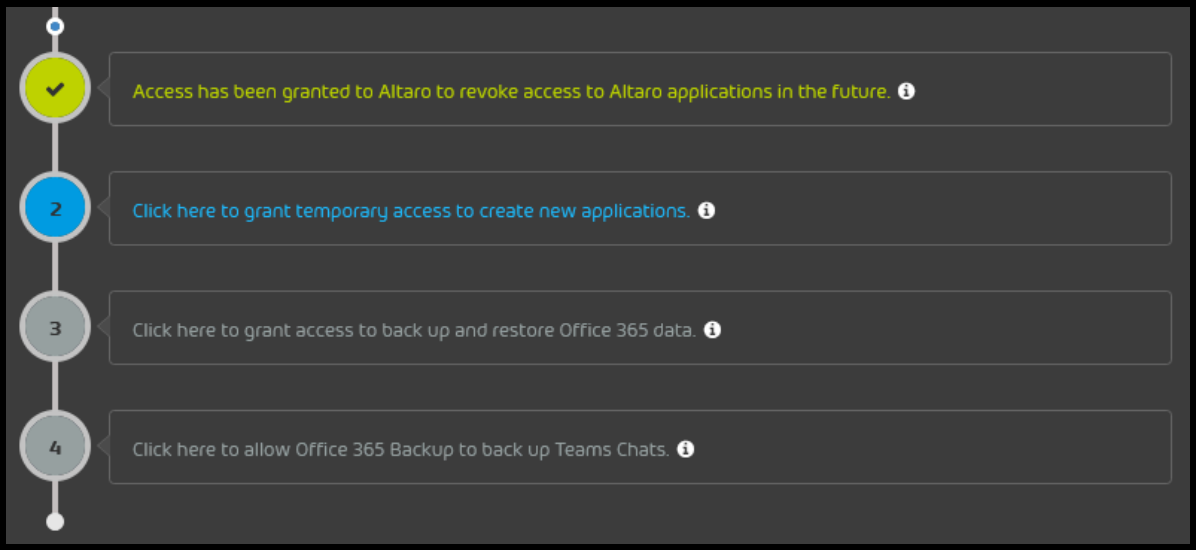

Figure 11: Perform step 2

The Microsoft 365 login page opens in a new tab.

11. Log in to Microsoft 365 with the customer's administrative credentials.

365 Total Backup is granted access to the customer's tenant. A confirmation message is displayed.

Figure 12: Confirmation window

12. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

13. Click on step 3.

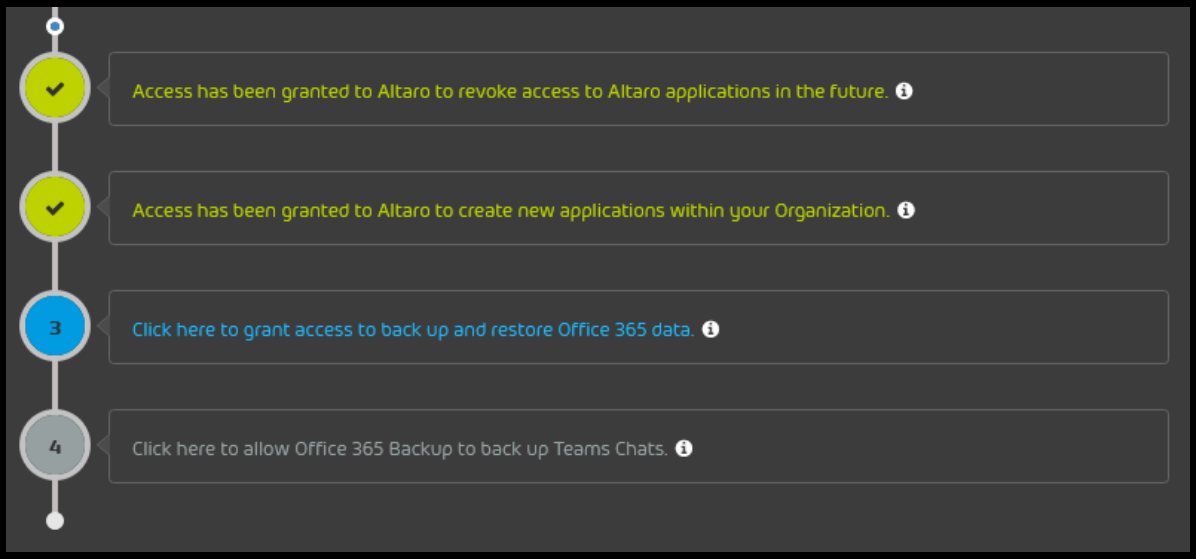

Figure 13: Perform step 3

The Microsoft 365 login page opens in a new tab.

14. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

15. Grant the requested permissions.

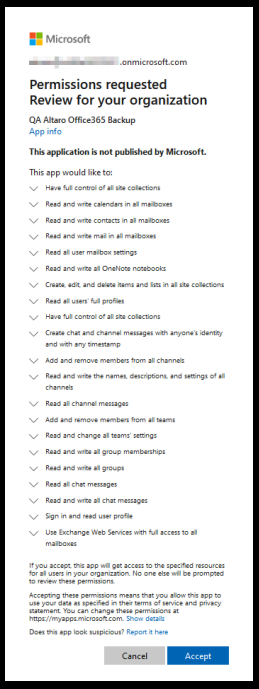

Figure 14: Grant permissions

The permissions are granted. A confirmation message is displayed.

Figure 15: Confirmation window

16. Click on step 4.

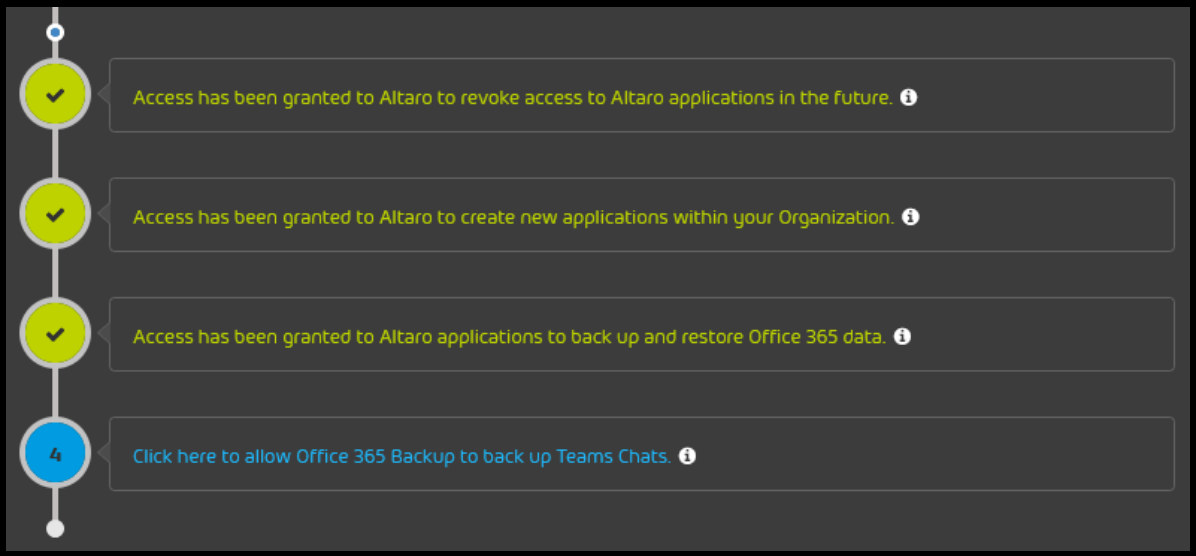

Figure 16: Perform step 4

The Microsoft 365 login page opens in a new tab.

17. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

18. Grant the requested permissions.

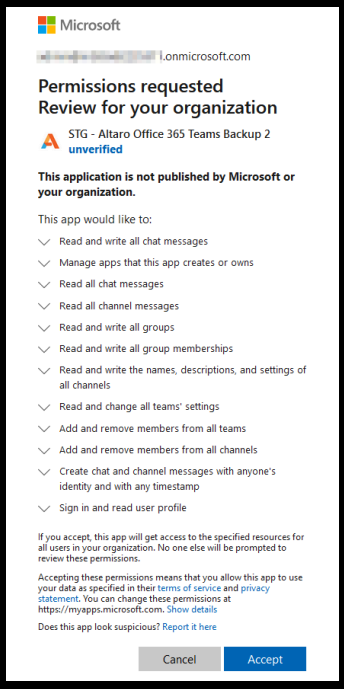

Figure 17: Grant permissions

The permissions are granted. A confirmation message is displayed.

Figure 18: Confirmation window

19. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

20. Click on **Finish**.

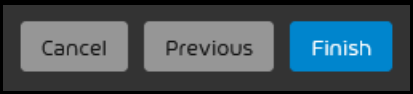

Figure 19: Finish configuration

The tab closes. In the Control Panel, the configuration of 365 Total Backup is displayed as completed in the **365 Total Protection** > **365 Total Protection** module.

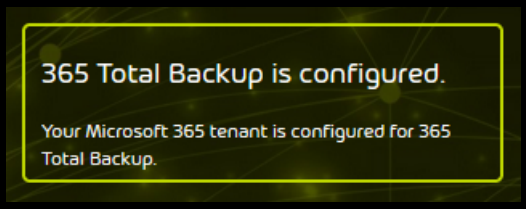

Figure 20: Configuration status of 365 Total Backup

365 Total Backup has been configured.

Upgrade to 365 Total Protection as a Customer

If a customer has a Microsoft 365 tenant and is already using our services, they can upgrade to 365 Total Protection (see About 365 Total Protection on page 6) themselves using the Control Panel (see Upgrading to 365 Total Protection on page 25).

Customers who upgrade to the Enterprise or Enterprise Backup version and have used an on-premises Exchange server in the past can migrate mailbox data from their on-premises Exchange server to their Microsoft 365 tenant during the upgrade (see About Mailbox Migration on page 43). This makes it easier for customers to switch to Microsoft 365.

During the upgrade to 365 Total Protection, all domains and mailboxes created in Microsoft 365 are automatically transferred to the Control Panel.

Upgrading to 365 Total Protection

You have a Microsoft 365 tenant and use our services.

As an existing customer, you can upgrade to 365 Total Protection (see About 365 Total Protection on page 6) in the Control Panel.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **365 Total Protection** > **365 Total Protection**.

4.

Important:

During the upgrade to 365 Total Protection, the mailboxes and domains in the Control Panel are sycnhronized with Microsoft 365. New mailboxes are added to the Control Panel and existing mailboxes are updated according to the settings in Microsoft 365.

Important:

The upgrade cannot be performed if the option **POP3/IMAP** has been selected as the primary environment in the **Spam and Malware Protection** module (see Adjusting the Primary Environment Settings).

Important:

The option **Enterprise Backup** can only be selected if the partner has enabled 365 Total Backup (see Activating 365 Total Backup).

Click on the 365 Total Protection version to which you would like to upgrade. You have the following options:

- **Business**
- **Enterprise**
- **Enterprise Backup**

Notice:

For more information about the versions, see About 365 Total Protection on page 6.

Figure 21: Select version

If multi-factor authentication is enabled for the domain in the Control Panel (see Enabling Multi-Factor Authentication), a message about multi-factor authentication is displayed. Otherwise, a warning message is displayed.

5. **Important:**

   The upgrade to 365 Total Protection is only possible if multi-factor authentication is deactivated in the Control Panel. After the upgrade to 365 Total Protection, users from the Microsoft 365 tenant log in to the Control Panel with their credentials from Microsoft 365 and the authentication policies of the tenant apply (see Enabling Multi-Factor Authentication).

   If a message about multi-factor authentication is displayed, click on **Confirm**.

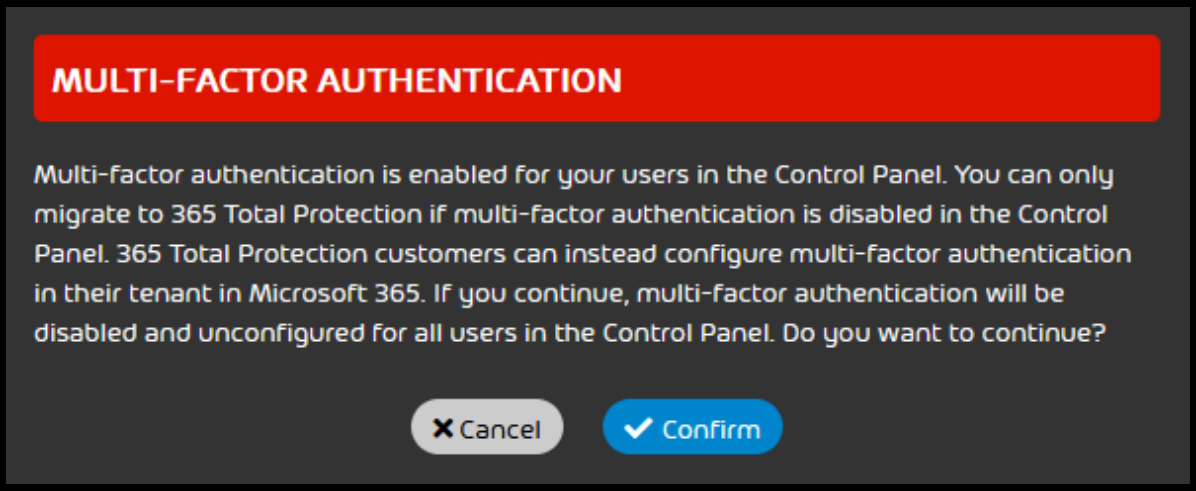

Figure 22: Deactivate multi-factor authentication

Multi-factor authentication is deactivated for the users of the domain. For users who had multi-factor authentication already configured, the configuration is deleted. A warning message is displayed.

6. In order to start the upgrade to 365 Total Protection, click on **Confirm**.

Figure 23: Confirm

7.

Important:

Customers cannot use 365 Total Protection and LDAP connections in the Control Panel at the same time. If the customer has active LDAP connections or LDAP mailboxes (see LDAP Connection), the LDAP connections will be deactivated and all LDAP mailboxes will be converted to regular mailboxes. Users and groups will no longer be synchronized with the directory service via LDAP. The customer's settings in the **LDAP Connection** tab of the **Service Dashboard** module are stored in the background but not displayed as long as the customer uses 365 Total Protection.

If the customer cancels the upgrade to 365 Total Protection or cancels 365 Total Protection and would like to use their LDAP connections again, customer-level administrators can reactivate the LDAP connections (see Activating the LDAP Connection). Mailboxes that are synchronized with the directory service will then become LDAP mailboxes again within 24 hours.

To deactivate your active LDAP mailboxes and to convert your LDAP mailboxes to regular mailboxes, click on **Confirm**.

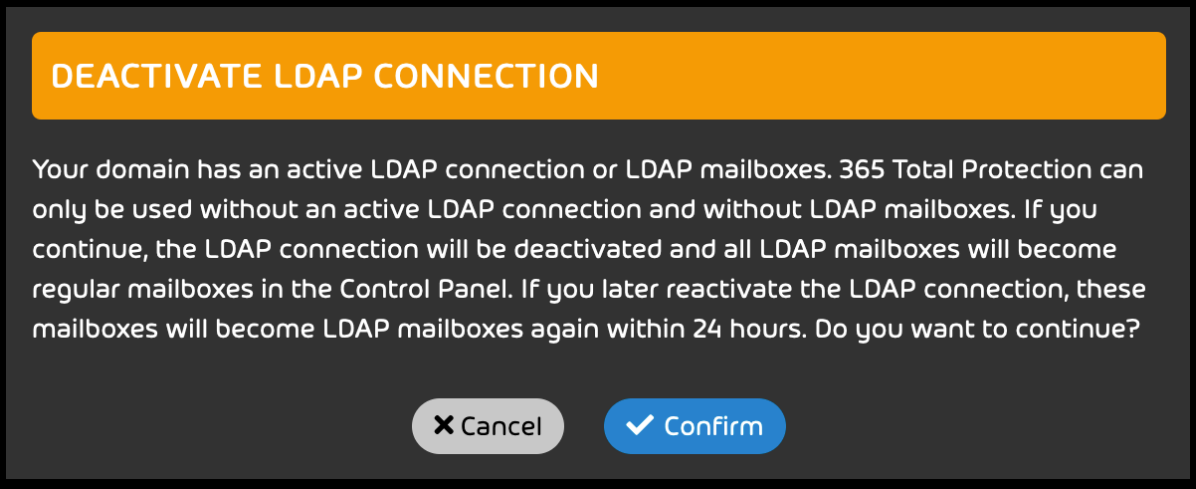

Figure 24: Deactivating the LDAP Connection

The first step for setting up 365 Total Protection is displayed.

8. Select whether existing mailboxes from the primary environment that are not managed in the customer's Microsoft 365 tenant should be assigned to an existing or a new secondary environment after the upgrade.

> **Notice:**
>
> After the upgrade to 365 Total Protection, only Microsoft 365 mailboxes from the customer's tenant may be assigned to the primary environment. Therefore, other mailboxes that already exist in the Control Panel and are currently assigned to the primary environment must be assigned to a secondary environment instead. These mailboxes can be assigned either to an existing secondary environment or to a new secondary environment.
>
> If no secondary environment exists for the customer yet, the **Existing environment** option will be hidden.

Figure 25: Select an environment for non-Microsoft-365 mailboxes from the primary environment

If the option has been selected, a form for creating a secondary environment is displayed.

9. If you have selected the **Existing environment** option, select a secondary environment from the drop-down menu **Select environment**.

> **Notice:**
>
> If only one secondary environment exists for the customer, it is already selected.

10. If you have selected the **New environment** option, create a secondary environment in the form.

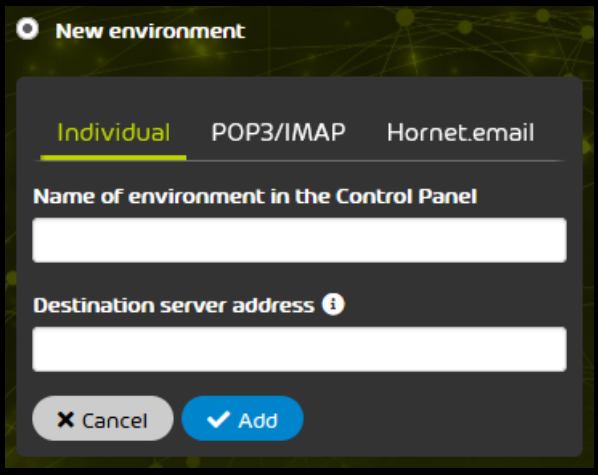

Figure 26: Create an environment

> **Notice:**
>
> For more information on how to create secondary environments, see Creating a Secondary Environment.

11. Click on **Next**.

The next step for setting up 365 Total Protection is displayed.

12. Optional: If you would like to enable mailbox migration, tick the checkbox **Enable mailbox migration**.

> **Notice:**
>
> Mailbox migration makes it easier for customers to switch from an on-premises Exchange server to Microsoft 365. With this feature, the customer can transfer mailbox data from their on-premises Exchange server to their Microsoft 365 tenant. For more information, see About Mailbox Migration on page 43.

> **Notice:**
>
> Mailbox migration is only available in the versions 365 Total Protection Enterprise and Enterprise Backup. In the Business version the checkbox is grayed out.

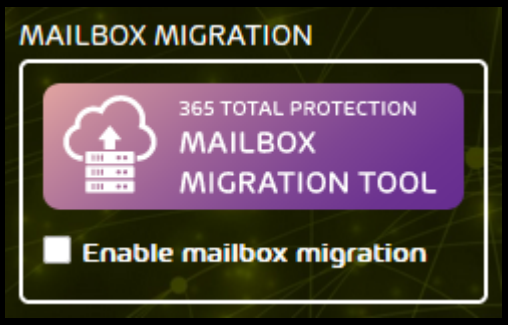

Figure 27: Enable mailbox migration

13. Click on **Next**.

If the checkbox **Enable mailbox migration** has been ticked, a confirmation window is displayed. Otherwise, the next step for setting up 365 Total Protection is displayed.

14. If a confirmation window is displayed, click on **Confirm**.

Attention:

Mailbox migration is subject to a fee. For more information, please contact your contact person.

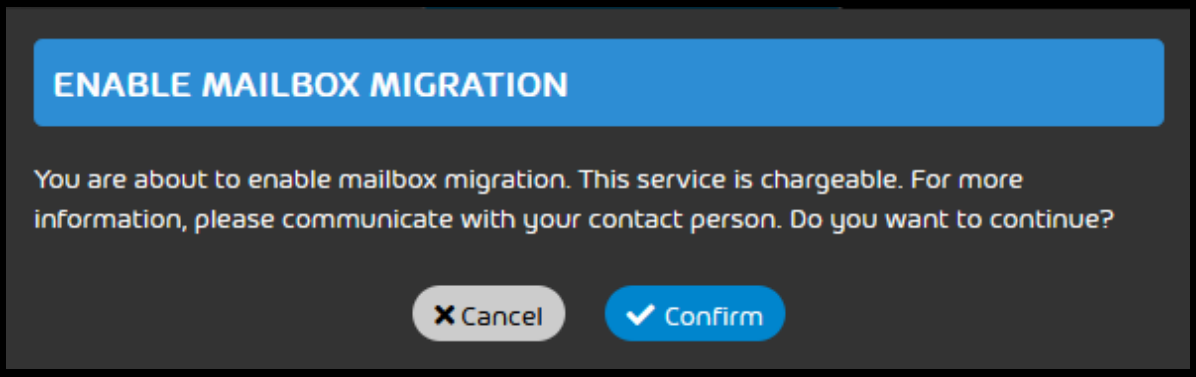

Figure 28: Confirm the enabling of mailbox migration

Mailbox migration is enabled. Once the customer has started the upgrade to 365 Total Protection, the customer can transfer mailbox data from their on-premises Exchange server to their Microsoft 365 tenant.

The next step for setting up 365 Total Protection is displayed.

15. Select to which environment Microsoft 365 mailboxes that already exist in the Control Panel and are currently assigned to a secondary environment shall be assigned. Toggle the switch of the desired option.

> **Notice:**
>
> After the upgrade to 365 Total Protection, the customer's Microsoft 365 tenant is set as the primary environment in the Control Panel (see Primary Environment Settings). Microsoft 365 mailboxes that are added to the Control Panel during synchronization with Microsoft 365 after the upgrade to 365 Total Protection are automatically assigned to the primary environment.
>
> The choices refer to Microsoft 365 mailboxes that already exist in the Control Panel before the upgrade and that are assigned to a secondary environment. After the upgrade, these Microsoft 365 mailboxes can either be assigned to the primary environment or remain in their current environment. Regardless if such mailboxes actually exist in the Control Panel, an option must be selected for the customer.

> **Notice:**
>
> If mailbox migration has been enabled, this setting cannot be edited. If mailboxes from the customer's Microsoft 365 tenant that are currently assigned to a secondary environment exist in the Control Panel, these mailboxes will be assigned to the new primary environment after the upgrade to 365 Total Protection.

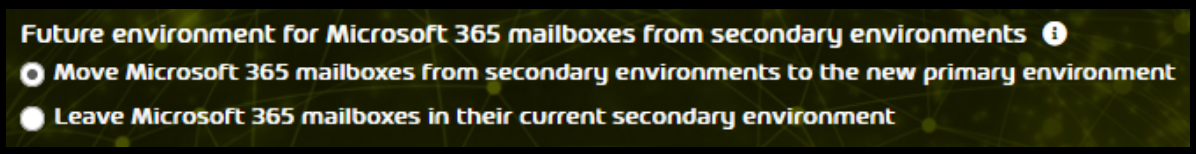

Figure 29: Select an environment for Microsoft 365 mailboxes from secondary environments

16. Click on **Next**.

A form is displayed.

17. Enter your contact data in the form.

> **Notice:**
>
> The contact data will allow us to contact you in case of problems or queries.

Figure 30: Enter contact data

18. If you would like to receive our IT Security News, tick the checkbox **I would like to receive IT Security News regularly.**.
19.

> **Attention:**
>
> Once 365 Total Protection is activated, a 14-day free trial period starts. In order for a customer to continue using the service after the trial period, the customer must purchase the service (see Ordering 365 Total Protection on page 109).

In order to start the upgrade, click on **Migrate now**.

The Microsoft 365 login page is displayed.

20. Log in with administrative credentials of the customer's Microsoft 365 tenant.

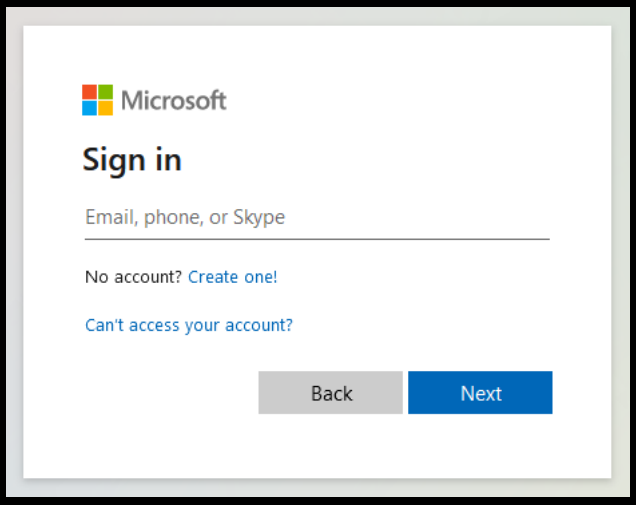

Figure 31: Log in

21. To synchronize our services with Microsoft 365, accept the requested permissions.

Notice:

During synchronization, domains and mailboxes from Microsoft 365 are transferred to the Control Panel. The Microsoft settings are not modified.

If groups exist in the Control Panel that have the same name as groups in Microsoft 365, the assignment of Microsoft 365 mailboxes to these groups is also synchronized in the Control Panel (see Group Management in the Control Panel on page 112 and Synchronizing Groups from Microsoft 365 in the Control Panel on page 112).

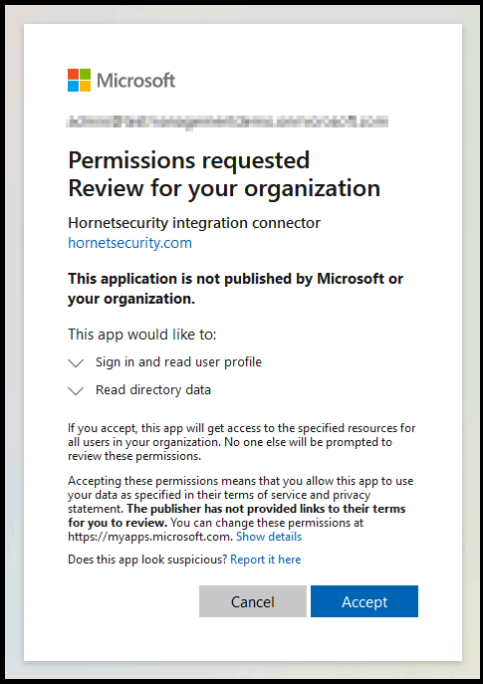

Figure 32: Accept permissions

22. If you have enabled mailbox migration (see step 12 on page 32), accept the requested permissions.

> **Notice:**
>
> These permissions grant us access to the mailboxes in the Microsoft 365 tenant and are only required for performing mailbox migration. We recommend removing the permissions of the Hornetsecurity Mailbox Migration app from the customer's Microsoft 365 tenant after the upgrade to 365 Total Protection has been completed.

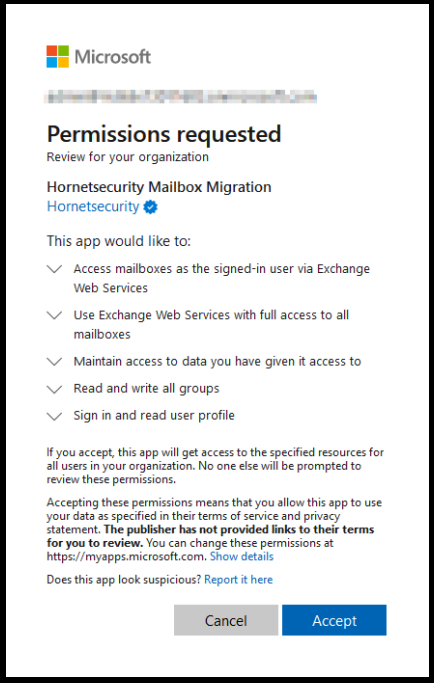

Figure 33: Accept the permissions for mailbox migration

If mailbox migration has been enabled (see step 12 on page 32), the upgrade to 365 Total Protection is paused so the customer can transfer mailbox data from their on-premises Exchange server to their Microsoft 365 tenant (see About Mailbox Migration on page 43). Only after the customer has finalized mailbox migration, the upgrade to 365 Total Protection is performed.

If mailbox migration has not been enabled, the upgrade to 365 Total Protection is directly performed. Once the upgrade has been successfully completed, the number of synchronized domains and mailboxes is displayed. The Microsoft 365 domains and

mailboxes have been created in the Control Panel under the customer. The domains are added to the **Customer Settings** > **Domains** module (see Domains). The domains are first

assigned the state **Not verified** in the column **Verified**. After a few minutes, we check whether the domains can be verified (see Domain Verification).

Notice:

During the upgrade, different actions are performed, including, for example, the creation or modification of environments, email addresses, domains, and mailboxes. These actions are documented in the **Auditing 2.0** module (see Auditing 2.0).

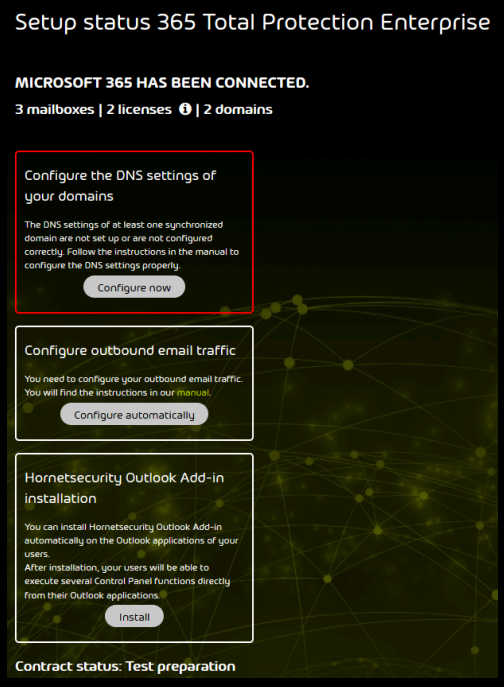

Figure 34: Successful upgrade

Important:

If the upgrade fails, the reason is displayed. Once the error has been fixed, the upgrade can be started again.

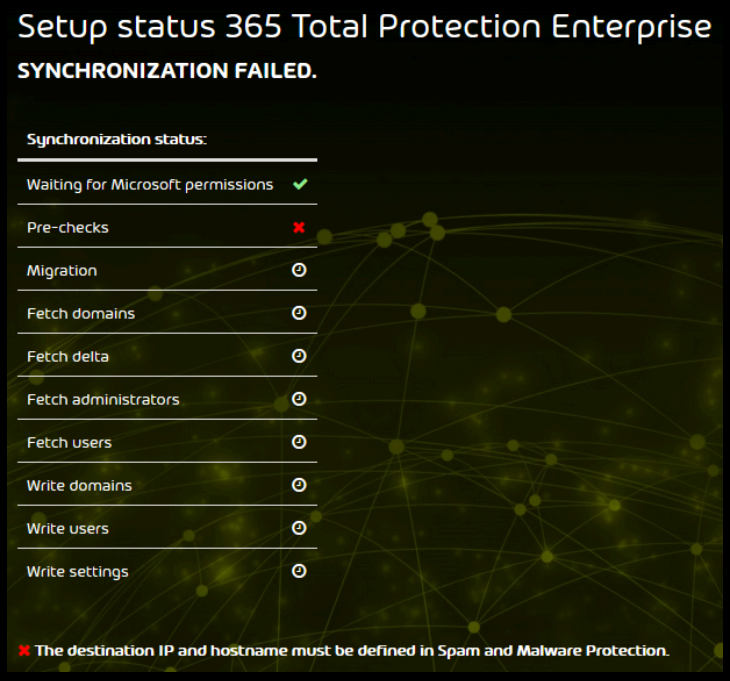

Figure 35: Failed upgrade

The Microsoft 365 domains and mailboxes have been transferred to 365 Total Protection. The domains and mailboxes have been created in the Control Panel. From now on, you can log in to the Control Panel with your Microsoft 365 credentials and configure the services.

To take full advantage of our services, adjust the settings of the synchronized domains (see Configuration of Microsoft Services on page 94) and configure the outgoing email traffic.

If you have selected 365 Total Protection Enterprise Backup, you must also configure 365 Total Backup (see Configuring 365 Total Backup on page 82) to back up data from your Microsoft 365 tenant.

Language and Icons Used in the Documentation

Gender Equality

For better readability, the generic masculine form is used in this documentation. Nevertheless, the information refers to members of all genders.

Used symbols

The following symbols are used to improve the recognizability of relevant steps within instructional chapters:

Symbol	Description	Explanation
	Prerequisites	Condition that must be fulfilled before performing the next step
	Interim result	Result that is reached after executing a step
	Final result	Result that is reached after the described order of steps

Safety instructions and warnings

Warnings and safety instructions are used to inform the user about residual risks and dangers and how to avoid them with the recommended procedure. Following safety instructions and warnings are used in this documentation:

Symbol	Description	Explanation
	NOTE	Further information within a given paragraph that is relevant for the execution of later steps.
	TIP	Note about configuration options.
	IMPORTANT	Warning containing information about restrictions or important configuration options of a service.
	ATTENTION	Warning about additional costs that may be incurred depending on the booked services.
	WARNING	Warning about a potential loss of data.

Symbol	Description	Explanation
	DANGER	Warning about a potential system infection with malware.

About Mailbox Migration

We would like to make it easier for existing customers who have used an on-premises Exchange server in the past to switch to Microsoft 365. Therefore, we offer customers who upgrade to 365 Total Protection Enterprise or Enterprise Backup (see Upgrade to 365 Total Protection as a Customer) the option to transfer the data of mailboxes from their on-premises Exchange server to their Microsoft 365 tenant.

Notice:

Mailbox migration is supported for Exchange Server as of version 2007.

During mailbox migration, the following data is transferred:

- Emails including attachments
- Contacts
- Calendars
- Tasks
- Notes

Notice:

If possible, the flags of emails (e. g., read, unread, important) are kept in the Microsoft 365 tenant.

Notice:

The following mailbox data cannot be migrated:

- Public folders
- Archives
- Journals
- User-specific settings
- Distribution lists
- Mailbox permissions

Notice:

For information on other restrictions of mailbox migration, see Restrictions of Mailbox Migration on page 45.

Partner-level and customer-level administrators can enable mailbox migration during the customer's upgrade to 365 Total Protection (see Upgrading to 365 Total Protection). If mailbox migration is enabled, the upgrade is paused so administrators can transfer the data of all desired mailboxes from the on-premises Exchange server to the customer's Microsoft 365 tenant.

Attention:

Mailbox migration will increase costs according to the price list.

But before mailbox migration can be performed, prerequisites must be met on the on-premises Exchange server, in the Microsoft 365 tenant, and in the Control Panel (see Prerequisites for Mailbox Migration on page 46). Once these preparations have been made, administrators can migrate mailbox data in the Control Panel (see Migration of Mailbox Data on page 64).

Notice:

A mailbox migration may take several days. Exact times cannot be given because the duration depends on the following factors:

- Number and size of the mailboxes to be migrated
- Overall load due to other queued mailbox migrations

Administrators are informed by email about state changes. Furthermore, administrators can see the current state in the **365 Total Protection** > **365 Total Protection** module at any time. During mailbox migration, the Control Panel can be used as usual.

Once administrators have finalized mailbox migration, the upgrade to 365 Total Protection is resumed.

Restrictions of Mailbox Migration

Mailbox migration (see About Mailbox Migration on page 43) has limitations. The limitations affect the data that can be migrated. The limitations are listed below.

Limitations caused by Exchange Web Services (EWS)

EWS limitations are used by Microsoft to restrict the server resources that a user or application can use. This ensures the reliability and operation time of servers. This results in the following limitations for mailbox migration:

- The owner of a mailbox becomes the organizer of all their appointments in the Microsoft 365 tenant.
- The participant status in appointments (accepted or rejected) cannot be migrated.
- Mailbox migration attempts to resolve system-internal addresses (e. g., X500 addresses) and replace them with a valid email address. If this operation fails, the address will not be transferred to the Microsoft 365 tenant.
- During mailbox migration, invalid entries (e. g., invalid URLs in website fields) are filtered out because they would be rejected by the Microsoft 365 tenant.

Limitations caused by the on-premises Exchange server

Depending on the version of the on-premises Exchange server, the following additional limitations may apply:

- If an email exceeds the data volume limit of the Microsoft 365 tenant, the email will not be migrated. The user will be notified in this case.
- Emails with a size of more than 64 MB will not be migrated.
- The maximum data volume per mailbox must not exceed 50 GB.
- The appearance of certain email messages (e. g., specific MIME formats) in the Microsoft 365 tenant differs from the appearance on the on-premises Exchange server.
- The mapping of element properties is limited (e. g., in case of missing support by the Microsoft 365 tenant).
- The mapping of shared folders is limited.

Prerequisites for Mailbox Migration

Before mailbox migration (see About Mailbox Migration on page 43) can be performed, requirements must be met on the on-premises Exchange server, in the Microsoft 365 tenant and in the Control Panel. Only then can customer-level administrators perform mailbox migration in the Control Panel (see Migration of Mailbox Data on page 64).

As mailbox migration can only migrate data between existing mailboxes, the mailboxes must already exist on the on-premises Exchange server, in the Microsoft 365 tenant and in the Control Panel (see Prerequisites for Mailboxes on page 47).

On the on-premises Exchange server, another requirement must be met. During mailbox migration, we access the mailboxes to be migrated on the on-premises Exchange server using an administrator's credentials, thus the administrator of the on-premises Exchange server must be authorized to log in to the users' mailboxes. Therefore, the administrator must be assigned the **ApplicationImpersonation** role (see Creating a Role Group on the Exchange Server on page 47).

Other requirements must also be met in the Microsoft 365 tenant. Just like the administrator of the on-premises Exchange server, the administrator of the Microsoft 365 tenant must be assigned the **ApplicationImpersonation** role (see Creating a Role Group in Microsoft 365 on page 53). To speed up the validation of environments (see Validating an Environment on page 65) during mailbox migration, you can grant the administrator of the Microsoft 365 tenant permissions to read and manage the mailboxes to which the data is to be migrated. You can either grant the administrator access to individual mailboxes via the Exchange Admin Center (see Granting Read and Manage Permissions for Mailboxes in Microsoft 365 on page 57) or grant them access to all mailboxes of the Microsoft 365 tenant via PowerShell (see Granting Read and Manage Permissions for Mailboxes in Microsoft 365 using PowerShell on page 60). As Exchange Web Services are used to access the mailboxes in the Microsoft 365 tenant,

preparations must also be made in Exchange Web Services. To allow access to the mailboxes via Exchange Web Services, access to Exchange Web Services must be allowed (see Allowing Access to Exchange Web Services on page 60). In addition, the throttling of Exchange Web Services must be temporarily deactivated (see Deactivating the Throttling of Exchange Web Services on page 62) so data can be migrated at a higher bandwidth.

Prerequisites for Mailboxes

Mailbox migration (see About Mailbox Migration on page 43) uses the Control Panel to transfer mailbox data from a customer's on-premises Exchange server to their Microsoft 365 tenant. However, no new mailboxes are created in the process. Therefore, prior to mailbox migration, the customer must ensure that the mailboxes to be migrated exist in the following systems:

- On-premises Exchange server
- Microsoft 365 tenant
- Control Panel

Important:

In order for us to be able to match the mailboxes in the different systems, the email addresses of a mailbox must match each other exactly up to the @ character. The domains on the on-premises Exchange server and in the Microsoft 365 tenant must be different because the mailboxes are assigned to different servers.

To add multiple mailboxes to the Microsoft 365 tenant at once, the customer's administrators can first export the mailboxes from the on-premises Exchange server and then import the mailboxes into the Microsoft 365 tenant as a CSV file.

To add the mailboxes to the Control Panel, customer-level administrators can synchronize the mailboxes in the Control Panel with the directory service of the on-premises Exchange server via an LDAP connection (see LDAP Connection), import them from a CSV file (see Importing Mailboxes from a CSV File) or add them manually to the Control Panel (see Adding a Mailbox).

Creating a Role Group on the Exchange Server

The mailboxes whose data is to be migrated exist on the on-premise Exchange server (see Prerequisites for Mailboxes on page 47). You are an administrator of the customer's on-premise Exchange server.

Mailbox migration (see About Mailbox Migration on page 43) requires access to the customer's on-premise Exchange server. The credentials of an administrator of the on-premise

Exchange server are used for this purpose. As mailbox migration requires reading the data of all mailboxes to be migrated, the administrator must be authorized to log in to the mailboxes. To grant the administrator this permission, you must create a role group on the on-premises Exchange server. Via the role group, you can grant the administrator the permissions of the **ApplicationImpersonation** role.

1. Open the Exchange Admin Center of the on-premises Exchange server in your browser.

   Notice:

   By default, the Exchange Admin Center is accessible under the link **https://<domain name>/ecp**. The placeholder **<domain name>** stands for the absolute address of the on-premises Exchange server in the Domain Name System.

2. Log in to the Exchange Admin Center with your administrative credentials of the on-premises Exchange server.
3. Navigate to **permissions**.
4. Select the **admin roles** tab.

5. Click on the plus sign.

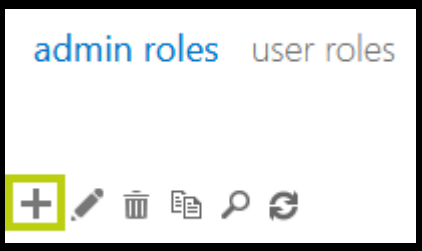

Figure 36: Add an administrator role

The **new role group** window is displayed.

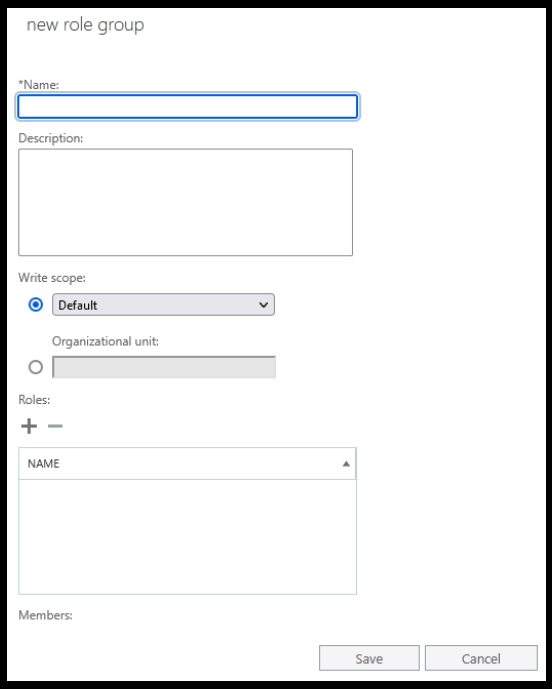

Figure 37: new role group

6. Enter a name for the role group in the **Name** field. You can choose any name.
7. Optional: Enter a description of the role group in the **Description** field.

8. Click on the plus sign under **Roles**.

Figure 38: Add a role

The **Select a Role** window is displayed.

9. Select the **ApplicationImpersonation** role from the list.

> **Notice:**
>
> The **ApplicationImpersonation** role authorizes the administrator to log in to the on-premise Exchange server on behalf of other mailboxes.

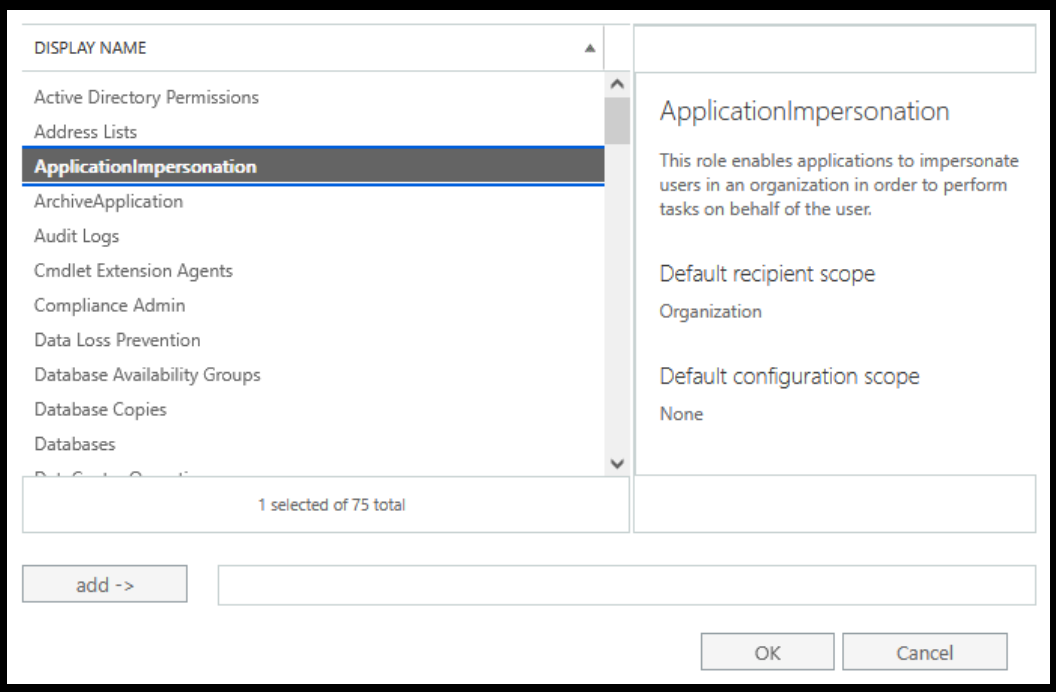

Figure 39: Select ApplicationImpersonation

10. Click on **add**.

    The role is selected.

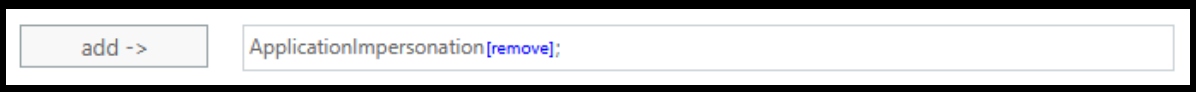

Figure 40: Selected role

11. Click on **OK**.

    The window **Select a Role** closes. The **ApplicationImpersonation** role is displayed in the **new role group** window under **Roles**.

Figure 41: Added role

12. Click on the plus sign under **Members**.

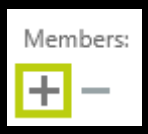

Figure 42: Add a member

    The **Select Members** window opens.

13. From the list in the **Select Members** window, select the administrator whose credentials for the on-premises Exchange server will be used to perform mailbox migration in the Control Panel (see Migration of Mailbox Data on page 64).

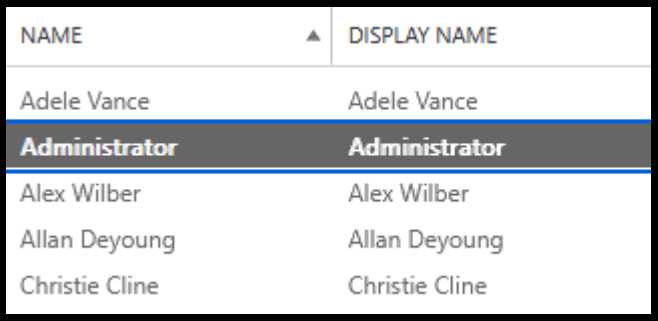

Figure 43: Select an administrator

14. Click on **add**.

The administrator is selected.

Figure 44: Selected administrator

15. Click on **OK**.

The window **Select Members** closes. The selected administrator is displayed in the **new role group** window under **Members**.

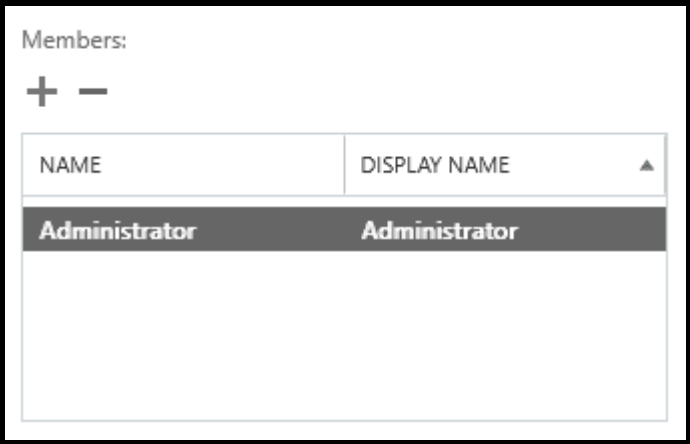

Figure 45: Added administrator

16. Click on **Save**.

    The window **new role group** closes. The role group is added to the list in the **admin roles** tab under **permissions** in the Exchange Admin Center. The administrator is now authorized to log in to all mailboxes on the on-premises Exchange server.

An administrator has been granted the permissions of the **ApplicationImpersonation** role on the customer's on-premises Exchange server.

Creating a Role Group in Microsoft 365

The mailboxes to which data is to be migrated already exist in the customer's Microsoft 365 tenant (see Prerequisites for Mailboxes on page 47). You are an administrator of the Microsoft 365 tenant.

Mailbox migration (see About Mailbox Migration on page 43) requires access to the customer's Microsoft 365 tenant. The credentials of an administrator of the Microsoft 365 tenant are used for this purpose. As mailbox migration requires access to all mailboxes in the Microsoft 365 tenant to which data is to be migrated, the administrator must be authorized to log in to the mailboxes. To grant the administrator this permission, you must create a role group in the Microsoft 365 tenant. Via the role group, you can grant the administrator the permissions of the **ApplicationImpersonation** role.

1. Open the website **admin.exchange.microsoft.com**.
2. Log in with your administrative credentials of the Microsoft 365 tenant.
3. Navigate to **Roles** > **Admin roles**.

4. Click on **Add role group**.

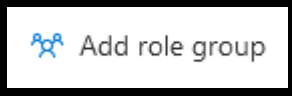

Figure 46: Add a role group

The page **Set up the basics** is displayed.

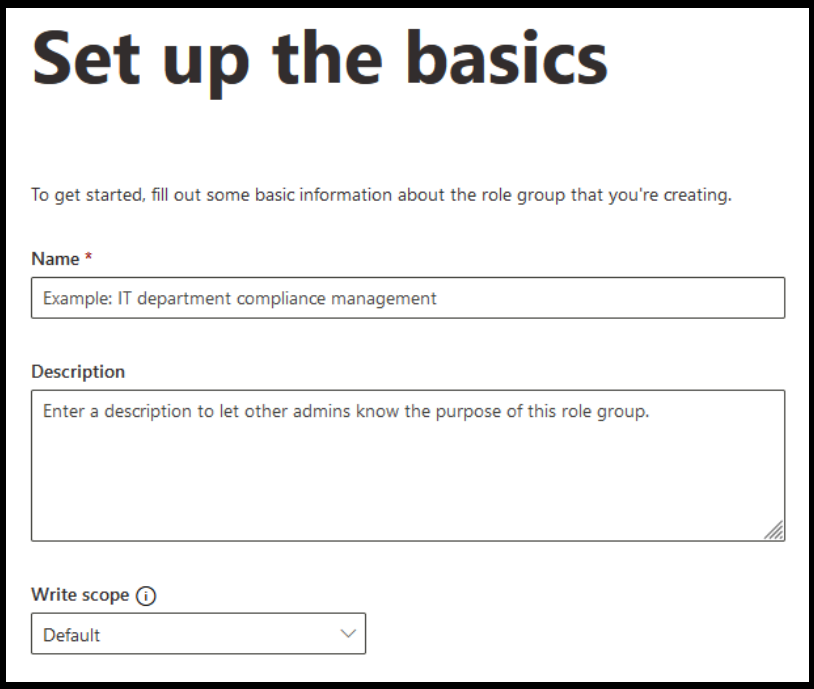

Figure 47: Set up the basics

5. Enter a name for the role group in the **Name** field. You can choose any name.
6. Optional: Enter a description of the role group in the **Description** field.
7. Click on **Next**.

The page **Add permissions** is displayed.

8. Select the **ApplicationImpersonation** role from the list of roles.

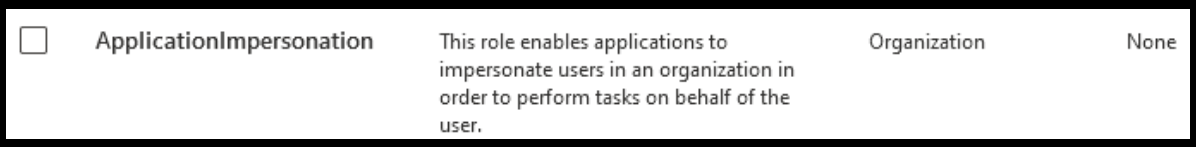

Figure 48: Select ApplicationImpersonation

9. Click on **Next**.

The page **Assign admins** is displayed.

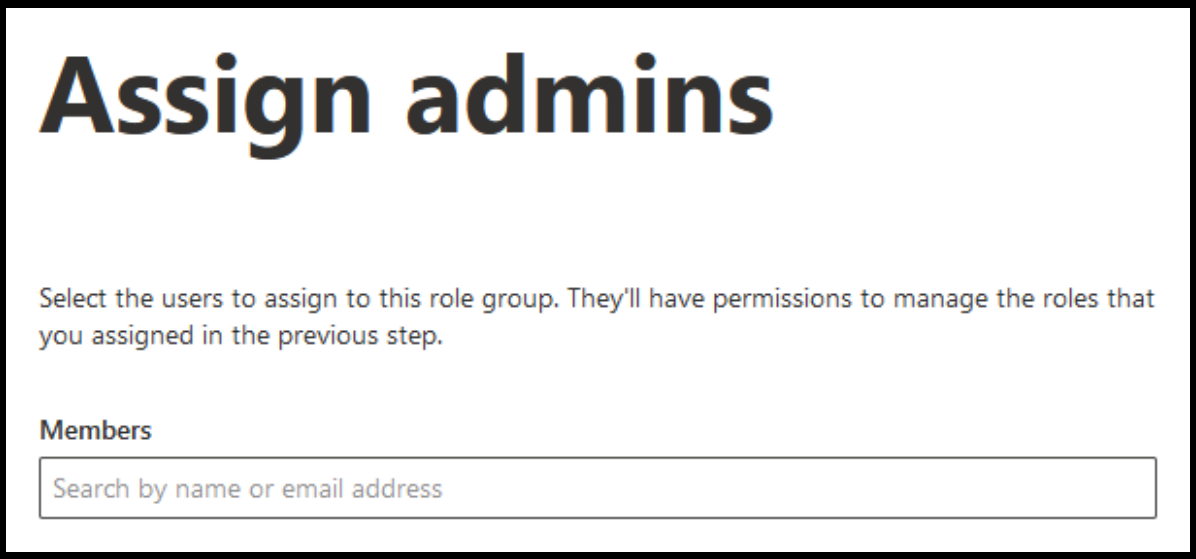

Figure 49: Next

10. In the **Members** field, enter the name or email address of the administrator whose credentials will be used for mailbox migration, and select the administrator.

11. Click on **Next**.

The page **Review role group and finish** is displayed.

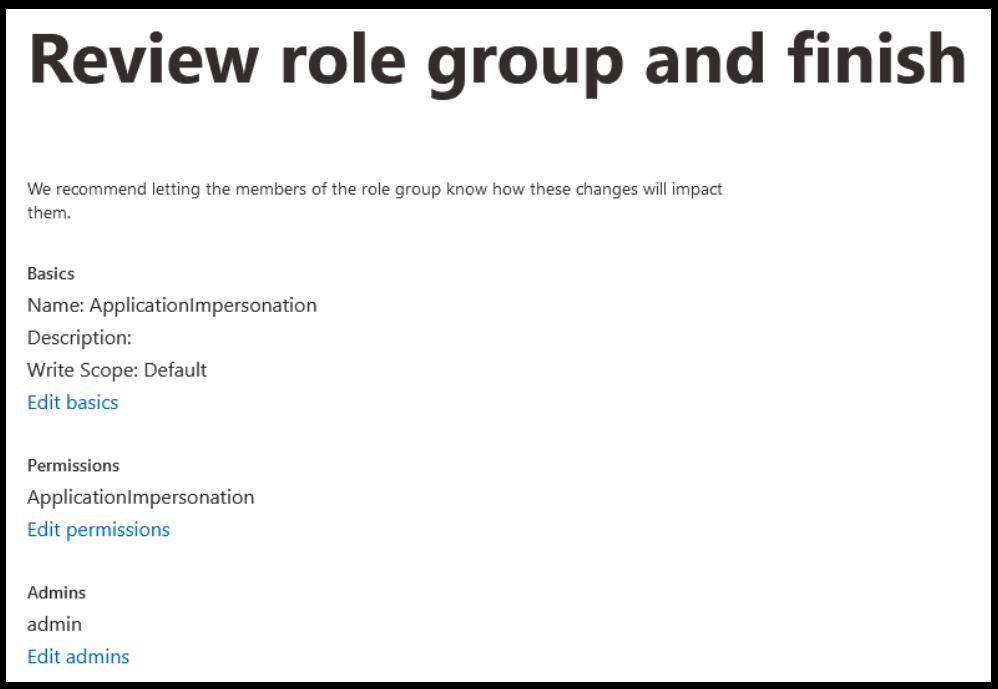

Figure 50: Review role group and finish page

12. Click on **Add role group**.

The role group is created. The creation may take up to 1 minute. Once the role group has been created, a success message is displayed.

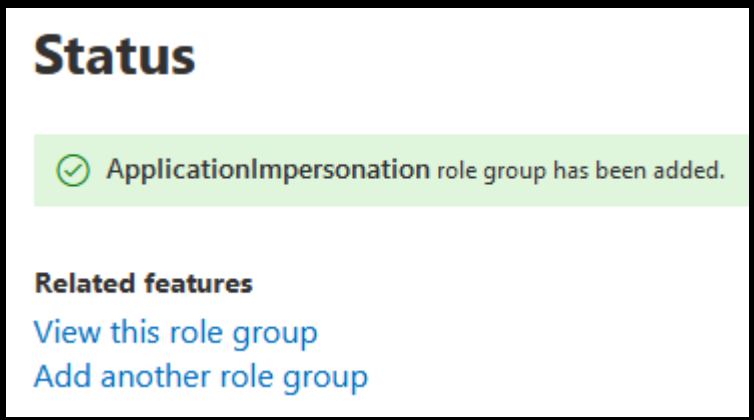

Figure 51: Success message

13. Click on **Done**.

    The success message is closed. The **Roles** > **Admin roles** module is displayed again. The new role group is displayed in the list of role groups.

An administrator has been granted the permissions of the **ApplicationImpersonation** role in the customer's Microsoft 365 tenant.

Granting Read and Manage Permissions for Mailboxes in Microsoft 365

The mailboxes to which data is to be migrated already exist in the customer's Microsoft 365 tenant (see Prerequisites for Mailboxes on page 47). You are an administrator of the Microsoft 365 tenant.

To speed up the validation of environments (see Validating an Environment on page 65) during mailbox migration (see About Mailbox Migration on page 43), you can grant permissions to read and manage the mailboxes to be migrated to the administrator whose credentials for the customer's Microsoft 365 tenant will be used for mailbox migration. This gives the administrator direct access to the mailboxes.

Notice:

When validating environments (see Validating an Environment on page 65) for mailbox migration, the first step is to check whether the mailboxes to be migrated can be accessed directly using the administrator's credentials. If direct access is not possible, the mailboxes are accessed via the **ApplicationImpersonation** role (see Creating a Role Group in Microsoft 365 on page 53) instead. As a result, the validation takes longer.

For mailbox migration, we recommend you to first validate an environment with a small number of mailboxes and grant the administrator direct access to these mailboxes in the Microsoft 365 tenant. This way, the result of the validation is available soon and the administrator can familiarize themselves with the process.

Notice:

In the Microsoft Admin Center, the administrator can be granted permission for direct access to individual mailboxes. Only via PowerShell, it is possible to grant the administrator direct access to all mailboxes at once (see Granting Read and Manage Permissions for Mailboxes in Microsoft 365 using PowerShell on page 60).

1. Open the website **admin.microsoft.com**.
2. Log in with your administrative credentials of the Microsoft 365 tenant.
3. Navigate to **Users** > **Active users**.

   A list with all active users of the Microsoft 365 tenant is displayed.
4. In the list, click on the display name of a user to whose mailbox data from the customer's on-premises Exchange server shall be migrated later on.

   On the right side of the window, information about the user is displayed.
5. Select the **Mail** tab.

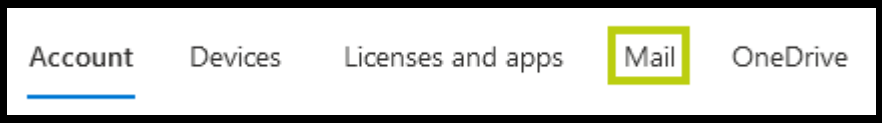

Figure 52: Select the Mail tab

6. Click on **Read and manage permissions** under **Mailbox permissions**.

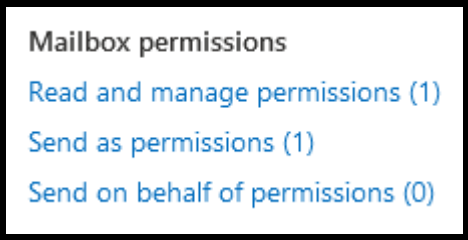

Figure 53: Select permissions

The page **Read and manage permissions** is displayed.

7. Click on **Add permissions**.

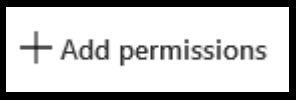

Figure 54: Add permissions

The page **Add user mailbox permissions** is displayed.

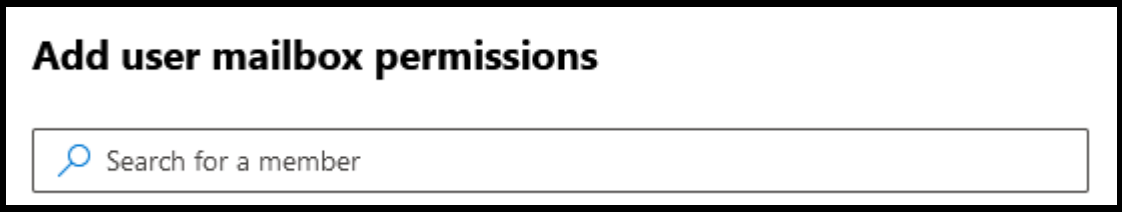

Figure 55: Add user mailbox permissions page

8. Search for and select the administrator whose Microsoft 365 tenant credentials will later be used for mailbox migration.
9. Click on **Add**.

The **Read and manage permissions** page is displayed again. The administrator is displayed in the list of permissions. The administrator is granted permissions to read and manage the mailbox. It may take up to 1 hour for the changes to take effect.

10. Click on the cross icon in the upper right corner.

The page is closed. The **Users** > **Active users** module is displayed again.

11. Repeat steps 4 on page 58 to 10 on page 59 for all mailboxes to which data is later to be transferred from the customer's on-premises Exchange server.

An administrator has been granted permissions to read and manage mailboxes in the customer's Microsoft 365 tenant.

Granting Read and Manage Permissions for Mailboxes in Microsoft 365 using PowerShell

The mailboxes to which data is to be migrated already exist in the customer's Microsoft 365 tenant (see Prerequisites for Mailboxes on page 47). You are an administrator of the Microsoft 365 tenant.

To speed up the validation of environments (see Validating an Environment on page 65) during mailbox migration (see About Mailbox Migration on page 43), you can grant permissions to read and manage the mailboxes to be migrated to the administrator whose credentials for the customer's Microsoft 365 tenant will be used for mailbox migration. This gives the administrator direct access to the mailboxes. Instead of giving the administrator access to individual mailboxes (see Granting Read and Manage Permissions for Mailboxes in Microsoft 365 on page 57), you can use PowerShell to give the administrator access to all mailboxes in the Microsoft 365 tenant at once.

1. Open the PowerShell of your Microsoft 365 tenant.
2. Run the following command and replace the **<administrator email address>** placeholder with the email address of the administrator who shall be granted permissions to read and manage all mailboxes of the Microsoft 365 tenant:

   get-mailbox | add-mailboxpermission -User <administrator email address> -AccessRights FullAccess

   

   The administrator is granted permissions to read and manage all mailboxes of the Microsoft 365 tenant. PowerShell lists the users to whom the administrator now has full access.

An administrator has been granted permissions to read and manage all mailboxes in the customer's Microsoft 365 tenant.

Allowing Access to Exchange Web Services

You are an administrator of the customer's Microsoft 365 tenant.

During mailbox migration (see About Mailbox Migration on page 43), we need to access the data of the mailboxes in the customer's Microsoft 365 tenant. For access, we use the Exchange

Web Services. Therefore, you must allow access to the Exchange Web Services of the Microsoft 365 tenant.

1. Open the website aad.portal.azure.com.
2. Log in with your administrative credentials of the Microsoft 365 tenant.
3. Navigate to **Azure Active Directory Admin Center**.

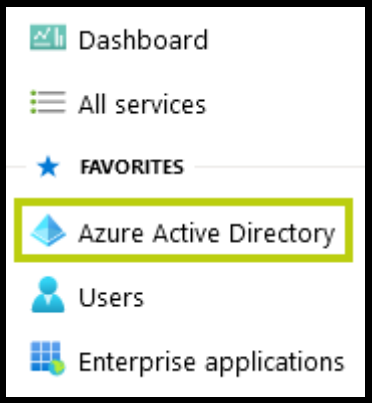

Figure 56: Open Azure Active Directory

4. Click on **Properties** under **Manage**.

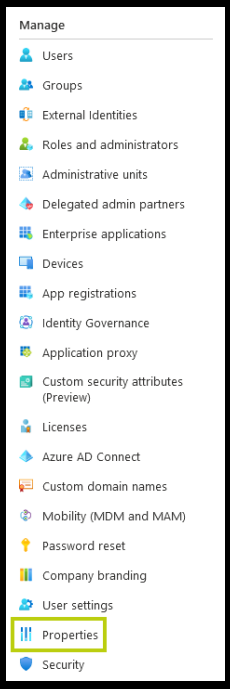

Figure 57: Opening the settings

5. At the bottom of the page, click on the link **Manage security defaults**.

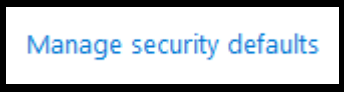

Figure 58: Open security defaults

The page **Enable security defaults** is displayed.

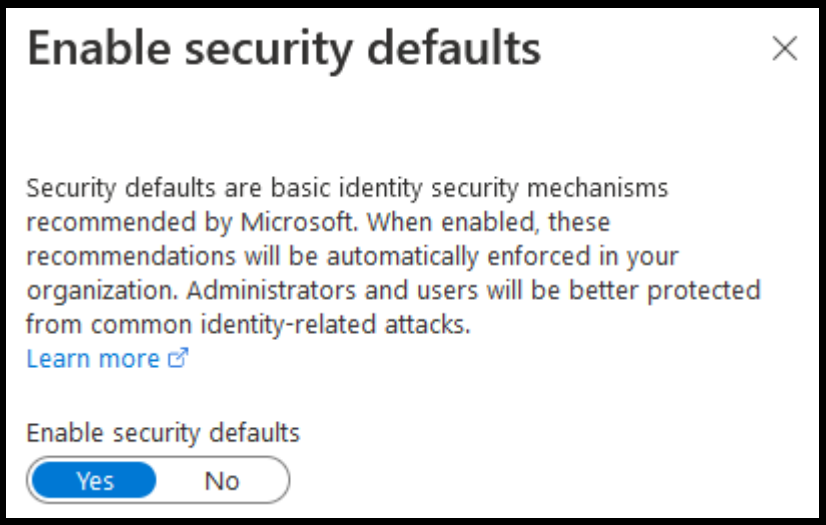

Figure 59: Security defaults

6. Click on **No**.
7. Click on **Save**.

The changes are saved.

Access to the Exchange Web Services has been allowed.

Deactivating the Throttling of Exchange Web Services

You are an administrator of the customer's Microsoft 365 tenant.

To migrate data to the customer's Microsoft 365 tenant at a higher bandwidth during mailbox migration (see About Mailbox Migration on page 43), you must temporarily deactivate the Exchange Web Services throttling.

1. Open the website admin.microsoft.com.
2. Log in with your administrative credentials of the Microsoft 365 tenant.
3. Enter the following text in the input field: **EWS Throttling**.
4. Click on **Run Tests**.

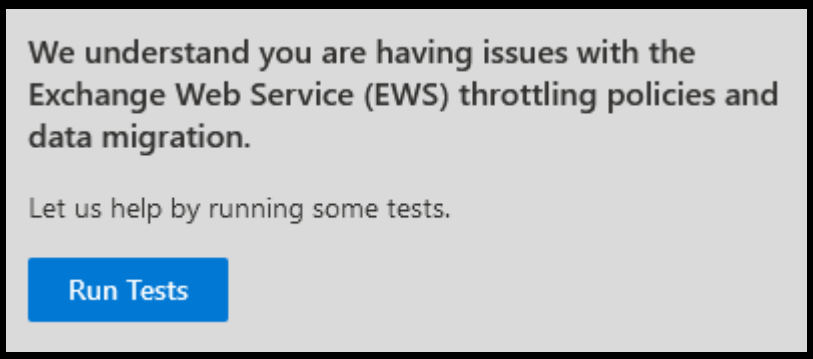

Figure 60: Run tests

The tests are performed. If the Exchange Web Services are throttled, the following text is displayed.

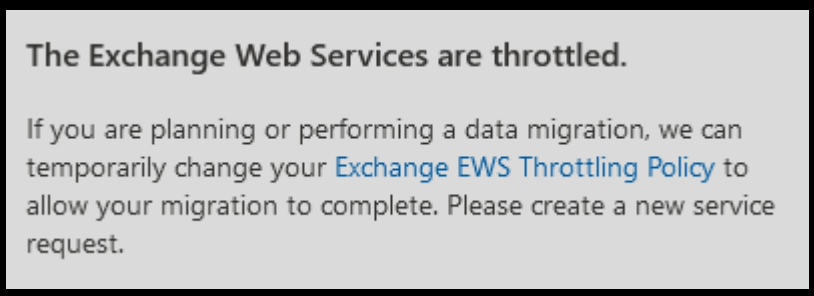

Figure 61: Throttling active

5. Create a support request at Microsoft to deactivate the throttling of the Exchange Web Services for 30 days.

Microsoft support temporarily deactivates the Exchange Web Services throttling.

The throttling of the Exchange Web Services has been temporarily deactivated.

Migration of Mailbox Data

During the upgrade of an existing customer to 365 Total Protection Enterprise or Enterprise Backup (see Upgrading to 365 Total Protection), partner-level and customer-level administrators can transfer mailbox data from an on-premises Exchange server to the customer's Microsoft 365 tenant (see About Mailbox Migration on page 43).

Important:

Before administrators can perform mailbox migration in the Control Panel, the requirements on the on-premises Exchange server, in the Microsoft 365 tenant and in the Control Panel must be met (see Prerequisites for Mailbox Migration on page 46).

Notice:

A mailbox migration may take several days. Exact times cannot be given because the duration depends on the following factors:

- Number and size of the mailboxes to be migrated
- Overall load due to other queued mailbox migrations

Administrators are informed by email about state changes. Furthermore, administrators can see the current state in the **365 Total Protection** > **365 Total Protection** module at any time. During mailbox migration, the Control Panel can be used as usual.

In order to migrate mailbox data, administrators must perform several steps in the Control Panel. First, administrators must validate the environment of the mailboxes whose data they would like to transfer to the customer's Microsoft 365 tenant (see Validating an Environment on page 65). With the validation, we ensure that the on-premises Exchange server and the Microsoft 365 tenant can be accessed.

Notice:

Administrators can validate several environments. This way, it is possible to transfer mailbox data from different Exchange servers to the customer's Microsoft 365 tenant.

Once an administrator has validated an environment, they can select one or multiple mailboxes from the environment and migrate the data of these mailboxes (see Migrating Mailboxes on page 72).

Important:

Administrators can only migrate mailboxes from environments that they have validated themselves.

Once the data of all desired mailboxes have been transferred to the customer's Microsoft 365 tenant, administrators can finalize mailbox migration (see Finalizing Mailbox Migration on page 81). After that, the upgrade to 365 Total Protection is automatically resumed (see Upgrading to 365 Total Protection).

Important:

Mailbox migration is only possible once. After finalizing mailbox migration, it is no longer possible to migrate any more mailbox data.

Validating an Environment

You have started the upgrade to 365 Protection Enterprise or Enterprise Backup and enabled mailbox migration (see Upgrading to 365 Total Protection). You have prepared the on-premises Exchange server, the Microsoft 365 tenant and the Control Panel for mailbox migration (see Prerequisites for Mailbox Migration on page 46). You have added mailboxes to the environment you want to validate (see Secondary Environments).

During the upgrade of an existing customer to 365 Total Protection Enterprise or Enterprise Backup (see Upgrading to 365 Total Protection), you can transfer mailbox data from an on-premises Exchange server to the customer's Microsoft 365 tenant (see About Mailbox Migration on page 43). The migration of mailbox data (see Migration of Mailbox Data on page 64) is only possible with access to the on-premises Exchange server and the Microsoft 365 tenant. Before migrating data of mailboxes (see Migrating Mailboxes on page 72), you must validate the environment (see Secondary Environments) to which the mailboxes of the on-premises Exchange server are assigned in the Control Panel. To do this, you must enter the credentials of the on-premises Exchange server. With the validation, we ensure that the on-premises Exchange server can be accessed.

Notice:

Administrators can validate several environments. This way, it is possible to transfer mailbox data from different Exchange servers to the customer's Microsoft 365 tenant.

1. Log in to the Control Panel with your administrative credentials.

2. From the scope selection, select the domain for which you want to validate an environment.
3. Navigate to **365 Total Protection** > **365 Total Protection**.

   

   The **Mailbox migration** page is displayed in the module.

4. **CAUTION:**

   If the entered credentials of the on-premises Exchange server become invalid during the mailbox migration, no further data can be transferred from the on-premises Exchange server to the Microsoft 365 tenant. This can cause mailbox data to be incomplete in the Microsoft 365 tenant. To ensure that the mailbox data is transferred completely, do not change the credentials of the on-premises Exchange server until the mailbox migration is complete (see Finalizing Mailbox Migration on page 81).

   In the **Environment validation** column, fill in the **On-premises Exchange server** form.

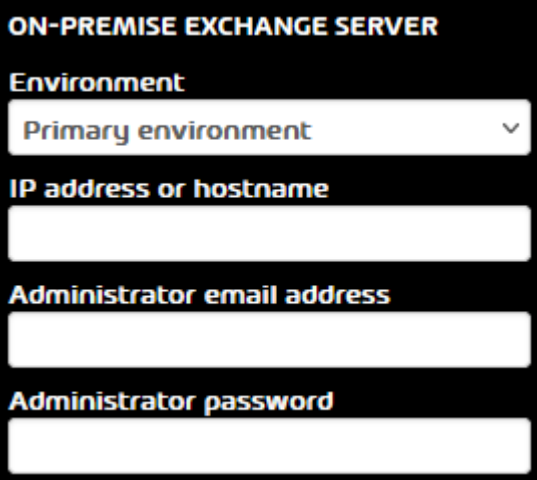

Figure 62: Fill in the form

a) From the **Environment** drop-down menu, select the environment of the mailboxes whose data you want to migrate.

b) In the **IP address or hostname** field, type the IP address or hostname of the on-premises Exchange server where the mailbox data is located.

c) In the **Administrator email address** field, enter the email address of an administrator of the on-premises Exchange server.

d) In the **Administrator password** field, enter the password of the administrator of the on-premises Exchange server.

5. Click on **Validate environment**.

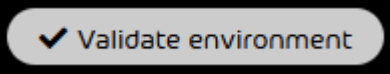

Figure 63: Validate environment

The environment is added to the list in the **Validated environments** column. The envinronment is validated. Once the result of the validation is available, the environment is

assigned to this result within the list. If the list contains at least one successfully validated environment, the **Select mailboxes to migrate** button below the list will be enabled.

Notice:

The list in the **Validated environments** column is not updated automatically. Administrators can reload the list by clicking the **Refresh** button.

Notice:

During the validation process, we check whether access to the on-premises Exchange server and the Microsoft 365 tenant is possible with the credentials entered. We also spot-check that the administrator has access to the mailboxes assigned to the environment in the Control Panel on the on-premises Exchange server and in the Microsoft 365 tenant.

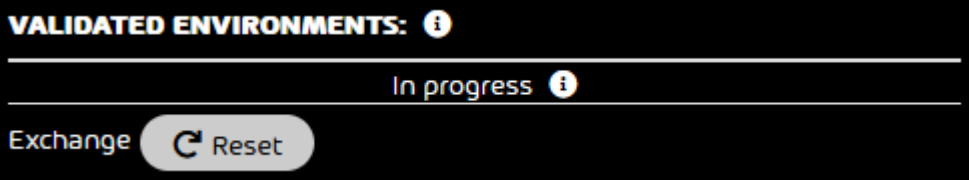

Figure 64: Validation in progress

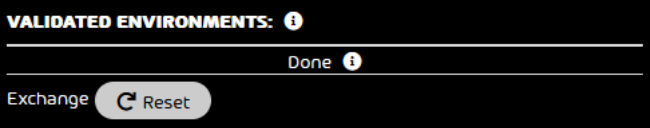

Figure 65: Successful validation

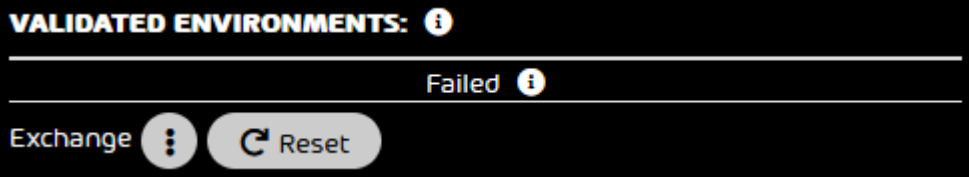

Figure 66: Failed validation

Notice:

If the validation failed, clicking the button with three dots will display information about the reason. To retry validating the environment, the validation must be reset first (see Resetting the Validation of an Environment on page 70).

The environment has been validated.

Important:

The credentials of the on-premises Exchange server and the Microsoft 365 tenant must not be changed until the migration of the mailbox data of this environment is completed.

Next, you can transfer mailbox data from the on-premises Exchange server to the customer's Microsoft 365 tenant (see Migrating Mailboxes on page 72).

Resetting the Validation of an Environment

You have validated an environment (see Validating an Environment on page 65). Mailbox migration is currently not performed for the environment (see Migrating Mailboxes on page 72).

You can reset the validation of an environment for mailbox migration (see About Mailbox Migration on page 43). Resetting the validation is useful if the credentials of the on-premises Exchange server or the Microsoft 365 tenant have changed since the validation was performed, or if the validation failed. After you have fixed possible validation errors on the on-premises Exchange server, in the Microsoft 365 tenant, or in the Control Panel and have reset the environment validation, you can revalidate the environment later.

Notice:

Each administrator only views the validations in the **365 Total Protection** > **365 Total Protection** module that they have performed themselves. Therefore, an administrator can only reset their own validations.

Important:

As long as an environment is not validated for an administrator, the administrator cannot migrate data from mailboxes in that environment (see Migrating Mailboxes on page 72).

Important:

Validation can be reset only for environments for which mailbox migration is currently not performed.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you want to reset the validation of an environment.
3. Navigate to **365 Total Protection** > **365 Total Protection**.
4. In the **Validated environments** column, click on **Reset** in the row of the environment whose validation you want to reset.

Figure 67: Reset validation

A confirmation window is displayed.

5. Click on **OK**.

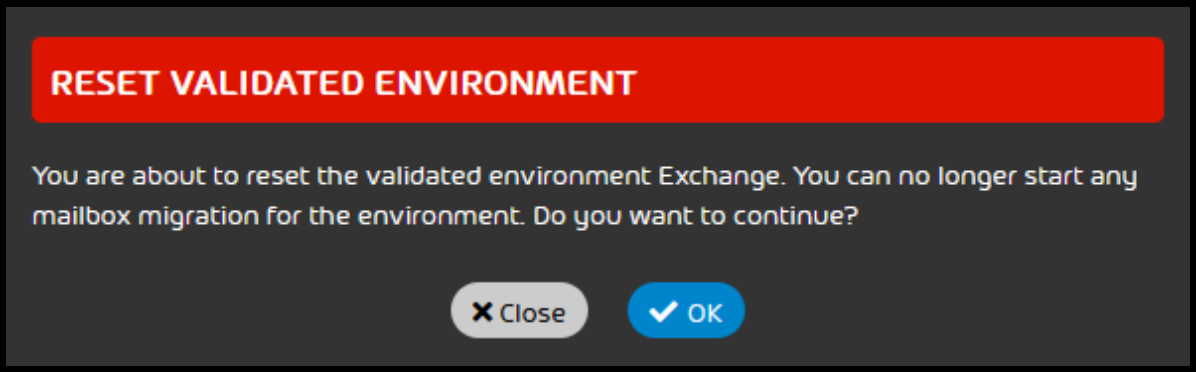

Figure 68: Confirm reset of validation

The validation of the environment is reset. The environment is removed from the list in the **Validated environments** column.

Next, you can validate the environment again (see Validating an Environment on page 65).

Migrating Mailboxes

You have prepared the on-premises Exchange server, the Microsoft 365 tenant and the Control Panel for mailbox migration (see Prerequisites for Mailbox Migration on page 46). You have validated the environment of the mailboxes whose data you would like to migrate (see Validating an Environment on page 65).

With mailbox migration (see About Mailbox Migration on page 43), you can migrate the data of mailboxes from validated environments (see Validating an Environment on page 65). In the **Customer Settings** > **Mailboxes** module, you can select one or multiple mailboxes for migration.

Notice:

Only the data of mailboxes of the types **LDAP mailbox** and **Mailbox** can be migrated (see Mailbox Types).

Notice:

We recommend to only select a few mailboxes the first time in order to get used to the process.

In general, we recommend you to migrate the data of mailboxes from one environment in batches of 50 to 100 mailboxes.

Notice:

A mailbox migration may take several hours or days. Exact times cannot be given because the duration depends on the following factors:

- Number and size of the mailboxes to be migrated
- Overall load due to other queued mailbox migrations

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain of the customer whose mailbox data you would like to migrate.
3. Navigate to **Customer Settings** > **Mailboxes**.

   Notice:

   Alternatively, administrators can navigate to the **Customer Settings** > **Mailboxes** module by clicking on the button **Select mailboxes to migrate** in the **365 Total Protection** > **365 Total Protection** module.

4. Filter the displayed mailboxes as desired (see Mailboxes).

   Notice:

   It is also possible to filter the mailboxes by their mailbox migration state.

5. If you would like to migrate the data of all displayed mailboxes, proceed as follows:

a) Click on **Migrate all mailboxes to Microsoft 365**.

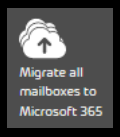

Figure 69: Migrate all displayed mailboxes

A confirmation window is displayed.

b) Click on **OK**.

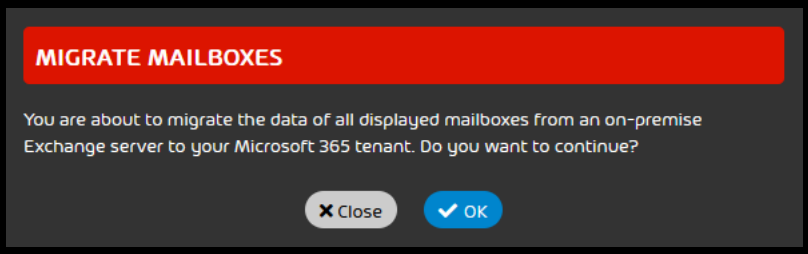

Figure 70: Confirm the migration of all displayed mailboxes

The window closes.

If the migration can be started for the mailboxes, a success message is displayed.

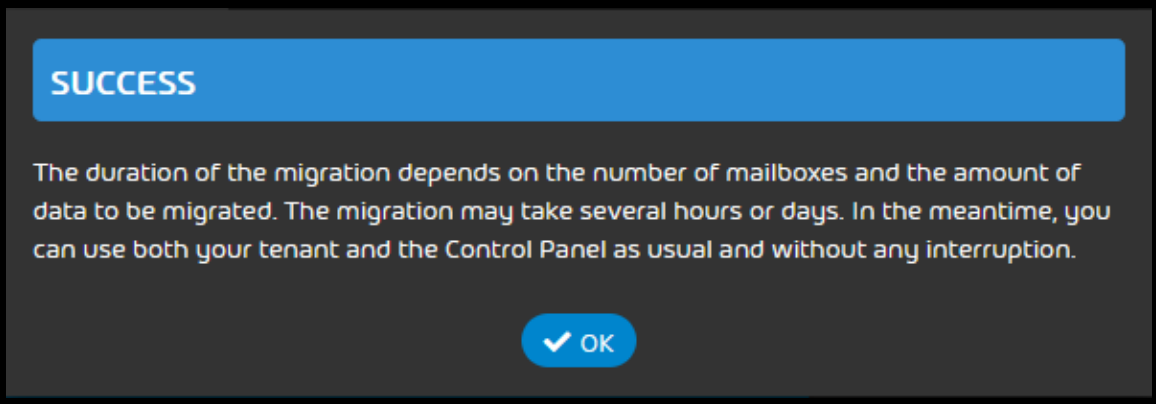

Figure 71: Success message

If the migration cannot be started for all selected mailboxes, an error message or a warning message is displayed. In this case, the migration is not started for the other mailboxes either.

Notice:

An error message is, for instance, displayed if a migration is already in progress for one of the selected mailboxes because only one migration can be performed for each mailbox.

A warning message is, for instance, displayed if the environment of a selected mailbox has not yet been validated by the logged-in administrator. In this case, the administrator must first validate the environment (see Validating an Environment on page 65).

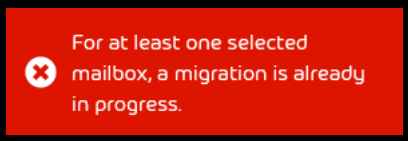

Figure 72: Error message

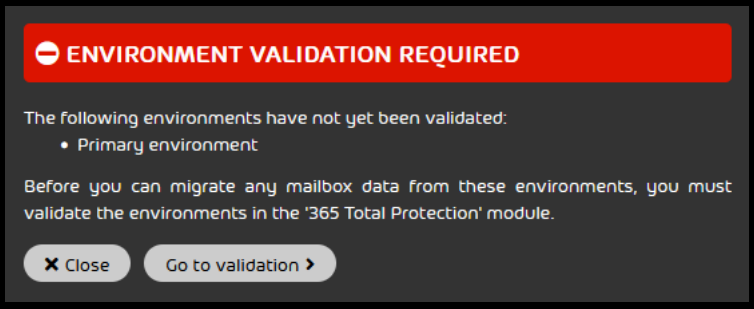

Figure 73: Warning message about non-validated environments

6. If you would only like to migrate the data of selected mailboxes, proceed as follows:

a) Click on .

A column with checkboxes is displayed in the list of mailboxes.

b) Tick the checkboxes of the mailboxes whose data you would like to migrate.

Figure 74: Select mailboxes

The **Migrate selected mailboxes to Microsoft 365** button is enabled.

c) Click on **Migrate selected mailboxes to Microsoft 365**.

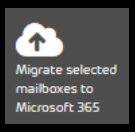

Figure 75: Migrate selected mailboxes

A confirmation window is displayed.

d) Click on **OK**.

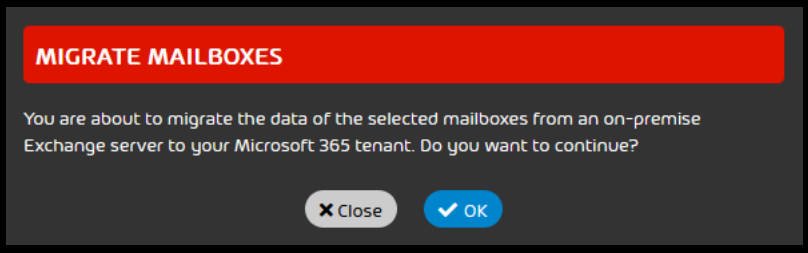

Figure 76: Confirm the migration of the selected mailboxes

The window closes.

If the migration can be started for the mailboxes, a success message is displayed.

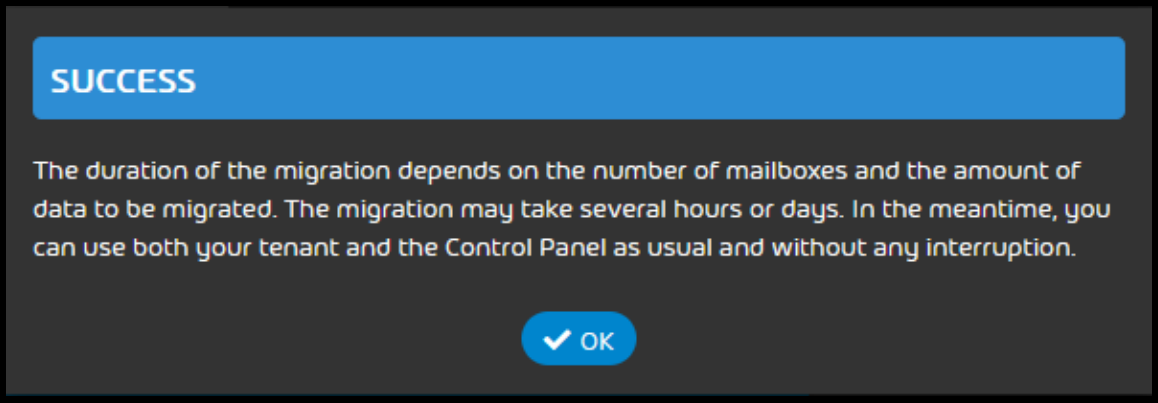

Figure 77: Success message

If the migration cannot be started for all selected mailboxes, an error message or a warning message is displayed. In this case, the migration is not started for the other mailboxes either.

Notice:

An error message is, for instance, displayed if a migration is already in progress for one of the selected mailboxes because only one migration can be performed for each mailbox.

A warning message is, for instance, displayed if the environment of a selected mailbox has not yet been validated by the logged-in administrator. In this case, the administrator must first validate the environment (see Validating an Environment on page 65).

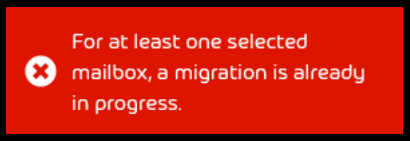

Figure 78: Error message

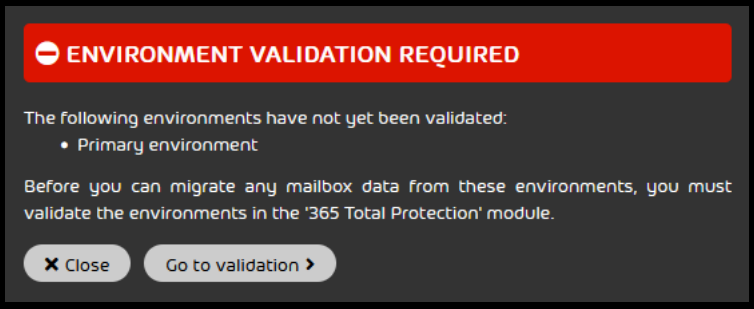

Figure 79: Warning message about non-validated environments

7. If a success message is displayed, click on **OK**.

8. Navigate to **365 Total Protection** > **365 Total Protection**.

The new migration job is displayed in the column **Migrations currently in progress**. If mailboxes from multiple environments have been selected for migration, separate jobs are displayed for each environment instead of a single job.

Notice:

The migration consists of the following stages:

- **queued**: The migration job is queued and has not started yet.
- **processing**: The migration job has started to be processed.
- **migrating**: The mailbox data of the mailboxes is migrated from the on-premises Exchange server to Microsoft 365 tenant.
- **ready for rerouting**: The migration of mailbox data has been completed. Once this state has been reached, the administrator has 14 days to reroute the migrated mailboxes in the Control Panel (see step 9 on page 79).
- **rerouting**: The administrator has rerouted the migrated mailboxes. The on-premises Exchange server is no longer used as the environment of the migrated mailboxes in the Control Panel, but the Microsoft 365 tenant is used instead. Hence, our servers now route the email traffic of the migrated mailboxes to the Microsoft 365 tenant.

If an error occurs during the migration, the migration is paused and is assigned the state **paused**. In this case, the administrator must take action during the migration.

Notice:

By clicking on the button next to the migration job, a log of the migration is downloaded. The log contains information about the migrated mailboxes and potential errors.

9. Once the migration job has reached the **ready for rerouting** state, click on the button next to the migration job.

A confirmation window is displayed.

10. Click on **Start rerouting**.

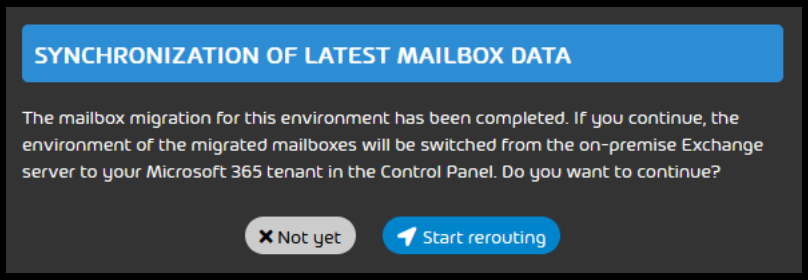

Figure 80: Confirm rerouting

The environment of the migrated mailboxes changes in the Control Panel from the on-premises Exchange server to the Microsoft 365 tenant. If the rerouting is performed within 14 days after the migration of the mailbox data, the data of the migrated mailboxes that has changed on the on-premises Exchange server in the meantime is synchronized in the Microsoft 365 tenant.

Important:

After 14 days, it is no longer possible to automatically synchronize the latest mailbox data from the on-premises Exchange server in the Microsoft 365 tenant.

The migration job is completed and marked by a green checkmark. Once all migration jobs have been completed, the button **Finalize mailbox migration** in the column **Migrations currently in progress** is enabled.

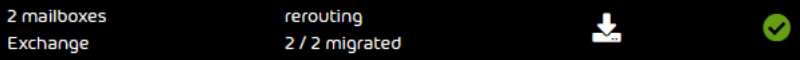

Figure 81: Completed migration job

The data of mailboxes has been migrated from an on-premises Exchange server to the customer's Microsoft 365 tenant.

Once all migration jobs have been completed, you can finalize mailbox migration (see Finalizing Mailbox Migration on page 81).

Finalizing Mailbox Migration

You have migrated the data of all desired mailboxes (see Migrating Mailboxes on page 72).

Once all migration jobs (see Migrating Mailboxes on page 72) have been completed, you can finalize mailbox migration (see About Mailbox Migration on page 43). After that, the customer's upgrade to 365 Total Protection is automatically resumed (see Upgrading to 365 Total Protection). Only after the upgrade to 365 Total Protection has been completed, the mailboxes, groups and domains from the customer's Microsoft 365 tenant can be synchronized in the Control Panel.

Important:

After finalizing mailbox migration, no more mailbox data can be migrated. Thus, make sure that the data of all desired mailboxes has been migrated.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to finalize mailbox migration.
3. Navigate to **365 Total Protection** > **365 Total Protection**.
4. Click on **Finalize mailbox migration** in the column **Migrations currently in progress**.

Notice:

The button is only enabled if all mailbox migrations in the column **Migrations currently in progress** have been completed.

Figure 82: Finalize mailbox migration

A confirmation window is displayed.

5. Click on **Finalize mailbox migration**.

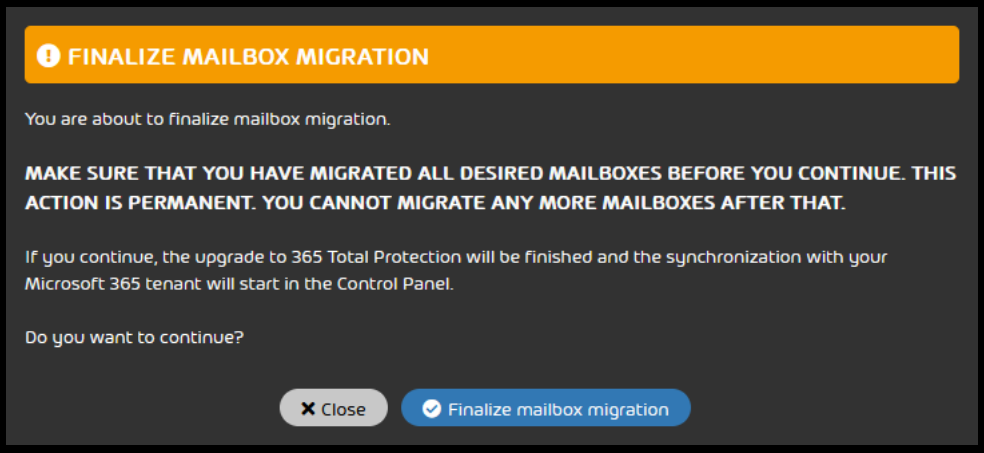

Figure 83: Confirm the finalization of mailbox migration

Mailbox migration is finalized. The customer's upgrade to 365 Total Protection is resumed (see Upgrading to 365 Total Protection).

Mailbox migration has been finalized.

Configuring 365 Total Backup

You have migrated to 365 Total Protection Enterprise Backup (see Upgrading to 365 Total Protection on page 25).

The 365 Total Protection Enterprise Backup service combines the 365 Total Protection Enterprise and 365 Total Backup services (see About 365 Total Protection on page 6). Once you have migrated to 365 Total Protection Enterprise Backup as a customer, you can configure 365 Total Backup. Using this procedure, you will configure 365 Total Backup according to the default settings. In that case, all Microsoft 365 mailboxes, files stored in OneDrive for Business accounts and SharePoint document libraries, as well as Teams chats for users and groups from your tenant are backed up.

Notice:

Customer-level or partner-level administrators can configure 365 Total Backup with other settings by opening 365 Total Backup via the **Backup** > **365 Total Backup** module (see Launching 365 Total Backup).

With 365 Total Backup, data from Windows-based endpoints can also be backed up. However, endpoints are not included in the default configuration. Only partner-level administrators can configure backups of endpoints. To do so, partner-level administrators can open 365 Total Backup via the **Backup** > **365 Total Backup** module.

Important:

Customer-level administrators can configure 365 Total Backup only if their partner has granted them access to 365 Total Backup (see Granting Access to 365 Total Backup). Otherwise, only partner-level administrators can configure 365 Total Backup for the customer.

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.

3. Navigate to **365 Total Protection** > **365 Total Protection**.

   The setup status of 365 Total Protection Enterprise Backup is displayed.

Figure 84: Setup status

4. Click on **Configure now** under **Configure 365 Total Backup**.

   A page for configuring 365 Total Backup opens in a new tab. The customer's data is predefined.

> **Notice:**
>
> The page uses the language that is set for the customer's parent partner in the Control Panel (see Setting Default Values for Timezone and Language).

5. Click on **Next**.

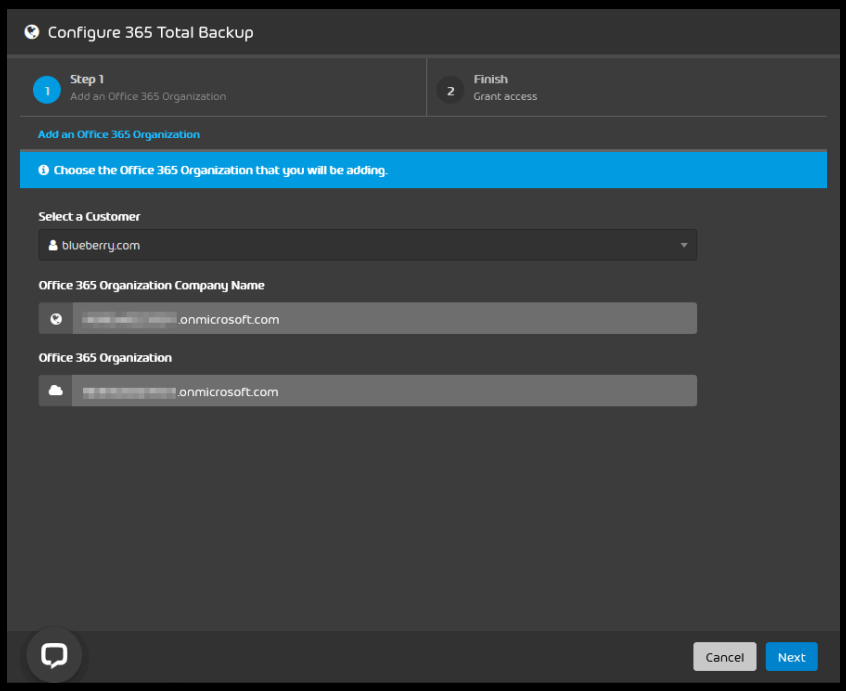

Figure 85: Check data

A window with an overview of the configuration steps opens.

6. Click on step 1.

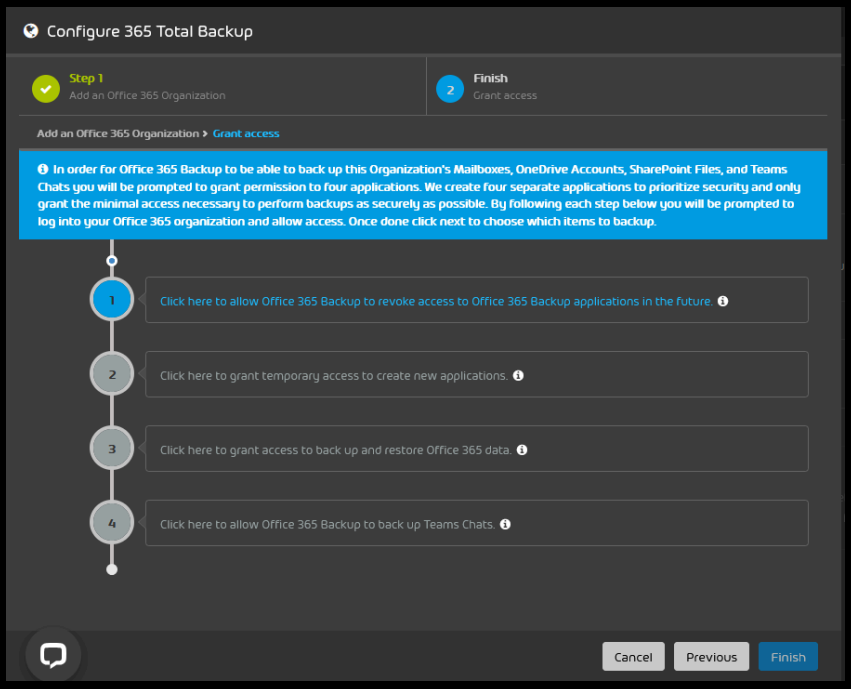

Figure 86: Perform step 1

The Microsoft 365 login page opens in a new tab.

7. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

8. Grant the requested permissions.

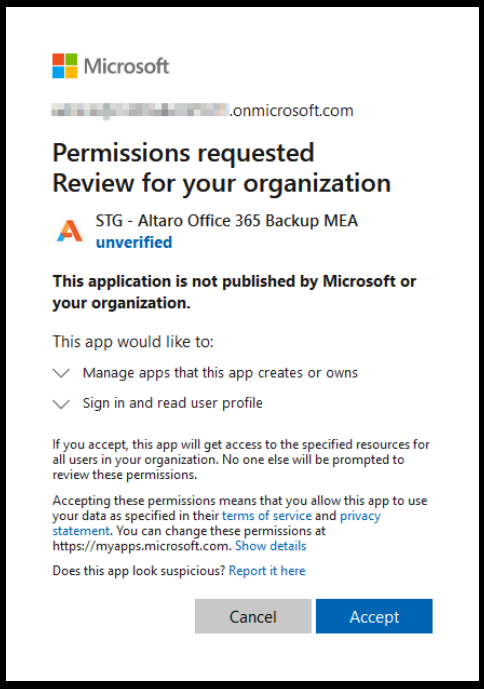

Figure 87: Grant permissions

The permissions are granted. A confirmation message is displayed.

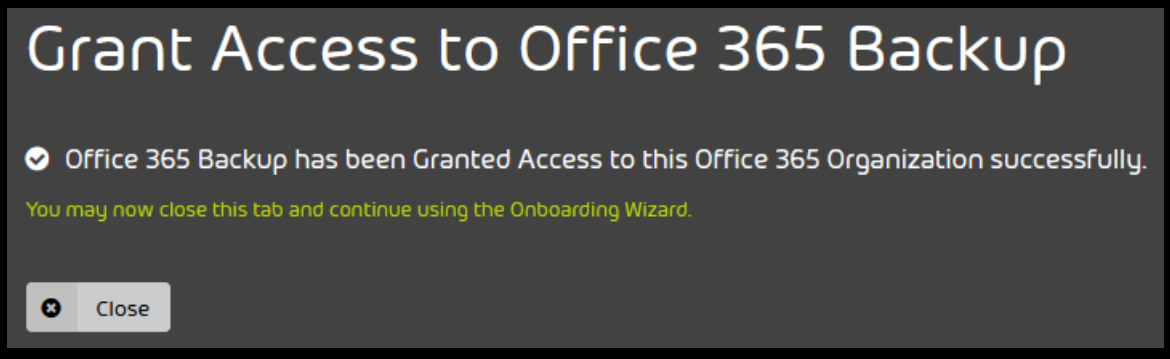

Figure 88: Confirmation window

9. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

10. Click on step 2.

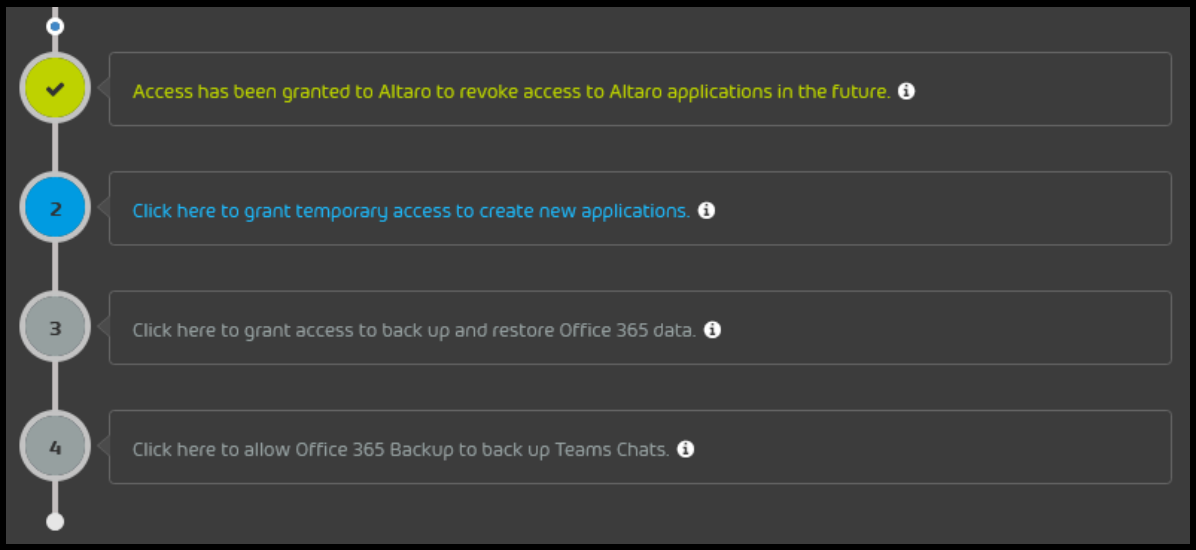

Figure 89: Perform step 2

The Microsoft 365 login page opens in a new tab.

11. Log in to Microsoft 365 with the customer's administrative credentials.

365 Total Backup is granted access to the customer's tenant. A confirmation message is displayed.

Figure 90: Confirmation window

12. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

13. Click on step 3.

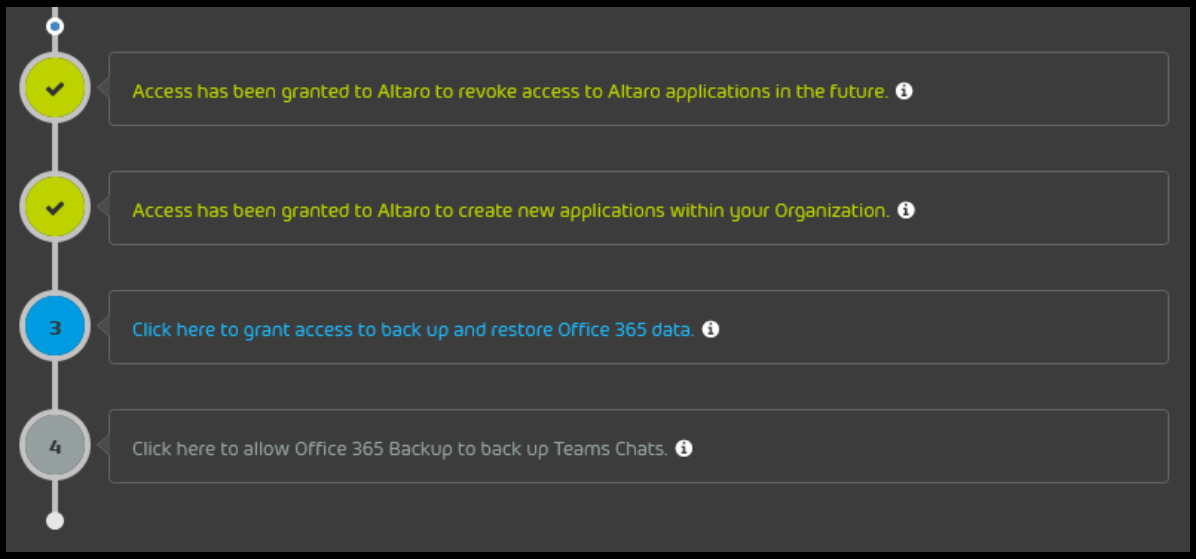

Figure 91: Perform step 3

The Microsoft 365 login page opens in a new tab.

14. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

15. Grant the requested permissions.

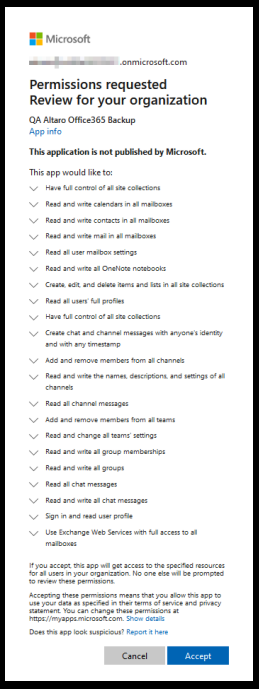

Figure 92: Grant permissions

The permissions are granted. A confirmation message is displayed.

Figure 93: Confirmation window

16. Click on step 4.

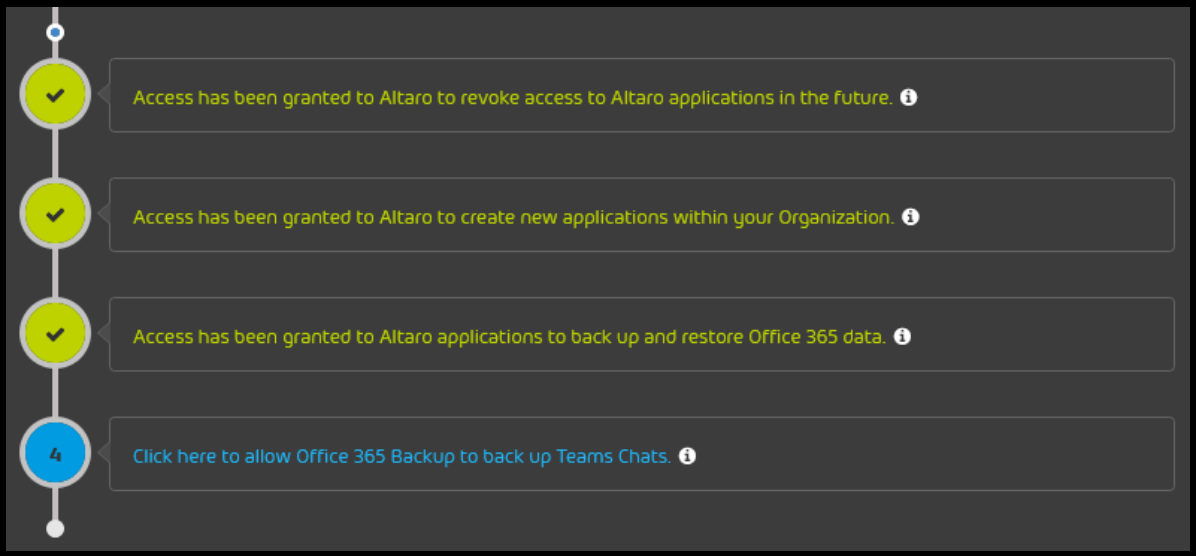

Figure 94: Perform step 4

The Microsoft 365 login page opens in a new tab.

17. Log in to Microsoft 365 with the customer's administrative credentials.

A page with requested permissions is displayed.

18. Grant the requested permissions.

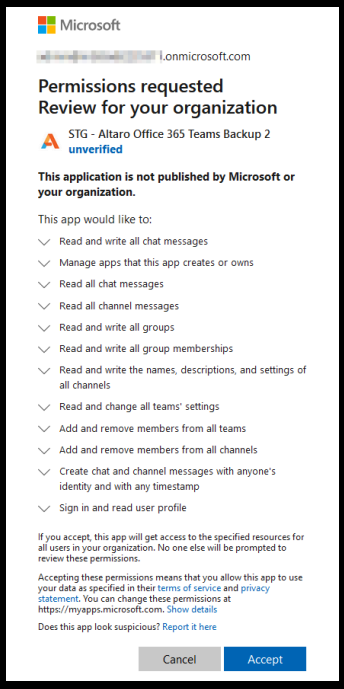

Figure 95: Grant permissions

The permissions are granted. A confirmation message is displayed.

Figure 96: Confirmation window

19. Click on **Close**.

The tab closes. The overview of the configuration steps is displayed again.

20. Click on **Finish**.

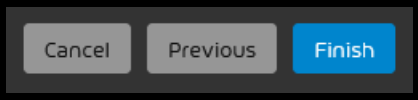

Figure 97: Finish configuration

The tab closes. In the Control Panel, the configuration of 365 Total Backup is displayed as completed in the **365 Total Protection** > **365 Total Protection** module.

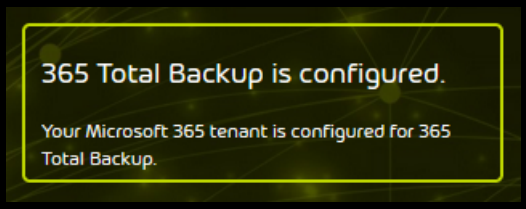

Figure 98: Configuration status of 365 Total Backup

365 Total Backup has been configured.

Configuration of Microsoft Services

To ensure the correct operation of 365 Total Protection (see About 365 Total Protection on page 6), after the synchronization of the mailboxes, Microsoft services must be configured for all created domains. You can adjust the following settings:

- Basic Settings on page 94: These settings are required for the correct operation of 365 Total Protection.
- Advanced Settings on page 107: These settings are only required for optional services of 365 Total Protection.

Basic Settings

Basic Settings

365 Total Protection (see About 365 Total Protection on page 6) can only protect your mailboxes if all incoming emails from senders outside your organization and all outgoing emails to recipients outside your organization are routed to our servers. The following requirements apply:

- The MX records of the DNS zones of your domains point to our servers (see Adjusting MX Records on page 95). As a result, incoming emails from the domains are first routed to our servers. Our servers then forward the incoming emails to Microsoft 365.

  Notice:

  Our servers forward incoming emails to the address of the Microsoft 365 destination server that was automatically determined during the initial synchronization (see Setting up 365 Total Protection on page 10). Thus, this address does not need to be communicated to us separately.

  As soon as mailboxes are assigned a primary or secondary environment, our servers will no longer forward those mailboxes' incoming emails to the automatically determined address, but to the addresses of the assigned environments (see Adjusting the Primary Environment Settings and Secondary Environments).

- Your mailboxes can only receive emails that have been processed by our services. This requires setting up a connector in Microsoft 365 for inbound email traffic that allows only emails from our IP address ranges. This connector can be created automatically (see Configuring Inbound and Outbound Email Traffic Automatically on page 98).

- The spam filter of Microsoft 365 is deactivated for the IP address ranges of our servers (see Deactivating the Microsoft 365 Spam Filter for the IP Address Range of Hornetsecurity on page 101). Otherwise, the Microsoft 365 spam filter would classify the emails we process as spam.

  Important:

  The Microsoft 365 spam filter can only be deactivated for our IP address range after the customization of the Microsoft 365 organization has been enabled in Exchange Online (see Enabling Organization Customization on page 100).

- For outbound email traffic, a connector has been set up to redirect the outgoing emails from your mailboxes to our smarthost. Only then can our services process all outgoing emails to mailboxes outside your organization. After the processing, our smarthost sends the outgoing emails to their recipients. This connector can be created automatically (see Configuring Inbound and Outbound Email Traffic Automatically on page 98).
- The SPF records of your domains point to our SPF records (see Adjusting SPF Records on page 106). This is the only way that the emails sent via our smarthost can be recognized as legitimate and accepted by the recipients' incoming email servers during an SPF check (see SPF check)

Adjusting MX Records

You have configured your domains.

Notice:

If you are not sure if the configuration of your domains is complete, contact support.

MX records point to the servers that receive incoming emails for the mailboxes of a domain. You can add our servers to the MX records of your domain so that the incoming emails of your domain are routed to our servers first. This allows the emails to be filtered before being forwarded to Microsoft 365.

1. Set the MX records depending on your region. You can select one of the following regions:
   - Europe (see MX Records for Customers in Europe on page 97)
   - USA (see MX Records for Customers in the USA on page 97)
   - Canada (see MX Records for Customers in Canada on page 98)

   Notice:

   Customers whose organization is located outside of the aforementioned regions can select a region based on data protection criteria.

2. To check if the MX records are set correctly, click on **Show configuration**.

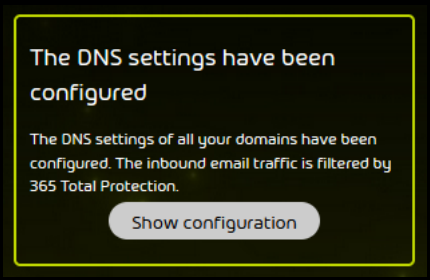

Figure 99: Show configuration

The status report shows the successful update of the MX records.

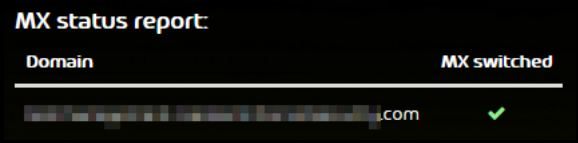

Figure 100: Status report

The MX records have been adjusted.

Next, you can configure the incoming and outgoing email traffic automatically (see Configuring Inbound and Outbound Email Traffic Automatically on page 98).

MX Records for Customers in Europe

Customers from Europe must set certain MX records in the DNS zones of their domains in order for our services to be able to filter and process their incoming emails (see #unique_40). The placeholder **<domain.tld>** stands for the customer's domain.

Table 1: MX records for customers in Europe

Domain	Class	Type	Priority	Email server
<domain.tld>	IN	MX	10	mx01.hornetsecurit
<domain.tld>	IN	MX	20	mx02.hornetsecuril
<domain.tld>	IN	MX	30	mx03.hornetsecuril
<domain.tld>	IN	MX	40	mx04.hornetsecuril

For customers of the DNS provider 1&1, the following MX records apply instead:

Table 2: For customers of the DNS provider 1&1, the following MX records apply instead:

Domain	Class	Type	Priority	Email server
<domain.tld>	IN	MX	10	mx23a.antispameu
<domain.tld>	IN	MX	20	mx23b.antispameu
<domain.tld>	IN	MX	30	mx23c.antispameu
<domain.tld>	IN	MX	40	mx23d.antispameu

MX Records for Customers in the USA

Customers from the USA must set certain MX records in the DNS zones of their domains in order for our services to be able to filter and process their incoming emails (see #unique_40). The placeholder **<domain.tld>** stands for the customer's domain.

Table 3: MX records

Domain	Class	Type	Priority	Email server
<domain.tld>	IN	MX	10	mx-cluster-usa01.hornetsecuri

Domain	Class	Type	Priority	Email server
<domain.tld>	IN	MX	20	mx-cluster-usa02.hornetsecuri
<domain.tld>	IN	MX	30	mx-cluster-usa03.hornetsecuri
<domain.tld>	IN	MX	40	mx-cluster-usa04.hornetsecuri

MX Records for Customers in Canada

Customers from Canada must set certain MX records in the DNS zones of their domains in order for our services to be able to filter and process their incoming emails (see #unique_40). The placeholder **<domain.tld>** stands for the customer's domain.

Table 4: MX records for customers in Canada

Domain	Class	Type	Priority	Email server
<domain.tld>	IN	MX	10	mx-cluster-ca01.hornetsecurity
<domain.tld>	IN	MX	20	mx-cluster-ca02.hornetsecurit
<domain.tld>	IN	MX	30	mx-cluster-ca03.hornetsecurit
<domain.tld>	IN	MX	40	mx-cluster-ca-fallback.hornetsecu

Configuring Inbound and Outbound Email Traffic Automatically

Inbound and outbound email traffic connectors ensure that all emails from senders and to recipients outside your organization are routed to our servers. You can automatically configure these connectors on the status page of **365 Total Protection** (see About 365 Total Protection on page 6).

1. Log in to the Control Panel with your administrative credentials.
2. Select your domain from the scope selection.
3. Navigate to **365 Total Protection** > **365 Total Protection**.

4. Click on **Configure automatically**.

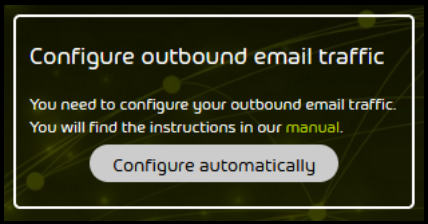

Figure 101: Configure automatically

Notice:

The automatic configuration of the outbound email traffic also configures the inbound email traffic automatically.

The inbound and outbound email traffic are configured.

Connectors for the inbound and outbound email traffic have been configured.

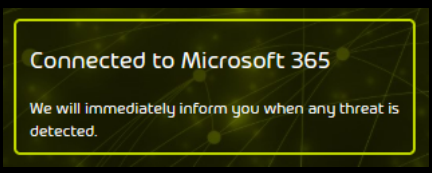

Figure 102: Successful configuration

Important:

Already installed connectors can cause errors in the automatic configuration of the outbound email traffic.

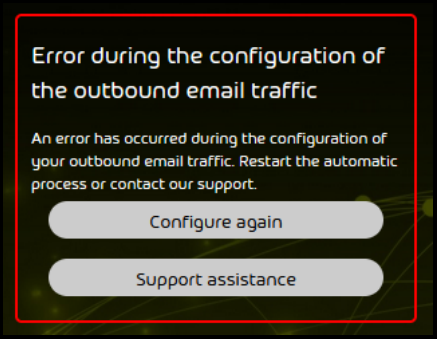

Figure 103: Configuration errors

Troubleshooting

- Delete already configured connectors and click on **Configure again** to start the configuration OR
- click on **Support assistance** to contact support.

Next, you can disable the Microsoft 365 spam filter for our IP address range (see Deactivating the Microsoft 365 Spam Filter for the IP Address Range of Hornetsecurity on page 101).

Enabling Organization Customization

By default, Microsoft 365 organizations are dehydrated in Exchange Online. This means that some objects are consolidated in the Microsoft data centers to save storage space. Therefore, some objects cannot be edited for dehydrated Microsoft 365 organizations in Exchange Online. Before you can edit these objects, you must enable the customization of your Microsoft 365 organization in Exchange Online by running a command once. You can also deactivate the Microsoft 365 spam filter for our IP address range (see Deactivating the Microsoft 365 Spam Filter for the IP Address Range of Hornetsecurity on page 101) only after running the command. The command will hydrate the organization.

Important:

The command can only be run once and cannot be undone.

1. Open the Exchange Online PowerShell.

2. Optional: In order to check whether the customization of your Microsoft 365 organization has already been enabled in Exchange Online, run the following command: **Get-OrganizationConfig | fl IsDehydrated**.

   If the customization has already been enabled, the value **False** is returned. If the customization has not yet been enabled, the value **True** is returned.

3. Run the following command: **Enable-OrganizationCustomization**.

   The Microsoft 365 organization is hydrated in Exchange Online. The customization of the Microsoft 365 organization is enabled in Exchange Online. It may take some time for the changes to take effect.

The customization of a Microsoft 365 organization has been enabled in Exchange Online.

Next, you can disable the Microsoft 365 spam filter for our IP address range (see Deactivating the Microsoft 365 Spam Filter for the IP Address Range of Hornetsecurity on page 101).

Deactivating the Microsoft 365 Spam Filter for the IP Address Range of Hornetsecurity

You have enabled the customization of your Microsoft 365 organization in Exchange Online (see Enabling Organization Customization on page 100).

If you want your incoming emails to be filtered by our services, you need to disable the Microsoft 365 spam filter. Otherwise, the Microsoft 365 spam filter would classify incoming emails to your domains as spam. Our services filter your incoming emails for spam.

Notice:

Email authentication via SPF is not automatically enabled. Setting up SPF checks is not mandatory, but recommended. For setup information, see About Email Authentication.

1. Log in to admin.microsoft.com with your administrative credentials.

2. Under **Admin Centers**, select the item **Security**.

> **Notice:**
>
> If the Admin Center is not displayed in your default view, extend the menu with **Show all**.

The home page of **Microsoft 365 Defender** opens.

3. Click on the menu item **Policies & rules** on the left side.

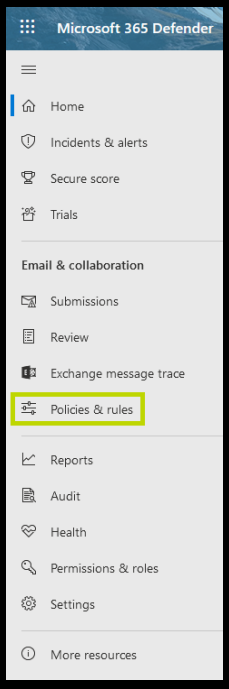

Figure 104: Select menu item

4. Click on **Threat policies**.

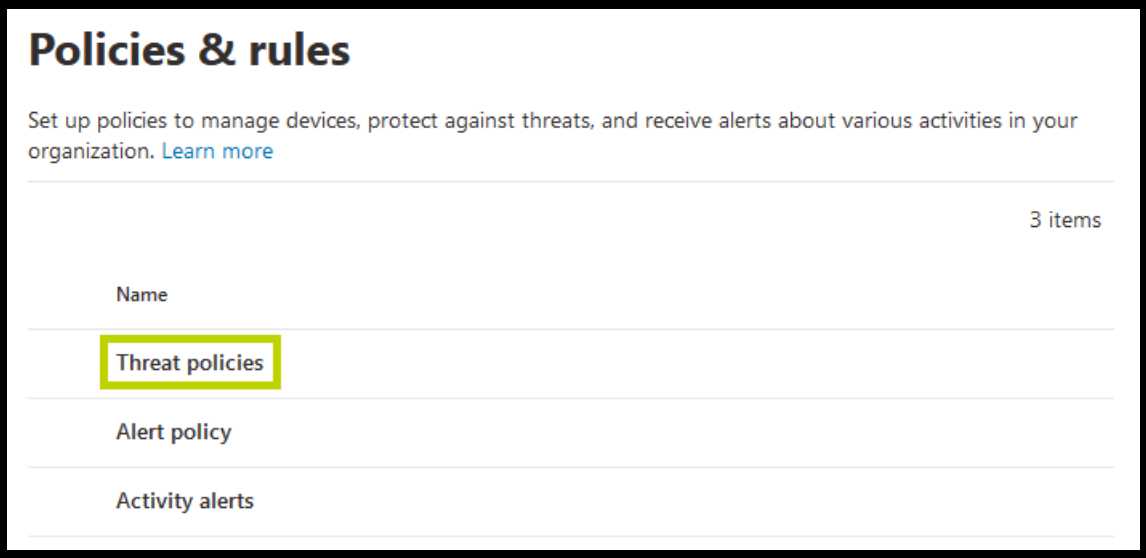

Figure 105: Threat policies select

5. Click on **Anti-spam** under **Policies**.

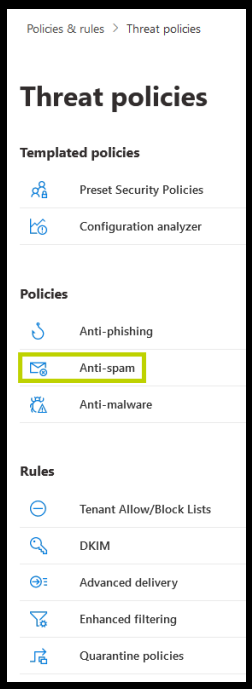

Figure 106: Anti-spam select

The page **Anti-spam policies** opens.

6. Click on **Connection filter policy (Default)**.

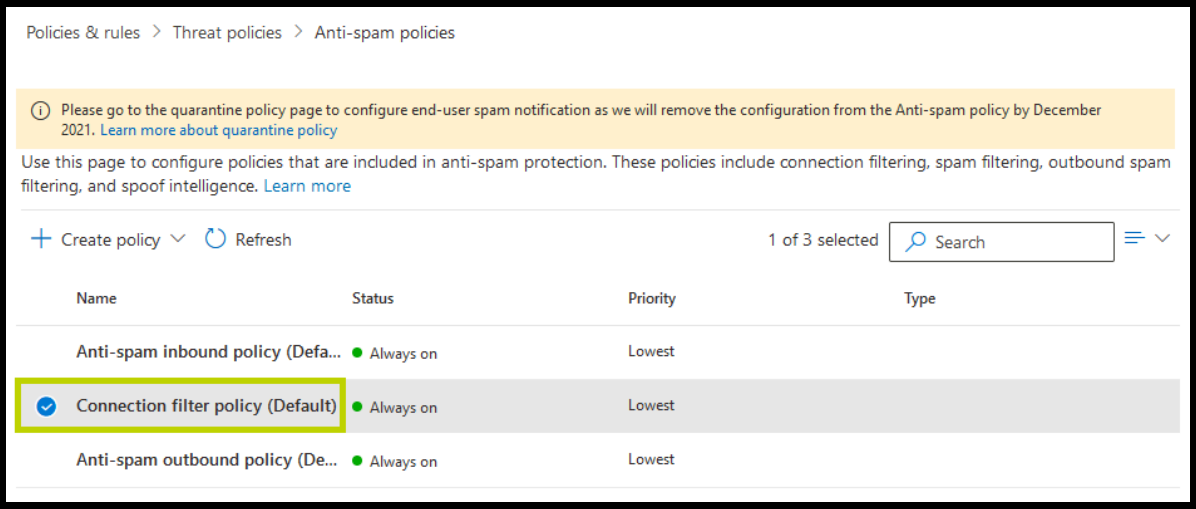

Figure 107: Connection filter policy (Default) select

The policy settings open.

7. Click on **Edit connection filter policy**.

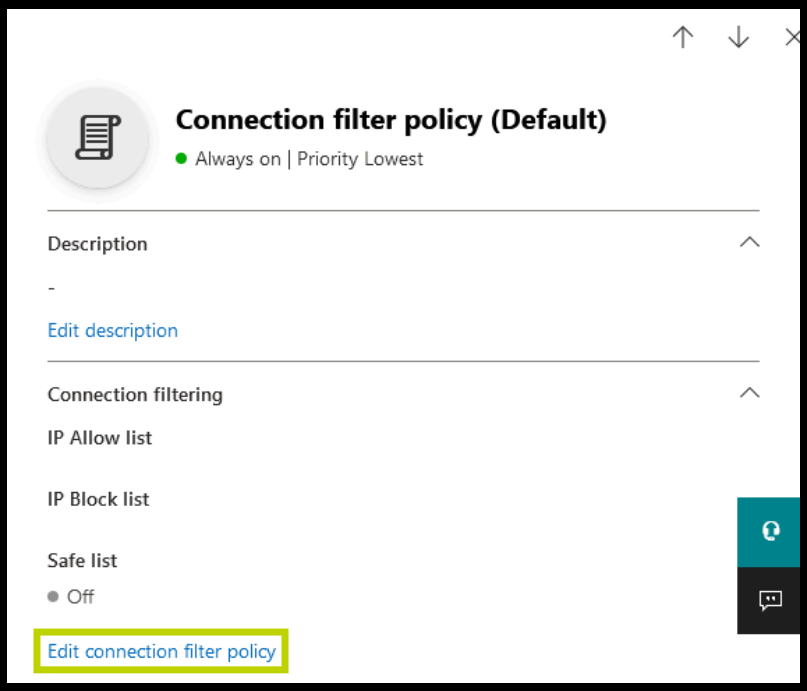

Figure 108: Edit policy

Additional settings are displayed.

8. Enter the following IP addresses in the input field under **Always allow messages from the following IP addresses or address range:**.

83.246.65.0/24 94.100.128.0/24 94.100.129.0/24
94.100.130.0/24 94.100.131.0/24 94.100.132.0/24
94.100.133.0/24 94.100.134.0/24 94.100.135.0/24
94.100.136.0/24 94.100.137.0/24 94.100.138.0/24
94.100.139.0/24 94.100.140.0/24 94.100.141.0/24
94.100.142.0/24 94.100.143.0/24 173.45.18.0/24
185.140.204.0/24 185.140.205.0/24 185.140.206.0/24

185.140.207.0/24

Notice:

Customers in Canada must additionally enter the following IP addresses:

108.163.133.224/27 199.27.221.64/27 209.172.38.64/27
216.46.2.48/29 216.46.11.224/27

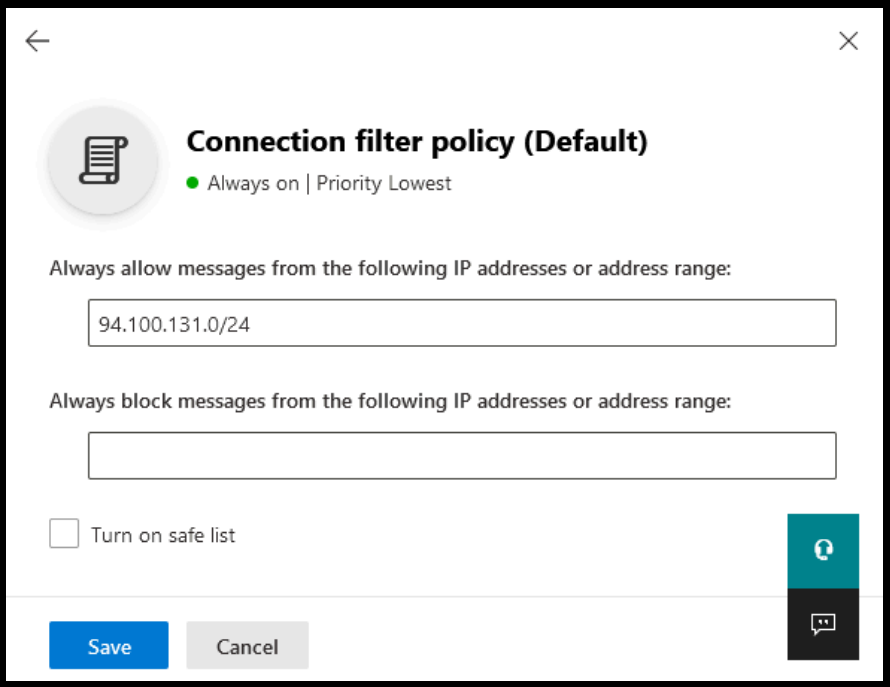

Figure 109: Add IP addresses to the list of allowed IP addresses

9. Click on **Save**.

The settings are saved.

The spam filter of Microsoft 365 has been deactivated for emails from our IP address range.

Adjusting SPF Records

The SPF records of your domains must point to our own SPF records. Thus, Hornetsecurity is recognized as a valid sender by the incoming email servers, and the emails sent via our smarthost are not classified as spam during the SPF check (see SPF check).

Notice:

Our SPF record is not required for customers who have configured their primary environment with the **IP/Hostname** option but have not specified any relay server addresses for outgoing emails. For more information on how to set the primary environment, see Primary Environment Settings.

1. Log in to the administration environment of Microsoft 365.
2. Navigate to **Setup** > **Domains**.
3. Select the domain you have registered with Hornetsecurity.
4. Add the following SPF record: **TXT "v=spf1 include:spf.protection.outlook.com include:spf.hornetsecurity.com ~all"**

Important:

If you have additional systems sending outgoing emails for the affected domain, add those to the SPF record as well.

Your SPF records have been adjusted.

Advanced Settings

Advanced Settings

In addition to the basic settings (see Basic Settings on page 94), advanced settings can be configured for 365 Total Protection (see About 365 Total Protection on page 6) in order to be able to use additional options or to avoid problems related to automatic settings.

- To make the process of setting up user accounts in email programs easier, the Autodiscover service can be set up (see Setting up Autodiscover on page 108).
- If the automatic setup of connectors for inbound and outbound email traffic (see Configuring Inbound and Outbound Email Traffic Automatically on page 98) fails, it is possible to create the connectors manually. In this case, it is necessary to enable archiving of email traffic within your organization by creating a journal rule. For more information, see the manual Manual Initial Service Setup with Microsoft 365

- If you manage some mailboxes of a domain using a primary environment in Microsoft 365 and some using other secondary environments (see Secondary Environments), you need to set up a forward to the secondary environments. Otherwise, emails to mailboxes in the secondary environments will be rejected. For more information on how to set up the forward, see the manual Email Routing from Microsoft 365.
- Multi-factor authentication for Microsoft 365 accounts is also used for the Control Panel login (see Multi-Factor Authentication on page 108).

Setting up Autodiscover

Configuring the Autodiscover service makes the process of setting up user accounts in email programs easier. Users do not need to enter a server name or port number: this information is automatically passed on by the Autodiscover service.

Set a CNAME record for the Autodiscover service:

Table 5: Setting MX Records

TYPE	PRIORITY	HOSTNAME	POINTS TO	TTL
CNAME		autodiscover	autodiscover.hornetsecurity.com	1 hour

The Autodiscover service has been set up successfully.

Multi-Factor Authentication

All users of a domain protected by 365 Total Protection log in to the Control Panel with their credentials from Microsoft 365. If multi-factor authentication is activated in Microsoft 365, it is also used in the Control Panel.

Ordering 365 Total Protection

You can order 365 Total Protection (see About 365 Total Protection on page 6) in the Control Panel directly if you would like to use the product after the 14-day trial period.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the domain for which you would like to order 365 Total Protection.
3. Select **365 Total Protection**.
4. Click on **Purchase now**.

   An overview showing the number of mailboxes and the price appears.

5. Click on **Purchase** to buy 365 Total Protection.

   You receive a confirmation email with an overview of your product.

365 Total Protection has been ordered.

Display of the Number of Mailboxes, Licenses and Domains

After the onboarding, the number of mailboxes, licenses and domains is displayed under **365 Total Protection** > **365 Total Protection** for 365 Total Protection customers (see About 365 Total Protection on page 6).

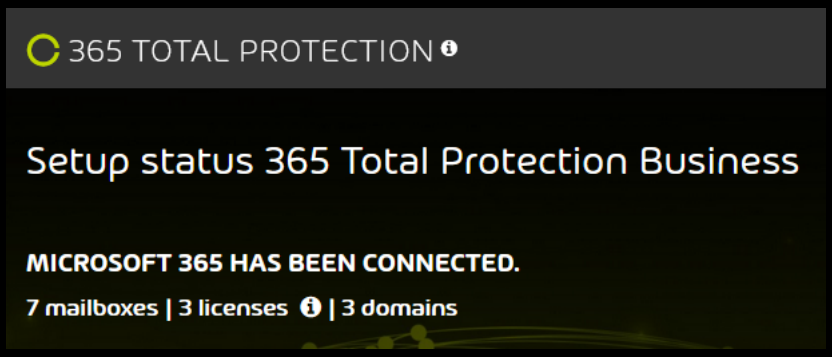

Figure 110: Number of mailboxes, licenses and domains.

Under **Mailboxes**, the number of mailboxes that are synchronized with Microsoft 365 is displayed. This number includes mailboxes of both regular users and administrators.

Under **licenses**, the number of billed licenses is displayed. The license count is based on the number of primary mailboxes of 365 Total Protection users, not counting those of administrators. The displayed number has different meanings depending on the license status:

- During the trial period of 365 Total Protection, the number of primary mailboxes reported during the last synchronization with Microsoft 365 is displayed.
- In the first month after the end of the trial period or the purchase of the paid version of 365 Total Protection, the number of primary mailboxes that were protected by 365 Total Protection when the trial period expired or the paid version was purchased is displayed. This number determines the billing for the first month.
- From the second month after the end of the trial period or the purchase of the paid version of 365 Total Protection, the maximum number of primary mailboxes that were simultaneously protected by 365 Total Protection in the current month is displayed. This number determines the billing for the current month.

Under **Domains**, the number of domains for which 365 Total Protection is activated is displayed. This number includes both the primary domain and alias domains of the customer.

Management of Mailboxes

In the **Customer Settings** > **Mailboxes** module, mailboxes can be managed (see "Customer Settings" in the Control Panel manual). 365 Total Protection customers (see About 365 Total Protection on page 6) can manage both Microsoft 365 mailboxes and manually created mailboxes from other email providers (see Mailbox Types). Different functions are available in the Control Panel for Microsoft 365 mailboxes and for manually created mailboxes.

Unlike Microsoft 365 mailboxes, manually created mailboxes (see "Adding a Mailbox" in the Control Panel manual) are not synchronized with Microsoft 365. All functions of the **Mailboxes** module can be applied to manually created mailboxes. Secondary environments must be assigned to these mailboxes (see "Secondary Environments" in the Control Panel manual).

For Microsoft 365 mailboxes, the functions of the **Mailboxes** module are limited:

- Microsoft 365 mailboxes cannot be manually added.
- Microsoft 365 mailboxes cannot be manually removed.
- The basic data of Microsoft 365 mailboxes cannot be edited.
- The passwords of Microsoft 365 mailboxes cannot be changed.
- No alias addresses can be assigned to Microsoft 365 mailboxes.

To distinguish between Microsoft 365 mailboxes and manually created mailboxes, the **Mailboxes** module offers 365 Total Protection customers the following additional mailbox types for Microsoft 365 mailboxes:

- **Microsoft 365 mailbox**
- **Microsoft 365 functional mailbox**
- **Microsoft 365 administration mailbox**

Group Management in the Control Panel

In the Control Panel, mailboxes can be combined into groups (see "Groups"). If groups are available, settings can be made for groups instead of single mailboxes. The group membership of Microsoft 365 mailboxes (see Mailbox Types) is managed exclusively in Microsoft 365. Thus, Microsoft 365 mailboxes cannot be added to groups from the Control Panel. However, groups from Microsoft 365 can be copied to the Control Panel by creating groups with the same names there (see Synchronizing Groups from Microsoft 365 in the Control Panel on page 112). Synchronization is possible for Microsoft 365 groups, distribution lists, security groups and mail-enabled security groups.

Except for some restrictions described in the Control Panel manual, the same options are available for synchronized groups as for non-synchronized groups in the Control Panel (see "Groups"). In addition to Microsoft 365 mailboxes, mailboxes from secondary environments (see "Secondary Environments") can be added to synchronized groups in the Control Panel. These mailboxes are not affected by synchronizations from Microsoft 365 but preserved after each synchronization.

Synchronizing Groups from Microsoft 365 in the Control Panel

You can synchronize groups from Microsoft 365 with the Control Panel (see Group Management in the Control Panel on page 112). This way, the Control Panel receives information about the composition of your Microsoft 365 groups so group-specific settings can be made.

Notice:

Synchronization is possible for Microsoft 365 groups, distribution lists, security groups and mail-enabled security groups.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the customer for whom you would like to synchronize a group with Microsoft 365.
3. Navigate to **Customer Settings** > **Groups**.

4. Click on **Add**.

   A drop-down menu opens.

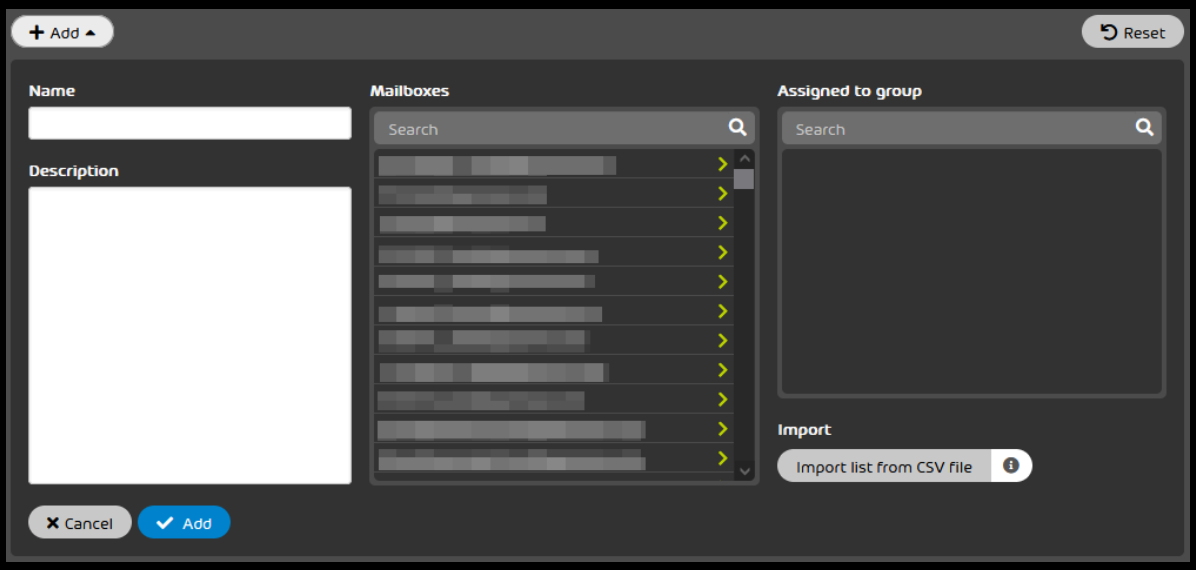

Figure 111: Add a new group

5. **Important:**

   The name of the group in the Control Panel must match the name of the group in Microsoft 365 exactly in order for the Control Panel to connect both groups. Otherwise, the group cannot be synchronized.

   Under **Name**, enter the name of the group from Microsoft 365 that you would like to synchronize in the Control Panel.

6. Click on **Add**.

   The group is added to the Control Panel. During the next synchronization, the group members from Microsoft 365 will be added to the group.

   Notice:

   The data in the Control Panel is synchronized with Microsoft 365 several times per hour. It can thus take several minutes until the group data is available in the Control Panel.

A group from Microsoft 365 has been copied to the Control Panel and synchronized with Microsoft 365.

Combination of 365 Total Protection and Other Services

365 Total protection includes several services (see About 365 Total Protection on page 6) that depend on its settings. In the following, some dependencies are described.

Notice:

For a complete and up-to-date list of 365 Total Protection features, see 365 Total Protection on the Hornetsecurity website.

- Administrators must activate the Email Encryption service separately (see Email Encryption on page 115).
- Administrators must activate the Continuity Service, which is only part of 365 Total Protection Enterprise, separately (see Activating the Continuity Service (Only 365 Total Protection Enterprise) on page 116).
- For the Signature and Disclaimer service, most attributes from the Azure Active Directory, the directory service of Microsoft 365, are synchronized (see Synchronized Attributes from the Azure Active Directory on page 118).

Email Encryption

Email Encryption is part of the products 365 Total Protection Business and Enterprise (see About 365 Total Protection on page 6). Email Encryption must be activated manually because some settings must be configured. Follow the instructions in the chapter "Email Encryption".

Important:

In the **Email Encryption** module, customer-level administrators can order S/MIME certificates for users. An S/MIME certificate is bound to a user's primary address. If the user's email address changes, the S/MIME certificate is no longer valid for the user.

If a user's email address is renamed in Microsoft 365, the user's email address will be renamed also in the Control Panel during the next synchronization. The customer's administrators will be notified by email about the renaming of synchronized users who used to have a valid S/MIME certificate. For more information, see Adding S/MIME Users.

Activating the Continuity Service (Only 365 Total Protection Enterprise)

If the Microsoft services fail or the services are temporarily unavailable, this also affects your access to your mailbox. Emails can then be neither sent nor received that can harm your entire business processes. In such an event, Continuity Service is your stand-by system that – activated in mere seconds – keeps your email correspondence up and running. For more information, see About the Continuity Service.

Notice:

Continuity Service is only included in 365 Total Protection Enterprise, and you must activate it manually and configure the settings.

1. Log in to the Control Panel with your administrative credentials.
2. Select the domain from the scope selection.
3. Navigate to > .
4. Toggle the switch .

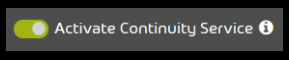

Figure 112: Activate the Continuity Service

A confirmation window is displayed.

5. **Attention:**

   Once the Continuity Service is activated, a 30-day free trial period starts. Once the trial period has expired, the service becomes chargeable and your account is billed.

   The Continuity Service is priced per customer, not per user.

   Important:

   Administrators cannot deactivate the Continuity Service by themselves. Only Support can deactivate the Continuity Service for a domain.

   Click on .

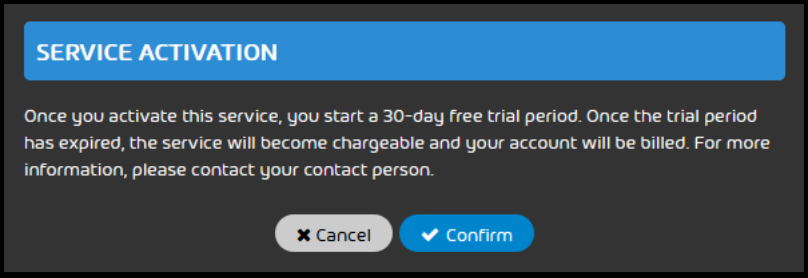

Figure 113: Confirm

The Continuity Service is activated.

6. Select the users for which you would like to activate the Continuity Service. You have two options:

   - : All users of the domain are added to the Continuity Service. For more steps, see #unique_49.
   - : Only selected users of the domain are added to the Continuity Service. For more steps, see #unique_50.

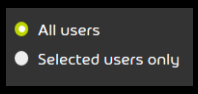

Figure 114: Select option

The Continuity Service has been activated.

Synchronized Attributes from the Azure Active Directory

With the Azure Active Directory of Microsoft, certain attributes are synchronized for Signature and Disclaimer (see #unique_51).

Important:

It is not possible to synchronize the attributes with Microsoft 365 and LDAP (see "LDAP Connection") at the same time. For Microsoft 365 mailboxes (see Mailbox Types), only the attributes from the table below are synchronized. For manually created mailboxes, basic data (see #unique_52) is used. LDAP attributes are not synchronized and cannot be used.

The following attributes are synchronized for Microsoft 365 mailboxes and can be used to create signatures and disclaimers:

AD variable	Description
countryCode	Country/Region
department	Department
displayName	Complete name
givenName	First name
info	Job title/Position **Notice:** The field Title is often used for other purposes. Therefore, the term Info is used here for the LDAP attribute Title (Job title/Position).
l (lower case L)	City
mail	Email address

AD variable	Description
mobile	Mobile phone number
postalCode	Postal code
sn	Last name
st	State
streetAddress	Street
telephoneNumber	Phone number

Offboarding after Termination of the Trial Period or Cancellation

If a customer has completed the 365 Total Protection (see About 365 Total Protection on page 6) trial period and no longer wishes to use the product, or if they canceled 365 Total Protection at any time, they need to undo some settings in their Microsoft 365 configuration to ensure their emails will still be delivered.

1. The customer must delete or deactivate their connector for inbound email traffic. (firewall setting)
2. If the customer has configured their outbound email traffic, they must also delete or deactivate the corresponding connector. (Relaying)

   Notice:

   For information on how to delete or deactivate connectors in the Microsoft 365 environment, see Deleting or Deactivating the Connector on page 120.
3. The customer must delete the MX records in the DNS zone of their domains.

The customer's emails will then no longer be routed through our services.

Partner-level administrators can delete the customer from the Control Panel (see Deleting a Customer on page 121).

Deleting or Deactivating the Connector

If you no longer want to use 365 Total Protection (see About 365 Total Protection on page 6) (see Offboarding after Termination of the Trial Period or Cancellation on page 120), you must delete or deactivate the connectors for inbound and outbound email traffic in Microsoft 365.

1. Open Office.com and log in with your administrative credentials.
2. Navigate to **Administrator** > **Admin Centers** > **Exchange**.
3. Select **Mail flow** and click on the tab **Connectors**.
4. Select the desired connector.

5. You can delete or deactivate the connector:
   - To delete the connector, click on **Delete**.
   - To deactivate the connector, click on **Deactivate** in the connector overview.

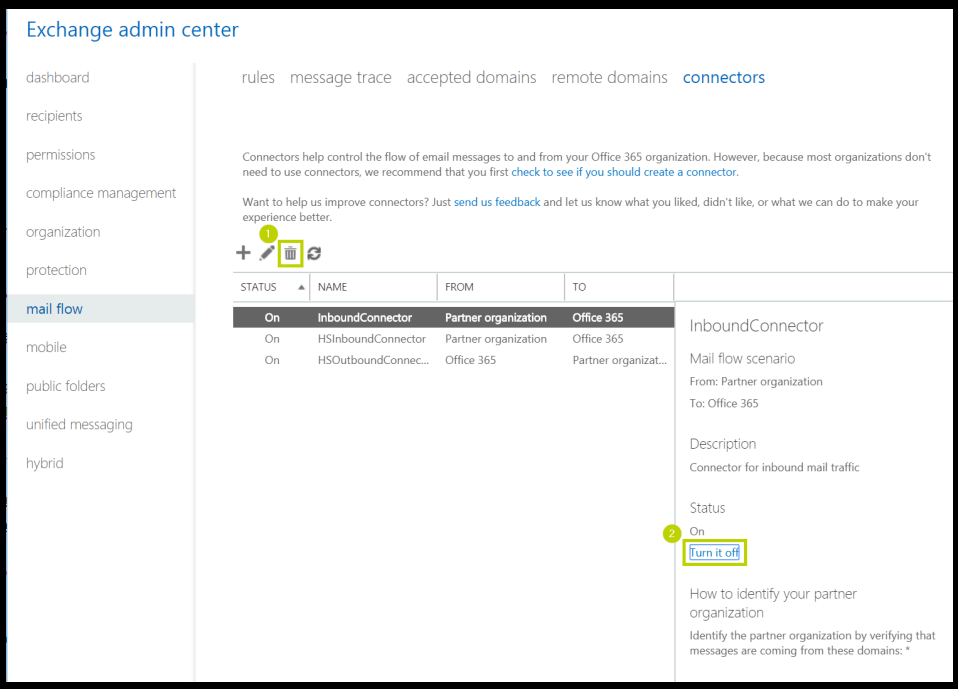

Figure 115: Deleting or Deactivating the Connector

6. Confirm the notification with **Yes**.

A connector has been deleted or deactivated.

Deleting a Customer

As a partner-level administrator, you can delete an existing 365 Total Protection customer (see About 365 Total Protection on page 6) during or after the trial period.

CAUTION:

Once you delete a customer, all data from that customer will be deleted from the Control Panel. The customer data cannot be restored. Be sure that you want to delete the customer.

1. Log in to the Control Panel with your administrative credentials.
2. From the scope selection, select the partner whose customers you would like to delete.
3. Navigate to **Service Dashboard**.
4. Select the **Service Dashboard** tab.
5. Click on the menu arrow next to the customer you would like to delete.

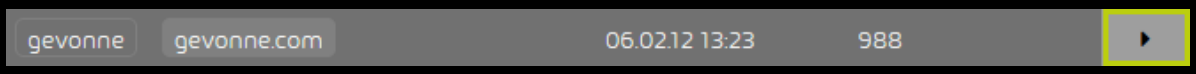

Figure 116: Open menu

A menu opens.

6. Click on **Delete selected customer**.

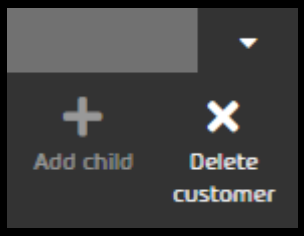

Figure 117: Delete customer

A warning message is displayed.

7. Click on **Confirm**.

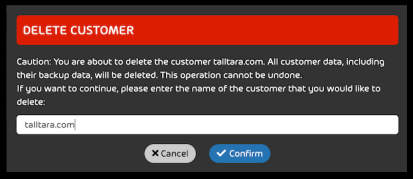

Figure 118: Confirm

The customer is deleted.

The 365 Total Protection customer has been deleted.

Numerics

A

C

D

E

F

G

I

L

M

N

O

P

R

S

T

U

V

W

HORNETSECURITY

Hornetsecurity GmbH
Am Listholze 78 | 30177 Hannover | Germany
Phone:+49 511 515 464-0 | info@hornetsecurity.com
www.hornetsecurity.com