ESET Cloud Office Security

User guide

Click here to display the online version of this document

Digital Security
Progress. Protected.

ESET Cloud Office Security was developed by ESET, spol. s r.o.

For more information visit https://www.eset.com.

Technical Support: https://support.eset.com

REV. 12/20/2023

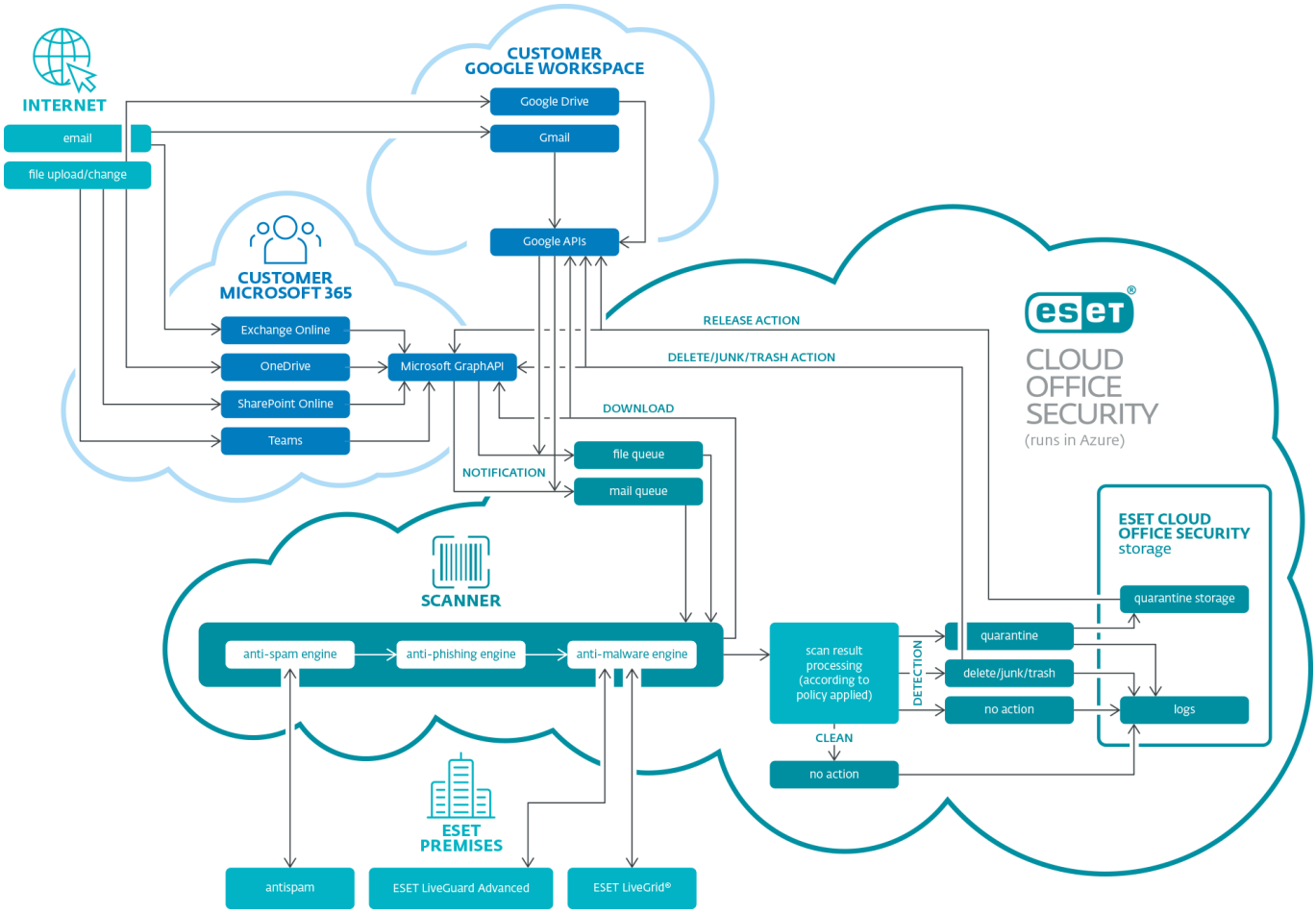
Overview

ESET Cloud Office Security is a multitenant and scalable cloud service in Microsoft Azure. ESET Cloud Office Security is a Software-as-a-Service (SaaS) product that operates entirely in the cloud without the need for your own hardware. It is the ultimate combination of spam filtering, Anti-Malware scanning, and Anti-Phishing protection that helps protect your company communications against malware, minimizes the adverse effects of unsolicited messages on everyday productivity, and prevents incoming external emails from being used as a channel for targeted attacks.

ESET Cloud Office Security security services cover leading cloud platform providers and deliver comprehensive email protection with cutting-edge anti-malware engines and ESET LiveGuard Advanced. This solution offers advanced threat defense through cloud-based sandboxing, analyzing suspicious samples in an isolated environment.

The ESET Cloud Office Security architecture enables you to initiate protection quickly by connecting to your cloud platform - Microsoft 365 and Google Workspace. It gives you the power to manage protection through a web-based console accessible from anywhere.

ESET Cloud Office Security provides advanced preventive protection to safeguard your company's Microsoft 365 apps - Exchange Online, OneDrive, SharePoint Online, and Teams. The same protection is provided to your Google Workspace apps - Gmail and Google Drive.



ESET Cloud Office Security protects OneDrive and Mailbox of licensed users, as well as Team groups and SharePoint sites. Each store of these Microsoft 365 applications is protected regardless of who uploaded a file or who sent an email. The content itself is protected regardless of who the author is. The author can also be a guest user to ensure the best possible protection.

Key features

The following table provides a list of available features in ESET Cloud Office Security.

Multi-tenant	You can protect and manage multiple Microsoft 365 and Google Workspace tenants from one ESET Cloud Office Security console. Azure Active Directory (Azure AD) organizes objects like users and apps into groups called tenants. Tenants allow you to set policies on users and apps within your organization to meet security and operational policies.

Antispam	Antispam is an essential component for any mail server. ESET Cloud Office Security uses a state-of-the-art Antispam engine that prevents spam and phishing attempts with very high catch rates. ESET Cloud Office Security has consecutively won spam filtering tests by Virus Bulletin, a leading security testing authority, and received the VBSpam+ certification for several years. The Antispam engine has achieved a 99.99% spam catch rate with zero false positives making it an industry-leading technology in spam protection. ESET Cloud Office Security Antispam is cloud-based, and most of the cloud databases are located in ESET data centers. Antispam cloud services allow for prompt data updates that provide quicker reaction time when new spam emerges.
Anti-Phishing protection	This feature prevents users from accessing web pages known for phishing. Email messages may contain links that lead to phishing web pages. ESET Cloud Office Security uses a sophisticated parser that searches the message body and subject of incoming email messages to identify such links (URLs). The links are compared against a phishing database that is updated continuously.
Anti-Malware protection	An award-winning and innovative defense against malware, this leading-edge technology prevents attacks. It eliminates all types of threats, including viruses, ransomware, rootkits, worms, and spyware, with cloud-powered scanning for even better detection rates. Its small footprint is light on system resources and does not compromise performance. Anti-Malware detection uses a layered security model. Each layer, or phase, has several core technologies. The Pre-execution phase includes the following technologies: Unified Extensible Firmware Interface (UEFI) Scanner, Network Attack Protection, Reputation & Cache, In-product Sandbox, DNA Detections. The Execution phase technologies are Exploit Blocker, Ransomware Shield, Advanced Memory Scanner, and Script Scanner (AMSI). The Post-execution phase uses Botnet Protection, Cloud Malware Protection System, and Sandboxing. This feature-rich set of core technologies provides an unrivaled level of protection.
Policies	Larger organizations usually have multiple departments and want to configure different protection settings for each organizational unit. ESET Cloud Office Security provides policy-based protection settings that can be assigned to selected Tenants, Users, Team groups or SharePoint sites. You can customize each policy according to your needs.
Quarantine manager	Inspect quarantined objects and perform an appropriate action (download, delete, or release). This feature offers simple management of email messages, attachments, and files from Exchange Online / OneDrive / Team groups / SharePoint sites that have been quarantined by ESET Cloud Office Security . The download gives you the option of analyzing quarantined objects with third-party tools, if required, to help when deciding what action to take.
Dashboard with detection statistics	Get a quick overview of security activities within Microsoft 365. The dashboard provides essential information in each of the overview tabs (Exchange Online / OneDrive / Team groups / SharePoint sites). User overview shows the number of Tenants and License usage, and statistics per each Tenant — Number of users, Top recipients of spam/phishing/malware, and Top suspicious OneDrive accounts, Top suspicious Team groups and SharePoint sites. You can choose a time period and a Tenant to display the statistics for. Further detection statistics and graphs are visible in the Exchange Online, OneDrive, Team groups and SharePoint sites overview tabs. These are statistics such as the number of scanned emails and files and the number of detected spam/phishing/malware. The graphs show the traffic for each detection type — spam, malware, and phishing.
Detections with filtering options	This feature contains all records about detections. The records include logs of every detection by email scan in the Exchange Online tab and file scan in the OneDrive / Team groups / SharePoint sites tabs. This makes it possible to filter and effectively find what you are looking for by using additional information about the specific detection (for example, a name of the infiltration, file hash).

Users	The central entity that ESET Cloud Office Security protects is the user account. Find useful information by opening the Details of a user, such as an Overview, Settings defined by Policies, list of Policies assigned to the user, and Detections for Exchange Online and OneDrive. This feature helps to investigate detections related to a specific user. You can also choose which users to protect. Users are sorted into groups. Each group is an Microsoft 365 tenant containing its users. Use multiple filtering criteria to make searching for a specific user within a group easier.
Reporting & Machine Learning Protection	Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection based on Machine learning. Read more about this type of protection in the glossary. You can configure Reporting levels for the following categories: Malware, Potentially unwanted applications (PUAs), Potentially suspicious applications, and Potentially unsafe applications.
Reports (Statistical and Mail quarantine)	Receive statistical data for Exchange Online, OneDrive, Team groups and SharePoint sites via email, or generate and download a one-off report for a chosen period. You can schedule reports to generate and get distributed to specified email recipients regularly. Choose PDF or CSV as an output format. Reports contain data such as a number of scanned emails, detected malware, phishing, and spam. PDF format includes data shown in graphs. There is a graph for each — scanned emails, malware traffic, phishing traffic, and spam traffic. It also contains separate statistics for top recipients for each category: malware, phishing, and spam. There are several available options for generating reports. Additionally, you can have a Mail Quarantine report — a list of quarantined email messages — delivered to selected recipients. The Mail Quarantine report is sent on the specified date and time, but only if there are new items to be reported.
Teams & Sites	ESET Cloud Office Security provides protection for Team groups or SharePoint sites. This widens protection to Microsoft 365 collaboration solutions by protecting SharePoint and Teams enabling secure file sharing. If you have been using ESET Cloud Office Security, you may be asked to update consent before using Teams & Sites.
ESET LiveGuard Advanced	An additional layer of protection against advanced zero-day threats. ESET LiveGuard Advanced is a cloud-based sandboxing solution that analyzes submitted files by executing suspicious code in an isolated environment to evaluate its behavior. ESET Cloud Office Security submits suspicious email attachments and files from Exchange Online, OneDrive, Team groups and SharePoint sites to ESET LiveGuard Advanced for analysis. Enable and configure ESET LiveGuard Advanced feature using policies. Results of the analysis are shown in Scan logs.
Audit log	The Audit log enables the Administrator to inspect the activities performed in the ESET Cloud Office Security. This feature may be useful, especially when you have multiple ESET Cloud Office Security console users. The Audit log records are evidence of the activities and show the sequence in which they occurred. Audit logs store information about the specific operation or event. Audit logs are created whenever a ESET Cloud Office Security object (License pool, User, Policy, Report, Quarantine item such as attachment) is created or modified.
Google Workspace (Gmail and Google Drive protection)	ESET Cloud Office Security expands the security services coverage to another leading cloud email provider, Google Workspace. ESET Cloud Office Security provides comprehensive protection to Gmail and Google Drive users by utilizing all its features. It keeps Google Workspace users safe from malware, phishing, and spam.

What's new

Information about new features and improvements implemented in each ESET Cloud Office Security version:

^ Portal version 353 released November 23, 2023

- Added Google Workspace Integration.
- Product Navigator to quickly access ESET Business Account (more consoles to follow in coming months).
- *Other bug fixes and back-end improvements.*

Portal version 342.3 released October 24, 2023

- Added Google Workspace Admin Account Verification.
- Added User Type Column.
- *Other bug fixes and back-end improvements.*

Portal version 311.2 released July 31, 2023

- Added Google Workspace (Gmail and Google Drive protection) – access the Preview Features from the Quick Links.
- Added Dark mode theme.
- Added Product Navigator for ESET HUB Early Access Users.
- *Other bug fixes and back-end improvements.*

Portal version 293.7 released July 13, 2023

- Added Tenant Association to ESET Business Account (EBA) sites. This change ensures compatibility with the future customer portal ESET PROTECT HUB, which will replace ESET MSP Administrator (EMA) and ESET Business Account (EBA). It affects only a handful of customers using licenses from multiple sites to protect a single tenant. If this is your case, you will be prompted to associate your tenants with EBA sites.
- Other minor improvements and bug fixes.

Portal version 251.1 released March 21, 2023

- Improvements in lazy loading of screens to better support tenants with tens of thousands of users.
- Changes to the add tenant wizard.
- Updates on the About page.
- Terms of Use and Privacy Policy updates (Limitations and Data Retention Policy).

Portal version 205 released November 9, 2022

- Added a What's new window to appear when you first log in to the ESET Cloud Office Security console, describing the newly added features.
- Included option to export Scan logs and Audit log to CSV file.
- Added a new setting when Merging policies with lists and notification emails.

Portal version 180.2 released July 27, 2022

- The new Audit log feature.
- Change Logs section to Scan logs.

Portal version 156.2 released April 26, 2022

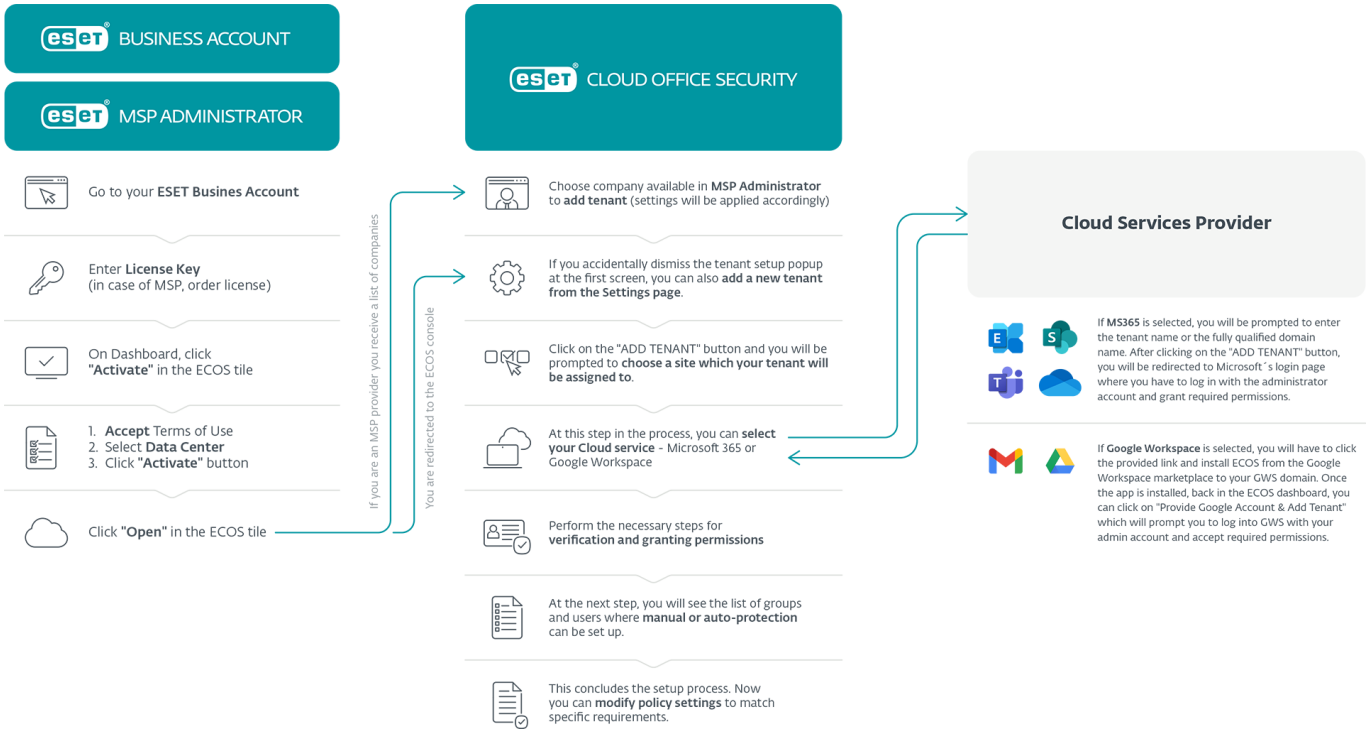
- Dynamic Threat Defense was renamed to ESET LiveGuard Advanced.
- Submission of false positive / false negative samples for analysis.
- Import/Export Approved, Blocked, and Ignored lists in Policies.
- Dashboard shows unprotected users count in Overview tab.
- Fixed a bug that was placing notification emails into quarantine.

Portal version 140.6 released February 9, 2022

- Ability to whitelabel reports (co-branding or custom logo only).
- Option to define the preferred language for notification email (mailbox owner notifications).
- Option to define the preferred language for email notifications for tenant members.
- Filter emails by Message-ID.

Integration

The flow of ESET Cloud Office Security integration with your cloud services provider:



Specifications

A reference technical specifications for ESET Cloud Office Security:

- Requirements
- Supported Microsoft 365 plans
- Supported Google Workspace plans
- Supported web browsers
- Limitations and Data Retention Policy

Requirements

To take advantage of ESET Cloud Office Security service protecting your Microsoft 365, the following is required:

- Supported Microsoft 365 subscription plan
- Admin access to Azure Active Directory (Azure AD)
- Azure Cloud Services – Exchange | OneDrive

- An account in ESET Business Account or ESET MSP Administrator portal

Supported Microsoft 365 plans

ESET Cloud Office Security supports the following Microsoft 365, Exchange Online and OneDrive plans.

Microsoft 365 enterprise plans:

- Microsoft 365 Apps for enterprise
- Microsoft 365 E3
- Microsoft 365 E5
- Microsoft 365 F3
- Office 365 E1
- Office 365 E3
- Office 365 E5
- Office 365 F3

Microsoft 365 business plans:

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard
- Microsoft 365 Business Premium
- Microsoft 365 Apps

Microsoft 365 Education plans:

- Microsoft 365 A3
- Microsoft 365 A5

Exchange Online plans:

- Exchange Online (Plan 1)
- Exchange Online (Plan 2)
- Microsoft 365 Business Standard

OneDrive plans:

- OneDrive for Business (Plan 1)
- OneDrive for Business (Plan 2)

- Microsoft 365 Business Basic
- Microsoft 365 Business Standard

Supported Google Workspace plans

ESET Cloud Office Security supports the following Google Workspace plans.

- Business Starter
- Business Standard
- Business Plus
- Enterprise

Supported web browsers

> For the best experience with the ESET Cloud Office Security, we recommend that you keep your web browsers up-to-date.

You can use the ESET Cloud Office Security console with the following web browsers:

- Mozilla Firefox 69 and later
- Microsoft Edge 44 and later
- Google Chrome 77 and later
- Opera 63 and later
- Safari 13.x and later

> Microsoft Internet Explorer is not supported.

Limitations and data retention Policy

In certain circumstances, there are ESET Cloud Office Security scanning limitations. A file is not scanned and will appear in Scan logs as **Not scanned** if the following occurs:

- The file size is over 200 MB
- The scan takes longer than 2 minutes and times out
- The archive file has a nesting level of 10 or more (usually, a file known as an archive bomb or zip bomb)
- The archive file is password-protected
- The file is damaged

Quarantine limits (when released from quarantine):

- 15 MB for one email attachment
- 150 MB for the whole email message, including attachments

Data retention policy:

Entity	Retention period	Comment
Quarantined objects	30 days	Objects older than 30 days will be removed permanently.
Detections	90 days	Records older than 90 days will be removed permanently.
Scan logs records	90 days	Records older than 90 days will be removed permanently.
Scan logs records with Clean scan result	3 days	If you have a policy that uses Log all objects, Clean scan results older than 3 days will be removed permanently.
ESET Cloud Office Security database backup	90 days	Backups older than 90 days will be permanently deleted.
Audit logs	90 days	Records older than 90 days will be removed permanently.
Application Insights logs	90 days	Records older than 90 days will be removed permanently.

Tenant removed from ESET Cloud Office Security console

When you remove a tenant from the ESET Cloud Office Security console, the retention period for tenant data is 30 days (quarantine, Scan logs, and Statistics are deleted after 30 days). If you add the tenant again within 30 days, all the data will be restored. Other objects (tenants, users, groups, sites, reports, policies) are permanently deleted after 90 days.

ESET Cloud Office Security deactivated in ESET Business Account or ESET MSP Administrator

If you deactivate ESET Cloud Office Security in ESET Business Account or ESET MSP Administrator, this process also removes tenants from ESET Cloud Office Security. ESET Cloud Office Security removal is permanent, and deleted data cannot be restored.

Antispam scan

ESET Cloud Office Security scans email messages stored in mailboxes for spam. For this reason, ESET Cloud Office Security cannot prevent a user from sending a spam message to an external email address. In a similarly unlikely scenario, if Office 365 user credentials get stolen, the credentials may be used by a spammer to send bulk spam messages (outbound email traffic).

Licensing for ESET Cloud Office Security

Manage ESET Cloud Office Security licenses via ESET Business Account or ESET MSP Administrator. You can try ESET Cloud Office Security with a 30-day trial license.

- Refer to ESET Business Account to create an account, add a license or manage a license.
- Refer to ESET MSP Administrator if you are an MSP.

ESET Business Account and ESET MSP Administrator (hybrid licensing account)

If you have the same email address registered in both ESET MSP Administrator and ESET Business Account (single sign-on), you can switch between ESET Business Account and ESET MSP Administrator views. Protect users or companies using License management for ESET Cloud Office Security.

Grace period for expiring license in ESET Business Account

When your license is close to expiring, an alert will display in the ESET Business Account interface. If the expiration date passes and you have not renewed your license or activated a new license, the license expired alert will display in ESET Business Account. If an eligible license is not in place, a notification that your license will be suspended in 14 days will be displayed in ESET Business Account, and you will receive an email at the address specified in your administrator account.

You have a 14-day grace period to renew after your license expires. You will be notified in ESET Business Account and by email halfway through the grace period. After 14 days, your ESET Cloud Office Security use will be suspended. The account will become inaccessible and non-functional. A suspended ESET Cloud Office Security account will be stored and reaccessed by adding a new ESET Cloud Office Security license to ESET Business Account. Your ESET Cloud Office Security account can remain suspended for up to 30 days, after which it will be deleted permanently.

If your account enters a suspended state, you will be notified in ESET Business Account and by email when there are 14 days left before your account is deleted. You must activate a new ESET Cloud Office Security license to restore access to your ESET Cloud Office Security account.

> Users continue to be fully protected during the grace period. When the grace period is over, the users will become unprotected.

Suspended license

If there is no valid ESET Cloud Office Security license present in ESET Business Account, your ESET Cloud Office Security instance will be suspended. The instance will become inaccessible and non-functional. Your ESET Cloud Office Security instance can remain suspended for up to 30 days, after which it will be deleted permanently. You must activate a new ESET Cloud Office Security license to restore access to your ESET Cloud Office Security instance.

ESET Business Account

ESET Business Account works as a unified access point for ESET Business Account and ESET Cloud Office Security. Use the ESET Cloud Office Security or ESET Business Account login page to access your ESET Cloud Office Security. Both pages redirect you through ESET Business Account authentication to verify your login.

- Create a new account if you do not have a registered account in ESET Business Account.
- If you have an ESET Business Account account, add your ESET Cloud Office Security license.
- Manage ESET Business Account.

Create a new ESET Business Account account

1. Open the ESET Business Account login page and click **Register for free**. Fill out the form carefully for registration. The email address entered will be used as your login name.

2. The password must contain at least 10 characters. Fill in your **Name** and **Company details** and click **Continue**. Read and confirm that you agree to the **ESET Terms of Use**. Complete the reCAPTCHA form and click **Register**.

3. You will receive a confirmation email after registering successfully (this may take up to 15 minutes). Click the link in the confirmation email to open a new **Activate account** window.

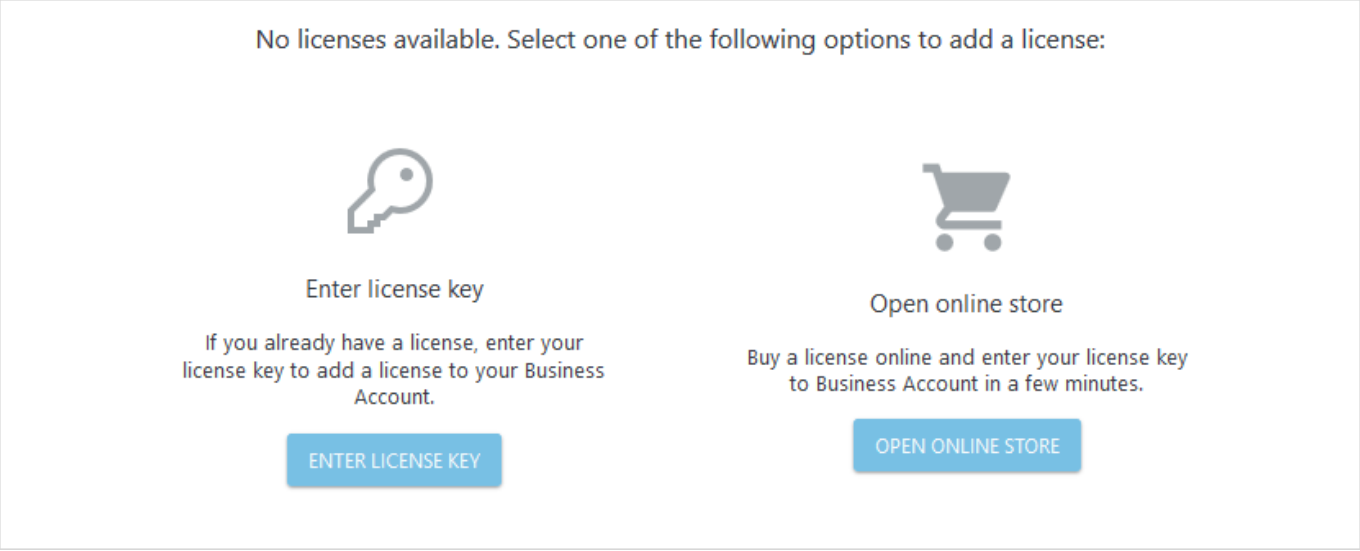
4. Type your password and click **Activate** to activate your ESET Business Account. You will receive another email verifying that your ESET Business Account account was successfully created. You are now ready to log in to ESET Business Account.

After you activate ESET Business Account, add your ESET Cloud Office Security license.

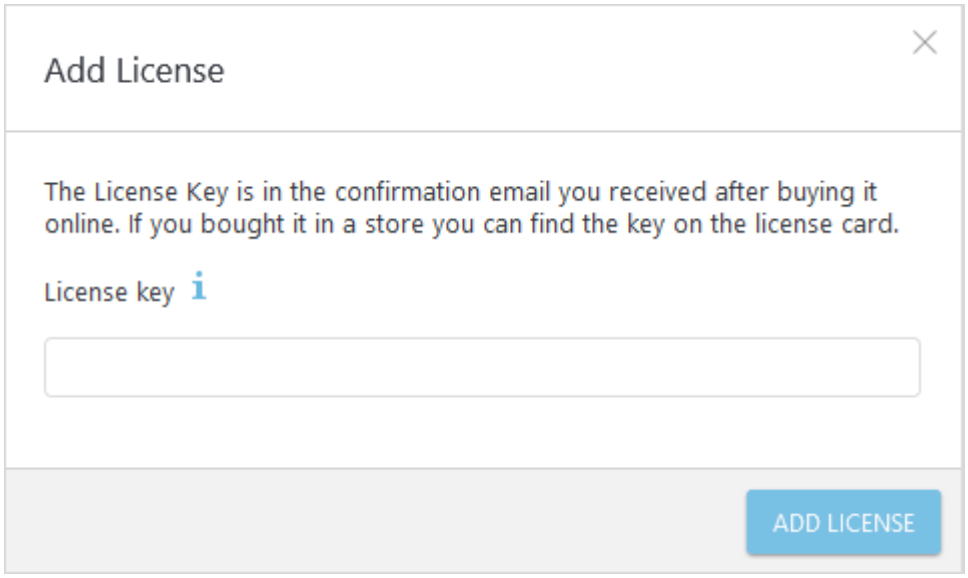
Add license for ESET Cloud Office Security in ESET Business Account

After a successful login to ESET Business Account, you will see a Welcome screen for ESET Business Account if you are a first-time user.

1. Click **Add license** to open the license window. If you are a regular ESET Business Account user, go to the **License** tab and click **Add license**.



2. Enter your **License key** and click **Add license**.



3. You will receive an email with a verification link. Click the link and enter your ESET Business Account portal login credentials when requested. For more information about license management, users and sites, refer to the ESET Business Account guide.

Manage ESET Business Account

Common activities related to licensing:

Sites and License pool

The licenses and license pools are loaded from ESET Business Account. License pools are available only if you have existing sites within ESET Business Account.

Create a New user in ESET Business Account

You can create a user to help you manage a share of your licenses.

1. Open ESET Business Account and log in.

2. Select **User management**, click **New user** and type the required information.

3. Select ESET Cloud Office Security **Access rights** for a user:

   • **Read**—User has access to ESET Cloud Office Security: see users, logs and detections but cannot manage a policy, protect users or release from quarantine

   • **Write**—User has full access to ESET Cloud Office Security: see and manage users, quarantine or create a policy

   • **No Access**—User cannot access ESET Cloud Office Security

4. Set a language in user **Preferences** for the ESET Cloud Office Security console.

5. Click **Create**, and the user will be created.

Create a new Site in ESET Business Account

Sites allow you to split or merge your licenses into license pools. Sites are individual groups that can have their own location and administrators.

1. Open ESET Business Account and log in.

2. Select **Details**, click **Create site** and type the required personal information.

3. Click **Add user**, select a user and click **Confirm**.

4. In the License pool, click **Add Units** and select the ESET Cloud Office Security license. You can change **Subunits** and click **Confirm**.

5. Click **Create**, and the site will be created.

ESET MSP Administrator

ESET MSP Administrator is a licensing management system that allows MSP users to create multiple MSP Customers and generate specific licenses with a seat count. The ESET MSP Administrator licensing portal supports volume pricing and billing based on an exact number of seat-days purchased.

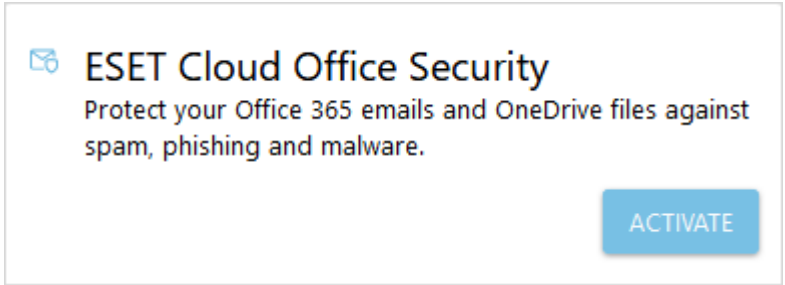
ESET Cloud Office Security is available to all MSP Managers, MSPs and managed MSPs. ESET MSP Administrator users with write access are eligible to activate ESET Cloud Office Security. ESET Cloud Office Security can be accessed by users with Write, Read or Custom access rights.

- Create a new MSP Customer (the customer's email address is required for ESET Cloud Office Security console activation).
- Activate ESET Cloud Office Security from ESET MSP Administrator.

Activate ESET Cloud Office Security

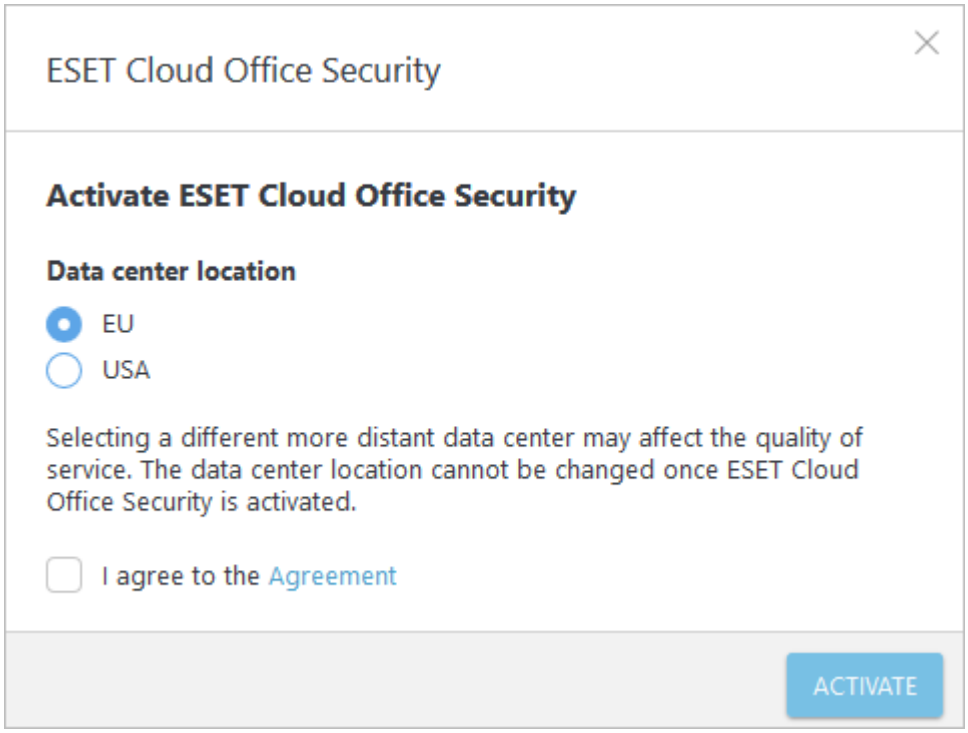
1. Log in to ESET Business Account or ESET MSP Administrator and locate the ESET Cloud Office Security tile in the **Dashboard**.

2. Click **Activate** in the bottom-right corner of the ESET Cloud Office Security tile.

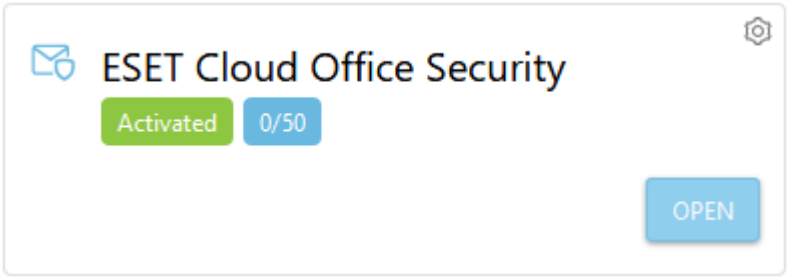


3. The activation wizard refers to the ESET Cloud Office Security Terms of Use and displays the optimal data center location based on your current location. Select **I agree to the Terms of Use** and click **Activate**. We do not recommend changing the data center location; however, you can make a different selection if you need to use another location.

Data centers are entirely separate. When you select the data center location, it cannot be changed, and you cannot migrate to another location. To change the data center, start the activation process from the beginning.

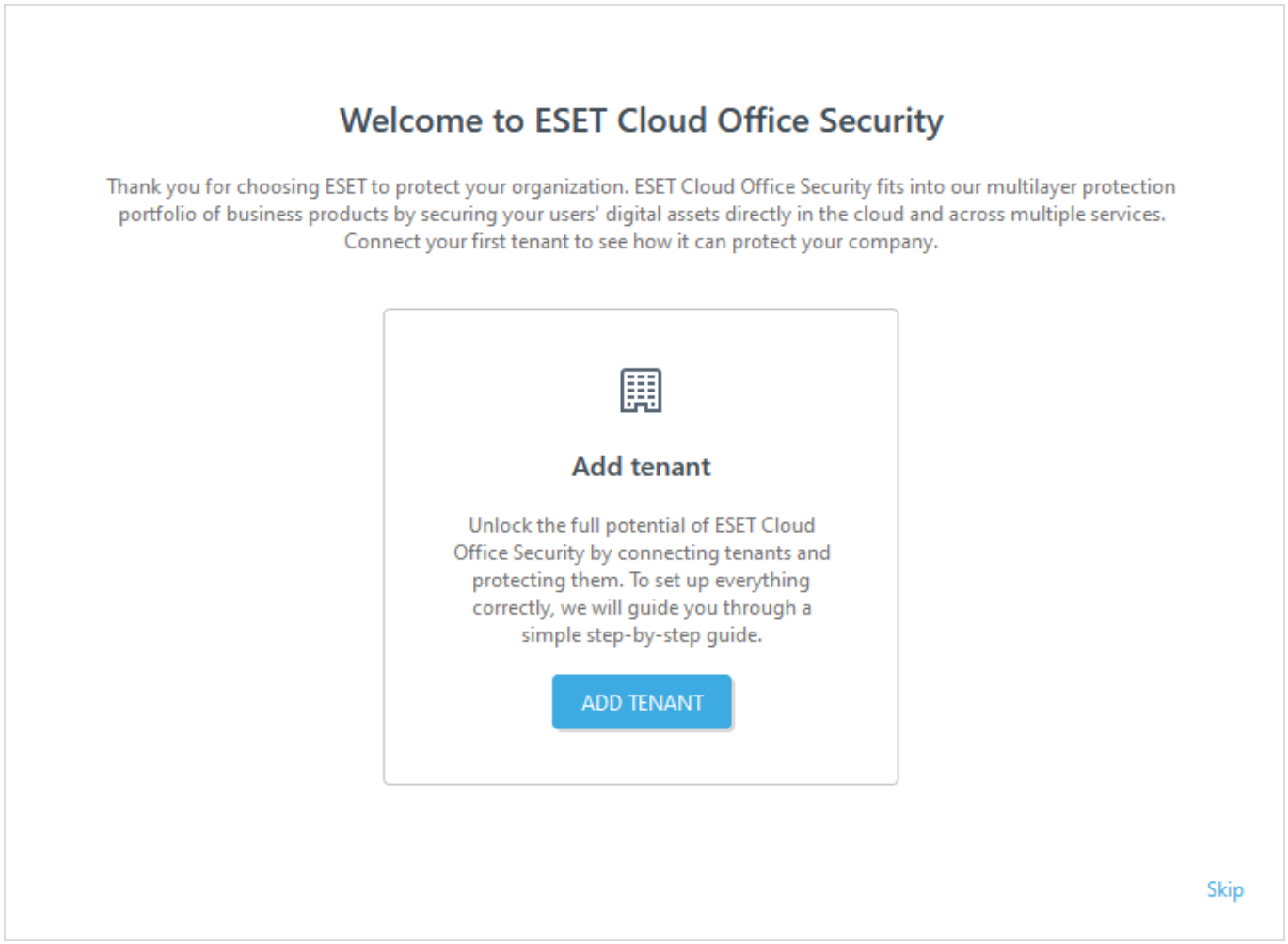


4. Click **Open** in the ESET Cloud Office Security tile. The ESET Cloud Office Security Dashboard opens in a new browser tab.

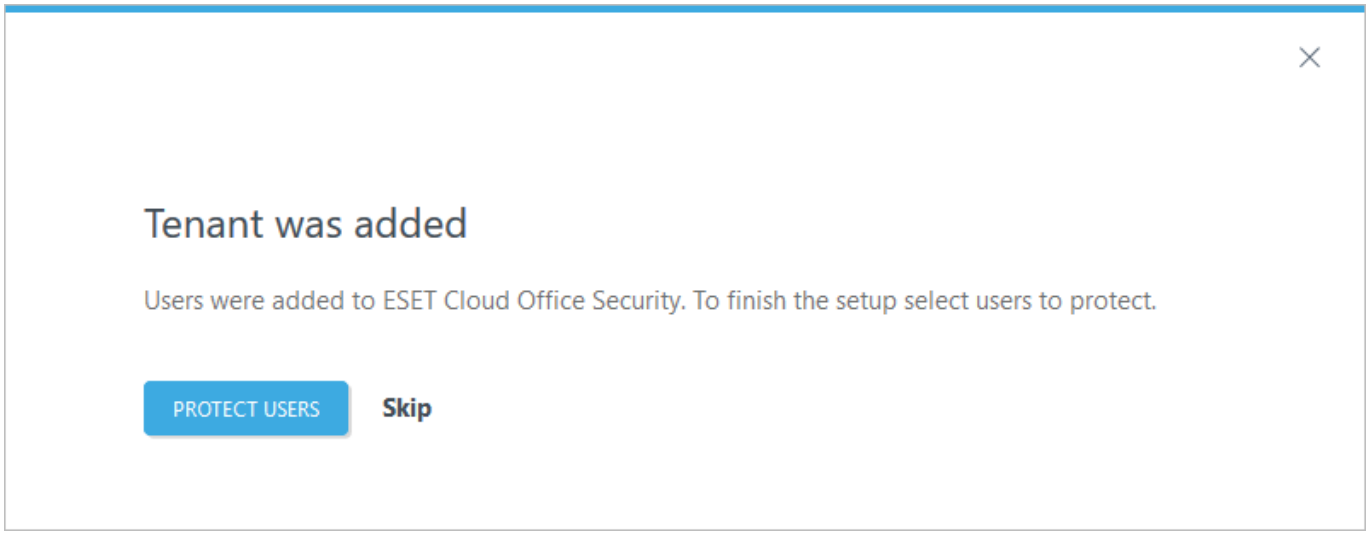


When you log into ESET Cloud Office Security for the first time, a **Startup wizard** appears. The Startup wizard takes you through the initial deployment process.

1. Add your tenant (Microsoft 365 or Google Workspace).



2. Protect users. If you **Skip**, you can protect users or companies later using License management for ESET Cloud Office Security.

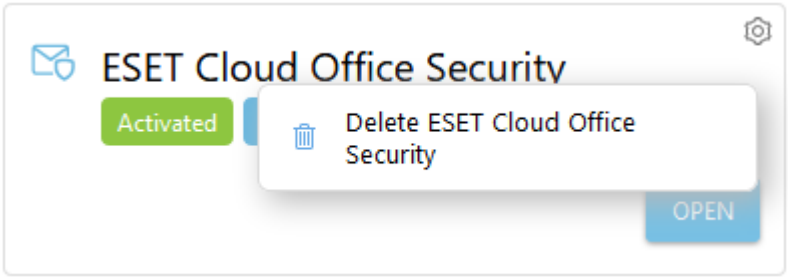


Deactivate ESET Cloud Office Security

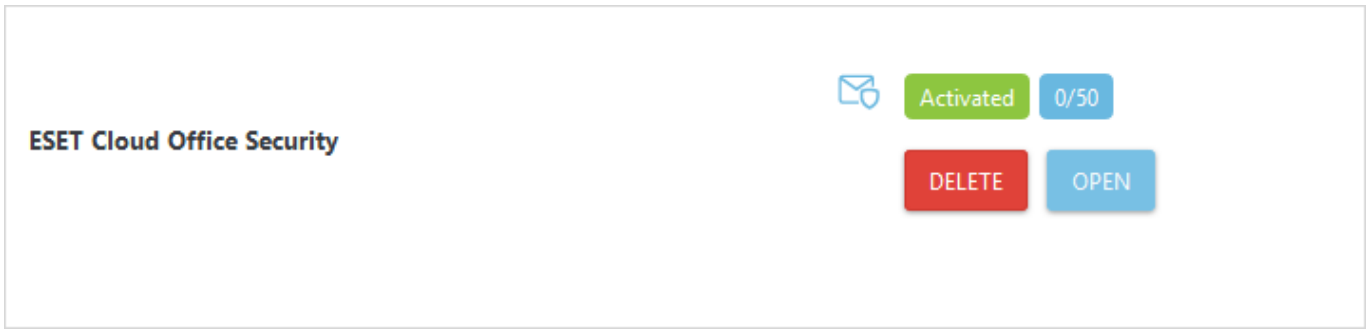
1. Log in to ESET Business Account or ESET MSP Administrator and locate the ESET Cloud Office Security tile in the **Dashboard**.

2. Click the gear icon in the upper-right corner of the ESET Cloud Office Security tile and select **Delete ESET**

Cloud Office Security.

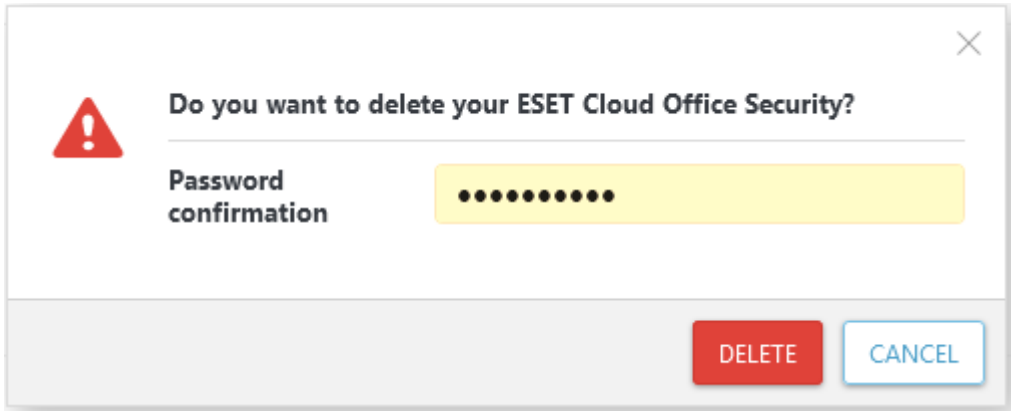


3. Alternatively, navigate to the **Details** section and click **Delete**.



4. A warning window pops-up, warning you that all data is about to be removed. Enter your ESET Business Account password to confirm, and click **Delete**.

Removal of ESET Cloud Office Security is permanent. Deleted data cannot be restored.



The ESET Cloud Office Security instance is deleted, and the ESET Cloud Office Security product tile reverts to **Not activated** state. You will also receive a confirmation email from ESET Business Account.

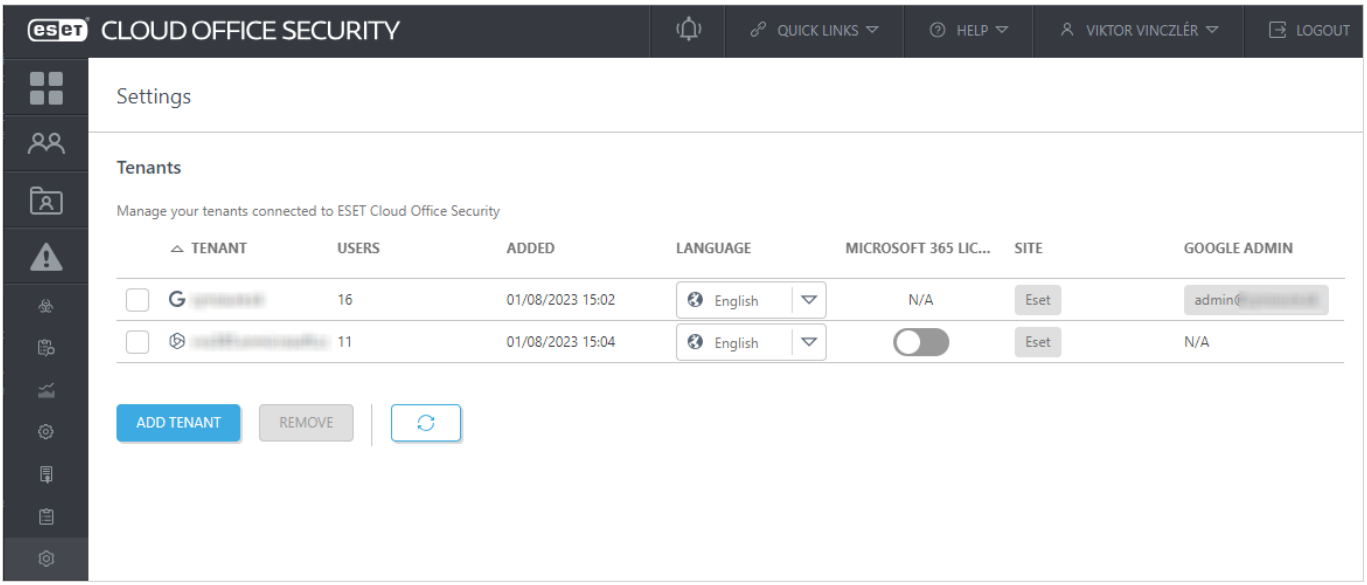
Manage your tenants in Settings

Manage tenants connected to ESET Cloud Office Security. You can see all registered tenants in the table with details for each tenant. Use the refresh button to reload the table with tenants.

If you want to add a new tenant, click Add tenant and choose Microsoft 365 or Google Workspace depending on what cloud platform you want to protect. After you finish tenant registration process, your Microsoft 365 or Google Workspace is protected by ESET Cloud Office Security.

After you have added the tenant, the screen changes, showing the list of tenants associated with a site, you can

manage your existing tenant or add more tenants. The table shows the tenant name, number of users, when the tenant was added, language setting, Microsoft 365 licensed users, site name, and Google admin.



Language

This setting determines the language of email notification messages to tenant members. You can define the language for each tenant separately, for example, in the case of MSP managing multiple companies.

Select the appropriate tenant and click Remove to delete a tenant from ESET Cloud Office Security. A confirmation window will appear for you to make a final decision. When deleted, all user data will be removed after 30 days.

Microsoft 365 licensed users

This option is enabled by default. This is equivalent to a list of users in the Microsoft 365 admin center under **Users** > **Active users** > Filter: **Licensed users**.

By disabling this option, ESET Cloud Office Security will display all users, including users without a Microsoft 365 license (for example, shared mailboxes). If you use Auto-protection for a group or tenant containing users without Microsoft 365 license, these users will become visible, protected, and consume ESET Cloud Office Security license units. Protection status of newly visible users may be **Pending** for up to 1 hour. When the Auto-protection process is complete, the protection status will change to **Protected** or the appropriate status in the Users section.

If your tenant or group with Auto-protection contains a user without Mailbox and OneDrive, this user will consume the ESET Cloud Office Security license unit. You will see a **Warning** protection status for this user.

When you re-enable Microsoft 365 licensed users, only users with Microsoft 365 licenses will remain displayed. If you had Auto-protected users without Microsoft 365 license, these users would disappear from the Users section, and ESET Cloud Office Security license units will be freed up. It may take up to 1 hour for the change to take place.

If you have manually protected users without Microsoft 365 license (while the **Microsoft 365 licensed users** setting was disabled), these users will remain visible and protected even after enabling the **Microsoft 365 licensed users** (until the users become unprotected).

Site

If you want to change the site the tenant is associated with, click the site name to open the **Select a site to protect** window and make the required changes.

Google admin

The Google admin should be an active email of your Google Workspace administrator.

> If the administrator's role or email address is about to change, update the Google admin information by clicking it. Do this in advance to ensure the tenant functionality and the protection of your site.

Update consent

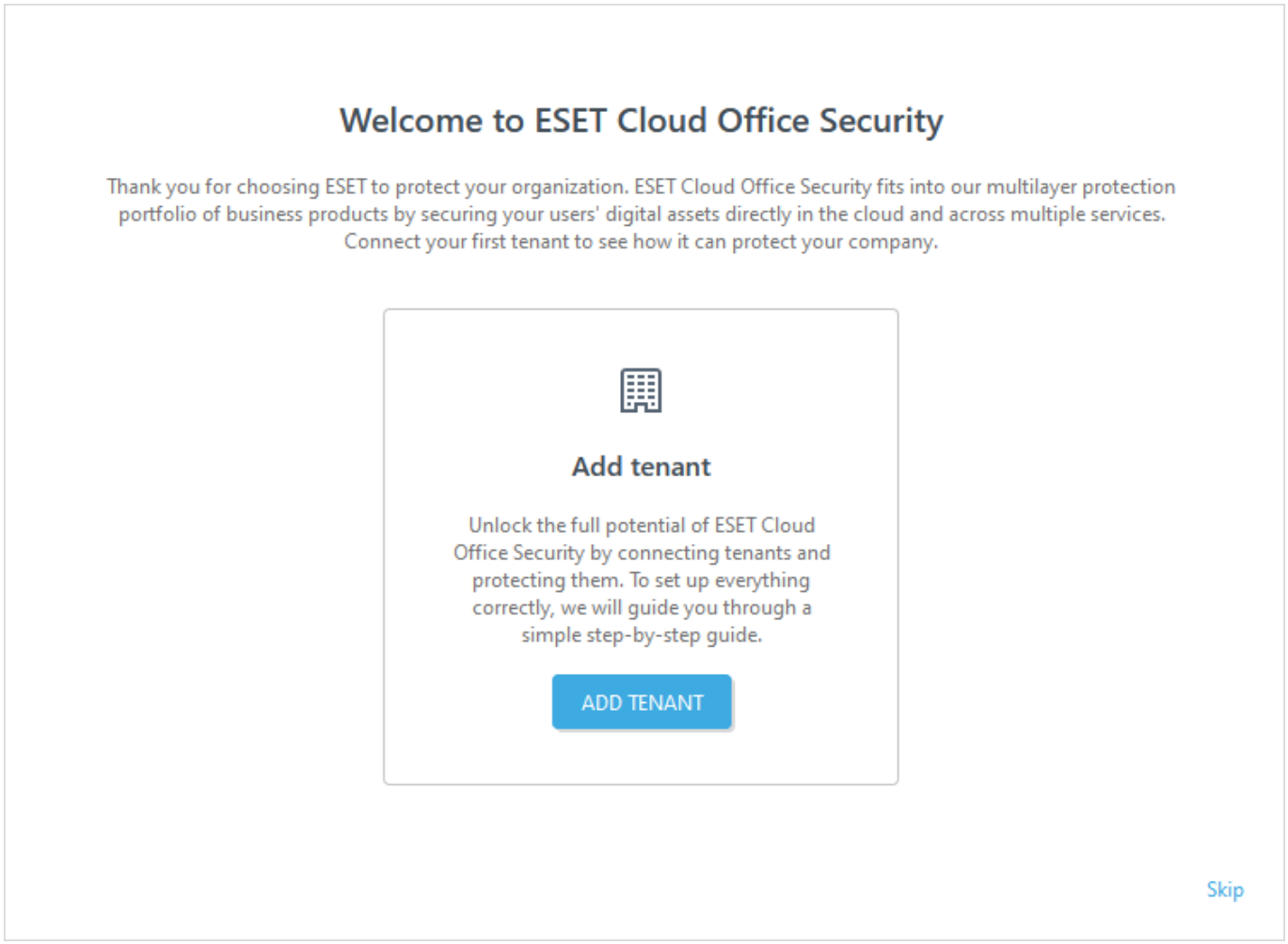
If a yellow button is shown, you can update your consent. Updating the consent for existing tenant extends the ESET Cloud Office Security permissions to your Microsoft 365 account, enabling a feature that provides information on the user type. User type is defined in the Azure Active Directory and will be displayed in the Users section in a dedicated column. For example, you can filter Microsoft 365 users based on their type if you want to list shared mailboxes only.

Click the **Update** button for each tenant you want to enable this feature for. It may take up to 24 hours to update the user type from your Azure AD.

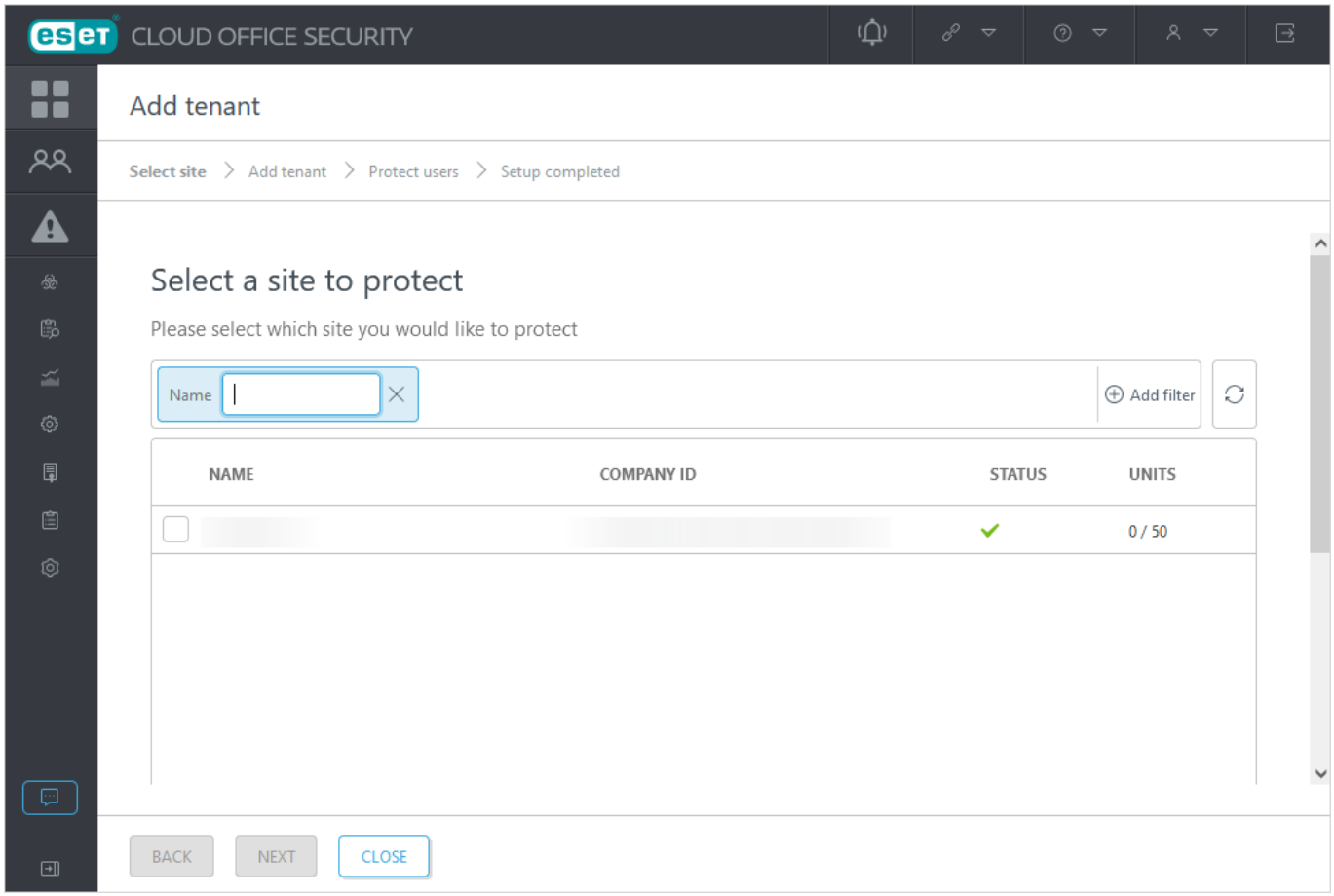
If a red button is shown, the consent has been revoked, or another change has been made that affected tenant integration with ESET Cloud Office Security. Click the **Update** button if you want to continue protecting users.

Add your first tenant

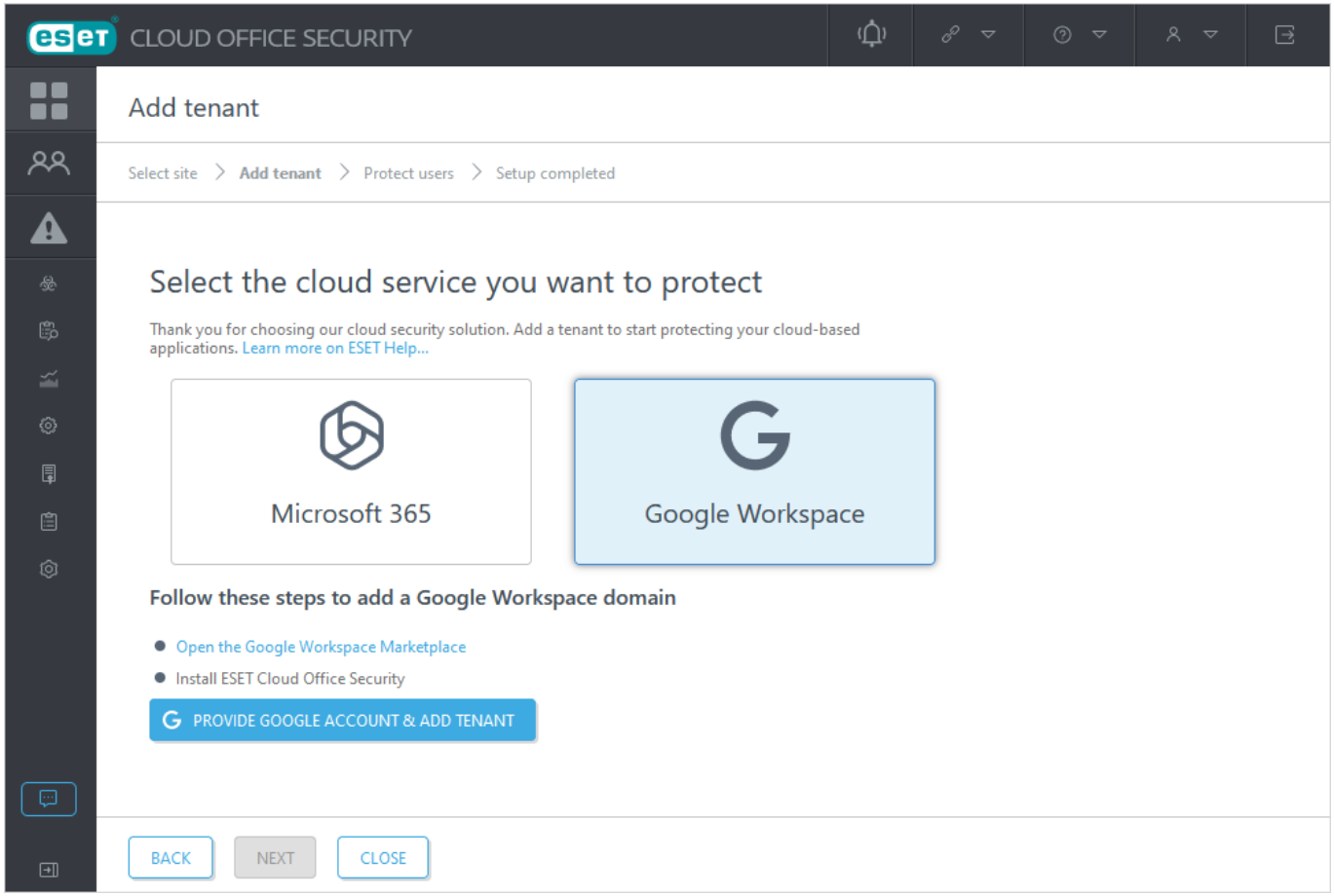
To protect your cloud platform, click **Add tenant** to connect your Microsoft 365 or Google Workspace to ESET Cloud Office Security.



You should see a list of available sites in the **Select a site to protect** window. Use the check box to select the site you want to associate with a tenant and click **Next**.



Click the Microsoft 365 or Google Workspace tile in the **Select the cloud service you want to protect** window and follow the bullet point steps:



Microsoft 365 tenant

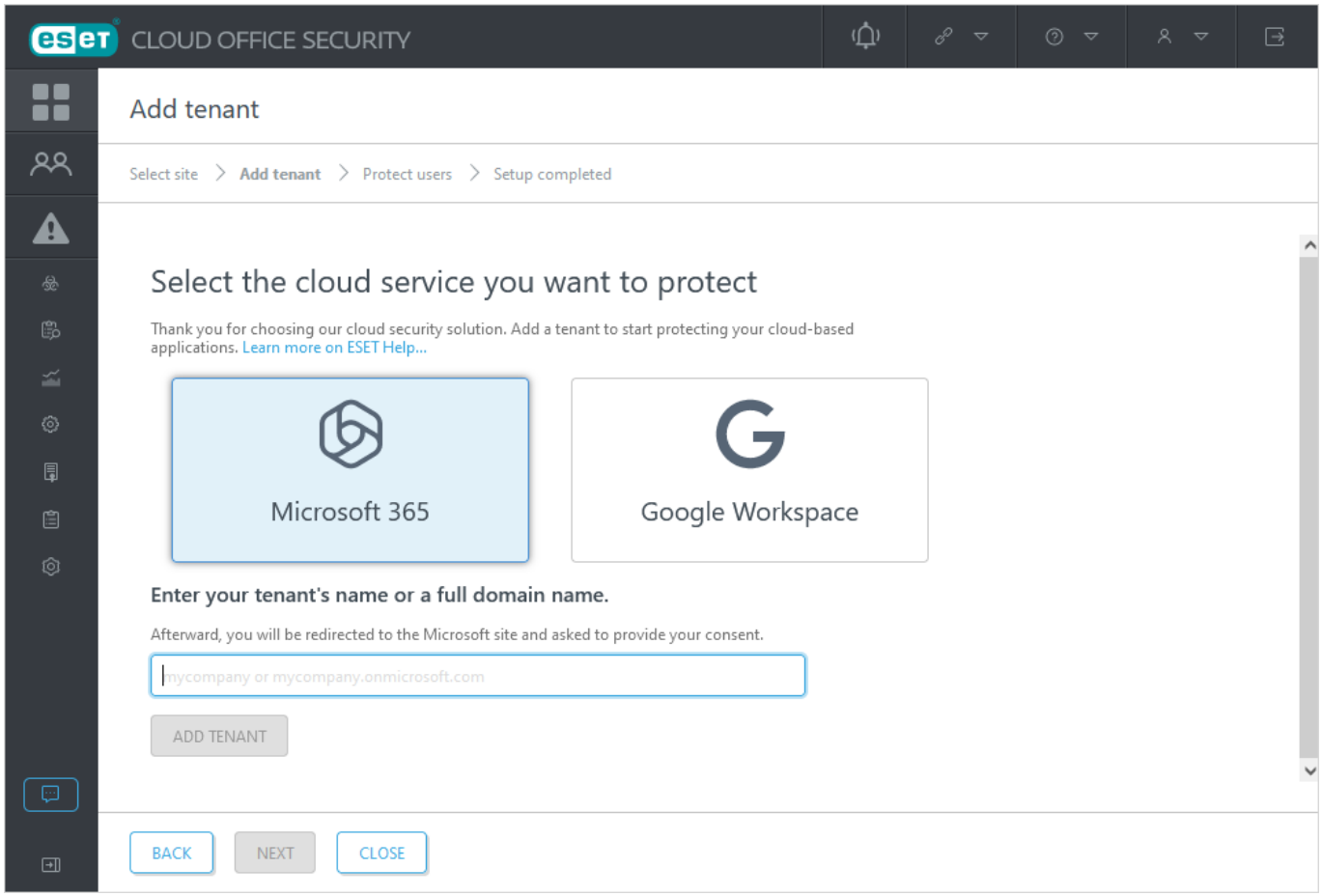
Azure Active Directory (Azure AD) organizes objects like users and apps into groups called tenants. A typical way to identify a tenant is using a domain name. If multiple users share a domain name, they are part of the same tenant. Tenants allow you to set policies on users and apps within your organization to meet security and operational policies. You can protect and manage multiple Microsoft 365 tenants using one ESET Cloud Office Security console.

For more details, see Microsoft's article about Tenancy in Azure Active Directory.

Add tenant

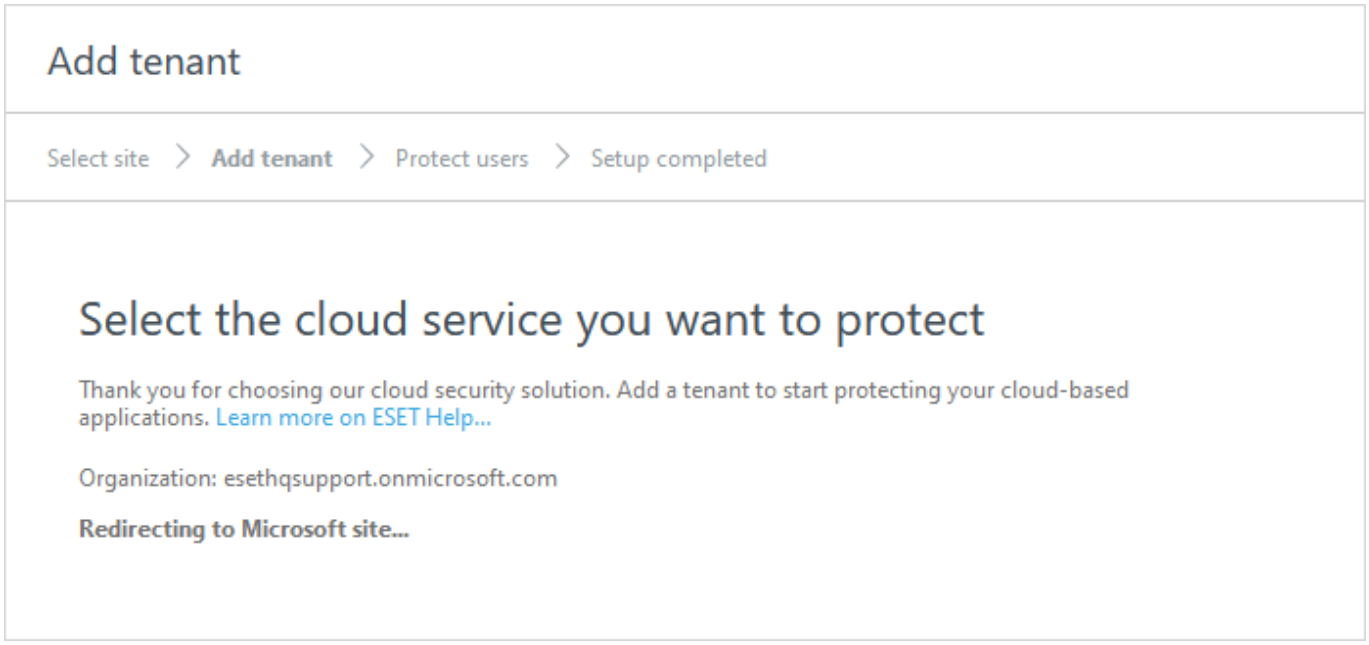
1. Go to **Settings** and click **Add tenant** (or anywhere you see the **Add tenant** button).

2. Click the **Microsoft 365** tile.

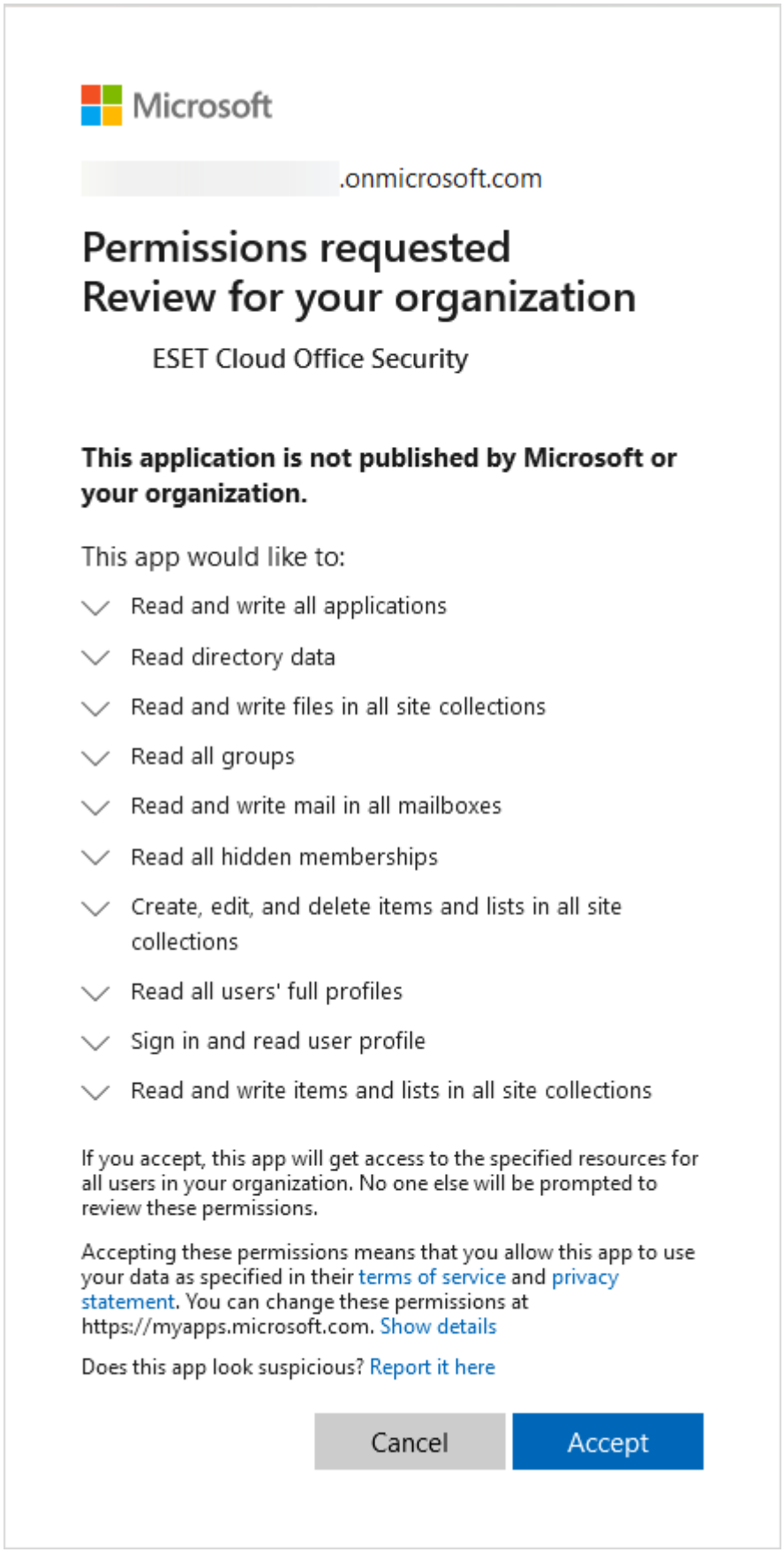


3. Type your Microsoft 365 tenant name or full domain name and click **Add tenant**.

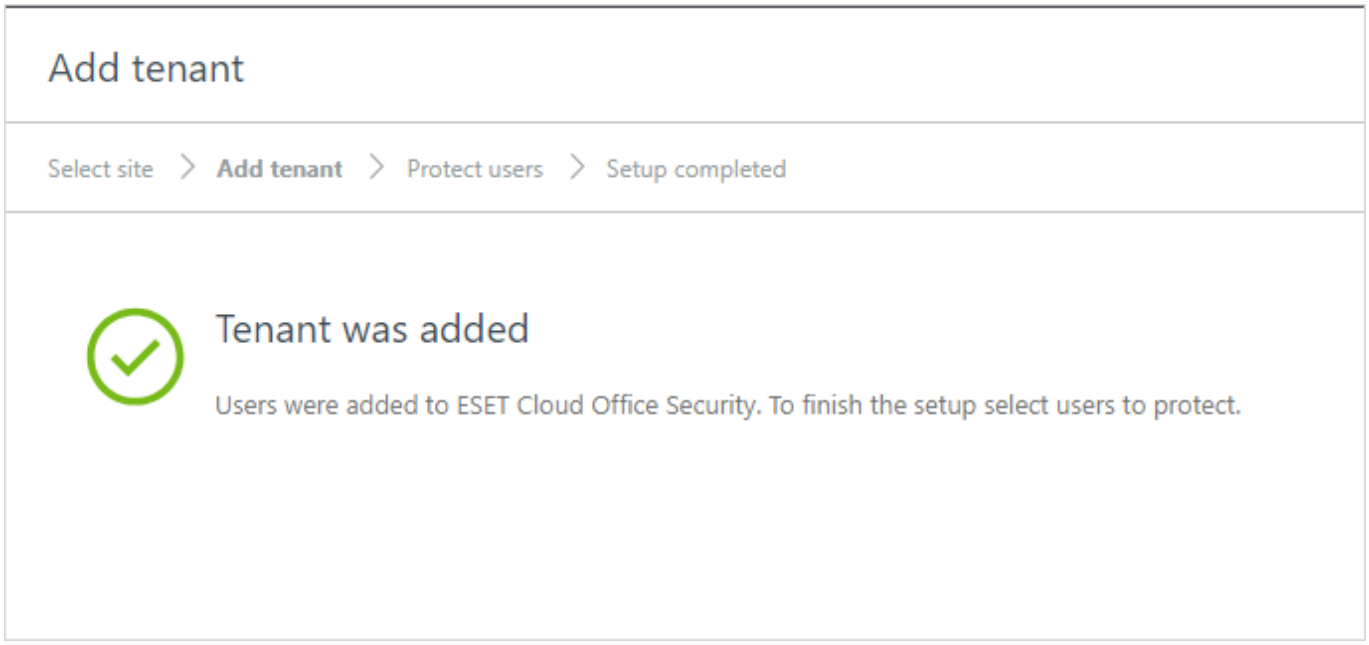
4. The screen redirects to the Microsoft Online consent page with a list of permissions required by ESET Cloud Office Security.



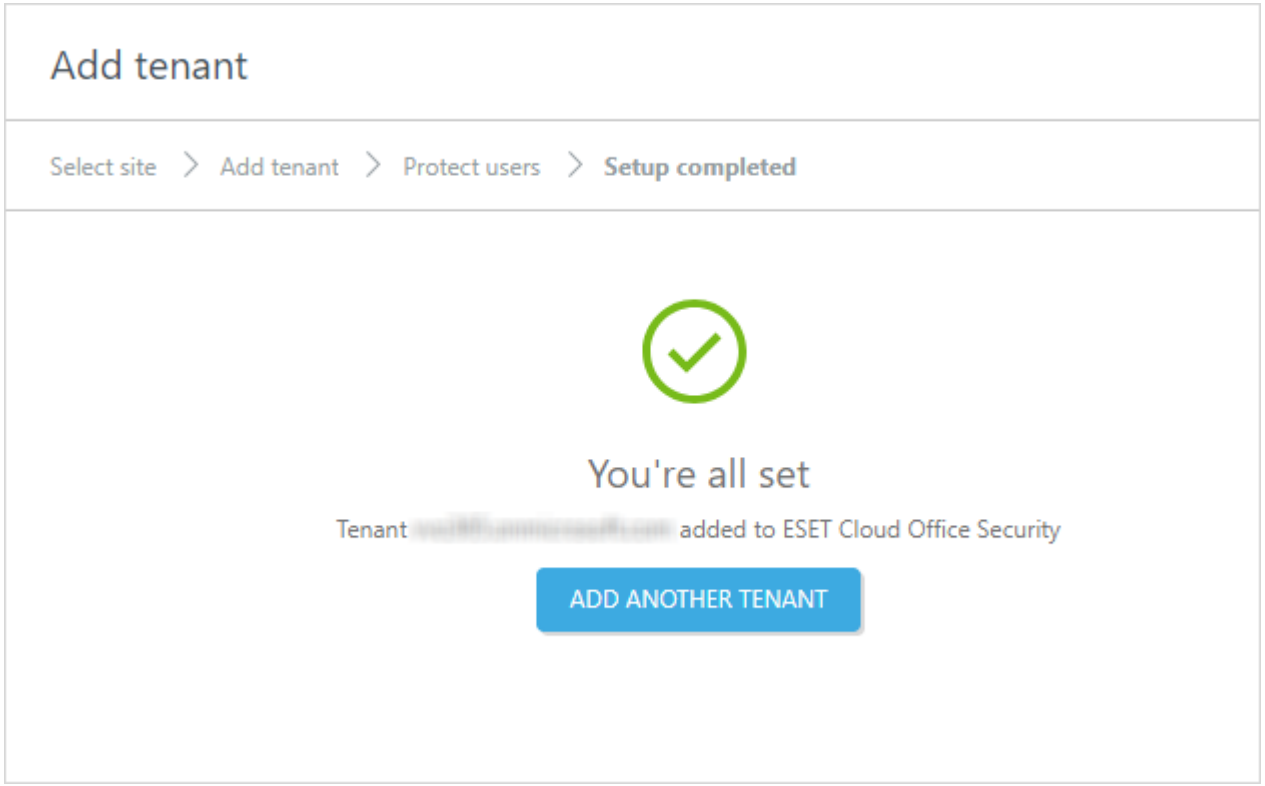
5. Enter your Microsoft 365 administrator account credentials to allow ESET Cloud Office Security access to your data located on your Microsoft account, click **Accept**.



6. Your Microsoft 365 tenant was added, including the users.



7. To finish the setup, click **Next** and select users to **Protect**.



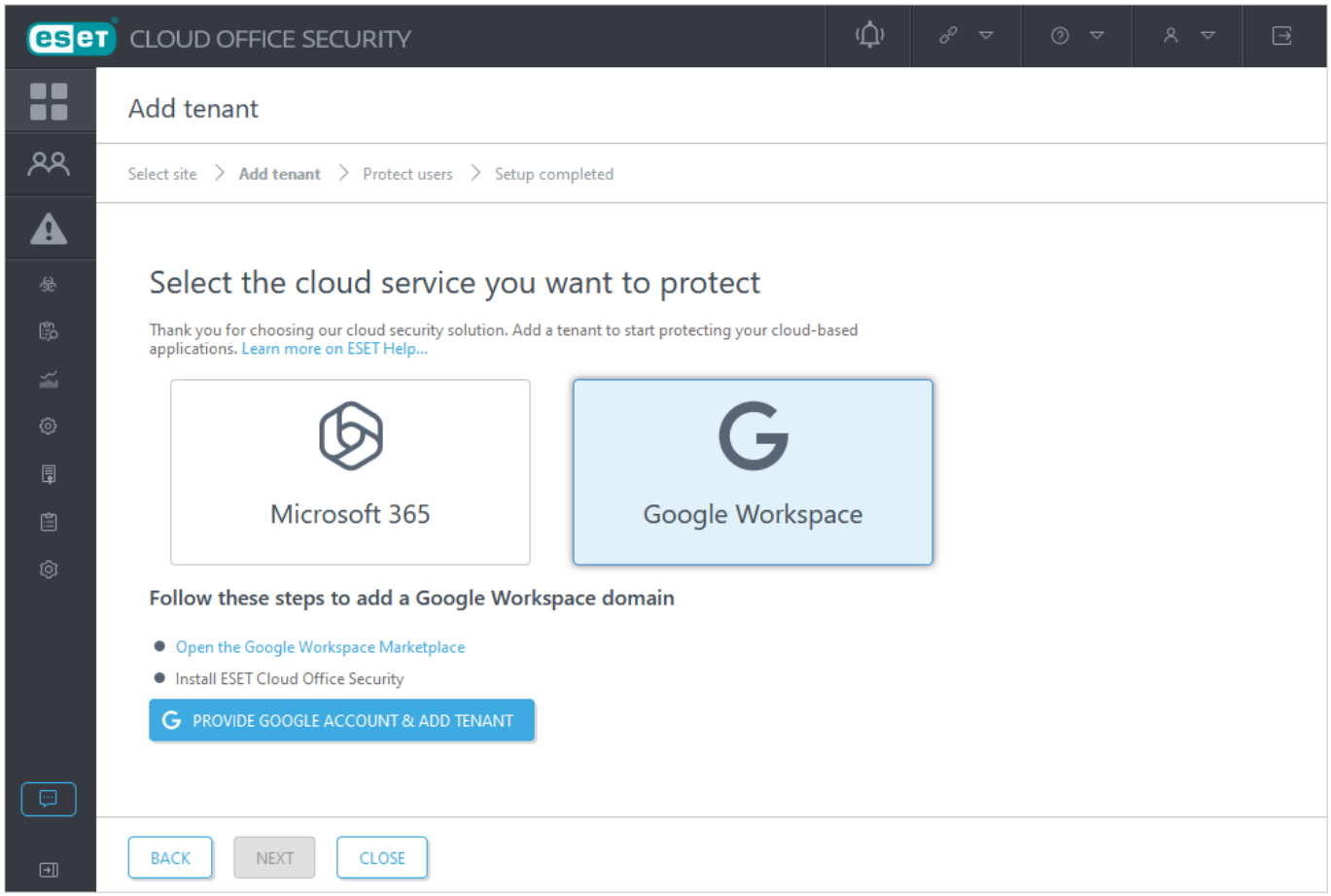
Google Workspace tenant

Integrate your Google Workspace tenant with ESET Cloud Office Security to enable the protection for the Google Workspace users.

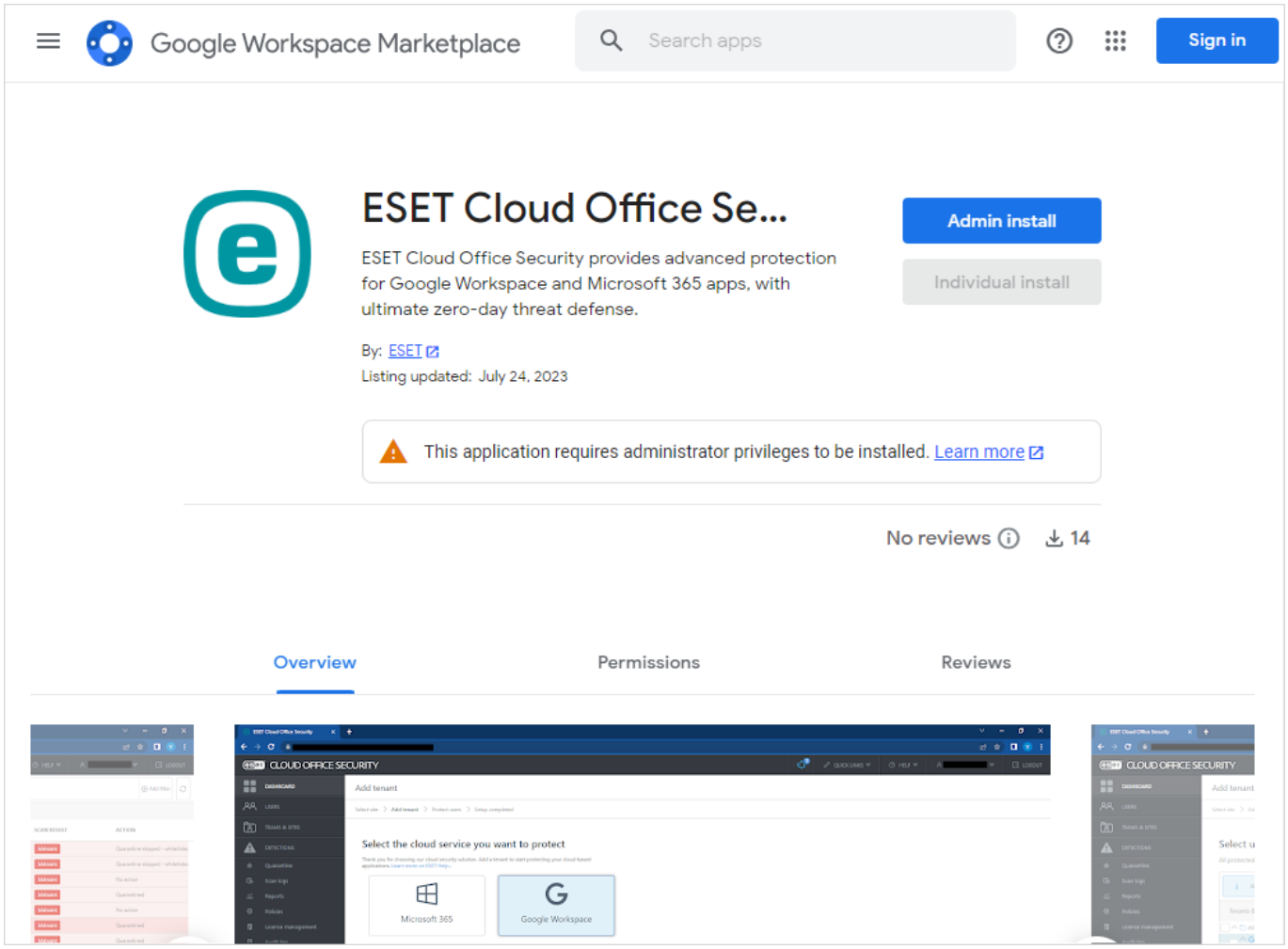
Add tenant

1. Go to **Settings** and click **Add tenant** (or anywhere you see the **Add tenant** button).

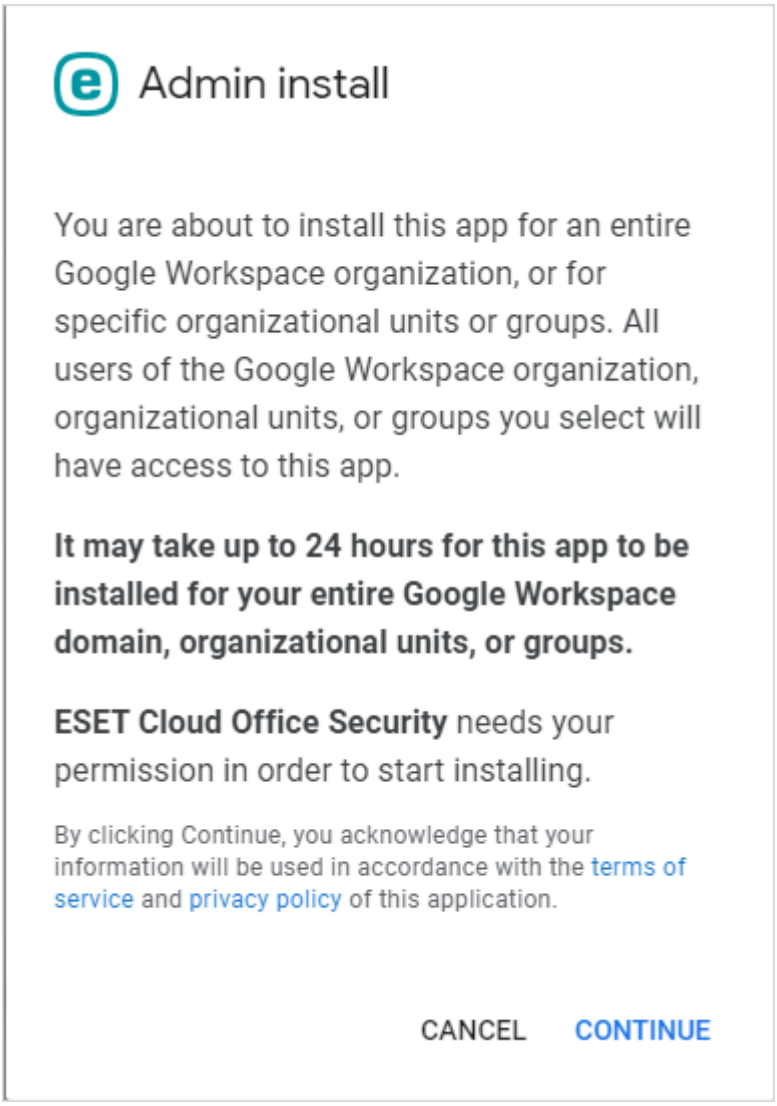
2. Click the **Google Workspace** tile.



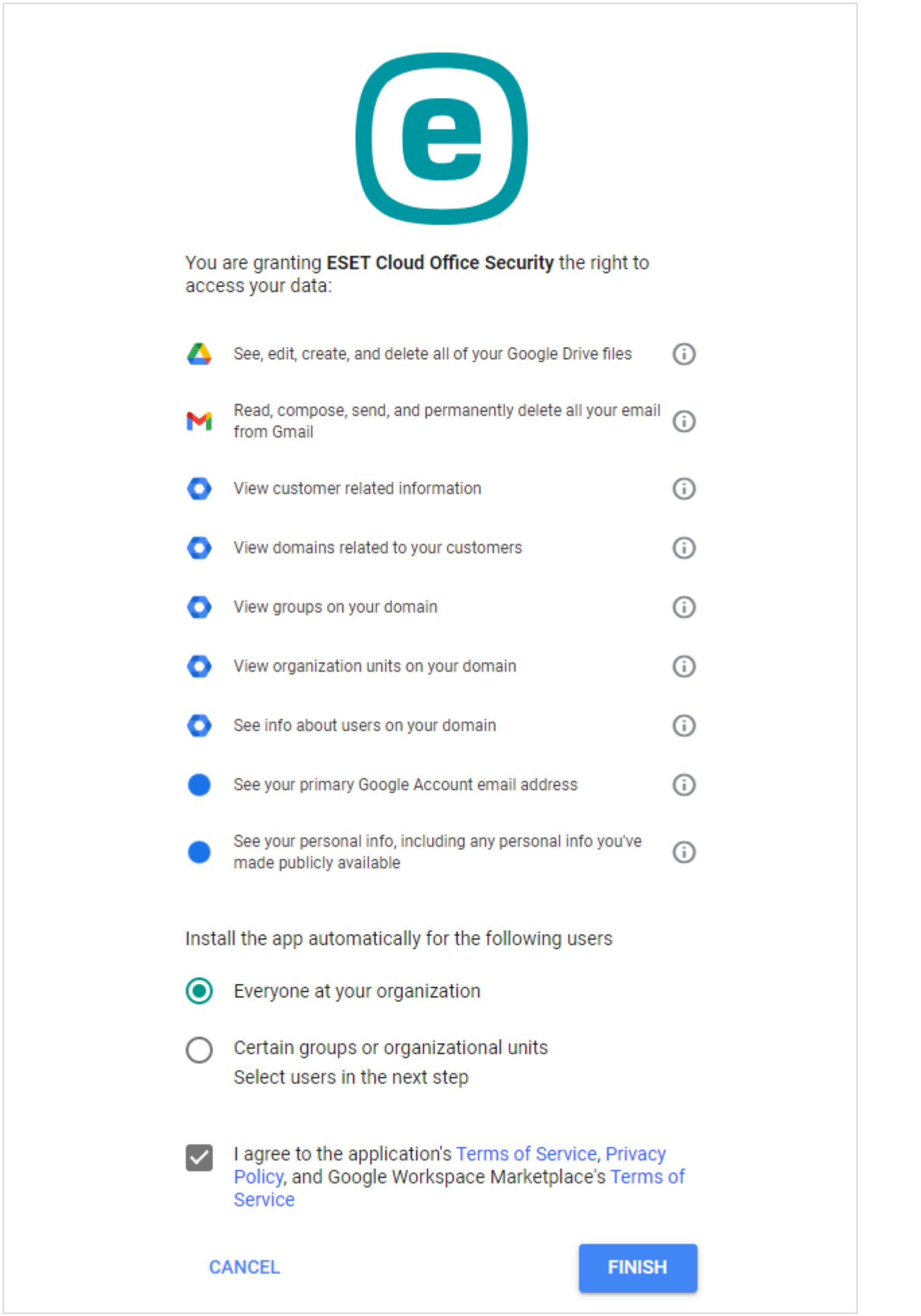
3. Click Open the Google Workspace Marketplace, install the ESET Cloud Office Security app using administrator account. The ESET Cloud Office Security app is currently available on the Google Workspace Marketplace only via the direct link from this wizard.



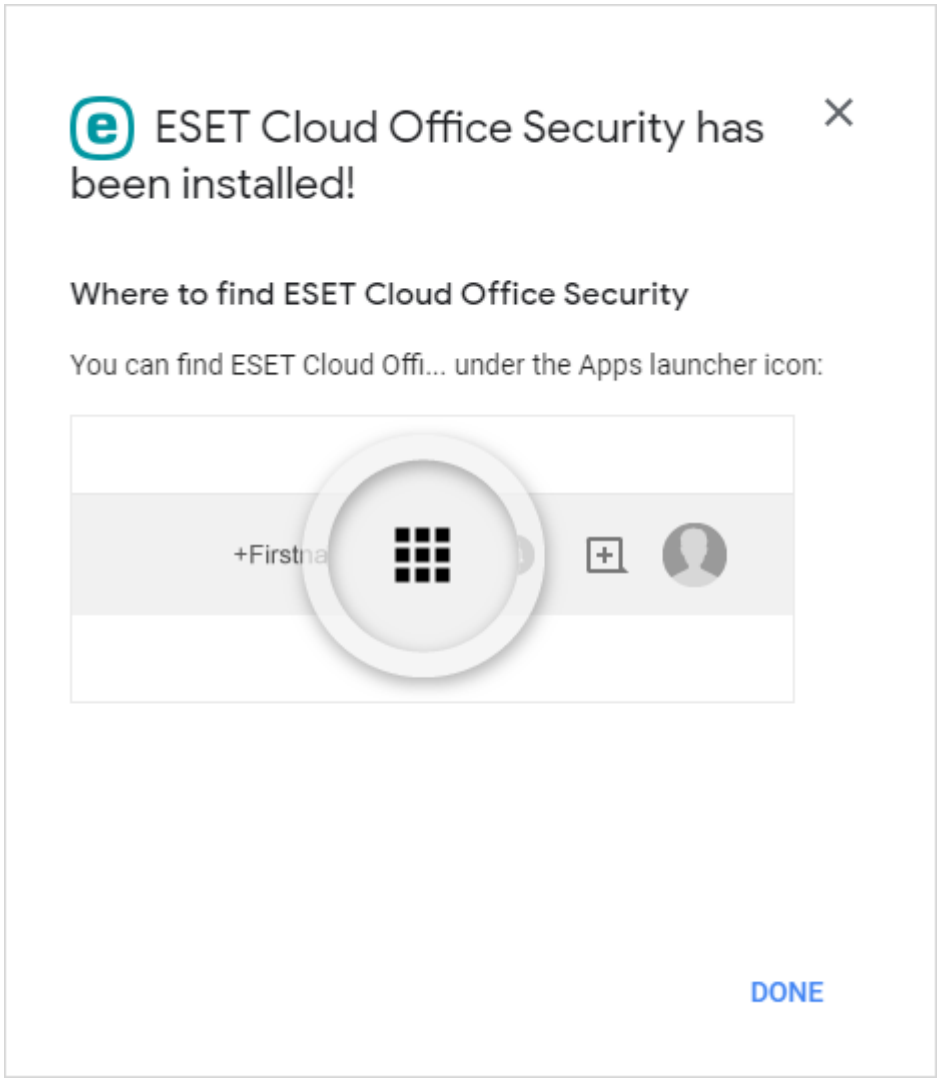
4. Click **Continue** on the **Admin install** screen.



5. Ensure **Everyone at your organization** option is selected on the access rights screen. Also, the Terms of service and Privacy Policy check box should be checked before you click **Finish**.

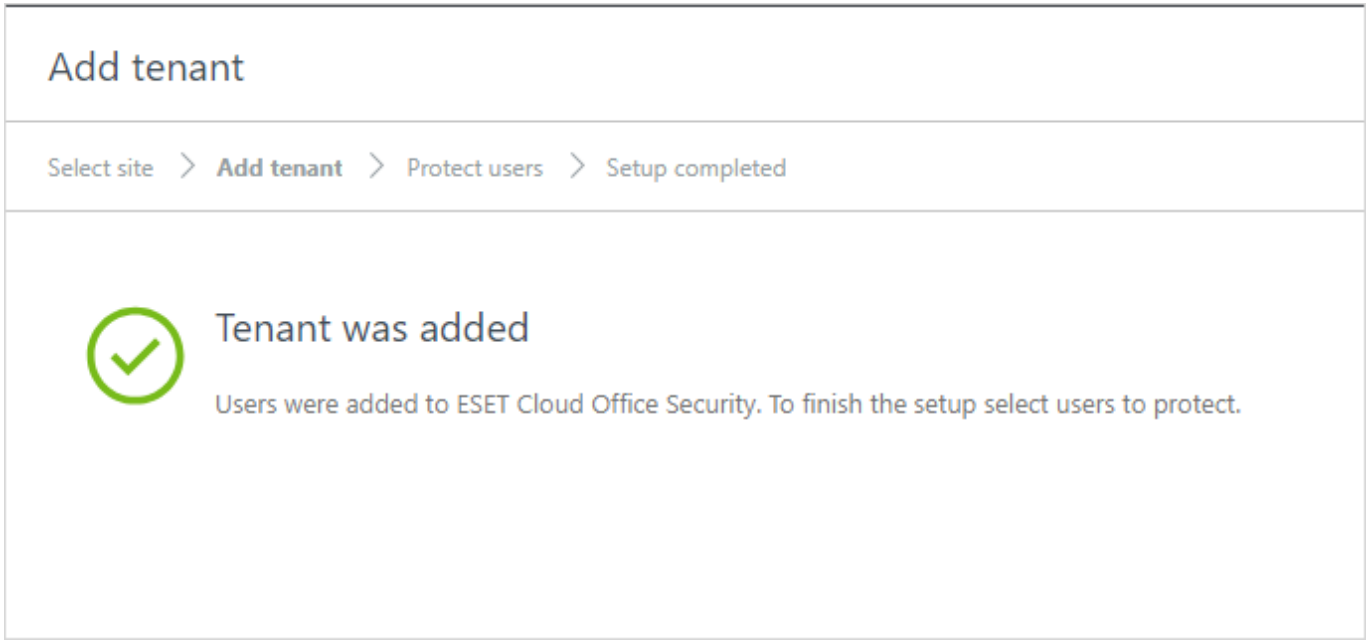

You are granting **ESET Cloud Office Security** the right to access your data:
See, edit, create, and delete all of your Google Drive files
Read, compose, send, and permanently delete all your email from Gmail
View customer related information
View domains related to your customers
View groups on your domain
View organization units on your domain
See info about users on your domain
See your primary Google Account email address
See your personal info, including any personal info you've made publicly available
Install the app automatically for the following users
Everyone at your organization
Certain groups or organizational units
Select users in the next step
I agree to the application's Terms of Service, Privacy Policy, and Google Workspace Marketplace's Terms of Service
CANCEL
FINISH

6. The ESET Cloud Office Security app is installed, click **Done**.

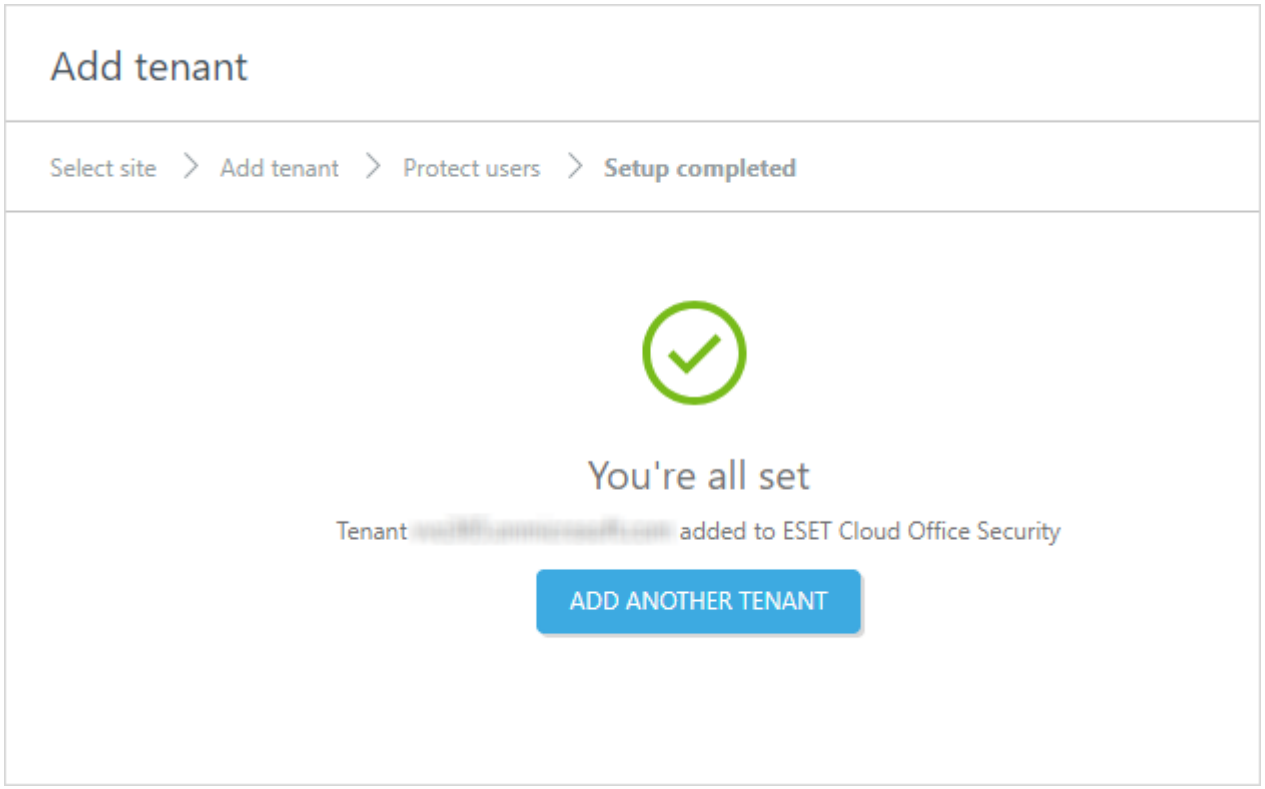


7. After the ESET Cloud Office Security app is completed, return to the ESET Cloud Office Security console. Click **Provide Google account & add tenant** to verify ownership and continue.

8. Your Google Workspace tenant was added, including the users.



9. To finish the setup, click **Next** and select users to **Protect**. Then you are all set.

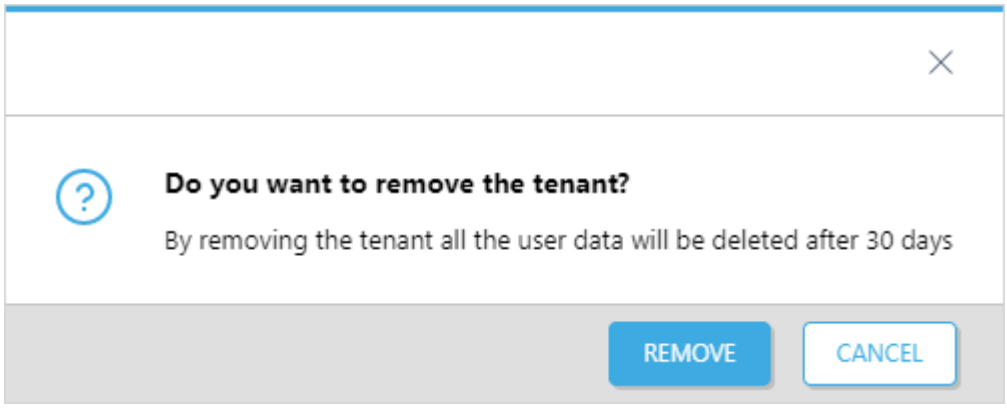


Remove tenant from ESET Cloud Office Security

1. Select **Settings**.

2. Choose the applicable tenant and click **Remove**.

3. A notification window warns you that this process will remove data as described in the Limitations and Data Retention Policy, and users will become unprotected. Click **Remove** to confirm the deletion.



When you remove a tenant from the ESET Cloud Office Security console, tenant data is retained for 30 days (quarantine, Scan logs, and Statistics are deleted after 30 days). If you add the tenant again within 30 days, all the data will be restored. Other objects (tenants, users, groups, sites, reports, policies) are permanently deleted after 90 days. For more information, refer to the Limitations and Data Retention Policy.

Remove ESET Cloud Office Security from Azure portal

1. Sign in to the Azure portal using an administrator account.

To delete an application, you must be listed as an application owner or have administrator privileges.

2. Navigate to the **Azure Active Directory** service and select **Enterprise applications**.

3. Find and click the **ESET Cloud Office Security** application on the overview page, go to **Properties** and click **Delete**.

Navigate the ESET Cloud Office Security

Look at how to navigate your way through the ESET Cloud Office Security interface. You can soon become familiar with the navigational elements and tools of the ESET Cloud Office Security, which aim to be intuitive and easy to use while being interactive.

Use the navigation bar on the left side to switch between different parts of the ESET Cloud Office Security console:

- Users
- Teams & Sites
- Detections
- Quarantine
- Scan logs
- Reports
- Policies
- License management
- Audit log
- Settings

Collapse—Expand and collapse the navigation menu. Collapsing the panel provides more dashboard screen space. To expand the navigation panel, click the icon.

Toolbar at the top is available at all times:

Product navigator—Quick access to ESET consoles and other useful links. (You can see respective products based on your license and access rights).

ESET Business Account and **ESET MSP Administrator** (hybrid licensing account)—If you have the same email address registered in both ESET MSP Administrator and ESET Business Account (single sign-on), you can switch between the ESET Business Account and ESET MSP Administrator view.

Show notifications—To view all notifications, click the bell icon in the top bar.

Quick links—Provides easy access to Add tenant, New policy, ESET Business Account or ESET MSP Administrator.

Help—The first link in this menu always links to Online Help for the current screen. If you cannot resolve a problem, search the ESET Knowledgebase or Support forum. Alternatively, you can Submit feedback or **Submit a sample for analysis**. The About page provides detailed information about the ESET Cloud Office Security version and links to legal documents.

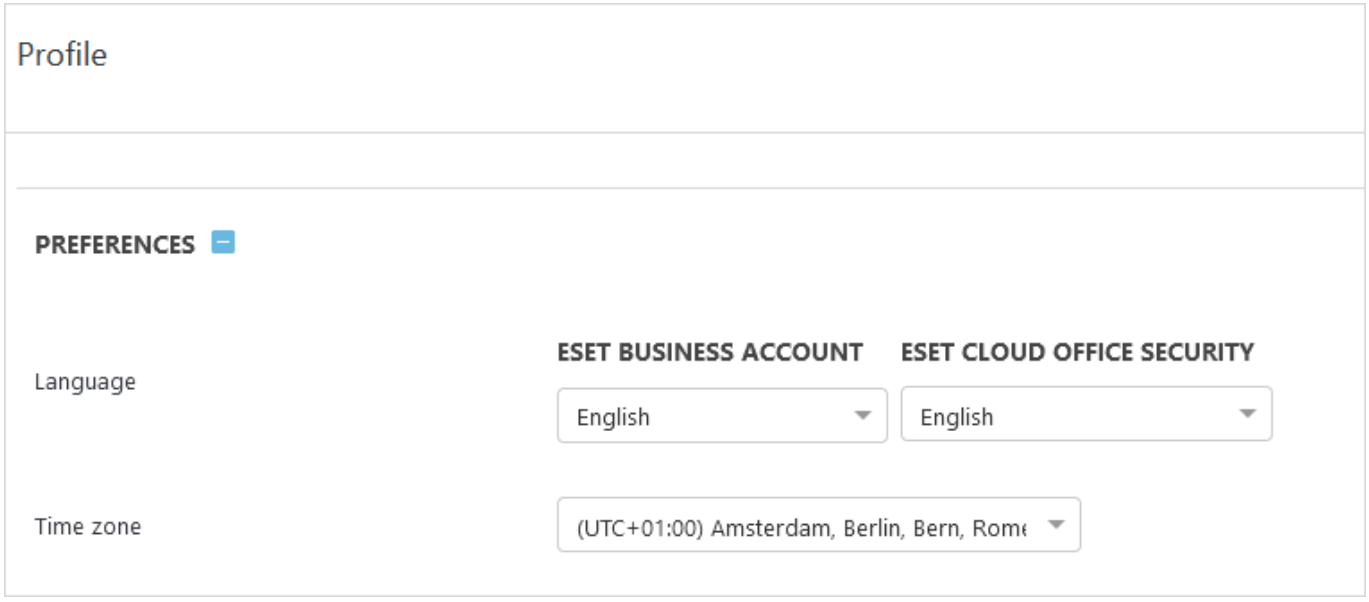
User (currently logged in)—Shows the username. Click **Set theme** and select desired one from the drop-down menu:

- **Default (light) theme**—The ESET Cloud Office Security will use a light color scheme (standard).
- **Dark theme**—The ESET Cloud Office Security will use a dark color scheme (dark mode).
- **Operating system theme**—The ESET Cloud Office Security color scheme is based on your operating system settings.

Logout—Hit this omnipresent pictogram to escape from the ESET Cloud Office Security console.

Change language for ESET Cloud Office Security portal

Log in to ESET Business Account or ESET MSP Administrator, navigate to **User management**, and **Edit** user. Look for ESET Cloud Office Security language setting, change to the preferred language, and click **Save** before leaving the **Profile** screen.



ESET LiveGuard Advanced

ESET LiveGuard Advanced provides another layer of security by utilizing advanced ESET Cloud-based technology to detect the new, never-before-seen type of threats. ESET LiveGuard Advanced gives you the advantage of being protected against consequences caused by new threats. If ESET LiveGuard Advanced detects suspicious code or behavior, it prevents further threat activity by temporarily putting it into quarantine.

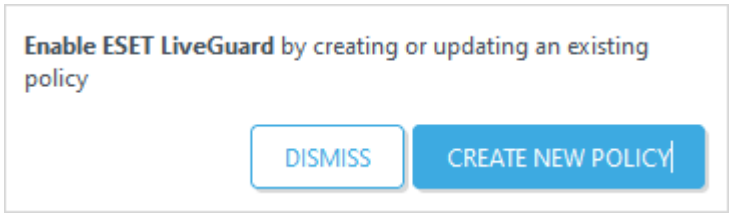
A suspicious sample (file or email message) is automatically submitted to the ESET Cloud, where the ESET LiveGuard Advanced server analyzes the sample using its cutting-edge malware detection engines. While files or emails are in the quarantine, ESET Cloud Office Security is waiting for the results from the ESET LiveGuard Advanced server.

After the analysis is completed, your ESET Cloud Office Security receives a report with a summary of the observed sample's behavior. If the sample proves harmless, it is released from the quarantine. Otherwise, it is kept in quarantine.

ESET LiveGuard Advanced results for samples usually arrive within a few minutes for email messages. However, the default waiting interval is set to 5 minutes. In rare cases, when ESET LiveGuard Advanced results do not arrive within the interval, the message is released. You can change the interval to your preferred time (anything between 5-60 minutes, in one-minute increments).

ESET Cloud Office Security license makes you eligible to use ESET LiveGuard Advanced feature at no extra fee. You will see the ELG label next to the License ID in License management.

When a small pop-up window appears, you can activate ESET LiveGuard Advanced by creating a new policy or updating an existing one.



For more detailed information about ESET LiveGuard Advanced, see How ESET LiveGuard Advanced detection layers work.

Dashboard

The Dashboard is a collection of widgets that provide an overview of Microsoft 365 security activities. The Dashboard provides essential information in each of its overview tabs (Overview, Exchange Online, OneDrive, Team groups, SharePoint sites, Gmail, Google Drive and ESET LiveGuard Advanced). The **Overview** is the main screen of the Dashboard that you see every time you log into the ESET Cloud Office Security console. It displays general and statistical information.

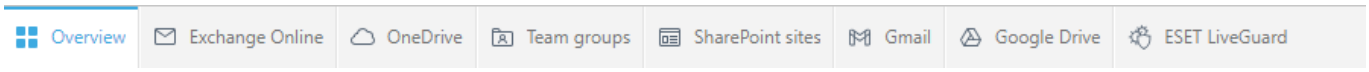
> The Dashboard refresh interval is 10 minutes if you do not see the latest information in your Dashboard, press **F5** to refresh it manually.

To view Dashboard statistics, use filters at the top to choose the applicable **Time period** (Last 24 hours, Last 7, 30 or 90 days) and **Tenant**. Additional detection statistics and graphs are visible in the **Exchange Online**, **OneDrive**, **Team groups SharePoint sites**, **Gmail**, **Google Drive** and **ESET LiveGuard Advanced** overview tabs. These are

statistics such as the number of scanned emails and files and the number of detected spam/phishing/malware. The graphs show the traffic for each detection type—spam, malware, and phishing.

Occasionally, the announcement bar may appear. Colors indicate the announcement type (blue = news, yellow = awareness, red = warning).

Use the Dashboard tabs to switch between the view panes:



Overview

shows
• number of Tenants and License usage
• statistics for each Tenant:
oTotal number of users / Unprotected users
oTop spam / phishing / malware recipients
oTop suspicious OneDrive accounts
oTop suspicious Team groups
oTop suspicious SharePoint sites
drill down
• click the tile Total number of users to open the Users section
• click a user in the statistics section (spam/phishing/malware/OneDrive) to see relevant Detections, or click a group or site to see detections and further details about suspicious Team group or SharePoint site.

Exchange Online

displays
• the overall number of scanned emails
• statistics of detected spam, malware, and phishing emails
• graphs where each represents traffic of spam, malware, and phishing
The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

OneDrive

displays
• the number of protected users
• the overall number of scanned files
• statistics of detected malware
• a graph that represents malware traffic
The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

Team groups

displays
• the number of protected groups
• the overall number of scanned files
• statistics of detected malware
• a graph that represents malware traffic
The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

SharePoint sites

displays
- the number of protected sites
- the overall number of scanned files
- statistics of detected malware
- a graph that represents malware traffic

The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

Gmail

displays
- the overall number of scanned emails
- statistics of detected spam, malware, and phishing emails
- graphs where each represents traffic of spam, malware, and phishing

The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

Google Drive

displays
- the number of protected users
- the overall number of scanned files
- statistics of detected malware
- a graph that represents malware traffic

The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

ESET LiveGuard Advanced

displays
- submitted files (the count includes duplicates, and the number may be higher than unique files)
- number of detections
- average analysis time
- a graph that represents submitted files
- top submitted files owners
- submitted file types

The tiles are interactive. Click a tile of interest and get to the relevant section within the ESET Cloud Office Security console. For example, the Scan logs section with relevant log records opens.

Users

The central entity that ESET Cloud Office Security protects is the user account. Double-click a user to find useful information such as the Overview, Settings defined by Policies, list of Policies assigned to the user, and Detections for Gmail, Google Drive, Exchange Online and OneDrive. You can also choose which users will be Protected or Unprotected. Users are sorted into groups, and each group is an Microsoft 365 tenant containing its users. To make searching for a specific user within a group easier, you can use filtering with multiple criteria.

> Users without Microsoft 365 license will not be shown in the ESET Cloud Office Security console by default. This includes shared mailboxes without a Microsoft 365 license.
> If you want to see and manage all Microsoft 365 users, navigate to Settings and disable Microsoft 365 licensed users.

Protection status:

Status	Description
Unprotected	A user is currently not being protected.
Auto protected	Protected user with auto-protection.
Pending	Transitional state that occurs during the process of protecting a user. Once it finishes, the user's status changes to Protected.
Protected	User's Mailbox and OneDrive are being protected by the Default or a Custom policy.
Warning	The process of protecting a user was unsuccessful. The error might have occurred for one of the resources, Mailbox or OneDrive. Likely, both resources are not available for the user. Check if the user has a valid Microsoft 365 license assigned.

Navigate within the tree to see users of a specific tenant or group. To see all users in every tenant and group, click **All**.

For more detailed information, double-click a user, click the icon, and select an action (**Show details**, **Protect** or **Unprotect**). Click a user to open the **Show details** window that consists of four parts:

Action	Usage
Overview	Shows necessary information about the user loaded from Microsoft 365 (Email, Group membership, Job title, etc.). Also, a current Protection status for Mailbox and OneDrive is shown.
Configuration	Contains a read-only list of Settings and assigned Policies for this user. Switch between the tabs to view the configuration or a list of assigned policies. You cannot modify Settings or assign Policies to users, go to the Policies section instead.
Detections	Show all detections for this user account (Gmail, Google Drive, Exchange Online or OneDrive).
Quarantine	Show all quarantine emails and files store from this user. You can also use an action: Release, Download, or Delete quarantine emails or files.

You can filter users by several criteria. Click **Add filter** and select a filter type from the drop-down menu or type a string (repeat when combining multiple criteria):

Add filter	Usage
Protection Status	Select Protected, Unprotected, Warning, or Pending status of a user.
Auto protected	Show automatically protected users only.
Name	Type a valid username.
Email	Type a valid user email.
Type	Select the user type (Unknown, User, Linked, Shared mailbox, Room, Equipment, Others).

Protect users

1. Select **Users** who will be protected, and click **Protect**.
2. Select the **License pool** loaded from ESET Business Account and click **OK**. The Default policy now protects selected users.
3. If required, specify a custom policy for users in the Policies section.

Unprotect users

Select **Users** who will be unprotected, and click **Unprotect**.

Teams & Sites

ESET Cloud Office Security provides protection for Team groups or SharePoint sites.

Switch between Team groups and SharePoint sites tabs. It displays a list of Team groups or SharePoint sites for each tenant.

Team groups

displays objects that are Microsoft 365 group type, including its default SharePoint team site and OneDrive:

- name
- status
- email
- tenant

To protect Team groups, Scan logs at least one member is a protected user by ESET Cloud Office Security. Each Microsoft 365 group has a default SharePoint team site and OneDrive which are also protected.

SharePoint sites

displays all SharePoint root sites not associated with Microsoft 365 group:

- name
- status
- URL
- tenant

SharePoint sites are protected automatically, including their Subsites (not shown).

For more detailed information, click a Team group or SharePoint site to open the **Show details** window that consists of four parts:

Action	Usage
Overview	Shows necessary information about the Team groups or SharePoint sites loaded from Microsoft 365 (Email, Owner, Members, Author, URL, etc.). Also, a current Protection status for Team group or SharePoint site is shown.
Configuration	Contains a read-only list of Settings and assigned Policies. Switch between the tabs to view the configuration or a list of assigned policies. You cannot modify Settings or assign Policies, go to the Policies section instead.
Detections	Show all detections for Team group or SharePoint site.
Quarantine	Show all quarantined files. You can also use an action: Release, Download, or Delete quarantined files.

Click **Add filter** to filter Team groups or SharePoint sites.

Detections

Lists all detections by ESET Cloud Office Security. Use the tabs to switch between Gmail, Google Drive, Exchange Online, OneDrive, Team groups, and SharePoint sites. View information on each detection, for example, detected files that were uploaded to a Team group in the Team groups tab.

Click the icon to open a sidebar with a summary of a specific log record (detection). For more detailed information, click the icon and select **Show details**.

Navigate within the tree to see detections only for a specific tenant or group. To see all detections in every tenant and group, click **All**. To make searching for a specific detection easier, you can filter using multiple criteria. Click **Add filter** and select the filter type from the drop-down menu or type a string (repeat when combining criteria):

Add filter	Usage
Occurred from	Specify a "date from" range.
Occurred to	Specify a "date to" range.
Subject	Applies to messages which contain or do not contain a specific string (or a regular expression) in the subject.
Message-ID	Filter email messages by unique Message-ID when searching for a specific message, especially in large logs with many messages or multiple delivery attempts.
From	Filter messages by a specific sender.
To	Filter messages by recipients.
Mailbox	Applies to messages located in a specific mailbox.
Scan result	Select one of the following options: Malware, Malware (detected by ESET LiveGuard Advanced), Phishing or Spam.
Action	Select one of the available actions.
Team	Type the valid team name.
Site	Type the valid site name.
Object	Type a valid object name.
Detection	Type a valid detection name.
Hash	Type a valid detection hash.

When you click the icon, an option **Remove whitelisted** will be available if you have whitelisted a file previously by releasing it from Quarantine for the same user. Use this option to remove a file from the whitelist. All such future files will be quarantined.

The retention period for detections is 90 days. Records older than 90 days will be removed permanently.

Report false positive (FP) / false negative (FN)

You can manually report FP and FN detections for Spam, Phishing, or Malware by sending a sample to ESET labs for analysis. Email addresses to send the samples to:

Spam - send an email to nospam_ecos@eset.com for emails incorrectly marked as spam or to spam_ecos@eset.com for undetected spam with the original message as an attachment in *.eml* or *.msg* format.

Phishing - to report false positive or negative phishing classification, create a new email message to be sent to samples@eset.com with *'phishing email'* in the subject line and include the phishing email as an attachment in

.eml or *.msg* format.

Malware - for false positive or negative classification of malware, create a new email message to be sent to samples@eset.com with *'False positive'* or *'Suspected infection'* in the subject line and include the file(s) compressed into a *.zip* or *.rar* format as an attachment.

Reports

ESET Cloud Office Security reports keep you informed with an overview of ESET Cloud Office Security protection statistics. You can choose from two types of reports, Statistical reports or Mail Quarantine reports.

Statistical reports contain information about Gmail, Google Drive, Exchange Online, OneDrive, Team groups, and SharePoint sites protection, including the number of scanned emails, files, detected malware, phishing, and spam for the specified period. The reports can be manually generated and downloaded in *PDF* or *CSV* format or scheduled and be delivered to selected recipients via email. *PDF* output format presents data in a graph form, shows the long-term average for comparison, and includes traffic information for each protection type, top recipients of malware, phishing, and spam.

Mail Quarantine report contains a list of newly quarantined objects. The report is delivered to selected recipients via email. The recipients can release spam messages (if considered safe or legitimate) by clicking the link **Release**. Applies to spam only; other types of quarantined objects cannot be released.

You can access the statistics via email, no need to log into the ESET Cloud Office Security console. Set up and schedule recurring reports and specify email recipients. In addition, you can generate report statistics immediately from within the ESET Cloud Office Security console. Select an existing report (can also be a scheduled report) and click **Generate & Download**. Right-click with the drop-down menu works as well. You can easily create a new report template with custom settings.

New report

Click New report to open a report template and specify custom settings. Type a report Name and Description.

Language

Choose desired language from the drop-down menu. The report will be generated in the selected language.

Type

Select what type you want to have included in the statistics.

Statistical reports

Create either scheduled or On-demand reports consisting of information according to options you choose.

Mail Quarantine reports

To inform users about their newly quarantined email messages, send notification emails to selected users. You can assign single or multiple recipients or a group. Choose an interval for the reports and starting date and time. If it is a repeated report, choose when it should end (on a date, after several occurrences, or never). Mail Quarantine report is triggered only when there are new items. The report recipients can release spam messages (if considered safe or legitimate) by clicking the link Release (a confirmation window opens in a web browser). The released spam message is delivered in a separate email as an attachment.

Tenant

This option is available for a multitenant environment. You can select multiple tenants for which to generate statistics. The report will be generated for each tenant separately and delivered in one ESET Cloud Office Security report email with multiple attachments.

Time period

Define the time period you want the results to be displayed (last 24 hours, week, month). When you select Custom, you can specify a range (Date from and Date to).

Output

Select the appropriate file format, and you can choose *PDF* or *CSV*. *PDF* format includes data shown in graphs. *CSV* is suitable as raw data. Reports will be collected according to specified options. If you make multiple selections (Exchange Online, OneDrive, Team groups, or SharePoint sites, Gmail, Google Drive), the output file would be an archive in a ZIP format containing *PDF* or *CSV* report files.

Whitelabel

If you require your company's logo to appear on the report, enable this feature. You have the option to choose a co-branded report header showing your logo along with the ESET logo or your logo only. Upload the logo in *PNG* or *JPEG* format.

Scheduled

Use the scheduler to generate the reports on a specified date and time, also as a recurring event. Scheduled reports are delivered to selected recipients, who will receive ESET Cloud Office Security report email with attachment(s).

Repeat

Choose if you want the report to be generated once or repeatedly:

- **Once**—The report will be performed only once.
- **Daily**—The report will be generated and delivered repeatedly, every day (unless you specify recurrence to end after occurrences).
- **Weekly**—The report will be generated and delivered repeatedly on the selected day(s) of the week.
- **Monthly**—The report will be generated and delivered once a month on a specified day.

Starting from

Choose starting date for the reports.

Ends

Select when the recurrence interval ends.

Recipients

Specify the report recipient's email address, hit enter to confirm. Repeat to add multiple recipients.

For detailed information or actions, click the icon and select an action:

Action	Usage
Show details	Displays detailed information about a report.
Generate & Download	Click Generate & Download and choose *PDF* or *CSV*. *PDF* format includes data shown in graphs. *CSV* is suitable as raw data. Reports will be collected according to specified options. If you selected both Exchange Online, OneDrive, Team groups, or SharePoint sites, the output file would be an archive in a *ZIP* format containing PDF or *CSV* report files.
Edit	Edit configuration of an existing report.
Delete	Remove selected report completely.

To filter reports, click **Add filter** and select a filter type from the drop-down menu or type a string (repeat when combining multiple criteria):

Add filter	Usage
Name	Type partial or full report name.
Scheduled	Select Not scheduled, Once, Daily, Weekly, or Monthly.
Data	Select Exchange Online, OneDrive, Team groups, or SharePoint sites to filter by data.

Quarantine

Simple management of objects (emails and files) that were quarantined by ESET Cloud Office Security. Switch between Gmail, Google Drive, Exchange Online, OneDrive, Team groups and SharePoint sites using the tabs. You can see substantial information on each object.

Click the icon to open a sidebar with a summary of a specific object. For more detailed information, click the icon and select **Show details**.

Navigate within the tree to see objects only for a specific tenant or group. To see all detections in every tenant and group, click **All**.

Inspect quarantined email messages or files and take action (**Delete** or **Release**). You can also **Download** Original file or Password protected archive in *.zip* format.

> When you consider a detection not malicious (false positive), you can **Release** a file from Quarantine. The released file is automatically put to a whitelist based on the hash. All future occurrences of the same file for the same user will not be detected as suspicious and will not be quarantined. Automatic whitelisting is done per user. For other users, the same file is still going to be detected as suspicious and quarantined. You can remove a file from the whitelist in the Detections list by using **Remove whitelisted** option.

Click the icon and select an action:

Action	Usage
Show details	Shows more detailed information about the quarantined email message.
Release (emails or files)	Releases email to its original recipient(s) in the form of a notification email from Quarantine with the original message as an attachment. In the case of a OneDrive item, the file will be uploaded to its original location in the user's OneDrive. When releasing a file from a Team group or SharePoint site, the file will appear back in its original location. The released file is automatically put to a whitelist based on the hash. This prevents the file from being quarantined again.

Action	Usage
Delete	Deletes item from quarantine.
Download Original file	Download not protected file in its original form.
Download Password protected archive	Download protected archive by a password.
Submit sample	The sample submission dialog enables you to send a suspicious file or spam to ESET for analysis. Choose a Reason for submitting sample from the drop-down menu.

To make searching for a specific quarantined object easier, you can filter using multiple criteria. Click **Add filter** and select filter type from the drop-down menu or type a string (repeat when combining criteria):

Add filter	Usage
Occurred from	Specify a "date from" range.
Occurred to	Specify a "date to" range.
Subject	Applies to messages which contain or do not contain a specific string (or a regular expression) in the subject.
Message-ID	Filter email messages by unique Message-ID when searching for a specific message, especially in large logs with many messages or multiple delivery attempts.
From	Filter messages by a specific sender.
To	Filter messages by recipients.
Mailbox	Applies to messages located in a specific mailbox.
Scan result	Select one of the following options: Malware, Malware (detected by ESET LiveGuard Advanced), Phishing or Spam.
Team	Type the valid team name.
Object	Type a valid object name.
Site	Type a valid site name.

The retention period for quarantined objects is 30 days. Objects older than 30 days will be removed from quarantine permanently.

Scan logs

Lists all scan results by ESET Cloud Office Security. Logs are similar to Detections, but additionally, you can have clean objects included in the list (enable the Log all objects setting in policies). Switch between Gmail, Google Drive, Exchange Online, OneDrive, Team groups, SharePoint sites, and Submitted files using the tabs. You can see a substantial amount of information for each detection. Submitted files is a list of files sent to ESET LiveGuard Advanced for analysis.

Click the icon to open a sidebar with a summary of a specific log record. For more detailed information, click the three dots icon and select **Show details**.

Navigate within the tree to see log records only for a specific tenant or group. To see all detections in every tenant and group, click **All**.

If a scan result is **Not scanned**, the reason may vary. See Limitations for details.

When you click the gear icon in the upper-right corner to access **Export to CSV** from the context menu, you

can export the table grid to *CSV* format and use it in other applications to work with the list.

To make searching for a specific log record easier, you can filter using multiple criteria. Click **Add filter** and select the filter type from the drop-down menu or type a string (repeat when combining criteria):

Add filter	Usage
Occurred from	Specify a "date from" range.
Occurred to	Specify a "date to" range.
Data source	Select one of the following options: Exchange Online, OneDrive, Team group and SharePoint site.
Mailbox	Applies to messages located in a specific mailbox.
From	Filter messages by a specific sender.
To	Filter messages by recipients.
Subject	Applies to messages that do or do not contain a specific string in the subject.
Message-ID	Filter email messages by unique Message-ID when searching for a specific message, especially in large logs with many messages or multiple delivery attempts.
Scan result	Select one of the following options: Malware,  Malware (detected by ESET LiveGuard Advanced), Phishing, Spam, Clean, Not scanned, Error, or Disabled.
Action	Select one of the available actions.
Owners	Type the valid owner name.
Object	Type a valid object name.
Detection	Type a valid detection name.
Hash	Type a valid detection hash.
Team	Type a valid team name.
Site	Type a valid site name.

There is a 90-day retention period for log records. Records older than 90 days will be removed permanently. If you have a policy that uses **Log all objects**, retention for the log records with a **Clean** scan result is 3 days. Clean scan results older than 3 days will be removed permanently.

Policies

Larger organizations usually have multiple departments and want to configure different protection settings for each organizational unit. ESET Cloud Office Security provides policy-based protection settings that you can customize and assign to selected Users and user Groups, Tenants, Team groups, or SharePoint sites.

To add filtering criteria, click **Add filter**, select the applicable item **Name** and type a valid policy name. The Policies tree shows Tenants and their user Groups, Team groups, or SharePoint sites, including a **Not assigned** group containing custom policies that are not assigned to a target.

You can add a new policy or modify an existing policy and its settings:

1. Click **Policies** > **New policy**.

2. Type a **Name** and **Description** for a new policy.

3. Select a target and configure a policy for:

   - **Tenants**—Gmail, Google Drive, Exchange Online, OneDrive, SharePoint sites, and Team groups protection

and assign it to selected Tenants

- **Users**—Gmail, Google Drive, Exchange Online and OneDrive protection, and assign it to selected users or a user Group(s)

- **Team groups**—Team groups protection and assign it to selected Team groups

- **SharePoint sites**—SharePoint sites protection and assign it to selected sites

4. Customize protection **Settings** for Exchange Online, Gmail, OneDrive, Google Drive, Team groups, SharePoint sites or ESET LiveGuard Advanced and click **Next**.

5. Click **Assign** and choose a target where the policy will be assigned.

6. Click **Save changes** to save the policy setting.

Policy principles

Default policy: • Applies to all users (protected and unprotected) • Cannot be modified or deleted
A custom policy can be assigned to: • **Users**—applies to manually selected individual users • **Groups**—applies to all members of the user Group • **Tenants**—applies to all entities within the Tenant • **Team groups**—applies to a Team group • **SharePoint sites**—applies to a SharePoint site
A custom policy assigned to a **Tenant** or **Group** is merged with the default policy. A custom **Tenant policy**, **Group policy**, **Team groups policy**, or **SharePoint sites policy** has priority over the default policy. A custom policy assigned to a **user** is merged with the **Tenant**, **Group**, **Team groups**, **SharePoint sites policy**, and the default policy. A custom **User** policy has priority over a Tenant or Group policy and a default policy. However, when a user uploads a file to the Team group or SharePoint site, policy for the Team group or SharePoint site is applied.
Users and Tenants can be assigned multiple **custom policies**, but the effective policy is calculated based on the priority (order).

Setting for Anti-Spam lists when merging policies

The merging option applies to Anti-Spam lists and Notify administrator settings (addresses for notification emails by antimalware and anti-phishing).
When you have multiple policies with Anti-Spam lists (Approved, Blocked, and Ignored lists of IP addresses, domains or email addresses) or antimalware and anti-phishing administrator addresses for notification emails, choose the merging strategy:
Replace—keep only the new list entries (default option). The new list entries of the current policy replace all lists from the previous policies.
Append—extend lists of the previous policies by appending new entries. Merge lists from the previous policies with new entries of the current policy. The new entries are placed at the end (bottom) of the existing lists of the previous policies.

Before the merging option became available, the default behavior was **Replace**. If you already use policies with specific Anti-Spam lists, you can keep the default **Replace** or change to **Append** if preferable.

Create a new policy with a defined Anti-Spam list, and select the merging option (assuming existing policies with Anti-Spam lists are in place).
1. Click **Policies** > **New policy**.
2. Type a **Name** and **Description** for the new policy, select **Tenants** as a target and click **Next**.
3. Expand **Exchange Online Anti-Spam** and click **Edit** next to the Blocked IP list.
4. Click **Add**, type the IP address, press the **Enter** key to complete the action (alternatively, import the list from a file) and click **Save changes**.
5. Choose **Append** as a merging option from the drop-down menu, and click **Next**.
6. Click **Assign**, choose **Assign to tenants** from the drop-down menu, select the check box next to the Tenant and click **OK**.
7. Click **Save changes** to finish the process.

To rearrange policy priority, click **Change order**. Select a policy or multiple policies, and click **Apply sooner** or **Apply later** to change their priority. Policies are applied globally (regardless of assignment–Tenant, Group, or User) in specified order from top to bottom. The default policy is always applied first.

To perform the following actions, select the policy and click the three dots icon :

Action	Usage
Show Details	Display detailed information about a created policy, settings, and to whom the policies are assigned.
Edit	Modify the configuration of an existing policy.
Assign	Select Users, Tenants, Team groups, or SharePoint sites to which the policy applies.
Duplicate	Create a new policy based on the selected template. A new name will be required for the duplicate policy.
Delete	Remove the selected policy completely.

Create a custom tenant policy to see all scan results (including clean) in Scan logs. The tenant policy applies to all users (protected and unprotected).

1. Click **Policies** > **New policy**.
2. Type a **Name** and **Description** for the new policy, select **Tenants** as a target and click **Next**.
3. Expand **Exchange online general** and click the toggle to enable **Log all objects**.
4. Expand **OneDrive general** and click the toggle to enable **Log all objects**.
5. Expand **Team groups general** and click the toggle to enable **Log all objects**.
6. Expand **SharePoint sites general** and click the toggle to enable **Log all objects** and click **Next**.
7. Click **Assign**, select the check box next to the Tenant and click **OK**.
8. Click **Save changes** to finish the process.

Create a custom policy for specific users with advanced settings that will affect how Malware, Spam, and Phishing are handled. With this policy in place, email attachments that contain malware will be deleted, spam messages will be moved to the user's junk folder, phishing emails will have their subjects tagged and put into quarantine and contents of malware files located on OneDrive will be replaced with plain text to prevent any harm.

1. Click **Policies** > **New policy**.
2. Type a **Name** and **Description** for the new policy, select **Users** as a target, and click **Next**.
3. Expand **Exchange Online Anti-Malware** and use the drop-down menu next to **When items are reported** to select **Delete attachment**.
4. Expand the **Exchange Online Anti-Spam** and use the drop-down menu next to **When items are reported** to select **Move to Junk**.
5. Expand the **Exchange Online Anti-Phishing** and click the toggle to enable the **Tag subject**. You can also change the **Tag subject text** to customize it.
6. Expand the **OneDrive Online Anti-Malware**, use the drop-down menu next to **When items are reported** to select **Replace** and click **Next**.
7. Click **Assign**, select check boxes next to the users you want to apply the policy to, and click **OK**. If a user has an existing custom policy applied, it will be overwritten with the new one.
8. Click **Save changes** to finish the process.

Protection settings for Exchange Online

This section provides information about changing Exchange Online general, Anti-Malware, Anti-Spam or Anti-Phishing settings and options.

Exchange Online general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about ESET LiveGrid® in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in Scan logs. The retention policy for clean scan results is three days. Scan results older than three days will be removed permanently.

Exchange Online Anti-Malware

Enable Exchange Online Anti-Malware
This feature is active when enabled, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, and the email is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it is sent as an attachment in a new email and delivered to the recipient.
- **Delete attachment**—The message attachment is deleted and will be delivered to the recipient without the attachment.
- **Replace attachment**—The attachment is replaced with a text file that contains detailed information about the action taken.
- **Quarantine attachment**—The attachment is removed from the email and placed into the file quarantine.

Attachment replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
Notify mailbox owner
When enabled, the user will receive a notification email when a detection is found.
Language
Choose a desired language from the drop-down menu. The mailbox owner will receive notification emails in the selected language when an object is released from Exchange Online quarantine. This option overrides the default tenant language in settings.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Exchange Online Anti-Spam

Enable Exchange Online Anti-Spam
This feature is active when enabled, and you can configure detailed options.
When items are reported
- **No action**—No action is performed, and the email is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it will be sent as an attachment in a new email and delivered to the recipient.

Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
You can configure **Approved**, **Blocked** and **Ignored** lists by specifying criteria such as IP address or range, domain name, etc. To add, modify or delete criteria, click **Edit** for the list you want to manage. Alternatively, you can import your custom list from a file instead of manually adding every entry, click **Import** and browse for your (*.txt*) file containing entries you want to add to the list. Likewise, if you need to export your existing list to a (*.txt*) file, select **Export** from the context menu.

Approved IP list	Automatically whitelists emails originating from specified IP addresses. Email content will not be checked.
Blocked IP list	Automatically blocks emails originating from specified IP addresses.
Ignored IP list	List of IP addresses that will be ignored during classification. Email content will be checked.
Approved senders list	Whitelists emails originating from a specified sender or domain. Only one sender address or a whole domain is used for verification based on the following priority: 1.SMTP 'MAIL FROM' address 2."Return-Path:" email header field 3."X-Env-Sender:" email header field 4."From:" email header field 5."Sender:" email header field 6."X-Apparently-From:" email header field
Blocked senders list	Blocks emails originating from a specified sender or domain. All identified sender addresses or whole domains are used for verification: SMTP 'MAIL FROM' address "Return-Path:" email header field "X-Env-Sender:" email header field "From:" email header field "Sender:" email header field "X-Apparently-From:" email header field

Exchange Online Anti-Phishing

Enable Exchange Online Anti-Phishing
This feature is active when enabled, and you can configure detailed options.
When items are reported
- **No action**—No action is performed, and an email with a malicious attachment is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it will be sent as an attachment in a new email and delivered to the recipient.

Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
Notify mailbox owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) that will receive notification emails whenever a detection is found for any Exchange Online user.

Protection settings for Gmail

This section provides information about changing Gmail general, Anti-Malware, Anti-Spam or Anti-Phishing settings and options.

Gmail general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about ESET LiveGrid® in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in Scan logs. The retention policy for clean scan results is three days. Scan results older than three days will be removed permanently.

Gmail Anti-Malware

Enable Gmail Anti-Malware
This feature is active when enabled, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, and the email is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it is sent as an attachment in a new email and delivered to the recipient.
- **Delete attachment**—The message attachment is deleted, and the message will be delivered to the recipient without the attachment.
- **Replace attachment**—The attachment is replaced with a text file that contains detailed information about the action taken.
- **Quarantine attachment**—The attachment is removed from the email and placed into the file quarantine.

Attachment replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
Notify mailbox owner
When enabled, the user will receive a notification email when a detection is found.
Language
Choose a desired language from the drop-down menu. The mailbox owner will receive notification emails in the selected language when an object is released from quarantine. This option overrides the default tenant language in settings.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Gmail Anti-Spam

Enable Gmail Anti-Spam
This feature is active when enabled, and you can configure detailed options.
When items are reported
- **No action**—No action is performed, and the email is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it will be sent as an attachment in a new email and delivered to the recipient.

Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
You can configure **Approved**, **Blocked**, and **Ignored** lists by specifying criteria such as IP address or range, domain name, etc. To add, modify or delete criteria, click **Edit** for to the list you want to manage. Alternatively, you can import your custom list from a file instead of manually adding every entry, click **Import** and browse for your (*.txt*) file containing entries you want to add to the list. Likewise, if you need to export your existing list to a (*.txt*) file, select **Export** from the context menu.

Approved IP list	Automatically whitelists emails originating from specified IP addresses. Email content will not be checked.
Blocked IP list	Automatically blocks emails originating from specified IP addresses.
Ignored IP list	List of IP addresses that will be ignored during classification. Email content will be checked.
Approved senders list	Whitelists emails originating from a specified sender or domain. Only one sender address or a whole domain is used for verification based on the following priority: 1.SMTP 'MAIL FROM' address 2."Return-Path:" email header field 3."X-Env-Sender:" email header field 4."From:" email header field 5."Sender:" email header field 6."X-Apparently-From:" email header field
Blocked senders list	Blocks emails originating from a specified sender or domain. All identified sender addresses or whole domains are used for verification: SMTP 'MAIL FROM' address "Return-Path:" email header field "X-Env-Sender:" email header field "From:" email header field "Sender:" email header field "X-Apparently-From:" email header field

Gmail Anti-Phishing

Enable Gmail Anti-Phishing
This feature is active when enabled, and you can configure detailed options.
When items are reported
- **No action**—No action is performed, and an email with a malicious attachment is delivered to the recipient.
- **Move to Junk**—The email is moved to the Junk folder.
- **Move to Trash**—The email is moved to the Trash folder.
- **Delete message**—The email is deleted.
- **Quarantine message**—The original email is deleted, and a copy of the email is stored in the quarantine. If you decide to release the email from quarantine, it will be sent as an attachment in a new email and delivered to the recipient.

Tag subject
When enabled, you can modify templates added to the subject of infected messages.
Tag subject text
You can add a custom tag to the subjects of affected messages.
Notify mailbox owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Protection settings for OneDrive

This section provides information about changing OneDrive general or OneDrive Anti-Malware settings and options.

OneDrive general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about these applications in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in the Scan logs. The retention policy for clean scan results is three days. Scan results older than three days will be removed permanently.

OneDrive Anti-Malware

OneDrive Anti-Malware
This feature is active when enabled, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, and the file stays in OneDrive.
- **Move to Trash**—The file is moved to the Recycle Bin.
- **Replace**—The original file's content is replaced by text defined below in the File replace text window.
- **Quarantine**—The original file is moved to Recycle Bin and copied to quarantine. When the file is released, the previously deleted file stays in the trash, and a new copy is uploaded to the original OneDrive folder.

File replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Notify owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Protection settings for Google Drive

This section provides information about changing Google Drive general or Google Drive Anti-Malware settings and options.

Google Drive general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about these applications in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in the Scan logs. The retention policy for clean scan results is three days. Scan results older than three days will be removed permanently.

Google Drive Anti-Malware

Google Drive Anti-Malware
This feature is active when enabled, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced Machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, and the file stays in Google Drive.
- **Move to Trash**—The file is moved to the Recycle Bin.
- **Replace**—The original file's content is replaced by text defined below in the File replace text window.
- **Quarantine**—The original file is moved to the Recycle Bin and copied to quarantine.
- **Delete**—The original file is permanently deleted from Google Drive.

File replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Notify owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Protection settings for Team groups

This section provides information about changing Team groups general or Team groups Anti-Malware settings and options.

Team groups general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about these types of applications in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in Scan logs. The retention policy for scan results that are clean is three days. Scan results older than three days will be removed permanently.

Team groups Anti-Malware

Team groups Anti-Malware
When enabled, this feature is active, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, file remains intact.
- **Move to Trash**—The file is moved to the Teams Recycle bin.
- **Replace**—The content of the original file is replaced by text defined below in the File replace text window.
- **Quarantine**—The original file is moved to the Teams Recycle bin and copied into Quarantine. When the file is released, the previously deleted file stays in the Recycle bin, and a new copy is put back to the original location.

File replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Notify owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) to receive notification emails whenever a detection is found.

Protection settings for SharePoint sites

This section provides information about changing SharePoint sites general or SharePoint sites Anti-Malware settings and options.

SharePoint sites general

ESET LiveGrid® feedback
Data will be sent to the ESET Research Lab for further analysis. Read more about these types of applications in the glossary.
Log all objects
If this option is selected, all scan results (including clean) will be shown in Scan logs. The retention policy for scan results that are clean is three days. Scan results older than three days will be removed permanently.

SharePoint sites Anti-Malware

SharePoint sites Anti-Malware
When enabled, this feature is active, and you can configure detailed options.
Reporting & Machine Learning Protection
Advanced machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read the following before modifying a threshold (or level) for category Reporting.
When items are reported
- **No action**—No action is performed, file remains intact.
- **Move to Trash**—The file is moved to the SharePoint Recycle bin.
- **Replace**—The content of the original file is replaced by text defined below in the File replace text window.
- **Quarantine**—The original file is moved to the SharePoint Recycle bin and copied into Quarantine. When the file is released, the previously deleted file stays in the Recycle bin, and a new copy is put back to the original location.

File replace text
Replaces the attachment with a text file that contains detailed information about an action taken.
Notify owner
When enabled, the user will receive a notification email when detection is found.
Notify administrator
Specify an email address (press Enter to add multiple addresses) that will receive notification emails whenever a detection is found.

Protection settings for ESET LiveGuard Advanced

To use ESET LiveGuard Advanced feature, configure a policy that enables ESET LiveGuard Advanced analysis. Users or groups assigned with this policy will have additional protection. Files sent for ESET LiveGuard Advanced analysis are listed in the Submitted files tab; this applies to unknown (never-before-seen) suspicious samples. Known malicious files (based on hash) are not sent for ESET LiveGuard Advanced analysis.

You will see the ESET LiveGuard Advanced results in the Scan logs (Exchange Online, OneDrive, Team groups or SharePoint sites) marked as Malware.

ESET LiveGuard Advanced

When enabled, this feature is active, and you can configure detailed options.

> ESET LiveGuard Advanced will automatically enable ESET LiveGrid® feedback. Data will be sent to the ESET Research Lab for further analysis. Read more about ESET LiveGrid® in the glossary.

Detection threshold

Results with a selected threshold level, and higher, will be considered as threats.

Automatic submission of suspicious samples (drop-down menu)

This setting is related to ESET LiveGrid® and allows for the following actions: All, All except documents, None.

Automatic submission of suspicious samples (sliders)

Choose what file types are submitted to ESET LiveGuard Advanced if they contain suspicious code resembling threats or present unusual characteristics or behavior:

- **Executables**—.exe, .dll, .sys
- **Archives**—.zip, .rar, .7z, .arch, .arj, .bzip2, .gzip, .ace, .arc, .cab
- **Scripts**—.bat, .cmd, .hta, .js, .vbs, .js, .ps1
- **Other**—.jar, .reg, .msi, .swf, .lnk

Delete suspicious samples from ESET's servers

Choose when to delete samples that were sent for analysis. Delete samples from ESET LiveGuard Advanced cloud: Never, After 30 days, Immediately after analysis.

Documents

Use the slider to allow Microsoft Office documents, PDFs, and other document types to be sent for ESET LiveGuard Advanced analysis.

Delete documents from ESET's servers

Delete document file format samples from ESET LiveGuard Advanced cloud: Never, After 30 days, Immediately after analysis.

Reporting & Machine Learning Protection

The detection engine guards against malicious system attacks by scanning files, emails, and network communication. If an object classified as malware is detected, remediation will start. The detection engine can eliminate it by first blocking it and then taking action such as cleaning, deleting, or moving to quarantine.

Real-time & Machine learning protection

Advanced machine learning is now a part of the detection engine as an advanced layer of protection, which improves detection. Read more about this type of protection in the glossary. You can configure Reporting levels for the following categories:

Malware

A computer virus is a piece of malicious code that is prepended or appended to existing files on your computer. However, the term “virus” is often misused. "Malware” (malicious software) is a more accurate term. Malware detection is performed by the detection engine module combined with the machine learning component. Read more about these types of applications in the glossary.

Potentially unwanted applications (PUAs)

A Potentially unwanted application is software with an intent not unequivocally malicious. However, it may install additional unwanted software, change the behavior of the digital device, perform activities not approved or expected by the user or has unclear objectives.
This category includes advertising display software, download wrappers, various browser toolbars, software with misleading behavior, bundleware, trackware..
Read more about these types of applications in the glossary.

Potentially suspicious applications

Is a software compressed with packers or protectors frequently used to deter reverse engineering or to obfuscate the content of the executable (for example, to hide the presence of malware) by proprietary methods of compression and/or encryption.
This category includes: all unknown applications compressed with a packer or protector frequently used to compress malware.

Potentially unsafe applications

This classification is given for commercial, legitimate software that might be misused for malicious purposes. An unsafe application refers to legitimate commercial software that has the potential to be misused for malicious purposes.
This category includes: cracking tools, license key generators, hacking tools, remote access or control tools, password-cracking applications, and keyloggers (programs that record each keystroke typed by a user). This option is disabled by default.
Read more about these types of applications in the glossary.

Reporting

Reporting is performed by the detection engine and machine learning component. You can set the reporting threshold to better suit your environment and needs. There is not a single correct configuration. Therefore, we recommend that you monitor the behavior within your environment and decide whether a different Reporting

setting is more suitable.

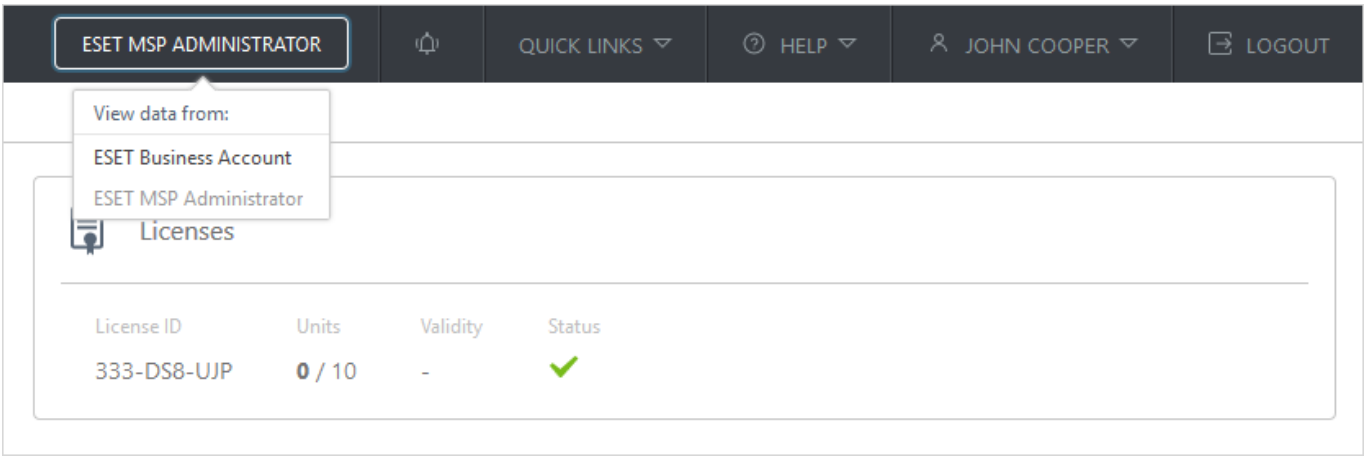
Reporting does not take action with objects. It passes information to a respective protection layer, and the protection layer tasks action accordingly.

Aggressive	**Reporting configured to maximum sensitivity. More detections are reported. While the Aggressive setting may appear to be the safest, it can often be too sensitive, which might even be counterproductive.** ℹ The aggressive setting may falsely identify objects as malicious, and action will be taken with such objects (depending on Protection settings).
Balanced	This setting is an optimal balance between performance and accuracy of detection rates and the number of falsely reported objects.
Cautious	Reporting configured to minimize falsely identified objects while maintaining a sufficient level of protection. Objects are reported only when the probability is evident and matches malicious behavior.
Off	Reporting is not active. Detections are not found, reported, or cleaned. ℹ Malware reporting cannot be deactivated; therefore, the Off setting is not available for Malware.

License management

The main window gives you an overview of the licenses pulled from ESET Business Account or ESET MSP Administrator. You can see all license pools, sites or companies available in the ESET Business Account or ESET MSP Administrator portal. License management enables you to protect or unprotect users.

If you have the same email address registered in both ESET MSP Administrator and ESET Business Account (single sign-on), you can switch between the ESET Business Account and ESET MSP Administrator views (hybrid licensing account).



The ESET Cloud Office Security license allows you to use the ESET LiveGuard Advanced feature at no extra fee. You will see the ELG label next to the License ID.

License management with ESET Business Account

Displays license information and usage (license pool name, license ID, units, validity and status). The licenses and license pools are loaded from ESET Business Account. License pools are available only if you have existing sites within ESET Business Account (sites are useful for categorization). One unit represents ESET Cloud Office Security protection of a single user for Exchange Online and OneDrive.

> One license unit is used by each protected user. This is regardless of what Microsoft 365 services are used.
> A user with Exchange Online or OneDrive (or both) always consumes one license unit.
> A license unit is not used by Team groups or SharePoint sites.

Every new user will appear in the Users section as Unprotected. If you use auto-protection by Tenant or Group, new users are protected automatically and will appear as Protected.

When protecting users, you have two options:

- **Auto-protection by Tenant or Group (recommended)**—maintenance-free, any newly added user that is in an Azure AD group or belongs to a Tenant is automatically protected. Refer to the note below for details.
- **Individual user protection**—requires management, and you must manually protect every new user.

Protect users (no License pool)

1. Click **Protect**.
2. Select Tenant or Group for user auto-protection and click **Protect**. For individual user protection, select the users you want to protect and click **Protect**. The Default policy now protects users.
3. If required, specify a custom policy for the users in the Policies section.

Protect users (using License pool)

1. Select the License pool and click the three-dots icon > **Show details** next to the license pool.
2. Click **Protect**.
3. Select a Tenant or Group for user auto-protection and click **Protect**. For individual user protection, select the users you want to protect and click **Protect**. The Default policy now protects users.
4. If required, specify a custom policy for the users in the Policies section.

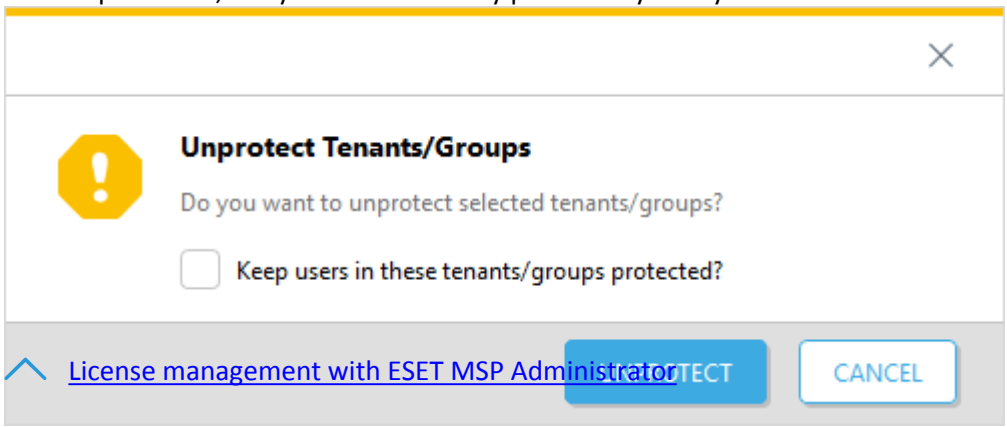
> Ensure you have enough license units, especially with auto-protection enabled when the number of users increases. Once all the license units are used, any new user that becomes a member of a Tenant or Group will not be protected. The protection of existing users remains unaffected.
> If you are temporarily short on license units and want to specify the users to protect, use unprotected groups (do not use auto-protection) and manually protect the users. When you increase license pools with more units, you can revert to auto-protection for easier management.

Move

To move users between license pools and for more advanced operations with licenses, click open ESET Business Account.

Unprotect

1. Select individual users, a Tenant or a Group and click **Unprotect**.
2. When removing Tenant or Group auto-protection, you will be asked whether to **Keep users in these tenants/groups protected**. If you opt not to use this option, users will become unprotected. If you select the check box, Tenant or Group auto-protection will be deactivated and changed to individual user protection. Users are still protected, but you must manually protect any newly added users.



License management with ESET MSP Administrator

Displays license information and usage (customer company, license ID, units and status).

> One license unit is used by each protected user. This is regardless of what Microsoft 365 services are used. A user with Exchange Online or OneDrive (or both) always consumes one license unit.
> A license unit is not used by Team groups or SharePoint sites.

Every new user will appear in the Users section as **Unprotected**. If you use auto-protection by Tenant or Group, new users are protected automatically and will appear as **Protected**.

When protecting users, you have two options:

- **Auto-protection by Tenant or Group (recommended)**—maintenance-free, any newly added user member of an Azure AD group or belongs to a Tenant is automatically protected. See the note below for details.
- **Individual user protection**—requires management, and you will need to manually protect each new user.

Protect users

1. Click **Protect**.
2. Select a Tenant or Group for user auto-protection and click **Protect**. For individual user protection, select the users you want to protect and click **Protect**. The Default policy now protects users.
3. If required, specify a custom policy for the users in the Policies section.

> Ensure you have enough license units, especially with auto-protection enabled when the number of users increases. Once all the license units are used, any new user that becomes a member of a Tenant or Group will not be protected. The protection of existing users remains unaffected.
> If you are temporarily short on license units and want to specify the users to protect, use unprotected groups (do not use auto-protection) and manually protect the users. When you increase license pools with more units, you can revert to auto-protection for easier management.

Unprotect

1. Select individual users, a Tenant or a Group and click **Unprotect**.
2. When removing Tenant or Group auto-protection, you will be asked whether to **Keep users in these tenants/groups protected**. If you opt not to use this option, users will become unprotected. If you select the check box, Tenant or Group auto-protection will be deactivated and changed to individual user protection. Users are still protected, but you must manually protect any newly added users.

ESET Cloud Office Security user access to specific company

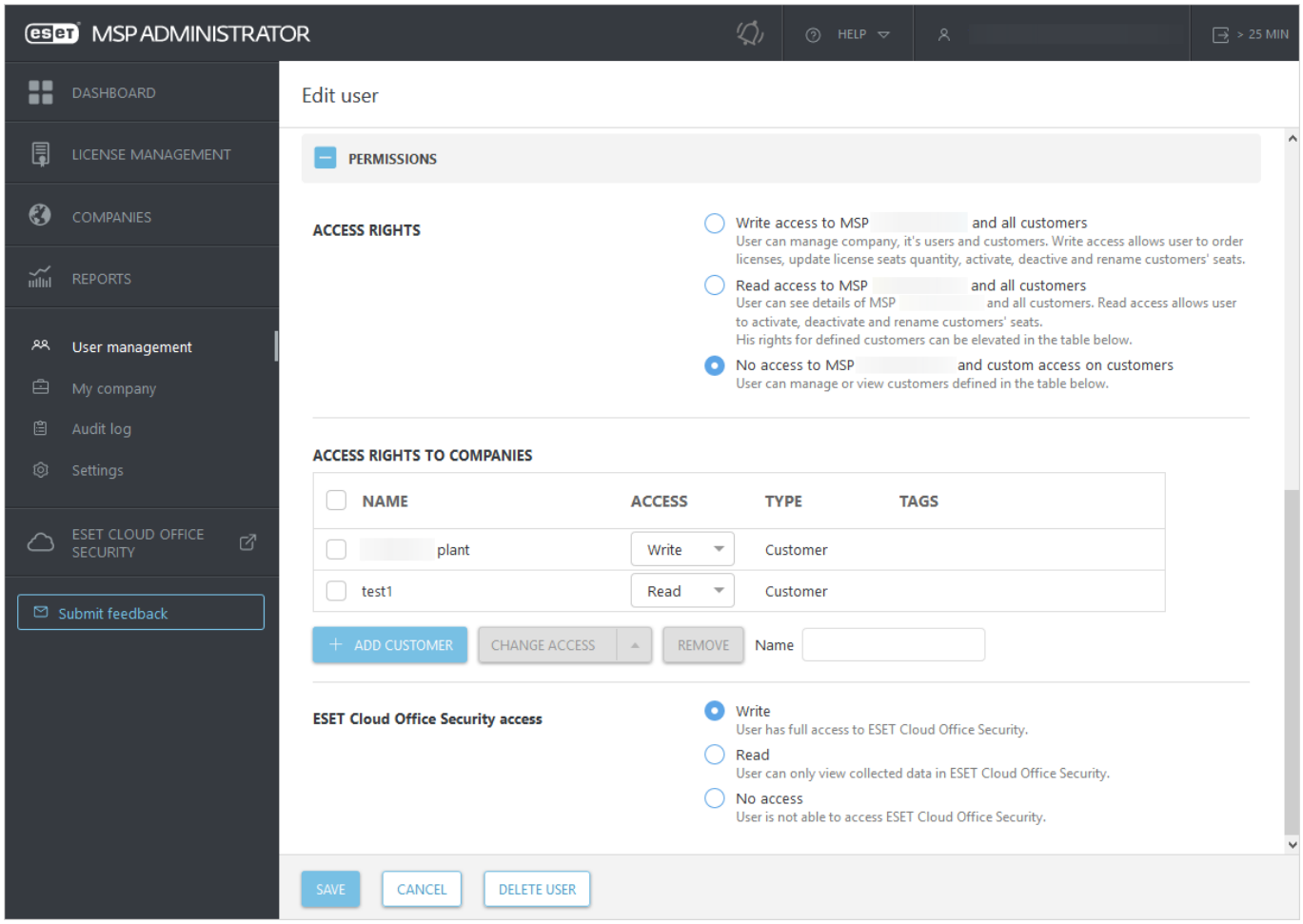
In a multi-tenant environment, you can provide a user with access to ESET Cloud Office Security, allowing the user to only see a specific company (with read or write permission). This is usually used by MSPs.

Configure user access rights in ESET MSP Administrator by assigning a company with **Write** permission and **Write** access to ESET Cloud Office Security:

1. Log in to ESET MSP Administrator as an administrator.

2. Edit a user, configure **Access rights to companies** under Permissions and select **Write** access. The user can only see the assigned company with its license pool.

3. Set **Write** access to ESET Cloud Office Security so the user can protect a company by adding a Tenant. A user with Read access cannot add or remove a Tenant.



Only one access type to ESET Cloud Office Security can be configured as a global setting and applies to all companies (if a user is assigned multiple companies).

Audit log

Tracks changes in ESET Cloud Office Security configuration or protection. The Audit log records are evidence of the activities and show the sequence in which they occurred. Audit logs store information about the specific operation or event. Audit logs are created whenever a ESET Cloud Office Security object (License pool, User, Policy, Report, or Quarantine item, such as an attachment) is created or modified.

When you click the gear icon in the upper-right corner to access the **Export to CSV** from the context menu, you can export the table grid to *CSV* format and use it in other applications.

Click the icon to open a sidebar with a summary of a specific audit log record. For more detailed information, click the three dots icon and select **Show details**.

Tile	Detail
Basic information	Shows general audit log data (Occurred, Action, Severity, Result, Section).
User	Shows information about the user who took action or made a change, including the user's email and IP address.
Changes	Details about the changes made.
Old settings	Shows previous policy setting(s).
New settings	Shows the current policy setting(s).

Tile	Detail
Objects	Lists objects affected by the change or action (user, policy, attachment, etc.).

You can filter users by several criteria. Click **Add filter** and select a filter type from the drop-down menu or type a string (repeat when combining multiple criteria):

Add filter	Usage
Action	Select one of the available actions.
Object	Type a valid object name.
Status	Select one of the following options: Succeeded, Failed, Started, or Partially succeeded
User	Type the user who performed changes.
Severity	Select the severity level: Low, Medium, or High
Occurred from / Occurred to	Filter by the time of occurrence. Use Occurred from and click the date to only show records newer than the date specified. Use Occurred for the records earlier than, or use both for the desired time range.
System initiated	Filter records made by the system.

Submit feedback

To send your feedback in your ESET Cloud Office Security console, use the toolbar in the top-right corner, hover the mouse cursor over **Help**, click **Submit feedback** and choose **Let us know what you think** (to share ideas and experiences) or **Report an issue or bug**.

Technical support

Use the following links with support information that will assist you in solving issues that you may encounter:

Search ESET Knowledgebase

ESET Knowledgebase Contains answers to the most frequently asked questions and recommended solutions to various issues. Regularly updated by ESET technical specialists, the Knowledgebase is the most powerful tool for resolving various problems.

Visit ESET Security Forum

Support forum The ESET Forum provides ESET users with an easy way to get help and help others. You can post any problem or question related to your ESET products.

Contact Technical Support

ESET Technical Support form Fill out the form to provide your details, including the issue description.

Contact your local ESET partner for support

Reach out to your local ESET support Locate support contact information for ESET support in your region from your ESET license email.

Send feedback

Submit feedback Let us know what you think (share ideas and experiences), or report an issue or bug.

Suggest Online Help improvement

You can post your rating and provide feedback on a specific topic in Online Help by clicking the **Was this information helpful?** link underneath the help page. Let us know if the content helped or how you think Technical Writer can improve it.

Service availability

The ESET Status Portal displays the current status of ESET cloud services, scheduled outages and past incidents. If you are experiencing an issue with a supported ESET service and do not see it listed in the Status Portal, contact ESET Technical Support.

Monitoring teams verify potential issues internally, and confirmed incidents are posted and updated manually to maintain credibility and accuracy. Therefore, they appear on the Status Portal with a slight delay. We may not post short incidents if they are resolved before being manually confirmed.

Security for ESET Cloud Office Security

Introduction

The purpose of this document is to summarize the security practices and security controls applied within ESET Cloud Office Security. Security practices and controls are designed to protect customer information confidentiality, integrity, and availability. Note that security practices and controls may change.

Scope

The scope of this document is to summarize security practices and security controls for ESET Cloud Office Security infrastructure, ESET Business Account (hereinafter referred to as "EBA"), ESET Data Framework, ESET LiveGrid, Update, AntiSpam, ESET Dynamic Threat Defense infrastructure, organization, personnel, and operational processes. Security practices and controls include:

1. Information security policies
2. Organization of information security
3. Human resource security
4. Asset management
5. Access control
6. Cryptography
7. Physical and environmental security
8. Operations security
9. Communications security
10. System acquisition, development, and maintenance
11. Supplier relationship
12. Information security incident management
13. Information security aspects of business continuity management
14. Compliance

Security Concept

ESET s.r.o. company is ISO 27001:2013 certified with integrated management system scope explicitly covering ESET Cloud Office Security, EBA and other services.

Therefore, the concept of information security uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layer of the network, operating systems, databases, applications, personnel, and operating processes. Applied security practices and security controls are intended to overlap and complement each other.

Security Practices and Controls

1. Information Security Policies

ESET uses information security policies to cover all aspects of the ISO 27001 standard, including information security governance and security controls and practices. Policies are reviewed annually and updated after significant change to ensure their continuing suitability, adequacy, and effectiveness.

ESET performs annual reviews of this policy and internal security checks to ensure consistency with this policy. Non-compliance with information security policies is subject to disciplinary actions for ESET employees or contractual penalties up to contract termination for suppliers.

2. Organization of Information Security

The organization of information security for ESET Cloud Office Security consists of multiple teams and individuals involved in information security and IT, including:

- ESET executive management
- ESET internal security teams
- Business applications IT teams
- Other supporting teams

Information security responsibilities are allocated in line with information security policies in place. Internal processes are identified and assessed for any risk of unauthorized or unintentional modification or misuse of ESET assets. Risky or sensitive activities of internal processes adopt the segregation of duties principle to mitigate the risk.

The ESET legal team is responsible for contacts with government authorities including, Slovak regulators on cybersecurity and personal data protection. The ESET Internal Security team is responsible for contacting special interest groups like ISACA. The ESET Research lab team is responsible for communication with other security companies and the greater cybersecurity community.

Information security is accounted for in project management using the applied project management framework from conception to project completion.

Remote work and telecommuting are covered through the use of a policy implemented on mobile devices that include the use of strong cryptographic data protection on mobile devices while traveling through untrusted networks. Security controls on mobile devices are designed to work independently of ESET internal networks and internal systems.

3. Human Resource Security

ESET uses standard human resource practices, including policies designed to uphold information security. These practices cover the whole employee lifecycle, and they apply to all teams that access the ESET Cloud Office Security environment.

4. Asset Management

The ESET Cloud Office Security infrastructure is included in ESET asset inventories with strict ownership and rules applied according to asset type and sensitivity. ESET has an internal classification scheme defined. All ESET Cloud Office Security data and configurations are classified as confidential.

5. Access Control

ESET's Access control policy governs every access in ESET Cloud Office Security. Access control is set on the infrastructure, network services, operating system, database, and application level. Full user access management on the application level is autonomous. ESET Cloud Office Security and ESET Business Account single sign-on is governed by a central identity provider, which ensures that a user can access the authorized tenant only. The application uses standard ESET Cloud Office Security permissions to enforce role-based access control for the tenant.

ESET backend access is strictly limited to authorized individuals and roles. Standard ESET processes for user (de)registration, (de)provisioning, privilege management, and review of user access rights are used to manage ESET employee access to ESET Cloud Office Security infrastructure and networks.

Strong authentication is in place to protect access to all ESET Cloud Office Security data.

6. Cryptography

To protect the ESET Cloud Office Security data, strong cryptography is used to encrypt data at rest and in transit. Generally trusted certificate authority is used to issue certificates for public services. Internal ESET public key infrastructure is used to manage keys within the ESET Cloud Office Security infrastructure. Data stored in the database is protected by cloud-generated encryption keys. All backup data are protected by ESET managed keys.

7. Physical and Environmental Security

Because ESET Cloud Office Security and ESET Business Account are cloud-based, we rely on Microsoft Azure for physical and environmental security. Microsoft Azure uses certified data centers with robust physical security measures. The physical location of the data center depends on customer region choice.

8. Operations Security

The ESET Cloud Office Security service is operated via automated means based on strict operational procedures and configuration templates. All changes, including configuration changes and new package deployment, are approved and tested in a dedicated testing environment before deployment to production. Development, test, and production environments are segregated from each other. ESET Cloud Office Security data is located only in the production environment.

The ESET Cloud Office Security environment is supervised using operational monitoring to swiftly identify problems and provide sufficient capacity to all services on the network and host levels.

All configuration data is stored in our regularly backed-up repositories to allow for automated recovery of an

environment's configuration. ESET Cloud Office Security data backups are stored both on-site and off-site.

Backups are encrypted and regularly tested for recoverability as a part of business continuity testing.

Auditing on systems is performed according to internal standards and guidelines. Logs and events from the infrastructure, operating system, database, application servers, and security controls are collected continuously. The logs are further processed by IT and internal security teams to identify operational and security anomalies and information security incidents.

ESET uses a general technical vulnerability management process to handle the occurrence of vulnerabilities in ESET infrastructure, including ESET Cloud Office Security and other ESET products. This process includes proactive vulnerability scanning and repeated penetration testing of infrastructure, products, and applications.

ESET states internal guidelines for the security of internal infrastructure, networks, operating systems, databases, application servers, and applications. These guidelines are checked via technical compliance monitoring and our internal information security audit program.

9. Communications Security

The ESET Cloud Office Security environment is segmented via native cloud segmentation with network access limited only to necessary services among network segments. The availability of network services is achieved via native cloud controls like availability zones, load-balancing, and redundancy. Dedicated load-balancing components are deployed to provide specific endpoints for ESET Cloud Office Security instance routing that enforce authorization of traffic and load-balancing. Network traffic is continuously monitored for operational and security anomalies. Potential attacks can be resolved by using native cloud controls or deployed security solutions. All network communication is encrypted via generally available techniques, including IPsec and TLS.

10. System Acquisition, Development, and Maintenance

Development of ESET Cloud Office Security systems is performed in accordance with the ESET secure software development policy. Internal security teams are included in the ESET Cloud Office Security development project from the initial phase and overlook all development and maintenance activities. The internal security team defines and checks the fulfillment of security requirements in various stages of software development. The security of all services, including newly developed ones, is tested continuously after release.

11. Supplier relationship

A relevant supplier relationship is conducted according to valid ESET guidelines, which cover whole relationship management and contractual requirements from the information security and privacy perspective. The quality and security of services provided by the critical service provider are assessed regularly.

12. Information Security Incident Management

Information security incident management in ESET Cloud Office Security is performed similarly to other ESET infrastructures and relies on defined incident response procedures. Roles within incident response are defined and allocated across multiple teams, including IT, security, legal, human resources, public relations, and executive management. The incident response team for an incident is established based on incident triage by the internal security team. That team will provide further coordination of other teams handling the incident. The internal security team is also responsible for evidence collection and lessons learned. Incident occurrence and resolution are communicated to affected parties. ESET legal team is responsible for notifying regulatory bodies if needed according to the General Data Protection Regulation (GDPR) and Cybersecurity Act transposing Network and Information Security Directive (NIS).

13. Information Security Aspects of Business Continuity Management

Business continuity of the ESET Cloud Office Security service is coded in the robust architecture used to maximize the availability of the provided services. Complete restoration from off-site backup and configuration data is possible in the event of a catastrophic failure of all redundant nodes for ESET Cloud Office Security components or the ESET Cloud Office Security service. The restoration process is tested regularly.

14. Compliance

Compliance with the regulatory and contractual requirements of ESET Cloud Office Security is regularly assessed and reviewed similarly to other infrastructure and processes of ESET, and necessary steps are taken to provide compliance on a continuous basis. ESET is registered as a digital service provider for Cloud Computing digital service covering multiple ESET services, including ESET Cloud Office Security. Note that ESET compliance activities do not necessarily mean that the overall compliance requirements of customers are satisfied as such.

Terms of Use

Effective as of October 23, 2023 | See a previous version of Terms of Use | Compare changes

This ESET Cloud Office Security Agreement (hereinafter referred to as "Terms") constitute a special agreement between ESET, spol. s r. o., having its registered office at Einsteinova 24, 85101 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "Provider") and you, a natural person or legal entity (hereinafter referred to as "You" or "User") who accesses an account for administration, ESET Cloud Office Security and who accesses web-based portal controlled by ESET (hereinafter referred to as "Account") in order to use ESET Cloud Office Security. If you use the Account and ESET Cloud Office Security (hereinafter jointly referred to as "Product") on behalf of an organization, then you agree to these Terms for that organization and guarantee that you have the authority to bind that organization to these Terms. In that case You and User will refer to that organization. Read these Terms carefully, they relate also to services provided by ESET through or in relation to the Product. The specific conditions for using individual services beyond these Terms are stated with each service, with their acceptance being part of the service activation process. The attached annexes supplement these Terms.

Security and Data Protection

The Account renders access to products and services provided by ESET. The user's full name, company name, country, valid email address, phone number, licensing data and statistic are required for registration and use of the Account and for the purpose of provision and maintenance of services accessed via Account. You hereby agree to data being collected and transferred to Provider's servers or those of its partners, the purpose of which is to ensure functionality of and authorization to use the Software and protection of the Provider’s rights. Following conclusion of these Terms, the Provider or its partners shall be entitled to transfer, process and store essential data identifying You for support purposes, and for the purpose of performance of these Terms. You are authorized to use the Account solely for the purposes and manner for which it is intended under these Terms, individual service terms and documentation.

You are responsible for the security of your Account and credentials required for logging in. ESET shall not be liable for any loss or damage resulting from your failure to comply with this obligation to maintain security. The User is also responsible for any activity related to the use of the Account, authorized or not. If the Account is compromised, you should notify the Provider immediately.

In order to provide administration service of Account, the collection of data concerning managed devices is

required together with administration information (hereinafter referred to as "Data"). Data are provided by You to ESET solely for the purpose of provision of administration service of Account. Data will be processed and stored in compliance with security policies and practices of ESET as well as in compliance with Privacy Policy.

Details about privacy, personal data protection and rights as a data subject can be found in Privacy Policy.

Fair Use Policy

You are obliged to comply with technical limitations stipulated in documentation. You agree that You will only use the Account and its functions in a way which does not limit the possibilities of other Users to access these services. The Provider reserves the right to limit the scope of services provided to individual Users, to enable use of the services by the highest possible number of Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Account and deletion of data and information.

Details about technical limitations can be found in Limitations.

Location

Provider may allow You to choose from available hosting locations for Account, including recommended location chosen by Provider. You acknowledge that by choosing of other than recommended location, your user experience may be affected. Based on the chosen location Data Protection Agreement included in the Annex no. 2 of this Agreement and Standard Contractual Clauses included in the Annex no. 3 of this Agreement may apply. ESET reserves the right to change specific location at any time without prior notice for the purpose of improvement of services provided by ESET in compliance with your location preferences (e.g. European Union). Notwithstanding the location selected by You for hosting the Account, You agree and understand that ESET, or its designated representatives, may access Your Data from locations other than the location chosen by You. This access is solely for the purposes of providing technical support, ensuring the security of the service, and enhancing the service quality. You acknowledge and accept that this access by ESET is necessary for efficient service provision.

Software

ESET or its respective suppliers own or exercise copyright to all software available as part of Product (hereinafter referred to as "Software"). The Software can be used only in accordance with the End User License Agreement included in the Annex no. 1 of this Agreement. Other information regarding licensing, copyright, documentation and trademarks are stipulated in the Legal Information.

Restrictions

You may not copy, distribute, extract components or make derivative works of the Account. When using the Account You are required to comply with the following restrictions:

(a) You may not use, modify, translate or reproduce the Account or transfer rights to use the Account or its components in any manner other than as provided for in these Terms.

(b) You may not sell, sub-license, lease or rent or borrow the Account or use the Account for the provision of commercial services.

(c) You may not reverse engineer, reverse compile or disassemble the Account or otherwise attempt to discover the source code of the Account, except to the extent that this restriction is expressly prohibited by law.

(d) You agree that You will only use the Account in a manner that complies with all applicable laws in the jurisdiction in which You use the Account, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

Disclaimers

AS THE USER, YOU HEREBY ACKNOWLEDGE THAT THE ACCOUNT AS WELL AS SERVICES ARE PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT ACCOUNT OR SERVICES WILL NOT INFRINGE ANY THIRD PARTY'S PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THE PROVIDER OR ANY OTHER PARTY MAKE NO GUARANTEE THAT THE ACCOUNT OR SERVICES WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF ACCOUNT OR SERVICES WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION AND USE OF ACCOUNT AND SERVICES TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE RESULTS OBTAINED FROM IT.

These Terms create no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

Limitation of Liability

TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR CONTRACTORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE ACCOUNT, EVEN IF THE PROVIDER, ITS CONTRACTORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES, CONTRACTORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE SERVICE OR ACCOUNT IN QUESTION.

Trade control compliance

(a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any activity, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies ("Affiliates") being in violation of, or being subject to, negative consequences under trade control laws which include:

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which ESET or any of its Affiliates are incorporated or operate and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under these Terms are to be performed, or in which

ESET or any of its Affiliates are incorporated or operate (legal acts referred to in points i, and ii. above together as "Trade Control Laws").

(b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of section (a) of this Trade control compliance clause of these Terms; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under these Terms could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

(c) Nothing in these Terms is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

Governing Law and Language

These Terms shall be governed by and construed in accordance with Slovak law. The End User and the Provider agree that conflict provisions of the governing law and United Nations Convention on Contracts for the International Sale of Goods shall not apply. If You are a consumer with habitual residence in the EU, You are also afforded additional protection granted to You by mandatory provisions of law applicable in your country of residence.

You expressly agree that exclusive jurisdiction for any claim or dispute with the Provider or relating in any way to your use of the Software, Account or Services or arising from these Terms or Special Terms (if applicable) resides in District Court Bratislava I, Slovakia and You further agree and expressly consent to the exercise of the personal jurisdiction in the District Court Bratislava I in connection with any such dispute or claim. If You are a consumer and have a habitual residence in the EU, You may also bring a claim to enforce your consumer rights in the place of exclusive jurisdiction or in the EU country in which You live. Moreover, You may also use an online dispute resolution platform, which can be accessed here: https://ec.europa.eu/consumers/odr/. However, consider contacting us first before raising any claim officially.

General provisions

ESET reserves the right to revise these Terms and documentation or any portion thereof at any time by updating the relevant document to reflect changes to the law or changes to Account. You will be notified about any revision of these Terms by email or via your Account. If You disagree with the changes to these Terms, You may cancel your Account. Unless You cancel your Account after being notified about the changes, You are bound by any amendments or revisions of these Terms. You are encouraged to periodically visit this page to review the current Terms that apply to your use of Account.

Notices

All notices must be delivered to: ESET, spol. s r. o., Einsteinova 24, 85101 Bratislava, Slovak Republic.

Annex no. 1

End User License Agreement

Annex no. 2

Data Processing Agreement

Annex no. 3

Standard Contractual Clauses

End User License Agreement

IMPORTANT: Please read the terms and conditions of product application set out below carefully prior to download, installation, copy or use. **THROUGH DOWNLOADING, INSTALLING, COPYING OR USING THE SOFTWARE YOU ARE EXPRESSING YOUR CONSENT TO THESE TERMS AND CONDITIONS AND YOU ACKNOWLEDGE PRIVACY POLICY.**

End User License Agreement

Under the terms of this End User License Agreement (hereinafter referred to as "the Agreement") executed by and between ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 (hereinafter referred to as "ESET" or "the Provider") and you, a physical person or legal entity (hereinafter referred to as "You" or "the End User"), You are entitled to use the Software defined in Article 1 of this Agreement. The Software defined in Article 1 of this Agreement can be stored on a data carrier, sent via electronic mail, downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources, subject to the terms and conditions specified below.

THIS IS AN AGREEMENT ON END USER RIGHTS AND NOT AN AGREEMENT FOR SALE. The Provider continues to own the copy of the Software and the physical media contained in the sales package and any other copies that the End User is authorized to make pursuant to this Agreement.

By clicking on "I Accept" or "I Accept…" while installing, downloading, copying or using the Software, You agree to the terms and conditions of this Agreement. If You do not agree to all of the terms and conditions of this Agreement, immediately click on the canceling option, cancel the installation or download, or destroy or return the Software, installation media, accompanying documentation and sales receipt to the Provider or the outlet from which You acquired the Software.

YOU AGREE THAT YOUR USE OF THE SOFTWARE ACKNOWLEDGES THAT YOU HAVE READ THIS AGREEMENT, UNDERSTAND IT AND AGREE TO BE BOUND BY ITS TERMS AND CONDITIONS.

1. **Software**. As used in this Agreement the term "Software" means: (i) computer program accompanied by this Agreement and all components thereof; (ii) all the contents of the disks, CD-ROMs, DVDs, e-mails and any attachments, or other media with which this Agreement is provided, including the object code form of the Software supplied on a data carrier, via electronic mail or downloaded via the Internet; (iii) any related explanatory written materials and any other possible documentation related to the Software, above all any description of the Software, its specifications, any description of the Software properties or operation, any description of the operating environment in which the Software is used, instructions for use or installation of the Software or any description of how to use the Software (hereinafter referred to as " Documentation "); (iv) copies of the Software, patches for possible errors in the Software, additions to the Software, extensions to the Software, modified versions of the Software and updates of Software components, if any, licensed to You by the Provider pursuant to Article 3 of this Agreement. The Software shall be provided exclusively in the form of executable object code.

2. **Installation, Computer and a License key**. Software supplied on a data carrier, sent via electronic mail,

downloaded from the Internet, downloaded from the Provider's servers or obtained from other sources requires installation. You must install the Software on a correctly configured Computer, complying at least with requirements set out in the Documentation. The installation methodology is described in the Documentation. No computer programs or hardware which could have an adverse effect on the Software may be installed on the Computer on which You install the Software. Computer means hardware, including but not limited to personal computers, laptops, workstations, palmtop computers, smart phones, hand-held electronic devices, or other electronic devices for which the Software is designed, on which it will be installed and/or used. License key means the unique sequence of symbols, letters, numbers or special signs provided to the End User in order to allow the legal use of the Software, its specific version or extension of the term of the License in compliance with this Agreement.

3. **License**. Subject to the condition that You have agreed to the terms of this Agreement and You comply with all the terms and conditions stipulated herein, the Provider shall grant You the following rights (hereinafter referred to as "License"):

a) **Installation and use**. You shall have the non-exclusive, non-transferable right to install the Software on the hard disk of a Computer or other permanent medium for data storage, installation and storage of the Software in the memory of a computer system and to implement, store and display the Software.

b) **Stipulation of the number of licenses**. The right to use the Software shall be bound by the number of End Users. One End User shall be taken to refer to the following: (i) installation of the Software on one computer system; or (ii) if the extent of a license is bound to the number of mail boxes, then one End User shall be taken to refer to a computer user who accepts electronic mail via a Mail User Agent (hereinafter referred to as "MUA"). If MUA accepts electronic mail and subsequently distributes it automatically to several users, then the number of End Users shall be determined according to the actual number of users for whom the electronic mail is distributed. If a mail server performs the function of a mail gate, the number of End Users shall equal the number of mail server users for which the said gate provides services. If an unspecified number of electronic mail addresses are directed to and accepted by one user (e.g., through aliases) and messages are not automatically distributed by the client to a larger number of users, a License for one computer shall be required. You must not use the same License at the same time on more than one Computer. The End User is entitled to enter the License key to the Software only to the extent in which has the right to use the Software in accordance the limitation arising from the number of Licenses granted by Provider. The License key is deemed confidential, You must not share the License with third parties or allow third parties to use the License key unless permitted by this Agreement or Provider. If your License key is compromised, notify Provider immediately.

c) **Business Edition**. A Business Edition version of the Software must be obtained to use the Software on mail servers, mail relays, mail gateways or Internet gateways.

d) **Term of the License**. Your right to use the Software shall be time-limited.

e) **OEM Software**. OEM Software shall be limited to the Computer You obtained it with. It cannot be transferred to a different Computer.

f) **NFR, TRIAL Software**. Software classified as "Not-for-resale", NFR or TRIAL cannot be assigned for payment and must only be used for demonstration or testing the Software's features.

g) **Termination of the License**. The License shall terminate automatically at the end of the period for which granted. If You fail to comply with any of the provisions of this Agreement, the Provider shall be entitled to withdraw from the Agreement, without prejudice to any entitlement or legal remedy open to the Provider in such eventualities. In the event of cancellation of the License, You must immediately delete, destroy or return at your own cost, the Software and all backup copies to ESET or to the outlet from which You obtained the Software. Upon termination of the License, the Provider shall be also entitled to cancel the End User's entitlement to use

the functions of the Software, which require connection to the Provider's servers or third-party servers.

4. **Functions with data collection and internet connection requirements**. To operate correctly the Software requires connection to the Internet and must connect at regular intervals to the Provider's servers or third-party servers and applicable data collection in compliance with Privacy Policy. Connection to the Internet and applicable data collection is necessary for the following functions of the Software:

a) **Updates to the Software**. The Provider shall be entitled from time to issue updates to the Software ("Updates"), but shall not be obliged to provide Updates. This function is enabled under the Software's standard settings and Updates are therefore installed automatically, unless the End User has disabled automatic installation of Updates. For the purpose of provisioning of Updates, License authenticity verification is required including information about Computer and/or the platform on which the Software is installed in compliance with Privacy Policy.

b) Forwarding of infiltrations and information to the Provider. The Software contains functions which collect samples of computer viruses and other malicious computer programs and suspicious, problematic, potentially unwanted or potentially unsafe objects such as files, URLs, IP packets and ethernet frames (hereinafter referred to as " Infiltrations ") and then send them to the Provider, including but not limited to information about the installation process, the Computer and/or the platform on which the Software is installed and information about the operations and functionality of the Software (hereinafter referred to as "Information "). The Information and Infiltrations may contain data (including randomly or accidentally obtained personal data) about the End User or other users of the Computer on which the Software is installed, and files affected by Infiltrations with associated metadata. Information and Infiltrations may be collected by following functions of Software:

i. LiveGrid Reputation System function includes collection and sending of one-way hashes related to Infiltrations to Provider. This function is enabled under the Software’s standard settings.

ii. LiveGrid Feedback System function includes collection and sending of Infiltrations with associated metadata and Information to Provider.

The Provider shall only use Information and Infiltrations received for the purpose of analysis and research of Infiltrations, improvement of Software and License authenticity verification and shall take appropriate measures to ensure that Infiltrations and Information received remain secure. By activating this function of the Software, Infiltrations and Information may be collected and processed by the Provider as specified in Privacy Policy and in compliance with relevant legal regulations. You can deactivate these functions at any time.

For the purpose of this Agreement, it is necessary to collect, process and store data enabling the Provider to identify You in compliance with Privacy Policy. You hereby acknowledge that the Provider checks using its own means whether You are using the Software in accordance with the provisions of this Agreement. You hereby acknowledge that for the purpose of this Agreement it is necessary for your data to be transferred, during communication between the Software and the Provider's computer systems or those of its business partners as part of Provider’s distribution and support network to ensure functionality of Software and authorization to use the Software and to protection of the Provider’s rights.

Following conclusion of this Agreement, the Provider or any of its business partners as part of Provider’s distribution and support network shall be entitled to transfer, process and store essential data identifying You for billing purposes, performance of this Agreement and transmitting notifications on your Computer. You hereby agree to receive notification and messages including but not limited to marketing information.

Details about privacy, personal data protection and Your rights as a data subject can be found in Privacy Policy which is available on Provider’s website and accessible directly from the installation process. You can also visit it from Software’s help section.

5. **Exercising End User rights**. You must exercise End User rights in person or via your employees. You are only entitled to use the Software to safeguard your operations and protect those Computers or computers systems for which You have obtained a License.

6. **Restrictions to rights.** You may not copy, distribute, extract components or make derivative works of the Software. When using the Software, You are required to comply with the following restrictions:

a) You may make one copy of the Software on a permanent storage medium as an archival back-up copy, provided your archival back-up copy is not installed or used on any Computer. Any other copies You make of the Software shall constitute breach of this Agreement.

b) You may not use, modify, translate or reproduce the Software or transfer rights to use the Software or copies of the Software in any manner other than as provided for in this Agreement.

c) You may not sell, sub-license, lease or rent or borrow the Software or use the Software for the provision of commercial services.

d) You may not reverse engineer, reverse compile or disassemble the Software or otherwise attempt to discover the source code of the Software, except to the extent that this restriction is expressly prohibited by law.

e) You agree that You will only use the Software in a manner that complies with all applicable laws in the jurisdiction in which You use the Software, including, but not limited to, applicable restrictions concerning copyright and other intellectual property rights.

f) You agree that You will only use the Software and its functions in a way which does not limit the possibilities of other End Users to access these services. The Provider reserves the right to limit the scope of services provided to individual End Users, to enable use of the services by the highest possible number of End Users. Limiting the scope of services shall also mean complete termination of the possibility to use any of the functions of the Software and deletion of Data and information on the Provider's servers or third-party servers relating to a specific function of the Software.

g) You agree not exercise any activities involving use the License key, contrary to the terms of this Agreement or leading to provide License key to any person who is not entitled to use the Software, such as the transfer of used or unused License key in any form, as well as the unauthorized reproduction, or distribution of duplicated or generated License keys or using the Software as a result of the use of a License key obtained from the source other than the Provider.

7. **Copyright**. The Software and all rights, without limitation including proprietary rights and intellectual property rights thereto are owned by ESET and/or its licensors. They are protected by international treaty provisions and by all other applicable national laws of the country in which the Software is being used. The structure, organization and code of the Software are the valuable trade secrets and confidential information of ESET and/or its licensors. You must not copy the Software, except as set forth in Article 6(a). Any copies which You are permitted to make pursuant to this Agreement must contain the same copyright and other proprietary notices that appear on the Software. If You reverse engineer, reverse compile, disassemble or otherwise attempt to discover the source code of the Software, in breach of the provisions of this Agreement, You hereby agree that any information thereby obtained shall automatically and irrevocably be deemed to be transferred to and owned by the Provider in full, from the moment such information comes into being, notwithstanding the Provider's rights in relation to breach of this Agreement.

8. **Reservation of rights**. The Provider hereby reserves all rights to the Software, with the exception of rights expressly granted under the terms of this Agreement to You as the End User of the Software.

9. **Multiple language versions, dual media software, multiple copies**. In the event that the Software supports

multiple platforms or languages, or if You receive multiple copies of the Software, You may only use the Software for the number of computer systems and for the versions for which You obtained a License. You may not sell, rent, lease, sub-license, lend or transfer versions or copies of the Software which You do not use.

10. **Commencement and termination of the Agreement**. This Agreement shall be effective from the date You agree to the terms of this Agreement. You may terminate this Agreement at any time by permanently uninstalling, destroying and returning, at your own cost, the Software, all back-up copies and all related materials provided by the Provider or its business partners. Irrespective of the manner of termination of this Agreement, the provisions of Articles 7, 8, 11, 13, 19 and 21 shall continue to apply for an unlimited time.

11. **END USER DECLARATIONS**. AS THE END USER YOU ACKNOWLEDGE THAT THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, AND TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW. NEITHER THE PROVIDER, ITS LICENSORS OR AFFILIATES, NOR THE COPYRIGHT HOLDERS MAKE ANY REPRESENTATIONS OR WARRANTIES, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY OR FITNESS FOR A PARTICULAR PURPOSE OR THAT THE SOFTWARE WILL NOT INFRINGE ANY THIRD-PARTY PATENTS, COPYRIGHTS, TRADEMARKS OR OTHER RIGHTS. THERE IS NO WARRANTY BY THE PROVIDER OR BY ANY OTHER PARTY THAT THE FUNCTIONS CONTAINED IN THE SOFTWARE WILL MEET YOUR REQUIREMENTS OR THAT THE OPERATION OF THE SOFTWARE WILL BE UNINTERRUPTED OR ERROR-FREE. YOU ASSUME ALL RESPONSIBILITY AND RISK FOR THE SELECTION OF THE SOFTWARE TO ACHIEVE YOUR INTENDED RESULTS AND FOR THE INSTALLATION, USE AND RESULTS OBTAINED FROM IT.

12. **No other obligations**. This Agreement creates no obligations on the part of the Provider and its licensors other than as specifically set forth herein.

13. **LIMITATION OF LIABILITY**. TO THE MAXIMUM EXTENT PERMITTED BY APPLICABLE LAW, IN NO EVENT SHALL THE PROVIDER, ITS EMPLOYEES OR LICENSORS BE LIABLE FOR ANY LOST PROFITS, REVENUE, SALES, DATA OR COSTS OF PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES, PROPERTY DAMAGE, PERSONAL INJURY, INTERRUPTION OF BUSINESS, LOSS OF BUSINESS INFORMATION OR FOR ANY SPECIAL, DIRECT, INDIRECT, INCIDENTAL, ECONOMIC, COVER, PUNITIVE, SPECIAL OR CONSEQUENTIAL DAMAGES, HOWEVER CAUSED AND WHETHER ARISING UNDER CONTRACT, TORT, NEGLIGENCE OR OTHER THEORY OF LIABILITY, ARISING OUT OF THE USE OF OR INABILITY TO USE THE SOFTWARE, EVEN IF THE PROVIDER OR ITS LICENSORS OR AFFILIATES ARE ADVISED OF THE POSSIBILITY OF SUCH DAMAGES. BECAUSE SOME COUNTRIES AND JURISDICTIONS DO NOT ALLOW THE EXCLUSION OF LIABILITY, BUT MAY ALLOW LIABILITY TO BE LIMITED, IN SUCH CASES, THE LIABILITY OF THE PROVIDER, ITS EMPLOYEES OR LICENSORS OR AFFILIATES SHALL BE LIMITED TO THE SUM THAT YOU PAID FOR THE LICENSE.

14. Nothing contained in this Agreement shall prejudice the statutory rights of any party dealing as a consumer if running contrary thereto.

15. **Technical support**. ESET or third parties commissioned by ESET shall provide technical support at their own discretion, without any guarantees or declarations. The End User shall be required to back up all existing data, software and program facilities prior to the provision of technical support. ESET and/or third parties commissioned by ESET cannot accept liability for damage or loss of data, property, software or hardware or loss of profits due to the provision of technical support. ESET and/or third parties commissioned by ESET reserve the right to decide that resolving the problem is beyond the scope of technical support. ESET reserves the right to refuse, suspend or terminate the provision of technical support at its own discretion. License information, Information and other data in compliance with Privacy Policy may be required for the purpose of technical support provision.

16. **Transfer of the License**. The Software can be transferred from one Computer to another, unless contrary to the terms of the Agreement. If not contrary to the terms of the Agreement, the End User shall only be entitled to permanently transfer the License and all rights ensuing from this Agreement to another End User with the

Provider's consent, subject to the condition that (i) the original End User does not retain any copies of the Software; (ii) the transfer of rights must be direct, i.e. from the original End User to the new End User; (iii) the new End User must assume all the rights and obligations incumbent on the original End User under the terms of this Agreement; (iv) the original End User has to provide the new End User with documentation enabling verification of the genuineness of the Software as specified under Article 17.

17. **Verification of the genuineness of the Software**. The End User may demonstrate entitlement to use the Software in one of the following ways: (i) through a license certificate issued by the Provider or a third party appointed by the Provider; (ii) through a written license agreement, if such an agreement was concluded; (iii) through the submission of an e-mail sent by the Provider containing licensing details (user name and password). License information and End User identification data in compliance with Privacy Policy may be required for the purpose of Software genuineness verification.

18. **Licensing for public authorities and the US Government**. The Software shall be provided to public authorities, including the United States Government, with the license rights and restrictions described in this Agreement.

19. **Trade control compliance**.

a) You will not, directly or indirectly, export, re-export, transfer or otherwise make available the Software to any person, or use it in any manner, or be involved in any act, that could result in ESET or its holding companies, its subsidiaries, and the subsidiaries of any of its holding companies, as well as entities controlled by its holding companies (hereinafter referred to as "Affiliates") being in violation of, or being subject to negative consequences under, Trade Control Laws which includes

i. any laws that control, restrict, or impose licensing requirements on export, re-export or transfer of goods, software, technology, or services, issued or adopted by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Export Control Laws") and

ii. any economic, financial, trade or other, sanction, restriction, embargo, import or export ban, prohibition on transfer of funds or assets or on performing services, or equivalent measure imposed by any government, state or regulatory authority of the United States of America, Singapore, the United Kingdom, the European Union or any of its Member States, or any country in which obligations under the Agreement are to be performed, or in which ESET or any of its Affiliates are incorporated or operate (hereinafter referred to as "Sanction Laws").

b) ESET shall have the right to suspend its obligations under, or terminate, these Terms with immediate effect in the event that:

i. ESET determines that, in its reasonable opinion, the User has breached or is likely to breach provision of Article 19.a of the Agreement; or

ii. the End User and/or the Software become subject to Trade Control Laws and, as a result, ESET determines that, in its reasonable opinion, the continued performance of its obligations under the Agreement could result in ESET or its Affiliates being in violation of, or being subject to negative consequences under, Trade Control Laws.

c) Nothing in the Agreement is intended, and nothing should be interpreted or construed, to induce or require either party to act or refrain from acting (or to agree to act or refrain from acting) in any manner which is inconsistent with, penalized, or prohibited under any applicable Trade Control Laws.

20. **Notices**. All notices and return of the Software and Documentation must be delivered to: ESET, spol. s r. o., Einsteinova 24, 851 01 Bratislava, Slovak Republic.

21. **Applicable law**. This Agreement shall be governed by and construed in accordance with the laws of the Slovak Republic. The End User and the Provider hereby agree that the principles of the conflict of laws and the United Nations Convention on Contracts for the International Sale of Goods shall not apply. You expressly agree that any disputes or claims ensuing from this Agreement with respect to the Provider or any disputes or claims relating to use of the Software shall be settled by Bratislava I District Court and You expressly agree to the said court exercising jurisdiction.

22. **General provisions**. Should any of the provisions of this Agreement be invalid or unenforceable, this shall not affect the validity of the other provisions of the Agreement, which shall remain valid and enforceable under the conditions stipulated therein. In case of a discrepancy between language versions of this Agreement, the English version shall prevail. This Agreement may only be modified in written form, signed by an authorized representative of the Provider, or a person expressly authorized to act in this capacity under the terms of a power of attorney.

This is the entire Agreement between the Provider and You relating to the Software and it supersedes any prior representations, discussions, undertakings, communications or advertising relating to the Software.

EULA ID: BUS-ECOS-20-01

Data Processing Agreement

According to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter referred to as the "GDPR"), Provider (hereinafter referred to as the "Processor") and You (hereinafter referred to as the "Controller") are entering into the data processing contractual relationship in order to define the terms and conditions for the processing of personal data, the manner of its protection, as well as to define other rights and obligations of both parties in the processing of personal data of data subjects on behalf of the Controller during the course of performing the subject matter of these Terms as the main contract.

1. **Personal Data Processing.** The services provided in compliance with these Terms include processing information relating to an identified or identifiable natural person listed in the Privacy Policy (hereinafter referred to as the "Personal Data").

2. **Authorization.** The Controller authorizes the Processor to process Personal Data, including the following instructions:

(i) Purpose of Processing shall mean the provision of services in compliance with these Terms. The Processor is only allowed to process Personal Data on behalf of the Controller regarding the provision of services requested by the Controller. All information collected for additional purposes is processed outside of Controller-Processor contractual relationship.

(ii) Processing Period shall mean the period from entering cooperation under these Terms to termination of services,

(iii) Scope and Categories of Personal Data. The Services are intended for the processing of general personal data only. However, the Controller is solely responsible for the personal data scope determination.

(iv) Data Subject shall mean a natural person as an authorized user of Controller’s devices,

(v) Processing Activities shall mean every and all operation necessary for processing,

(vi) Documented Instructions shall mean instructions described in these Terms, its Annexes, Privacy Policy, and service documentation. The Controller shall be responsible for the legal admissibility of the processing of Personal Data by the Processor regarding the respectively applicable provisions of data protection law.

3. **Obligations of Processor**. The Processor shall be obliged to:

(i) process Personal Data only on the grounds of Documented instructions and for the purpose defined in Terms, its Annexes, Privacy Policy, and service documentation,

(ii) to instruct the persons authorized to process the Personal Data (hereinafter referred to as the "Authorized Persons") about their rights and duties according to the GDPR, on their liability in case of breach and ensure that Authorized Persons have committed themselves to confidentiality and follow the Documented instructions,

(iii) implement and follow the measures described in the Terms, its Annexes, Privacy Policy, and service documentation,

(iv) assist the Controller with responding to requests from Data Subjects related to their rights. The Processor shall not correct, delete or restrict the processing of Personal Data without the instruction from the Controller. All requests from Data Subject related to Personal Data processed on behalf of the Controller shall be forwarded to the Controller without delay.

(v) assist the Controller with notification of personal data breach to the supervisory authority and Data Subject. The Processor shall notify the Controller of any breach of Personal Data processing or personal data security immediately after the discovery. The Processor shall cooperate to a reasonable extent in an investigation and remediation of such breach, and take reasonable measures to limit further negative implications.

(vi) at the choice of the Controller to delete or return all the Personal Data to the Controller after the end of the Processing Period. The Controller undertakes to inform the Processor about its decision within ten (10) days upon the end of the Processing Period. This provision shall not affect the Processor's right to keep the Personal Data to the necessary extent for archiving purposes in the public interest, scientific research purposes, statistical purposes or for the purpose of establishment, exercise or defense of legal claims.

(vii) keep an up-to-date register of all the categories of Processing Activities carried out on behalf of the Controller,

(viii) make all information necessary to demonstrate compliance as part of the Terms, its Annexes, Privacy Policy, and service documentation available to the Controller. In case of the audit or control of the Personal Data processing from the Controller's side, the Controller shall be obliged to inform the Processor in writing at least thirty (30) days before the planned audit or control.

4. **Engaging Another Processor.** The Processor is entitled to engage another processor for carrying out specific processing activities, such as the provision of cloud storage and infrastructure for the service in compliance with the Terms, its Annexes, Privacy Policy, and service documentation. Currently, Microsoft provides cloud storage and infrastructure as part of Azure Cloud Service. In such a case, the Processor shall remain the only point of contact and the party responsible for compliance. The Processor hereby undertakes to inform the Controller about any addition or replacement of another processor for purposes of possibility to object such change.

5. **Territory of Processing.** The Processor ensures that processing takes place in the European Economic Area or a country designated as safe by the decision of the European Commission based on the decision of the Controller. Standard Contractual Clauses shall apply in case of transfers and processing located outside of the European Economic Area or a country designated as safe by the decision of the European Commission upon the request of the Controller.

6. **Security.** The Processor is ISO 27001:2013 certified and uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layer of the network, operating systems, databases, applications, personnel, and operating processes. Compliance with the regulatory and contractual requirements is regularly assessed and reviewed similarly to other infrastructure and operations of the Processor, and necessary steps are taken to provide compliance on a continuous basis. The Processor has organized the data security using ISMS based on ISO 27001. The security documentation includes mainly policy documents for information security, physical security, security of equipment, incident management, handling of data leaks and security incidents, etc.

7. **Technical and Organizational Measures**. The Processor shall protect the Personal Data against casual and unlawful damage and destruction, casual loss, change, unauthorized access and disclosure. For this purpose, the Processor shall adopt adequate technical and organizational measures corresponding to the mode of processing and to the risk presented by processing for the rights of the Data Subjects in compliance with the requirements of the GDPR. A detailed description of the technical and organizational measures is stated in the Security Policy.

8. **Processor's Contact Information.** All notifications, requests, demands and other communication concerning personal data protection shall be addressed to ESET, spol. s.r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: dpo@eset.sk.

Standard Contractual Clauses

SECTION I

Clause 1 Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (1) for the transfer of personal data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2 Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant

to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3 Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4 Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5 Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6 Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the

purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8 Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

MODULE ONE: Transfer controller to controller

8.1 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B. It may only process the personal data for another purpose:

(i) where it has obtained the data subject's prior consent;

(ii) where necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iii) where necessary in order to protect the vital interests of the data subject or of another natural person.

8.2 Transparency

(a) In order to enable data subjects to effectively exercise their rights pursuant to Clause 10, the data importer shall inform them, either directly or through the data exporter:

(i) of its identity and contact details;

(ii) of the categories of personal data processed;

(iii) of the right to obtain a copy of these Clauses;

(iv) where it intends to onward transfer the personal data to any third party/ies, of the recipient or categories of recipients (as appropriate with a view to providing meaningful information), the purpose of such onward transfer and the ground therefore pursuant to Clause 8.7.

(b) Paragraph (a) shall not apply where the data subject already has the information, including when such information has already been provided by the data exporter, or providing the information proves impossible or

would involve a disproportionate effort for the data importer. In the latter case, the data importer shall, to the extent possible, make the information publicly available.

(c) On request, the Parties shall make a copy of these Clauses, including the Appendix as completed by them, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the Parties may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

(d) Paragraphs (a) to (c) are without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.3 Accuracy and data minimisation

(a) Each Party shall ensure that the personal data is accurate and, where necessary, kept up to date. The data importer shall take every reasonable step to ensure that personal data that is inaccurate, having regard to the purpose(s) of processing, is erased or rectified without delay.

(b) If one of the Parties becomes aware that the personal data it has transferred or received is inaccurate, or has become outdated, it shall inform the other Party without undue delay.

(c) The data importer shall ensure that the personal data is adequate, relevant and limited to what is necessary in relation to the purpose(s) of processing.

8.4 Storage limitation

The data importer shall retain the personal data for no longer than necessary for the purpose(s) for which it is processed. It shall put in place appropriate technical or organisational measures to ensure compliance with this obligation, including erasure or anonymisation (2) of the data and all back-ups at the end of the retention period.

8.5 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the personal data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The Parties have agreed on the technical and organisational measures set out in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(c) The data importer shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(d) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the personal data breach, including measures to mitigate its possible adverse effects.

(e) In case of a personal data breach that is likely to result in a risk to the rights and freedoms of natural persons, the data importer shall without undue delay notify both the data exporter and the competent supervisory

authority pursuant to Clause 13. Such notification shall contain i) a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), ii) its likely consequences, iii) the measures taken or proposed to address the breach, and iv) the details of a contact point from whom more information can be obtained. To the extent it is not possible for the data importer to provide all the information at the same time, it may do so in phases without undue further delay.

(f) In case of a personal data breach that is likely to result in a high risk to the rights and freedoms of natural persons, the data importer shall also notify without undue delay the data subjects concerned of the personal data breach and its nature, if necessary in cooperation with the data exporter, together with the information referred to in paragraph (e), points ii) to iv), unless the data importer has implemented measures to significantly reduce the risk to the rights or freedoms of natural persons, or notification would involve disproportionate efforts. In the latter case, the data importer shall instead issue a public communication or take a similar measure to inform the public of the personal data breach.

(g) The data importer shall document all relevant facts relating to the personal data breach, including its effects and any remedial action taken, and keep a record thereof.

8.6 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions or offences (hereinafter 'sensitive data'), the data importer shall apply specific restrictions and/or additional safeguards adapted to the specific nature of the data and the risks involved. This may include restricting the personnel permitted to access the personal data, additional security measures (such as pseudonymisation) and/or additional restrictions with respect to further disclosure.

8.7 Onward transfers

The data importer shall not disclose the personal data to a third party located outside the European Union (3) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') unless the third party is or agrees to be bound by these Clauses, under the appropriate Module. Otherwise, an onward transfer by the data importer may only take place if:

(i) it is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679 with respect to the processing in question;

(iii) the third party enters into a binding instrument with the data importer ensuring the same level of data protection as under these Clauses, and the data importer provides a copy of these safeguards to the data exporter;

(iv) it is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings;

(v) it is necessary in order to protect the vital interests of the data subject or of another natural person; or

(vi) where none of the other conditions apply, the data importer has obtained the explicit consent of the data subject for an onward transfer in a specific situation, after having informed him/her of its purpose(s), the identity of the recipient and the possible risks of such transfer to him/her due to the lack of appropriate data protection

safeguards. In this case, the data importer shall inform the data exporter and, at the request of the latter, shall transmit to it a copy of the information provided to the data subject.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.8 Processing under the authority of the data importer

The data importer shall ensure that any person acting under its authority, including a processor, processes the data only on its instructions.

8.9 Documentation and compliance

(a) Each Party shall be able to demonstrate compliance with its obligations under these Clauses. In particular, the data importer shall keep appropriate documentation of the processing activities carried out under its responsibility.

(b) The data importer shall make such documentation available to the competent supervisory authority on request.

MODULE TWO: Transfer controller to processor

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the

provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (4) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE THREE: Transfer processor to processor

8.1 Instructions

(a) The data exporter has informed the data importer that it acts as processor under the instructions of its controller(s), which the data exporter shall make available to the data importer prior to processing.

(b) The data importer shall process the personal data only on documented instructions from the controller, as communicated to the data importer by the data exporter, and any additional documented instructions from the data exporter. Such additional instructions shall not conflict with the instructions from the controller. The controller or data exporter may give further documented instructions regarding the data processing throughout

the duration of the contract.

(c) The data importer shall immediately inform the data exporter if it is unable to follow those instructions. Where the data importer is unable to follow the instructions from the controller, the data exporter shall immediately notify the controller.

(d) The data exporter warrants that it has imposed the same data protection obligations on the data importer as set out in the contract or other legal act under Union or Member State law between the controller and the data exporter (5).

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B., unless on further instructions from the controller, as communicated to the data importer by the data exporter, or from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including personal data, the data exporter may redact part of the text of the Appendix prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand its content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to rectify or erase the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the controller and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subject. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled

in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter or the controller. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify, without undue delay, the data exporter and, where appropriate and feasible, the controller after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the data breach, including measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify its controller so that the latter may in turn notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards set out in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the controller, as communicated to the data importer by the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union (6) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 of Regulation (EU) 2016/679;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another

natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter or the controller that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the controller.

(c) The data importer shall make all information necessary to demonstrate compliance with the obligations set out in these Clauses available to the data exporter, which shall provide it to the controller.

(d) The data importer shall allow for and contribute to audits by the data exporter of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. The same shall apply where the data exporter requests an audit on instructions of the controller. In deciding on an audit, the data exporter may take into account relevant certifications held by the data importer.

(e) Where the audit is carried out on the instructions of the controller, the data exporter shall make the results available to the controller.

(f) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(g) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

MODULE FOUR: Transfer processor to controller

8.1 Instructions

(a) The data exporter shall process the personal data only on documented instructions from the data importer acting as its controller.

(b) The data exporter shall immediately inform the data importer if it is unable to follow those instructions, including if such instructions infringe Regulation (EU) 2016/679 or other Union or Member State data protection law.

(c) The data importer shall refrain from any action that would prevent the data exporter from fulfilling its obligations under Regulation (EU) 2016/679, including in the context of sub-processing or as regards cooperation with competent supervisory authorities.

(d) After the end of the provision of the processing services, the data exporter shall, at the choice of the data importer, delete all personal data processed on behalf of the data importer and certify to the data importer that it has done so, or return to the data importer all personal data processed on its behalf and delete existing copies.

8.2 Security of processing

(a) The Parties shall implement appropriate technical and organisational measures to ensure the security of the data, including during transmission, and protection against a breach of security leading to accidental or unlawful

destruction, loss, alteration, unauthorised disclosure or access (hereinafter 'personal data breach'). In assessing the appropriate level of security, they shall take due account of the state of the art, the costs of implementation, the nature of the personal data (7), the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects, and in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner.

(b) The data exporter shall assist the data importer in ensuring appropriate security of the data in accordance with paragraph (a). In case of a personal data breach concerning the personal data processed by the data exporter under these Clauses, the data exporter shall notify the data importer without undue delay after becoming aware of it and assist the data importer in addressing the breach.

(c) The data exporter shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

8.3 Documentation and compliance

(a) The Parties shall be able to demonstrate compliance with these Clauses.

(b) The data exporter shall make available to the data importer all information necessary to demonstrate compliance with its obligations under these Clauses and allow for and contribute to audits.

Clause 9 Use of sub-processors

MODULE TWO: Transfer controller to processor

(a) The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (8) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

MODULE THREE: Transfer processor to processor

(a) The data importer has the controller's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the controller in writing of any intended changes to that list through the addition or replacement of sub-processors at least [Specify time period] in advance, thereby giving the controller sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the controller with the information necessary to enable the controller to exercise its right to object. The data importer shall inform the data exporter of the engagement of the sub-processor(s).

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the controller), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. (9) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's or controller's request, a copy of such a sub-processor agreement and any subsequent amendments. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10 Data subject rights

MODULE ONE: Transfer controller to controller

(a) The data importer, where relevant with the assistance of the data exporter, shall deal with any enquiries and requests it receives from a data subject relating to the processing of his/her personal data and the exercise of his/her rights under these Clauses without undue delay and at the latest within one month of the receipt of the enquiry or request. (10) The data importer shall take appropriate measures to facilitate such enquiries, requests and the exercise of data subject rights. Any information provided to the data subject shall be in an intelligible and easily accessible form, using clear and plain language.

(b) In particular, upon request by the data subject the data importer shall, free of charge:

(i) provide confirmation to the data subject as to whether personal data concerning him/her is being processed and, where this is the case, a copy of the data relating to him/her and the information in Annex I; if personal data has been or will be onward transferred, provide information on recipients or categories of recipients (as appropriate with a view to providing meaningful information) to which the personal data has been or will be onward transferred, the purpose of such onward transfers and their ground pursuant to Clause 8.7; and provide information on the right to lodge a complaint with a supervisory authority in accordance with Clause 12(c)(i);

(ii) rectify inaccurate or incomplete data concerning the data subject;

(iii) erase personal data concerning the data subject if such data is being or has been processed in violation of any of these Clauses ensuring third-party beneficiary rights, or if the data subject withdraws the consent on which the processing is based.

(c) Where the data importer processes the personal data for direct marketing purposes, it shall cease processing for such purposes if the data subject objects to it.

(d) The data importer shall not make a decision based solely on the automated processing of the personal data transferred (hereinafter 'automated decision'), which would produce legal effects concerning the data subject or similarly significantly affect him/her, unless with the explicit consent of the data subject or if authorised to do so under the laws of the country of destination, provided that such laws lays down suitable measures to safeguard the data subject's rights and legitimate interests. In this case, the data importer shall, where necessary in cooperation with the data exporter:

(i) inform the data subject about the envisaged automated decision, the envisaged consequences and the logic involved; and

(ii) implement suitable safeguards, at least by enabling the data subject to contest the decision, express his/her point of view and obtain review by a human being.

(e) Where requests from a data subject are excessive, in particular because of their repetitive character, the data importer may either charge a reasonable fee taking into account the administrative costs of granting the request or refuse to act on the request.

(f) The data importer may refuse a data subject's request if such refusal is allowed under the laws of the country of destination and is necessary and proportionate in a democratic society to protect one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679.

(g) If the data importer intends to refuse a data subject's request, it shall inform the data subject of the reasons for the refusal and the possibility of lodging a complaint with the competent supervisory authority and/or seeking judicial redress.

MODULE TWO: Transfer controller to processor

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

MODULE THREE: Transfer processor to processor

(a) The data importer shall promptly notify the data exporter and, where appropriate, the controller of any request it has received from a data subject, without responding to that request unless it has been authorised to do so by the controller.

(b) The data importer shall assist, where appropriate in cooperation with the data exporter, the controller in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable. In this regard, the Parties shall set out in Annex II the

appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the controller, as communicated by the data exporter.

MODULE FOUR: Transfer processor to controller

The Parties shall assist each other in responding to enquiries and requests made by data subjects under the local law applicable to the data importer or, for data processing by the data exporter in the EU, under Regulation (EU) 2016/679.

Clause 11 Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12 Liability

MODULE ONE: Transfer controller to controller

MODULE FOUR: Transfer processor to controller

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) Each Party shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages that the Party causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter under Regulation (EU) 2016/679.

(c) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(d) The Parties agree that if one Party is held liable under paragraph (c), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(e) The data importer may not invoke the conduct of a processor or sub-processor to avoid its own liability.

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13 Supervision

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) [Where the data exporter is established in an EU Member State:] The supervisory authority with responsibility

for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:] The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14 Local laws and practices affecting compliance with the Clauses

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards (12);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a). [For Module Three: The data exporter shall forward the notification to the controller.]

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation [for Module Three:, if appropriate in consultation with the controller]. The data exporter shall suspend the data transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by [for Module Three: the controller or] the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15 Obligations of the data importer in case of access by public authorities

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller (where the EU processor combines the personal data received from the third country-controller with personal data collected by the processor in the EU)

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the

country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

[For Module Three: The data exporter shall forward the notification to the controller.]

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.). [For Module Three: The data exporter shall forward the information to the controller.]

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request. [For Module Three: The data exporter shall make the assessment available to the controller.]

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16 Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for

whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority [for Module Three: and the controller] of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) [For Modules One, Two and Three: Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data.] [For Module Four: Personal data collected by the data exporter in the EU that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall immediately be deleted in its entirety, including any copy thereof.] The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17 Governing law

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be the law as defined in Terms.

MODULE FOUR: Transfer processor to controller

These Clauses shall be governed by the law of a country allowing for third-party beneficiary rights. The Parties

agree that this shall be the law as defined in Terms.

Clause 18 Choice of forum and jurisdiction

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts as defined in Terms.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

MODULE FOUR: Transfer processor to controller

Any dispute arising from these Clauses shall be resolved by the courts as defined in Terms.

APPENDIX

EXPLANATORY NOTE: It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Data exporter(s): [Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

Data importer(s): [Identity and contact details of the data importer(s), including any contact person with

responsibility for data protection]

1. Controller as defined in Data Processing Agreement

2. Processor as defined in Data Processing Agreement

(based on the flow of data)

B. DESCRIPTION OF TRANSFER

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

MODULE FOUR: Transfer processor to controller

Categories of data subjects whose personal data is transferred: As defined in Data Processing Agreement.

Categories of personal data transferred: As defined in Data Processing Agreement and Privacy Policy.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures: As defined in Data Processing Agreement and Privacy Policy.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis): Continuous basis.

Nature of the processing: Automated.

Purpose(s) of the data transfer and further processing: Provision of service as defined in Terms, its Annexes, Privacy Policy, and service documentation.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period: As defined in Data Processing Agreement.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing: As defined in Data Processing Agreement.

C. COMPETENT SUPERVISORY AUTHORITY

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

Identify the competent supervisory authority/ies in accordance with Clause 13: As defined in Privacy Policy

ANNEX II TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

MODULE ONE: Transfer controller to controller

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons: As defined in Security Policy

For transfers to (sub-) processors, also describe the specific technical and organisational measures to be taken by the (sub-) processor to be able to provide assistance to the controller and, for transfers from a processor to a sub-processor, to the data exporter

ANNEX III LIST OF SUB-PROCESSORS

MODULE TWO: Transfer controller to processor

MODULE THREE: Transfer processor to processor

EXPLANATORY NOTE: This Annex must be completed for Modules Two and Three, in case of the specific authorisation of sub-processors (Clause 9(a), Option 1).

The controller has authorised the use of the following sub-processors: As defined in Data Processing Agreement

References:

(1) Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

(2) This requires rendering the data anonymous in such a way that the individual is no longer identifiable by anyone, in line with recital 26 of Regulation (EU) 2016/679, and that this process is irreversible.

(3) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European

Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(4) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

(5) See Article 28(4) of Regulation (EU) 2016/679 and, where the controller is an EU institution or body, Article 29(4) of Regulation (EU) 2018/1725.

(6) The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union’s internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purposes of these Clauses.

(7) This includes whether the transfer and further processing involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person’s sex life or sexual orientation, or data relating to criminal convictions or offences.

(8) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(9) This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

(10) That period may be extended by a maximum of two more months, to the extent necessary taking into account the complexity and number of requests. The data importer shall duly and promptly inform the data subject of any such extension.

(11) The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

(12) As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.

Privacy Policy

Effective as of March 21, 2023 | See a previous version of Privacy Policy | Compare changes

The protection of personal data is of particular importance to ESET, spol. s r. o., having its registered office at Einsteinova 24, 851 01 Bratislava, Slovak Republic, registered in the Commercial Register administered by Bratislava I District Court, Section Sro, Entry No 3586/B, Business Registration Number: 31333532 as a Data Controller ("ESET" or "We"). We want to comply with the transparency requirement as legally standardized under the EU General Data Protection Regulation ("GDPR"). To achieve this goal, We are publishing this Privacy Policy with the sole purpose of informing our customer ("End User" or "You") as a data subject about following personal data protection topics:

- Legal Basis of Personal Data Processing,
- Data Sharing and Confidentiality,
- Data Security,
- Your Rights as a Data Subject,
- Processing of Your Personal Data
- Contact Information.

Legal Basis of Personal Data Processing

There are a few legal bases for data processing which We use according to the applicable legislative framework related to protection of personal data. The processing of personal data at ESET is mainly necessary for the performance of the Terms of Use ("Terms") with End User (Art. 6 (1) (b) GDPR), which is applicable for the provision of ESET products or services, unless explicitly stated otherwise, e.g.:

- Legitimate interest legal basis (Art. 6 (1) (f) GDPR), that enables us to process data on how our customers use our Services and their satisfaction to provide our users with the best protection, support and experience We can offer. Even marketing is recognized by applicable legislation as a legitimate interest, therefore We usually rely on it for marketing communication with our customers.
- Consent (Art. 6 (1) (a) GDPR), which We may request from You in specific situations when we deem this legal basis as the most suitable one or if it is required by law.
- Compliance with a legal obligation (Art. 6 (1) (c) GDPR), e.g. stipulating requirements for electronic communication, retention for invoicing or billing documents.

Data Sharing and Confidentiality

We do not share your data with third parties. However, ESET is a company that operates globally through affiliated companies or partners as part of our sales, service and support network. Licensing, billing and technical support information processed by ESET may be transferred to and from affiliates or partners for the purpose of fulfilling the EULA, such as providing services or support.

ESET prefers to process its data in the European Union (EU). However, depending on your location (use of our products and/or services outside the EU) and/or the service you choose, it may be necessary to transfer your data to a country outside the EU. For example, we use third-party services in connection with cloud computing. In these cases, we carefully select our service providers and ensure an appropriate level of data protection through contractual as well as technical and organizational measures. As a rule, we agree on the EU standard contractual clauses, if necessary, with supplementary contractual regulations.

For some countries outside the EU, such as the United Kingdom and Switzerland, the EU has already determined a comparable level of data protection. Due to the comparable level of data protection, the transfer of data to these

countries does not require any special authorization or agreement.

We rely on third-party services related to cloud computing provided by Microsoft as a cloud service provider.

Data Security

ESET implements appropriate technical and organizational measures to ensure a level of security which is appropriate to potential risks. We are doing our best to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services. However, in case of data breach resulting in a risk to your rights and freedoms, We are ready to notify the relevant supervisory authority as well as affected End Users as data subjects.

Data Subject's Rights

The rights of every End User matter and We would like to inform you that all End Users (from any EU or any non-EU country) have the following rights guaranteed at ESET. To exercise your data subject's rights, you can contact us via support form or by e-mail at dpo@eset.sk. For identification purposes, we ask you for the following information: Name, e-mail address and - if available - license key or customer number and company affiliation. Please refrain from sending us any other personal data, such as the date of birth. We would like to point out that to be able to process your request, as well as for identification purposes, we will process your personal data.

Right to Withdraw the Consent. Right to withdraw the consent is applicable in case of processing based on consent only. If We process your personal data on the basis of your consent, you have the right to withdraw the consent at any time without giving reasons. The withdrawal of your consent is only effective for the future and does not affect the legality of the data processed before the withdrawal.

Right to Object. Right to object the processing is applicable in case of processing based on the legitimate interest of ESET or third party. If We process your personal data to protect a legitimate interest, You as the data subject have the right to object to the legitimate interest named by us and the processing of your personal data at any time. Your objection is only effective for the future and does not affect the lawfulness of the data processed before the objection. If we process your personal data for direct marketing purposes, it is not necessary to give reasons for your objection. This also applies to profiling, insofar as it is connected with such direct marketing. In all other cases, we ask you to briefly inform us about your complaints against the legitimate interest of ESET to process your personal data.

Please note that in some cases, despite your consent withdrawal or your objection processing, we are entitled to further process your personal data on the basis of another legal basis, for example, for the performance of a contract.

Right of Access. As a data subject, you have the right to obtain information about your data stored by ESET free of charge at any time.

Right to Rectification. If we inadvertently process incorrect personal data about you, you have the right to have this corrected.

Right to Erasure. As a data subject, you have the right to request the deletion or restriction of the processing of your personal data. If we process your personal data, for example, with your consent, you withdraw it and there is no other legal basis, for example, a contract, We delete your personal data immediately. Your personal data will also be deleted as soon as they are no longer required for the purposes stated for them at the end of our retention period.

Right to Restriction of Processing. If we use your personal data for the sole purpose of direct marketing and you

have revoked your consent or objected to the underlying legitimate interest of ESET, We will restrict the processing of your personal data to the extent that we include your contact data in our internal black list in order to avoid unsolicited contact. Otherwise, your personal data will be deleted.

Please note that We may be required to store your data until the expiry of the retention obligations and periods issued by the legislator or supervisory authorities. Retention obligations and periods may also result from the Slovak legislation. Thereafter, the corresponding data will be routinely deleted.

Right to Data Portability. We are happy to provide You, as a data subject, with the personal data processed by ESET in the xls format.

Right to Lodge a Complaint. As a data subject, You have a right to lodge a complaint with a supervisory authority at any time. ESET is subject to the regulation of Slovak laws and We are bound by data protection legislation as part of the European Union. The relevant data supervisory authority is The Office for Personal Data Protection of the Slovak Republic, located at Hraničná 12, 82007 Bratislava 27, Slovak Republic.

Processing of Your Personal Data

Services provided by ESET implemented in our web-based product are provided under the Terms of Use ("Terms"), but some of them might require specific attention. We would like to provide You with more details on data processing connected with the provision of our products and services. We render various services described in the Terms and the product documentation. To make it all work, We need to collect the following information:

Licensing and Billing Data. The name, e-mail address, license key and (if applicable) address, company affiliation and payment data are collected and processed by ESET in order to facilitate the activation of license, license key delivery, reminders on expiration, support requests, license genuineness verification, provision of our service sand other notifications including marketing messages in line with applicable legislation or Your consent. ESET is legally obliged to keep the billing information for the period of 10 years, however the licensing information will be anonymized no later than 12 months after the expiration of license.

Update and Other Statistics. The processed information includes information concerning installation process and your computer including platform on which our product is installed and information about the operations and functionality of our products such as operation system, hardware information, installation IDs, license IDs, IP address, MAC address, configuration settings of product are processed for the purpose of provision update and upgrade services and for the purpose of maintenance, security and improvement of our backend infrastructure.

This information is kept apart from the identification information required for the licensing and billing purposes since it does not require the identification of End User. The retention period is up to 4 years.

ESET LiveGrid® Reputation System. One-way hashes related to infiltration are processed for the purpose of ESET LiveGrid® Reputation System which improves the efficiency of our anti-malware solutions by comparing scanned files to a database of whitelisted and blacklisted items in the cloud. The End User is not identified during this process.

ESET LiveGrid® Feedback System. Suspicious samples and metadata from the wild are collected as part of ESET LiveGrid® Feedback System which enables ESET to react immediately to needs of our end users and keep us responsive to the latest threats providing. We are dependent on You sending us

- Infiltrations such as potential samples of viruses and other malicious programs and suspicious; problematic, potentially unwanted or potentially unsafe objects such as executable files, email messages reported by You as spam or flagged by our product;
- Information concerning the use of internet such as IP address and geographic information, IP packets, URLs

and ethernet frames;
- Crash dump files and information contained.

We do not desire to collect your data outside of this scope but sometimes it is impossible to prevent it. Accidentally collected data may be included in malware itself (collected without our knowledge or approval) or as part of filenames or URLs and We do not intend it to form part of our systems or process it for the purpose declared in this Privacy Policy.

All information obtained and processed through the ESET LiveGrid® Feedback System are meant to be used without the identification of End User.

Technical Support. The contact and licensing information and data contained in your support requests may be required for service of support. Based on the channel You choose to contact us, We may collect your email address, phone number, license information, product details and description of your support case. You may be asked to provide us with other information to facilitate service of support. The data processed for technical support is stored for 4 years.

Please note that if the person using our products and services is not the End User who has purchased the product or service and concluded the Terms with Us, (e.g. an employee of the End User, a family member or a person otherwise authorized to use the product or service by the End User in compliance with Terms, the processing of the data is carried out in the legitimate interest of ESET within the meaning of Art. 6 (1) f) GDPR to enable the user authorized by End User to use the products and services provided by Us in accordance with Terms.

Contact Information

If You would like to exercise your right as a data subject or You have a question or concern, send us a message at:

ESET, spol. s r.o.
Data Protection Officer
Einsteinova 24
85101 Bratislava
Slovak Republic
dpo@eset.sk