WithSecure Elements Collaboration Protection

2026-08-20

Contents

Chapter 1

Introduction to the WithSecure Elements solution

Topics:

- Using WithSecure Elements Security Center

Introduction to the WithSecure Elements solution

Overview of the WithSecure Elements solution and its offering.

WithSecure Elements in a nutshell

WithSecure Elements is our single modular solution made up of a full range of cyber security applications that offer end-to-end business and cloud coverage. The product includes our award-winning technologies in vulnerability management, patch management, endpoint protection, and endpoint detection and response. In today's unpredictable, ever-changing business environment, our all-in-one security solution helps to build and ensure a resilient business.

The WithSecure Elements offering

WithSecure Elements has been specifically designed to support the modern agile business environment, which constantly needs to adapt not only to the external threat landscape, but also to the changing business needs.

To highlight some of the main benefits:

- Centralized and streamlined cyber security management to improve productivity
- All the needed software components integrated into one for smooth deployment
- Available as a fully managed service or as a self-managed cloud solution

The solution also offers flexible licensing options, which means that you can pick and choose which of WithSecure Elements applications your business needs.

Supported languages

The Elements Security Center supports the following languages:

- English (US), Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), Swedish

Endpoint products support the following languages:

- English, Czech, Danish, Dutch, Estonian, Finnish, French, French (Canadian), German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Portuguese (Brazilian), Romanian, Russian, Slovenian, Spanish, Spanish (Latin America), Swedish, Turkish, Traditional Chinese (Hong Kong), Traditional Chinese (Taiwan), and Simplified Chinese (PRC).

WithSecure Elements training

For an introductory Elements training session, log into the WithSecure Academy via the Partner Portal.

Accessing the WithSecure Elements Security Center

You can access Elements Security Center as follows: elements.withsecure.com

1.1 Using WithSecure Elements Security Center

Basic tasks for everyday use of WithSecure Elements Security Center, including managing access rights and administrator accounts.

This chapter describes the following tasks:

- managing access rights
- adding new administrator accounts
- adding customer companies

- using the *scope selector* to broaden or narrow the scope of information displayed in WithSecure Elements Security Center

You can order WithSecure Elements products to users in the customer companies, as well as manage the subscriptions of the products installed on the companies' computers and mobile devices.

1.1.1 Get started with WithSecure Elements Security Center

Get started with WithSecure Elements Security Center in four steps: log in, set up multi-factor authentication, add administrators, and assign a subscription.

You need a WithSecure Business Account to access Elements Security Center at https://elements.withsecure.com/. There are two ways to get an account:

- When you buy the product from a WithSecure partner, the partner usually creates the account for the first administrator. You then receive an email with a temporary password and a login link.

TIP: If the email has not arrived, check your junk mail folder first.

- If you have a subscription key but no account yet, create the first administrator account with the self-registration link https://elements.withsecure.com/self-register.

This quick start guide walks you through the four main steps to start using WithSecure Elements Security Center: log in, set up multi-factor authentication, add administrator accounts, and assign a subscription.

1. Log in to Elements Security Center.
   a) Log in at https://elements.withsecure.com/ with your Business Account credentials. For the login options, see Logging in.
   b) If you manage more than one company, switch between them with the scope selector, as described in Move between the managed companies.
2. Set up multi-factor authentication (MFA).
   a) Turn on MFA for your account, as described in Choose multi-factor authentication.
   b) Choose an authentication method that fits your needs. For the available methods, see MFA methods.
3. Add administrator accounts.
   a) Invite additional administrators and assign their roles, as described in Invite Security Administrator to company organization.
4. Assign a subscription and deploy a product.
   a) Assign a subscription key for the company, as described in Assign a subscription key for a customer company.
   b) Download the installer for the product that you want to deploy, as described in Download software from Elements Security Center.

Follow the quick start guide for the specific product that you want to deploy to complete the setup.

1.1.2 Logging in

Requirements for logging in to WithSecure Elements Security Center using a Business Account.

You need a WithSecure Business Account to access Elements Security Center. When you purchase the product from a WithSecure partner, the partner typically creates a Business Account for the first administrator in your organization. If this applies to you, you have received an email from WithSecure with a temporary password and a link to log in to Elements Security Center.

If your account has not yet been created, but you have received a subscription key from your partner, you can use the subscription key to create a WithSecure Business account for the first administrator in your organization. To do that, use the company self-registration link for your specific region.

Log in to non-federated domains

Logs in to a non-federated domain using your username and password.

To log in to a non-federated domain, do the following:

1. Open the following link in the web browser: https://elements.withsecure.com/.
   *The **Log in** page opens.*
2. Enter your username and password, and select **Log in**.

NOTE: If you do not have login credentials, ask your contact person for portal access. If you forget your password, you can order a new one by selecting **Forgot password**. Instructions for resetting your password are sent to your email address.

Elements Security Center opens. You can toggle between the services using the navigation menu in the sidebar.

Log in to federated domains

Logs in to a federated domain using Microsoft Entra ID credentials.

To log in to a federated domain, do the following:

NOTE: Before attempting authentication via SSO, make sure that you have an Entra account. If you are a new user, you must create one.

1. Open the following link in the web browser: https://elements.withsecure.com/.
   You are redirected to the Microsoft login page.
2. Enter your Entra credentials, and select **Log in**.

IMPORTANT: If you are a first-time user and you had a WithSecure Business Account before the domain was federated, you are redirected to the Microsoft login page to enter your Microsoft credentials for authentication. This links your account to federated single sign-on. For subsequent logins, authentication will be handled via SSO using the Microsoft Entra ID account.

Elements Security Center opens. You can toggle between the services using the navigation menu in the sidebar.

Multi-factor authentication

Multi-factor authentication (MFA), also know as two-factor authentication (2FA), is a method of increasing security during the login process to systems.

MFA protects you and your environment against, for example, phishing and credential stuffing attacks.

IMPORTANT: We strongly recommend that you use Multi-Factor Authentication (MFA) to keep your WithSecure Elements Security Center access secure. To keep your Elements Security Center use as smooth as possible, we suggest that you take MFA into use immediately.

IMPORTANT: We recommend that, as a backup, you use more than one multi-factor authentication method. If your only multi-factor authentication method is lost, the account needs to be re-created.

When users log in to a system with their username and password, their credentials may already have been compromised, for example, due to a vulnerability in their browser or password manager. These leaked credentials may be on some publicly accessible list, used by attackers to gain entry into systems. With the addition of MFA, an extra step is needed when logging in. System access is traditionally protected with username and password, something that only you know. MFA introduces additional factors; something that you have (a security key or device) and something that you are (your fingerprint or facial recognition).

MFA methods

WithSecure Elements has multiple MFA methods to keep your access safe as possible.

The methods include the following:

- *Authenticator applications with Time-Based One-Time Password (TOTP)*, such as Microsoft Authenticator, Google Authenticator, Auth0 Guardian, or other authenticator applications that are available either on your computer or mobile devices. A six-digit authentication code is sent to the Authenticator application, and you need to enter it into the login dialog to continue.
- *Push notifications with Auth0 Guardian authenticator* - allows you to approve an authentication request with a single click of a button. The Auth0 Guardian Multi-Factor Authenticator application is available in Google Play and AppStore.
- *Phone number for Short Message Service (SMS) messages with One-Time Passwords (OTP)* - A six-digit authentication code is sent to your configured mobile phone number via SMS. You need to enter the code into the login dialog to continue.

IMPORTANT: SMS messages are vulnerable to security breaches and malicious software, and receiving them may also charge you extra fees. For these reasons, we recommend that you only use SMS when there are no safer alternatives for you to use.

TIP: If you request several SMS codes in a short time, further messages might be blocked temporarily. The block clears after a short while. For everyday sign-in, we recommend an authenticator app or a security key (WebAuthn/FIDO2), which are more reliable than SMS.

- *Secure USB keys*, such as Yubico YubiKey, Google Titan, and others that support the FIDO2 standard (https://fidoalliance.org/fido2/)
- *Smartphones or other devices* that support the FIDO2 standard (https://fidoalliance.org/fido2/)
- *Device biometrics*, fingerprint or facial recognition or Windows Hello from your device using WebAuthn (https://www.w3.org/TR/webauthn/).

IMPORTANT: Device biometrics are specific to individual devices and it **must not be the only authentication method that you use**. You are prompted to add this authentication method for each device that you use.

Choose multi-factor authentication

Chooses one or more multi-factor authentication methods.

Before you choose a multi-factor authentication method:

- Install an authentication app, for example, Google Authenticator on your mobile device.

- Make sure that your mobile device can read QR codes.

Choose the most secure authentication method available to you. FIDO2 is the best option, followed by authenticator apps. SMS should only be used as a last resort. Note that if you lose your mobile device and have not backed up your security keys or authenticator app, you will lose access to your account, so SMS can be used as a backup method in such situations.

TIP: Register more than one authentication method. If you lose access to all of your authentication methods, the account cannot be reset and must be re-created.

To choose one or more multi-factor authentication methods:

1. Log in to WithSecure Elements Security Center with your email address and password.
2. Select
   
   at the top-right corner, then select **My settings**.

   NOTE: If you have already configured one or more MFA methods, select **Change**.

   *The **Multi-Factor Authentication Settings** window opens.*
3. Select **Add** to select one or more of the authentication options that you want to use.
   *The **Verify your identity** screen opens.*
4. Follow the instructions on the screen. The required actions depend on the MFA method that you selected.
   Multi-factor authentication is now set up for your WithSecure Elements account.

   NOTE: We recommend that you select multiple multi-factor authentication methods as a backup. If your only multi-factor authentication method is lost, there is no way to reset the multi-factor authentication. If all multi-factor authentication methods are lost, the account needs to be re-created.

Remove a multi-factor authentication

Removes a multi-factor authentication method.

To remove a multi-factor authentication method:

1. Log in with your email address and password.
2. Enter your multi-factor authentication code and select **Continue**.
3. Select
   
   at the top-right corner, then select **My settings**.
4. Select **Change** next to **Multi-factor Authentication enabled**.
   *The **Verify your identity** window opens.*
5. Follow the instructions on the screen.
6. Select **Remove** next to the multi-factor authentication methods that you want to remove.
7. Enter your email address and password.

Use device biometrics

Biometric authentication requires that you first have another multi-factor authentication (MFA) method in use.

To use device biometrics, do the following:

1. In Elements Security Center, select 
   at the top-right corner, and select **My settings**.
   *The **My settings** window opens.*
2. If you already have one or more MFA methods configured, select **Change**.
   *The **Use fingerprint or face recognition to log in** window opens.*
3. Select **Try another method**.
4. Use your already configured MFA method to verify your identity and select **Continue**.
   *The **Log in faster on this device** window opens.*
5. Select **Continue**.
   *The **Save your passkey** window opens.*
6. Select **Continue** to save the passkey to your device, and then select **Ok**.
   *The **Device registration successful** window opens.*
7. Select **Continue**.
   *The **Multi-factor authentication settings** window now shows your new device biometric key.*
8. At the bottom of the screen, select **Back** to return to the **Home** page

The next time that you log in to Elements Security Center on this device, you can authenticate using your biometric key, which makes the process faster and more secure.

1.1.3 User management

Instructions about access rights, adding and managing customer companies, and adding and managing administrator accounts.

This section describes how to manage who can access WithSecure Elements Security Center, including access rights and roles, the scope selector, and adding and managing administrator accounts.

About access rights

New users who have been granted access to Endpoint Protection (EPP) features do not automatically receive access to Extended Detection and Response (XDR) features. Administrators can assign EPP and XDR capabilities to separate user groups and combine them as necessary.

New users who get granted access to Exposure Management must also be assigned the Vulnerabilities role to manage vulnerability-related matters, including configuring scans and running reports.

You can set access rights when you create a new account, or edit an existing account.

Access rights by role

The roles and access rights available for each WithSecure Elements product area, with the audit-log entry for each role.

Exposure Management – Exposure

Full editing Allows access to the following Exposure Management features:

- Environment: Devices, Cloud, Network, Exposure, Identities
- Security configurations
- Reports

- Management
- Cloud onboarding

NOTE: Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)

Audit logs entry: cspm: admin

Exposure Management - Vulnerabilities

Management Allows full access to the Vulnerability Management views, settings, and findings

NOTE: Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)

Audit logs entry: vm: administrator

Team member Allows access to the Vulnerability Management views, settings, and findings, with no permission for managing users and the system.

Audit logs entry: vm: team_member

Read-only View-only access with no permission for managing users.

Audit logs entry: vm: readonly_team_member

Collaboration Protection

Admin Allows the access to the Collaboration Protection views and edit the following protection features:

- Handling detections
- Managing Exchange and shared files settings
- Managing policies, quarantining files, and generating reports

Audit logs entry: cpo365:admin

Read-only Grants view-only access to the Collaboration Protection views.

Audit logs entry: cpo: readonly

Quarantine manager Allows access to the Collaboration Protection views that are related to detections and quarantining files.

Audit logs entry: cpo365:quarantine_mgr

Collaboration Protection - Management

Admin Allows the access to management features, including user creation, role management, subscription details, and organization settings.

NOTE: Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)

Audit logs entry: fusion_admin

Endpoint Protection

No access

No access to Endpoint protection features including:

- Device management
- Patch management
- Device security posture
- Software reputation
- Security Events
- Profiles
- Home/Endpoint protection
- Reports

NOTE: Unless access is coming from some other role, for example Exposure.

Endpoint Protection - Computers and mobiles

Full editing

Allows the access to the following features:

- Security configuration/profiles
- Security information, including device status, dashboard, security events and patch management
- Security operations, such as removing or isolating devices, updating profiles
- Handling subscriptions
- Managing user accounts
- Do cloud onboarding

NOTE: The Security Administrator role, along with the "Servers - Full editing" role is required to create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role).

Audit logs entry: epp: manage_computers_mobiles_only

or epp: manage_all

Read-only

Read-only access with no permission to perform operations or manage other users and profiles.

Audit logs entry: epp: manage_servers_only

or epp: readonly

Endpoint Protection - Servers

Full editing

Allows the access to the following features:

- Security configurations/profiles
- Security information, including device status, dashboard, security events and software updates
- Security operations, such as removing or isolating devices, updating profiles
- Handling subscriptions
- Managing user accounts

NOTE: The Security Administrator role, along with the "Computers and mobiles - Full editing" role is required to create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role).

Audit logs entry: epp: manage_servers_only

or epp_manage_all

Read-only Read-only access with no permission to perform operations or manage other users and profiles.

Audit logs entry: epp: manage_computers_mobiles_only

epp: readonly

Extended Detection and Response – Toggle off

No access No access rights to view Extended Detection and Response (XDR) content across the following areas:

- Broad Context Detections
- Response actions
- Automated actions
- Dashboard content related to Detection and Response
- Software Reputation
- Organization Settings related to Detection and Response
- Event Search pages
- Elevate to WithSecure
- Subscription view

Extended Detection and Response – Broad Context Detections

Full editing Permission to manage:

- Broad Context Detections (for example, change status and close detections)
- My Reports
- Detection and Response-related content on the Dashboard
- Software Reputation and Organization Settings related to Detection and Response
- Elevate to WithSecure when applicable
- Requests

Limited access to:

- Devices view
- Cloud view
- Subscription view

Issuing Quick Actions requires additional roles, such as Execute Responses.

NOTE: This does not grant permission to configure the Cloud Tenant. Full editing rights under Computers and Mobiles are required for that level of access.

Audit logs entry: elements:xdr-incident-full

Read-only Default value when Extended Detection and Response (XDR), which allows read-only access to:

- Broad Context Detections
- My Reports
- Detection and Response-related content on the Dashboard
- Software Reputation
- Organization Settings related to Detection and Response
- Elevate to WithSecure when applicable
- Devices
- Cloud views
- Requests

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-incident-read

Extended Detection and Response – Response

Execute responses Access to execute:

- response actions
- configure Automated actions

Limited access to Cloud view.

Audit logs entry: elements:xdr-response-full

List responses Access to review:

- executed response actions
- respective results available

Limited access to:

- Devices view
- Cloud view

Download response results requires the Execute Responses permission.

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-response-read

No access No access to execute or review:

- Response actions
- Automated actions

Extended Detection and Response – Event Search

Read-only Access to review, execute filtered searches and create customized views to event data.

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-event-search

No access No access to review event data.

Elements Administration

No access	No rights to create new users or manage other users access rights.
Identity and Access Management	Rights to create, delete and manage all Elements users.

Move between the managed companies

Use the *scope selector* to broaden or narrow the scope of information displayed in WithSecure Elements Security Center.

In Elements Security Center, there are different account levels, which determine the access rights:

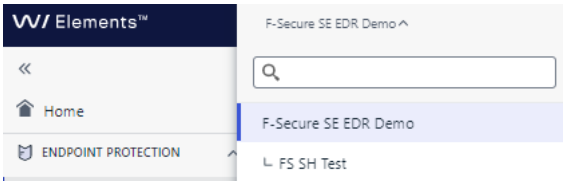
- Solution Providers (SoPs) manage Service Partners and groups of companies. They can access Elements Security Center to manage security and subscriptions for their directly managed companies, their Service Partners, and their Service Partners' companies.
- Service Partners (SePs) manage a group of companies. They can access Elements Security Center to manage security for their directly managed companies.
- Each company manages a single company. Companies that are managed by a SoP or SeP can request access from their provider, whereas companies that manage their own security can be provided full access to Elements Security Center. Companies that are managed by a SoP or SeP or directly by WithSecure get read-only rights to Elements Security Center.

To use the scope selector to focus on a particular company:

1. Select the

   icon at the title bar.
   A dropdown menu is displayed, listing all the customer companies associated with your account.

2. Select the desired company or write its name in the Search field, and then select **Enter**.
   The name of the selected company is shown with a blue background color and the page is updated to show the relevant information for the selected company.

Elements Identity and Access Management (IAM) role

The Identity and Access Management (IAM) role is authorized to grant and revoke all Elements permissions for security administrators within the IAM administrator's own organization and affiliated entities.

Overview

The IAM role is a powerful role within WithSecure Elements. It is designed to streamline and enhance the management of security capabilities and services.

IAM administrators have the authority to manage security roles within their own organization and affiliated entities. This includes granting and revoking roles for security administrators.

As the Elements ecosystem expands, IAM administrators will also manage new capabilities and services, eliminating the need for a cumbersome self-registration process.

Security administrators access Elements Security Center using WithSecure business accounts. Their access is organized according to specific features, capabilities, and services. The IAM role simplifies the process of assigning roles across different capabilities, which was complex before.

Benefits

The IAM role provides several benefits, including the following:

- Streamlined role management across WithSecure Elements
- Enhanced security through centralized control
- Adapting to future needs with the ability to manage new capabilities and services

Claiming the IAM role

For users whose IAM role does not involve an escalation of privilege (i.e., they posses all legacy user access management roles within the organization), the Security Administrators view shows a banner offering them the opportunity to claim the new IAM administrator role. Every organization should carefully consider how they manage IAM-related privileges, as these are distinct from security administrative roles. So, fewer individuals can act as IAM administrators compared to when this option was not available.

Elements IAM role properties

Holders of the IAM role (also known as IAM administrators) can grant or revoke access to any other capability or service-specific role within their organization and its child organizations.

IAM administrators can do the following:

- Grant themselves any other role, so they gain access to security capabilities or services
- Grant or revoke new roles introduced by WithSecure for Elements capabilities or services
- Create or delete WithSecure business accounts by granting or revoking roles.
- Transfer IAM permissions to other security administrators within the same organization or its child organizations.

Acquiring the IAM role

Organizations that manage their own security or provide security capabilities to others must have at least one IAM administrator. The IAM role can be acquired by one of the following ways:

- Being granted the role by another IAM administrator within the same or a parent organization
- Self-registration with an Elements subscription issued for the company
- Onboarding by WithSecure for new partners or customer companies

Existing capability or service-specific roles remain effective but they will eventually be managed through the IAM role. The IAM role will also safeguard access to features that are currently managed by other roles, such as configuring API keys.

Migration of IAM permissions

The migration process aims to transition from legacy, capability-specific IAM roles to the new Elements IAM role, which grants higher privileges. During this process, Elements identifies eligible users and prompts them to claim the new IAM role.

Candidates for the IAM role are identified based on their possession of legacy, capability-specific IAM roles and by reviewing active company subscriptions:

For customer companies Security administrators with the following identified legacy roles:

- Elements Exposure Management: Full editing
- Elements Collaboration Protection: Management administrator
- Elements Vulnerability Management: Administrator
- Elements Endpoint Protection - Computers, servers, and mobiles: Full editing

For Solution Providers and Service Partners	Security administrators with legacy roles for all capabilities and services used by the companies they manage

NOTE: The policy for partners differs from that for customer companies, making sure that only eligible administrators claim the IAM role.

When IAM administrator candidate cannot be identified

In some organizations, the allocation of legacy, capability-specific roles among security administrators may result in a situation where no single user possesses the same effective access as that granted by the IAM role. This could occur, for example, if a company employs both Elements Endpoint Protection and Elements Collaboration Protection capabilities, but these capabilities are managed independently by two different individuals, with no one person overseeing both at the same time.

Frequently asked questions about IAM roles

Answers to frequently asked questions about IAM roles.

Question	Answer
Can partners (SOP/SEP) create IAM roles for all companies under them?	Yes, IAM administrators at the partner level can fully manage their own organization and organizations under them excluding companies that have chosen to isolate their XM/CP access from SOPs.
What should a company administrator do if the company misses the IAM deadline (end of April 2025)?	The company administrator must contact their Service partner for assistance or reach out to WithSecure support.
When creating a new user using the self-registration portal, does the first administrator get an IAM role automatically?	Yes, the first administrator is granted the IAM role automatically.
What happens if someone accidentally selects Decline when claiming the highest-level administrative role?	If a user accidentally declines the IAM role claim, any other IAM administrator can still assign them an IAM role, if necessary.
Can an Endpoint Protection administrator user who selects **Decline** still add other Endpoint Protection administrator users?	Yes, for time being, this is still possible. In the future, all user management action rights will be restricted to IAM role holders only.
Can one organization have multiple IAM administrator users?	Yes, there is no limit to the number of IAM administrators that an organization can have.
Why are the Claim and Decline options not displayed for some administrator users?	In the first stage, the IAM Claim button is shown to users who have full administrator rights on all products for which the organization has subscriptions. For example, if a company has subscriptions for Elements Endpoint Protection and Collaboration Protection, the IAM Claim button is shown to users with full administrator roles on both products.
How can I find out who in my organization has claimed an IAM role?	The IAM role is shown, and users with the role can be filtered in a table under **Management** > **Security Administrators**.

Add a new administrator

You can provide a designated individual, known as an *administrator*, with a user account with required rights in WithSecure Elements Security Center.

You can add an administrator for the Solution Provider, Service Partner, or for a company account.

To create an administrator account:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
2. Select the **Security Administrators** tab.

   NOTE: You can create an administrator account for either your Elements Security Center account or for a specific customer company

3. Using the *scope selector*, select the organization level on which you want to create a new administrator account.
4. Select **Add administrator**.
5. In the **Add administrator** screen, fill in the administrator details:
   a) Enter the email address.

      NOTE: The email address must be a valid one and accessible by an actual account user. Do not use shared accounts.

   b) Select the desired language for the new administrator.
6. Select **Next**.
7. In the **Roles** screen, select the roles that the new administrator needs to have.

   NOTE: If the new administrator is not allowed to have a full access in a feature-specific role, leave the default **No access** option as is.

8. Select **Next**.
   The Summary screen opens.
9. Check that the administrator details the selected roles are correct, and then select **Add** to complete adding the new administrator.

A new administrator account is created.

NOTE: The user receives an email with instructions on how to set up a password for the new account.

Add a new service partner

To create a service partner account:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page is displayed.*
2. Select the **General** tab.
3. Select ··· and then select **Create service partner account**.
   *The **Create service partner account** view opens.*
4. Enter a name for the organization account, and select **Save**.

The service partner account is created.

Edit or remove administrators

You can edit or remove administrators accounts.

Edit an administrator's role assignments, or remove their access entirely — removing all roles automatically deletes the account.

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page is displayed.*
2. Select the **Security Administrators** tab.
3. In the **Email** column, select the email address of the administrator account that you want to edit or remove.
   *The **Summary** screen opens.*
4. To edit the details of the administrator account, do the following:
   a) Make the needed changes to the administrator roles.
   b) Select **Save**.
   The details of the administrator account are updated.
5. To remove the administrator account, select **Delete**.

NOTE: When you remove all the access rights from an administrator account, the account is automatically deleted when you save the changes.

The administrator account is deleted.

Create an API client

You can create an API client to let an application use the Elements API with specific access rights.

An API client provides credentials that let an application use the Elements API. An API client has either full access or is limited to read-only access, depending on whether you select the **Read-only** option when you create it. For the available API operations, see the Elements API reference.

To create an API client:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
2. Select the **API Clients** tab.
   The tab shows the organization's UUID and a list of existing API clients.
3. Select **Add new**.
   *The **Add new API client** dialog opens, starting with the **Details** step.*
4. Select the organization for the API client, enter a description, and select **Read-only** to limit the client to read-only access.
5. Select **Add**.
   *The **API client** step opens, showing the generated client ID and secret.*
6. Copy the secret and store it in a safe place.

IMPORTANT: You cannot view or access the secret again after this step.

7. Select **I have copied and stored the secret**, and then select **Done**.
   The new API client appears in the list, with its client ID, access rights, and creation date.

A new API client is created.

Delete an API client

You can delete an API client that an application no longer needs.

When you delete an API client, any application that uses its credentials can no longer access the Elements API with them.

To delete an API client:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
2. Select the **API Clients** tab.
   The tab shows a list of the organization's API clients.
3. In the row of the API client that you want to delete, select the trash icon, and confirm that you want to delete it.
   The API client is deleted.

Recover your password

If you have forgotten your password, you can recover it through the **Forgot password?** link.

To recover your password:

1. On the login page, select the **Forgot password?** link.
   The Reset password mail sent window opens.
2. Enter your username or email address.
3. Select **Send**.

You will receive an email message with instruction on how to change your password.

Change your account details

Change your user name in WithSecure Elements Security Center. Federated users manage their account details in their identity provider.

You can change your user name in WithSecure Elements Security Center from your account settings.

IMPORTANT: If your organization uses federated sign-in (Entra ID), you cannot change your account details in WithSecure Elements Security Center. Manage your details in your identity provider instead.

To change your user name:

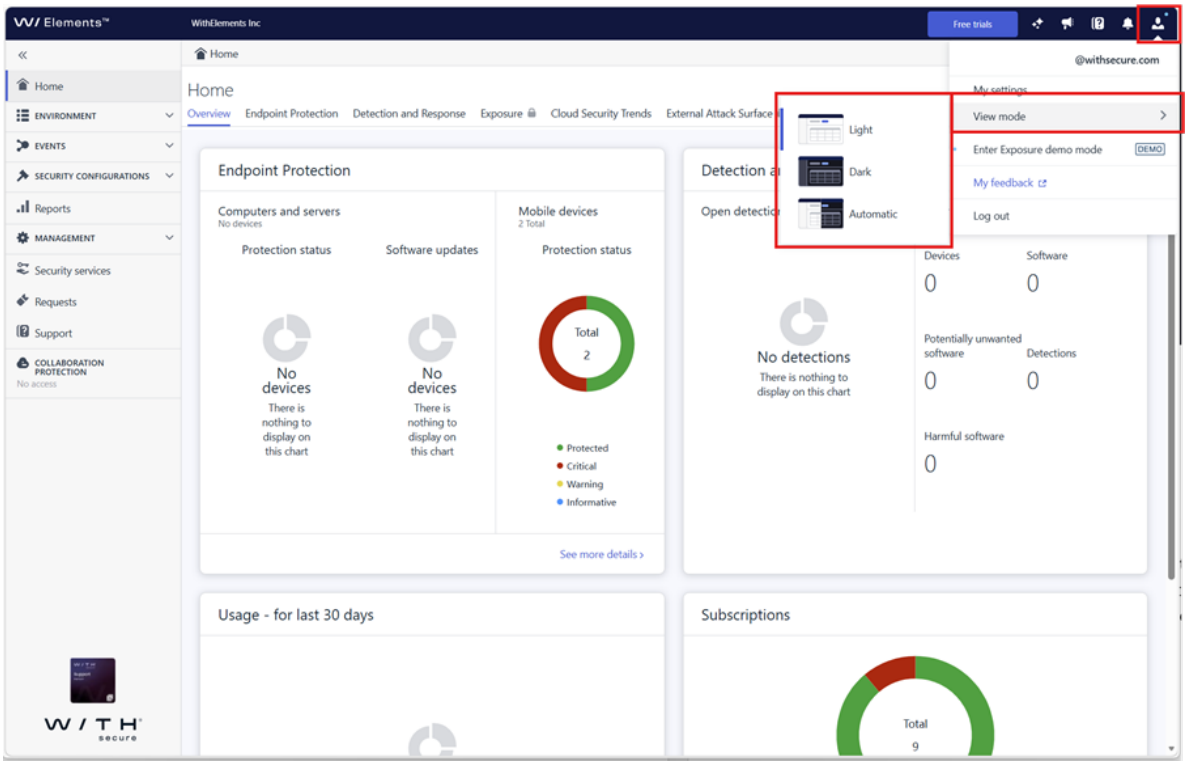
1. Select
   
   at the top-right corner, then select **My settings**.
2. Under **Details**, enter a new user name.
3. Select **Save**.

1.1.4 Change the view mode

Select a light, dark, or automatic view mode to customize the appearance of WithSecure Elements Security Center.

You can customize the appearance of Elements Security Center by selecting the view mode that best fits your preference. Dark mode is useful in low-light environments such as control rooms or during night shifts. To change the view mode:

1. Select the user profile menu icon at the top-right corner of the portal.
2. Select **View mode**.
3. Select one of the following options:
   - **Light** – a bright interface suitable for well-lit environments.
   - **Dark** – a darker interface that reduces eye strain in low-light conditions.
   - **Automatic** – matches the system settings of your device and switches between light and dark automatically.



The new view mode is applied immediately. You can change it at any time by repeating these steps.

1.1.5 Taking Elements products into use

Taking WithSecure Elements products into use includes a number of steps.

1. Adding a customer company, if not yet added.
2. Getting a subscription.

> **NOTE:** Under **Management** > **Subscriptions**, you can view all your products, your available subscription keys, and when they expire.

3. Adding the subscription to the customer company.
4. Deploying the product.

> **NOTE:** You can find instructions for deploying Elements products in Common deployment methods.

Adding a customer company

To add a new *customer company* to your WithSecure Elements Security Center account, you must first add it as a *new customer* to your *WithSecure Partner Portal* account and purchase at least one WithSecure Elements product for it.

NOTE: Only Solution Provider and Service Partner users can add customer companies.

If you need an administrator to manage the subscriptions and devices in the new customer company, create an administrator account through Elements Security Center.

NOTE: The WithSecure Partner Portal is an online service that works with Elements Security Center. It provides tools, materials and an integrated eOrdering system to help with sales and support of WithSecure solutions.

The purchase order for the new customer must first be added successfully from your Partner Portal account. Once this happens, the customer is automatically added as a new company to your Elements Security Center account.

You can then begin offering WithSecure Elements products to users in the customer company, as well as managing the subscriptions for purchased products.

Assign a subscription key for a customer company

By assigning a subscription key for a company, you can add more computers to WithSecure Elements Security Center.

You need to consider the following:

- Solution Providers and Service Partners can assign subscription keys for their customer companies.
- Company users can assign unused subscription keys that are provided by their partner to their own organizations.
- Users must be granted a full editing role in the Endpoint Protection software (applies to both computers and servers).
- The subscription must be allocated at a partner level (the subscription key must exist). The partner can find the subscription key in the **Subscriptions** view under **Management** on the sidebar.

NOTE: Company users must request for a subscription key from their partner.

To assign a subscription key:

1. Under **Management**, select **Subscriptions** on the sidebar.
2. Using the *scope selector*, select the company to which you want to assign the subscription key.
   A table opens listing the current subscriptions of the selected company.
3. Select **Assign subscription** above the filters.
   *The **Assign subscription** page opens.*
4. Enter the new subscription key for the company, and select **OK.**

The new subscription key is added to the company account.

Order products for an existing customer company

Order WithSecure Elements products for an existing customer company via WithSecure Partner Portal.

> **NOTE:** Only Solution Providers and Service Partners can order products for customer companies.

To order WithSecure Elements products for an existing customer company via WithSecure Partner Portal:

1. Log in to the portal by opening the following link in your web browser: Partner Portal

   > **NOTE:** WithSecure Partner Portal requires separate login credentials from WithSecure Elements Security Center. If you do not yet have your login details, fill in the **Request Credentials** form on the page and click **Send**. Please allow up to 24 hours to receive your access credentials.

   *The **eOrdering** page is displayed.*
2. On the main page, select **My Customers**, and then select the name of the customer company for which you are ordering products.
3. In the **Order** column, select either **New SaaS Order** or **New Yearly Order**.
   The Welcome to Ordering window opens.
4. Under **New Order**, enter a reference number for your order.
5. Under **Order Products**, select **Add Products**.
6. Select the required products and follow the ordering instructions.

Once your purchase order is completed, the change in product information will be updated in your WithSecure Partner Portal and Elements Security Center accounts.

Order products for a new customer company

Order WithSecure Elements products for a new customer company via WithSecure Partner Portal.

> **NOTE:** Only Solution Providers and Service Partners can order products for customer companies.

To order WithSecure Elements products for a new customer company via WithSecure Partner Portal:

1. Log in to the portal by opening the following link in your web browser: Partner Portal

   > **NOTE:** WithSecure Partner Portal requires separate login credentials from WithSecure Elements Security Center. If you do not yet have your login details, fill in the **Request Credentials** form on the page and click **Send**. Please allow up to 24 hours to receive your access credentials.

   *The **eOrdering** page is displayed.*
2. On the main page, select **New Order**.
3. Enter the name of the new customer company and select **Add New**.
   *The **New Customer** window opens.*
4. Fill in the customer details and select **Save**.
5. Under **New Order**, enter a reference number for your order.
6. Under **Order Products**, select **Add Products**.
7. Select the required products and follow the ordering instructions.

Once your purchase order is completed, the new customer company is listed in your Partner Portal account, together with the purchased products.

NOTE: It might take a while for the new customer company to show in your Elements Security Center account.

View available product subscriptions

To view the available subscriptions:

The Subscriptions view lists every product subscription for the scope you're viewing, along with keys, status, and expiration, so you can find and manage them across your organizations.

1. Under **Management**, select **Subscriptions**.
   The Subscriptions view opens showing the subscriptions for each product, the subscriptions keys, and the organizations to which the subscriptions belong.

   NOTE: If the *scope selector* is set to display all the customer companies, by default, you see all the subscriptions.

2. You can use filtering to find the following:
   - Subscription key - enter the relevant subscription key
   - Product - select from a list of available products
   - Expiration - select **Valid** to see valid subscriptions; **Expiring in 14 days** or **Expiring in 60 days** to see subscriptions that are expiring soon; or **Expired** to see only subscriptions that have expired
   - Type - you can select from the following subscription types: **Commercial**, **Evaluation**, **Governmental**, **Educational**, or **Not For Resale**.

   To see the subscriptions for a specific customer company, use the *scope selector* and select the company that you wish to view.

   NOTE: When you select to view a specific customer company, no filters are used.

Change the subscription key

Changes the subscription key for one or more devices in WithSecure Elements Security Center.

To change the subscription key:

NOTE: A subscription key cannot be changed for Elements Connector or any EPP subscription variant if the change would require downgrading to a subscription that does not include EPP.

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page opens.*
2. Select the devices for which you want to change the subscription key.
   A menu is displayed at the bottom of the page.
3. Select **Change subscription**.
4. Enter a new subscription key in the field that appears, and select **Change subscription**.

   NOTE: Under **Management** > **Subscriptions**, you can find the available subscription keys for the devices of the selected company.

   The new subscription key is applied to the selected devices.

Upgrading your subscriptions

Options for upgrading your WithSecure Elements subscriptions.

This chapter describes how to upgrade your WithSecure Elements subscriptions and the upgrade options that are available.

Upgrading your subscriptions

You can upgrade your subscription in two ways:

- By changing the type of your subscription key (ordering a new one)
- By changing to another subscription key on your device

You have the following options in upgrading your subscriptions:

- WithSecure Elements EPP for Computers to WithSecure Elements EPP for Computers Premium
- WithSecure Elements EPP for Computers to WithSecure Elements EDR and EPP for Computers
- WithSecure Elements EPP for Computers to WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EPP for Computers Premium to WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EDR and EPP for Computers to WithSecure Elements EDR and EPP for Computers Premium
- WithSecure Elements EPP for Servers to WithSecure Elements EPP for Servers Premium
- WithSecure Elements EPP for Servers Premium to WithSecure Elements EDR and EPP for Servers Premium

NOTE: You can use the same installer file for both Standard and Premium versions of WithSecure Elements EPP for Computers or WithSecure Elements EPP for Servers and any combination of WithSecure Elements EDR and EPP for Computers or WithSecure Elements EDR and EPP for Servers.

If WithSecure Elements EDR is installed on a Windows computer, you need to reinstall it before you can upgrade to WithSecure Elements EDR for Computers or WithSecure Elements EDR for Computers Premium.

1.1.6 Federated single sign-on

Federated single sign-on (FSSO) lets users authenticate once with an identity provider and access several applications without logging in separately.

Federated single sign-on (FSSO) lets users authenticate once and access several applications or services across different domains or organizations. Users do not need to log in separately for each one. When users log in, they submit their credentials, such as a username and password, to an identity provider. The identity provider then checks these credentials. After successful authentication, the identity provider generates a digitally-signed token. This token proves the user's identity. When users access other applications or services in different domains or organizations, their browser automatically uses this token. The cloud identity service checks the token and grants access without requiring the user to log in again.

FSSO makes access across various systems simpler. It lets users authenticate once and move smoothly between different applications or services. It also improves security and user experience by removing the need for multiple logins. When a user is removed from an identity provider, they automatically lose the ability to log in to Elements Security Center. This makes managing user access easier and more secure.

Prerequisites

To link an Entra account to a WithSecure Elements account, the Entra ID tenant account must have the email address set up and matching the email address of the corresponding Elements account.

If the email address is not set up or does not match the email address of the corresponding Elements account, the linking fails, and the user is not able to access WithSecure Elements Security Center. User email address information is visible in the Microsoft Entra Admin Center under **Contact Information** > **Email**.

NOTE: All users must have an Elements account. There is no automatic user provisioning from Microsoft Entra ID.

Before implementing single sign-on (SSO)

The following lists things that you must take into account before implementing single sign-on (SSO).

Why is plus addressing problematic?

Microsoft Entra ID does not support email aliases or email addresses with plus addressing for authentication. When you configure SSO and start to use it, all email aliases and Elements user accounts with plus addressing stop working.

IMPORTANT:

Do not configure SSO using email aliases or Elements user accounts with plus addressing.

How to avoid users losing access to remove federation?

When implementing federation, make sure that there is a user account without plus addressing or email alias. Otherwise, you may lose access to Elements Security Center.

How does SSO change the login process?

After federation, users authenticate through Microsoft Entra ID, eliminating the need for a separate login flow for Elements Security Center.

How often do users with Elements Entra ID need to authenticate to Elements Security Center?

If users do not have a valid federated authentication session, Elements Security Center requires them to log in and authenticate.

Global impact of SSO

Implementing SSO affects all organizations and hierarchies with user accounts from federated email domain. Some users have accounts across various partner- and service partner-level hierarchies, and changes will affect all these hierarchies. For example, if Partner A has their own Solution Provider (SOP) and shares a domain with other partners' SOPs, the SSO will affect everything at the Elements level, not just the specific SOP. An email domain can only be federated once within an organization, but this will affect all user accounts associated with that domain.

Hierarchy-level considerations

Make sure to generate SSO from the appropriate hierarchy level, because it can be only modified from there.

Handling Microsoft Entra ID account removal

If a Microsoft Entra ID account is removed, the Elements administrator is not automatically deleted, but the account will no longer function. You need to manually delete the administrator.

Set up federated single sign-on with Microsoft Entra ID

Sets up federated single sign-on so users can sign in with their Microsoft Entra ID credentials.

For creating federated single sign-on, you need the following:

- A non-federated domain - a domain name, for example `yourcompanydomain.com`, that is not federated with Elements Security Center
- Elements Security Center account - an account in Elements Security Center with the assigned `Endpoint Protection Full editing` permission. This account is necessary for managing federated domains and later logging in to Elements Security Center using an Entra ID account.
- Entra ID tenant account - an account in the Entra ID tenant that manages the domain that you want to federate. This account is essential for logging in to Elements Security Center and federating the domain.

NOTE: The user who is federating a domain must have a global administrator role in the Entra ID tenant for this scenario. Once the domain is federated, any user with an Entra account can log in, provided they also have a corresponding Elements account.

Set up federated single sign-on so users can sign in to Elements with their Microsoft Entra ID credentials.

1. Log in to https://elements.withsecure.com.
2. Under **Management** > **Organization Settings** > **Security Administrators**, select **Configure federated single sign-on**.
   *The **Configure federated single sign-on** window opens showing the status of the domain that matches your email address.*
3. Select **Log in to Microsoft**
4. In the pop-up window that opens, enter your password for the Entra tenant, and select **Sign in**.
5. Select **Consent on behalf of your organization** and then select **Accept**.
   *The **Single Sign-on Access Federation** window is refreshed and shows **Validation successful**.*

NOTE: If you select **Cancel**, the window shows **Validation failed**. Other reasons for unsuccessful validation may include the process taking too long or a lack of the Global Administrator role.

6. To federate the domain, select **Enable federated single sign-on**.
   *After you have federated the domain, its status changes to **The Federated single sign-on is enabled for [domain name]**.*

Link user identities

Links user identities in Elements Security Center for federated domains.

NOTE: Every user with an email address in the domain only needs to link their identity once, during their initial login after the domain has been federated.

Make sure you have the following:

- A federated domain
- A user with an Elements account whose email address belongs to the federated domain

> 👉 **NOTE:** These accounts are manually created by other administrators. This flow occurs when the users log in for the first time.

- The user must not be currently logged in
- The account that is used to log in to Elements Security Center should not have undergone identity linking before

To link identities:

1. Log in to https://elements.withsecure.com.
2. Enter your email address and select **Continue**.
3. If your email address is already authenticated in the domain, you are redirected to the identity linking flow; if your email address is not yet authenticated in the domain, you are asked to provide your domain password.

   > 👉 **NOTE:** Depending on the domain configuration, you may need to go through multi-factor authentication (MFA).

4. Enter your email address again, and select **Continue**.
5. Next, enter your Elements account password and select **Continue**
   A window opens confirming that your business account is now going to be linked (federated) with your Entra ID account.
6. Select **Continue** to proceed.

Remove federation from a domain

Removes single sign-on federation from a domain.

Before you can remove federation from a domain, make sure you have the following:

- A federated domain
- An account in Elements Security Center with `Endpoint Protection Full editing` permission and an email address in the federated domain.

> 👉 **NOTE:** When federation is removed from a domain, users that have email address in that domain must use their Elements credentials to log in. However, if an Elements account was created after the domain was federated, users have not received an email with their initial password and do not know their Elements credentials. In that case, they must reset their password.

To remove federation:

1. Log in to https://elements.withsecure.com.
2. Select **SSO Access Federation**.
   *The **Federated Single sign-on** window opens showing the status of the domain that matches your email address.*
3. Select **Remove Federated Single sign-on**.
   A confirmation window opens.
4. Select **Ok**.
   Single sign-on federation is removed from the domain account.

1.1.7 Adding devices for management

To monitor and manage the security of a computer or mobile device by using your WithSecure Elements account, you must first install an Endpoint Protection software on the computer or mobile device.

Once the software is installed, the device will be added to your WithSecure Elements Security Center account. Through Elements Security Center, you can follow the performance of the security product, as well as manage its subscription, updates and other standard tasks.

NOTE: When you add a new device, the default profile is applied to it.

There are several ways in which you can install the Endpoint Protection software on the device that you wish to manage:

- Send to the device user an email with a link to the software installer and instructions on how to install and activate it.
- Download the software directly from Elements Security Center and transfer it to the device.

NOTE: This does not apply to WithSecure Elements Mobile Protection.

- Deploy the software through GPO, images, or RMM or MDM tools.

You can add several mobile devices at one go by importing a CSV file containing the required details for each device.

NOTE: Before you can add a new device, you must have a subscription for an Endpoint Protection software with at least one free installation available. The number of free installations available to a company will determine the number of devices you can add to it.

Distributing WithSecure software

Ways to distribute WithSecure Elements Endpoint Protection software to your devices.

- You can install the following software using the same WithSecure Elements Agent for Computers installation package. The subscription key determines which software is installed:
  - WithSecure Elements EPP for Computers (Windows and Mac)
  - WithSecure Elements EDR and EPP for Computers (Windows and Mac)
  - WithSecure Elements EDR for Computers (Windows, Mac, and Linux)

NOTE: When installing the software as a standalone, you must add an additional command-line parameter '`--skip-sidegrade`' to turn off automatic uninstallation of the existing Endpoint Protection software.

  - WithSecure Elements EPP for Computers Premium (Windows only)
  - WithSecure Elements EDR and EPP for Computers Premium (Windows only)
  - WithSecure Elements Exposure Management (Windows only)

- You can install the following software using the same WithSecure Elements Agent for Servers installation package. The subscription key determines which software is installed:
  - WithSecure Elements EPP for Servers (Windows and Linux)
  - WithSecure Elements EDR for Servers (Windows only)
  - WithSecure Elements EPP for Servers Premium (Windows only)
  - WithSecure Elements EDR and EPP for Servers Premium (Windows and Linux)

    - WithSecure Elements Exposure Management (Windows only)

- You can install WithSecure Elements Mobile Protection in two ways:
    - By sending an installation email via the WithSecure Elements EPP portal using the **Add new device**.

      NOTE: With all the Elements software (except for the Elements Connector), you can add devices by selecting the **Add new device** option and then choosing to send either one invitation or importing data from a CSV file to send multiple invitations.

    - By sending an installation email via a third-party MDM software.

- For installing WithSecure Elements Connector, see instructions at here.

Send an installation link via email

You can send company users an email with an installation link for an WithSecure Elements software.

NOTE: The installation link is valid for 30 days.

Using the link, company users can install the product on one of their device at their own convenience. Once the product is installed, the device appears in your WithSecure Elements account.

To provide the users with the software that you want them to install:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select
   
   next to **Devices**.
   A menu is displayed.
3. From the menu, select **Add new device**.
   *The **Add new device** page opens.*

   NOTE: If the *scope selector* is set to focus on a specific company, an **Add new device** button will also appear on the Home page, which you can click to go directly to the **Add new device** form.

4. Select the product.
5. From the drop-down menu, choose the language in which you want to send the invitation.
6. Enter the email address of the recipient to whom you want to send the invitation and other, optional details.

   To send multiple invitations, under **Import from CSV file**, select **Choose file** to select a CSV file from which you want to import data. Multiple email addresses must be separated by commas.

7. Select **Send**.
   The listed recipients receive an email that contains a link to the download site and instructions for downloading and installing the product that you selected.

   NOTE: To see the pending invitations, first select ··· next to **Devices**, and then select **Manage device invitations**.

> **NOTE:** The software is customized to use the subscription key that you selected on the **Add new device** page.

Once the product has been installed and activated on the device, it will show on the **Devices** page and the invitation disappears from the managed devices invitations page.

Download software from Elements Security Center

You can download WithSecure software installation packages through WithSecure Elements Security Center.

To download the software:

1. Log in to Elements Security Center.
2. Select **Downloads** on the sidebar.
   *The **Downloads** page opens.*
3. Locate the section for your device type, for example **WithSecure Elements Agent for Computers** or **WithSecure Elements Agent for Servers**.
4. Select the download button for your operating system.

   The available buttons depend on the operating system:

   - Windows: **Download .exe** or **Download .msi**
   - Mac: **Download .mpkg**
   - Linux: **Download amd64** or **Download arm64**

   The software is downloaded. The subscription key associated with your account is embedded in the installer.

Once the desired software has been downloaded, you can transfer and install it on the computer or mobile device you wish to manage. The subscription key is embedded in the product.

> **IMPORTANT:** Do not use a subscription key for "WithSecure Elements EDR only" in devices that have the WithSecure Elements EDR for Computers or vice versa. It may break the software, which you then need to manually remove.

After downloading the software, you need to deploy it.

Manage automatic deletion of devices

You can select to automatically delete devices that have been offline for a set number of days.

> **NOTE:** This feature does not apply to mobile devices.

> **NOTE:** You can set the automatic removal of devices only on the Company level.

You can define the period that a device needs to be offline before it will be deleted. If a deleted device becomes active, it is shown again in Elements Security Center if there are free seats in the subscription. If the subscription is full, the device is not shown in Elements Security Center and is not protected.

To turn on automatic deletion of devices:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page opens.*
2. Select ••• next to **Devices**.
   A menu is displayed.

3. From the menu, select **Manage automatic deletion**.
   *The **Manage automatic deletion** page opens.*
4. Turn on **Automatically delete devices...**.
5. In the box, enter the number of days for a device to be offline before it is deleted.

   NOTE: The minimum number of days is seven (7).

6. Select **Save**.

   IMPORTANT: If a removed device resumes its activity after being removed, it is automatically added back to your subscription, if your subscription has free space. However, if your subscription is full, the device is not returned to the subscription and is left without protection.

Manage invitations

You can send an email with an installation link that allows the recipient to install the app on one device.

To manage the invitations:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select

   Manage device invitations.
   *The **Manage device invitations** page opens.*

   The **Pending** tab lists those email invitations that include an installation link that has not been used yet. The **Expired** tab lists the expired email invitations.
3. For the pending invitations, you can send a reminder by selecting **Send reminder** as long as the installation link is valid (for 30 days). After that the invitations are shown under the Expired tab.
4. For the expired invitations, you can send another invitation link by selecting **Send new invitation**.

   NOTE: If there are devices that are no longer needed, for example, the user has left the company, you can delete the expired invitations from the table by selecting **Delete pending**.

1.1.8 Enhancing device management with custom labels

You can use labels to add customizable, flexible tags to your devices.

Adding labels allows you to group devices in any way that you prefer. They are commonly used to provide information about the region, operating system, owner, department, workstation vs. server, or any other criteria that suit your needs.

Labels help analysts by providing more context and they make it easier for you to manage devices within Elements Security Center.

Add device labels

You can add device labels in three different ways.

You can add device labels in the following ways.

> **NOTE:** In the command line, labels are called tags.

Add device labels in one of the following ways:

- Manually in the **Device** view: select the devices on the **Device list** view, or open a single device on the **Device details** view, then on the **Actions** panel select **Manage labels** > **Add labels**, select an existing label or add a new one, and select **Add**.
- Using label-assignment rules in the **Profiles** section: in Elements Security Center, go to **Security Configurations** > **Profiles** > **Profile assignment rules**, and add labels to an **Outbreak rule** or **Profile assignment rule** so that the labels are applied automatically whenever the rule matches.
- During the Elements agent installation process: assign installation tags as you deploy the agent. See step 2 in Assigning a default profile and installation tags for details.

1.1.9 Managing devices in Elements Security Center

How to manage the selected devices in WithSecure Elements Security Center

You can manage your devices in WithSecure Elements Security Center in several ways:

- Organize them into asset groups
- View and customize the device list
- Automatically delete inactive computers
- Request diagnostics

Managing asset groups

Asset groups provide a structured way to manage devices within an organization.

You can assign devices to asset groups in two ways:

- Manual assignment - assign devices to management groups from the **Devices** page.
- Automatic assignment - assign devices to groups based on profile assignment rules.

> **NOTE:** A single rule can assign a device to multiple groups.

Once devices are organized into groups, you can do the following:

- Filter devices by group
- Filter security events associated with a specific group
- List software updates for devices within each group

By using asset groups, you can enhance device visibility, streamline security event management, and prepare for advanced access control mechanisms in an organization.

Create asset groups

Creates an asset group at the company level.

> **NOTE:** Asset groups can only be created on company level. For example, as a partner, you must first select a company from the *scope selector* or from the list in the **General** tab under **Management** > **Organization Settings**.

1. Under **Management**, select **Organization Settings** > **General**.
2. Select **Create asset group**.
   *The **Create asset group** pane opens.*
3. Enter a name for the asset group.

4. (Optional) In the **Description** box, enter a description for the asset group.
5. Select **Save**.

Next, go to the **Devices** page to add devices to the asset group that you just created.

Add devices to asset groups

Adds devices to one or more asset groups.

Asset groups organize devices so you can target scans, scheduling, and reporting at them.

1. Under **Environment**, select **Devices**.
2. In the **Devices** page, select the devices that you want to add to one or more asset groups.
3. From the action menu at the bottom of the page, select **Manage asset groups** > **Assign to asset groups**.
4. From the drop-down menu, select one or more asset groups to which you want to add the selected devices.
5. Select **Assign**.

Remotely manage a device

To send a command to a selected device or manage it via WithSecure Elements Security Center:

To remotely manage a device:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select one of the following tabs:
   - **Computers** - shows devices with WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers
   - **Mobile devices** - shows devices with WithSecure Elements Mobile Protection
   - **Connectors** - shows devices with WithSecure Elements Connector
   - **Unmanaged devices** - shows devices in a customer Active Directory (not in EPP)
3. Select the checkbox next to the name of the device.
   A menu is displayed at the bottom of the page.
4. Select the desired operation from the menu.

NOTE: You can find operations also on the **device details** page. Some of the operations are shown only there.

The instruction is sent to the selected device.

Automatically delete devices

You can set WithSecure Elements Security Center to automatically delete devices that have been offline for a set number of days.

NOTE: This feature does not apply to mobile devices.

NOTE: You can set the automatic removal of devices only on the Company level.

To manage automatic deletion:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page opens.*

2. Select ··· next to **Devices**.
   A menu is displayed.
3. Select **Manage automatic deletion**.
   The Manage automatic deletion page opens.
4. Turn on the **Automatically delete device...** option.
5. In the box, enter the number of days for a device to be offline before it is deleted.

   NOTE: The minimum number of days is seven (7).

6. Select **Save**.

   IMPORTANT: If a removed device resumes its activity after being removed, it is automatically added back to your subscription, if your subscription has free space. However, if your subscription is full, the device is not returned to the subscription and is left without protection.

Devices that stay offline for the specified number of days are deleted automatically.

View devices based on the Active Directory structure

You can filter devices based on the Active Directory structure of a company.

You can use this feature to assign a different profile for the devices in different Active Directory groups, for example, to be used in different sites.

To view devices based on the Active Directory structure:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the
   
   icon at the top-left corner.
   A drop-down menu is displayed, listing all the customer companies associated with your account.
3. Select the desired company.
4. Then, select the
   
   icon next to **All devices**.

   NOTE: The drop-down menu is shown only if the company has devices belonging to an Active Directory group.

   A drop-down menu shows the Active Directory structure of the selected company.
5. Select the desired Active Directory group to view all the devices in that group.

   NOTE: The Active Directory structure is built based on the data that is reported by company computers, so it may not be complete. A new Active Directory domain does not show in WithSecure Elements Security Center until WithSecure Elements EPP for Computers or WithSecure Elements EPP for Servers is activated in the computers in that domain.

Customize the Devices view

You can apply filters and you can select which columns you want to be visible in the Devices table.

To customize the Devices view:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Above the table, from the drop-down menu, select the name of a column for filtering the devices and the desired value for the selected column.

   NOTE: You can remove all the filters by selecting **Clear all filters**.

   A list of the devices that match the filtering criteria that you selected is shown.
3. At the right corner above the table, select
   |||
   .
   A drop-down menu opens showing the Visible columns list.
4. Select the columns that you want to be visible in the table.
   The columns that you selected appear in the table.
5. To change the order of the columns in the table:
   a) Point to the name of a column that you want to move.
   b) Depending on where you want the column to appear, drag it up or down in the list.
6. To define the number of rows shown in the table per page, do the following:
   a) At the right corner above the table, select
   .
   b) From the drop-down menu, select the desired number of rows.
   The number of rows changes according to your selection.
7. If there are more devices than can be shown in the table per page, use the navigation arrows
   (,
   >)
   located above the table to go to the previous or next page.
8. Select **View:** > **Save as** at the top-right corner to save the view that you have customized.

   NOTE: You can remove the views that you have customized by first selecting **Delete views**, then in the Delete views window selecting the view that you want to remove, and then selecting **Delete**.

Request diagnostic data

You can remotely request for a diagnostic file to be uploaded to a WithSecure support team.

If there is an issue with a device in your managed accounts, the WithSecure Elements Security Center administrator can select the device and make a request to the customer, who allows a diagnostics (WSDIAG) file to be collected and uploaded to WithSecure Elements Security Center. The diagnostics file is essential in finding out more about the issue and its root cause.

NOTE: This functionality is available for Elements Agent for Windows - on both servers and workstations - as well as for Elements Mobile Protection.

To request diagnostic data:

1. Log in to Elements Security Center.
2. If you are managing multiple accounts, go to the relevant customer account.
3. Once in the correct account, under **Environment**, select **Devices**, and select the link for the relevant device (the device that has the issue and for which the `wsdiag` file is needed).
   This opens up a page with device details.
4. On the **Actions** panel at the bottom of the page, select **Request diagnostic file** > **Request**. For privacy purposes, a notification appears for the end user; this does not appear on the server side.

NOTE: To check that the request has been sent to the user, in the customer account, go to **Environment** > **Devices** and select the three dots icon on the right side and select **Manage operations**. Verify whether a WSDIAG operation appears in the list with the status **Waiting for delivery to the device**.

5. Make sure that the user allows the diagnostic (WSDIAG) file to be collected. To do this, they must select **Allow** once they see the notification on their device.
6. When the user has allowed the diagnostic (WSDIAG) file to be collected, go back to the **Manage operations** page in the customer account.
7. Check if the status has changed to **Success, operation was performed**.
8. On the **Manage operations** page, get the reference number for the created WSDIAG file.
9. Include the reference number in the support ticket to WithSecure Support.

NOTE: In the support ticket, WithSecure can see the reference number and download the file for further investigation.

10. Optionally, download the diagnostic file by selecting the three dots icon in the **Action** column.

NOTE: The WSDIAG file is automatically deleted after two weeks from the portal.

1.1.10 Elements data recovery

WithSecure maintains the availability of the Elements service and takes care of the necessary backups and any needed recovery actions.

No actions are required from you.

IMPORTANT: This backup includes only data that is directly relevant to the service provided by WithSecure. It is your responsibility to backup your own documents and other data.

Chapter 2

Elements Collaboration Protection overview

Topics:

- Solution overview
- System requirements
- Features
- Get started with WithSecure Elements Collaboration Protection

Elements Collaboration Protection overview

Overview of WithSecure Elements Collaboration Protection (formerly WithSecure Cloud Protection for Microsoft Office 365): what it protects, requirements, and how to get started.

This guide describes WithSecure Elements Collaboration Protection: what it protects in your Microsoft Office 365 environment, its system requirements and main features, and how to get started.

2.1 Solution overview

WithSecure Elements Collaboration Protection is a cloud-based solution to detect, protect from, and respond to security threats in Microsoft Office 365.

WithSecure Elements Collaboration Protection protects Exchange email messages from malicious content. It provides advanced protection against inbox rule-based attacks. The solution also provides real-time protection for SharePoint, OneDrive, and Teams content.

Combined with WithSecure's award-winning endpoint protection, detection, and response capabilities, the solution provides more comprehensive protection for your business than any email security solution alone. Cloud-to-cloud integration lets you deploy and manage the solution.

2.2 System requirements

System requirements for WithSecure Elements Collaboration Protection, including supported browsers, languages, and Microsoft 365 plans.

Supported browsers

The WithSecure Elements Collaboration Protection portal supports the latest versions of the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Safari

Supported languages

The WithSecure Elements Collaboration Protection portal and documentation are localized into the following languages:

English, Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), and Swedish.

Supported Microsoft 365 and Office 365 plans

The WithSecure Elements Collaboration Protection solution supports a variety of Microsoft 365 and Office 365 plans including the following:

- Microsoft 365 enterprise plans:
  - Microsoft 365 E3
  - Microsoft 365 E5
  - Microsoft 365 F1
  - Microsoft 365 F3

- Microsoft 365 business plans:
  - Microsoft 365 Business Basic (formerly Office 365 Business Essentials)
  - Microsoft 365 Business Standard (formerly Office 365 Business Premium)
  - Microsoft 365 Business Premium (formerly Microsoft 365 Business)
  - Microsoft 365 Apps for Business
- Microsoft 365 educational plans:
  - Microsoft 365 A1
  - Microsoft 365 A3
  - Microsoft 365 A5
- Office 365 enterprise plans:
  - Office 365 E1
  - Office 365 E3
  - Office 365 E5
- Office 365 educational plans:
  - Office 365 A1
  - Office 365 A3
  - Office 365 A5

2.3 Features

Some of the main features of WithSecure Elements Collaboration Protection are described here.

Compromised account detection	Email is one of the biggest threat vectors for companies of all sizes. Access to user email accounts often grants access to a wide range of other company services and gives attackers an opportunity to steal company and customer data. A breached account is an easy way for the attacker to get into an organization. The attacks done using a breached account, such as phishing campaigns or impersonation, are hard to detect because they use a legitimate company user account. The Compromised account detection feature detects compromised accounts as soon as information about the breach is available. It informs users and administrators to take action to remediate the accounts by changing the password or by taking other security measures, such as turning on the multi-factor authentication to avoid further exploitation of the breached data.
Inbox rule scanning	Inbox rules in Outlook work as a trigger to perform specific actions on incoming emails automatically. After gaining access to a mailbox, an attacker creates inbox rules to carry out different types of attacks, such as auto-forwarding and auto-deleting of emails. The scanning feature analyzes all the inbox rules in a mailbox. This analysis helps detect any suspicious rules that may indicate a compromise of the account. It also notifies the owner of the mailbox and the administrators to take action.
File and URL protection	Whenever an end user receives or sends an email in their mailbox, all included attachments and URLs are analyzed for harmful content, such as malware, Trojans, ransomware, or phishing.
Multilayered security	WithSecure Elements Collaboration Protection uses WithSecure Security Cloud, which combines award-winning multi-engine antivirus, machine learning -based heuristic analysis, and threat intelligence database updated in real-time. WithSecure Security Cloud finds instantly emerging and unseen malware variants as well as detects broader range of malicious features, behavior patterns and trends.
Advanced threat detection	Advanced threat detection runs suspicious files in an isolated virtual environment (known as a sandbox) that mimics a normal computer. As the file is detonated -

	that is, allowed to run in the sandbox - the process examines its behavior for any harmful actions. It then returns a verdict on whether the file is clean or harmful. Clean files are allowed to run normally, while harmful files are blocked.
Advanced analytics	Advanced security analytics gives full visibility into analyzed content and ensures fast and efficient response capabilities.
Worry-free administration	As a product administrator, you can configure settings, detections, user notifications, and actions in accordance with your company security policies. The WithSecure Elements Collaboration Protection portal allows you to manage detections and quarantined items for multiple Microsoft Office 365 tenants. WithSecure partners can administer the solution for multiple end customers.
Seamless integration	WithSecure Elements Collaboration Protection supports cloud-to-cloud integration without additional software to be installed or changes made to server or client side. The protection is totally platform agnostic and capable of detecting threats regardless of which device or application is used by the end user.
Quarantine management	Microsoft Office 365 mailbox emails that contain harmful files, harmful URLs, or both can be quarantined immediately. Later on you can review and restore them using quarantine management.
Reporting	WithSecure Elements Collaboration Protection allows you to generate scheduled reports to provide a complete overview of the secured environment which can be shared to show the value provided by the solution over a certain period of time.
Microsoft Exchange protection	The solution protects your Exchange email messages.
SharePoint protection	The solution protects the content in your SharePoint sites. Whenever you store files in SharePoint, WithSecure Elements Collaboration Protection analyzes the files for harmful content, such as malware, Trojans, ransomware or phishing. Advanced SharePoint protection is included in the product and can be used with no additional charge.
OneDrive protection	The solution protects the content in your OneDrive drives. Whenever you store files in OneDrive or share them in private or group chats in Teams, WithSecure Elements Collaboration Protection analyzes the files for harmful content, such as malware, Trojans, ransomware or phishing. OneDrive protection is included in the product and can be used with no additional charge.
Teams protection	The solution protects the files that you share in your Team channels. WithSecure Elements Collaboration Protection scans the uploaded content and if found harmful, the content can be deleted or quarantined.

2.4 Get started with WithSecure Elements Collaboration Protection

Gets started with WithSecure Elements Collaboration Protection (formerly known as WithSecure Cloud Protection for Microsoft Office 365).

You can manage WithSecure Elements Collaboration Protection in one of two roles:

- As an end customer, using it for your own organization
- As a partner, managing it on behalf of a customer

This quick start guide walks you through the main steps to start using WithSecure Elements Collaboration Protection. See the related tasks for full instructions on each step.

1. Create the first WithSecure business account for your organization.
2. Log in to Elements Security Center and connect your Microsoft 365 tenant as a cloud service.
3. Create a default policy for your company.
4. Configure protection for your Exchange, SharePoint, OneDrive, and Teams assets.

5. Add administrator accounts for your team.

Chapter 3

Setting up the WithSecure Elements Collaboration Protection portal

Topics:

- Switch between the managed companies
- Set up the portal
- Change your user name
- Create a default policy
- Connect WithSecure Elements Collaboration Protection to the Microsoft Office 365
- Set up Exchange protection
- Set up SharePoint protection
- Set up OneDrive protection
- Set up Teams protection
- Restrict partner access

Setting up the WithSecure Elements Collaboration Protection portal

Sets up the WithSecure Elements Collaboration Protection portal (formerly known as WithSecure Cloud Protection for Microsoft Office 365).

Before you can protect your organization, set up the WithSecure Elements Collaboration Protection portal. Setup includes connecting the portal to your Microsoft Office 365 organization, creating a default policy, and enabling protection for mailboxes, SharePoint, OneDrive, and Teams.

3.1 Switch between the managed companies

Use the *scope selector* to broaden or narrow the scope of information displayed in the WithSecure Elements Collaboration Protection portal.

The scope selector shows all the companies that are managed by the reseller, even the ones with restricted access that are not visible in the portal.

In the WithSecure Elements Collaboration Protection portal, there are different account levels.

NOTE: If the account was created to manage only one company, only the company name is shown next to the portal logo instead of a drop-down menu.

To use the scope selector to focus on a particular company:

1. Select the
   
   icon at the top of the page next to the logo.
   A drop-down menu is displayed, listing all the companies associated with your account.
2. Select the desired company.

   TIP: Use the **Search** field to narrow the list.

   The page is updated to show the relevant information for the selected company.

3.2 Set up the portal

On the My settings page, you can select the language and timezone for the portal, and help us improve the product by sending usage data.

To set up the portal:

1. Select
   
   at the top right corner.
   *The **My settings** window opens.*
2. To select the language, under **Details**, from the **Language** drop-down menu, select the correct language.
   The selected language is used across the WithSecure Elements Collaboration Protection portal.
3. To select the timezone, from the **Timezone** drop-down menu, select the timezone to be used in the WithSecure Elements Collaboration Protection portal.

4. To send usage data, under **UI Analytics**, turn on **Allow the portal to collect anonymized statistics on usage**.
   The portal collects anonymized statistics about how its features are used.

3.3 Change your user name

You can change your user name in the settings.

To change your user name:

1. Select
   
   at the top right corner, and then select **My settings**.
2. Under **Details**, enter a new user name.
3. Select **Save**.

3.4 Create a default policy

A policy is a set of rules and settings that define how WithSecure Elements Collaboration Protection acts when a security threat is detected.

IMPORTANT: Before rolling out WithSecure Elements Collaboration Protection, you need to create a default policy for your company. If you do not create a default policy, WithSecure Elements Collaboration Protection uses WithSecure Policy that is created by WithSecure and cannot be modified.

To create a default policy:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Policies**.
3. Select **Add policy** at the top of the page.

NOTE: By default, a WithSecure policy is available and you can use it as a template.

NOTE: You can create a new policy also by copying from an existing policy. To do that, select ··· in the Menu column next to the policy that you want to copy, and select **Copy**.

4. On the page that opens, under **General**, in the **Policy name** field, enter a name for the new policy.

NOTE: You may add also a description and enter one or more tags to make it easier to find the policy later.

5. Under **Notifications**, enter a recipient email address for sending notifications.
6. Select **Save**.
   You have created a new policy
7. On the Policies page, select ··· in the Menu column next to the policy that you just created, and select **Set as default**.

The new policy is now the default policy. It is automatically assigned to every new cloud service that is created for a given company when you connect WithSecure Elements Collaboration Protection to your Microsoft Office 365 tenant.

Next, you need to set up the new default policy.

3.5 Connect WithSecure Elements Collaboration Protection to the Microsoft Office 365

You can connect WithSecure Elements Collaboration Protection to the Microsoft Office 365 Exchange service and to the SharePoint service for more comprehensive protection.

To connect WithSecure Elements Collaboration Protection:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Cloud services**.
3. Select **Add connection**.

NOTE: On a partner level, to add a new connection, either switch to a company level, or go to **Organization view**, select

,

and then select **Add new connection**.

*The **Add new connection** page opens.*

4. Under **Connection details**, do the following:
   a) In the **Name** field, enter a name for the new connection.
   b) In the **Specify Microsoft Azure Active Directory tenant name or ID** field, specify a name or ID for the Microsoft Azure Active Directory tenant that is dedicated for your Microsoft Office 365 service. For more information, see Determine the tenant name of your Azure Active Directory and Office 365 on page 83.
   c) If you have several subscriptions, select the proper subscription key from the drop-down menu.

NOTE: If you have only one subscription, it is shown automatically.

5. Select **Next** to continue.
   *The **Summary** screen opens.*
6. Review the information on the **Summary** page, and select **Add connection**.
   *The new connection is added and the **Finish** screen opens.*
7. Select **Close**.
8. On the Cloud services page, do one of the following:
   - To authorize and connect the new cloud service, select **Authorize** in the Exchange column, and then select **Connect**.
   - To authorize and connect the new cloud service, select **Authorize** in the SharePoint column, and then select **Connect**.
   - To authorize and connect the new cloud service, select **Authorize** in the OneDrive column, and then select **Connect**.
   - The authorization for Teams is received by authorizing SharePoint to protect the Teams channels.

> **NOTE:** If you are not an administrator, select **Copy URL** to get the URL that you need to finish the setup. You need appropriate rights to visit this page grant the required permissions to connect to the cloud service.

9. When prompted to accept permissions requested by WithSecure Elements Collaboration Protection, do the following:

> **NOTE:** Your browser may block pop-up windows. In that case, the portal shows a warning and a link that you can select to open the Microsoft page manually.

a) Make sure that the link under WithSecure Elements Collaboration Protection points to the WithSecure Elements Collaboration Protection portal.
b) Check the WithSecure service agreement and privacy policy.
c) Select **Accept**.

> **NOTE:** By accepting, you allow WithSecure Elements Collaboration Protection to access data in your Microsoft Office 365 tenant.

A pending connection appears on the Cloud services page. When the connection between WithSecure Elements Collaboration Protection and the Microsoft Office 365 Exchange, SharePoint, or OneDrive service has been established, the status of the service changes to "Configure protection".

Next, you need to set up protection for the mailboxes.

3.6 Set up Exchange protection

Sets up protection for the mailboxes in a configured domain.

To set up protection for the mailboxes:

1. Select **Cloud services** on the sidebar.
2. Select **Configure protection** in the row of the new connection in the **Exchange** column.
3. In the page that opens, do the following:
   - Select **Protect all mailboxes** if you want to protect all the existing mailboxes in your account in Microsoft Exchange.
   - Select **Customize protection for mailboxes** if you want to select the mailboxes that you want to protect.
     - To add protection for an existing unprotected mailbox on your account, select the mailbox from the mailbox list and at the bottom of the page, select **Turn on protection**. The status of the mailbox changes to "Protected".
     - To automatically protect all the new mailboxes, turn on **Automatically protect newly-added mailboxes**. You must, however, have enough licenses available. If this setting is off, you must manually select the new mailboxes to add them to the list of protected mailboxes.

> **NOTE:** It can take up to 2-3 hours for WithSecure Elements Collaboration Protection to discover new mailboxes after they are added to the tenant.

The selected mailboxes show the status Protected.

3.7 Set up SharePoint protection

Sets up protection for the sites in a configured domain.

To set up protection for the sites:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **SharePoint** column.
3. In the page that opens, do the following:
   a) Turn on **Automatically protect newly-added SharePoint and Teams assets** to automatically protect all the newly-added SharePoint sites and Teams channels. If the setting is turned off, you must select in the table those newly-added sites that you want to be protected.

> **NOTE:** It can take up to 2-3 hours for WithSecure Elements Collaboration Protection to discover SharePoint or Teams assets after they are added to the tenant.

   b) From the list of sites, select the sites that you want to protect.

> **NOTE:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

   c) To add protection for an existing unprotected site on your account, select the site from the list, and at the bottom of the page, select **Turn on protection**.
   The status of the site changes to "Protected".

3.8 Set up OneDrive protection

Sets up protection for the user drives in a configured domain.

To set up protection for the drives:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **OneDrive** column.
3. In the page that opens, do the following:
   a) Turn on **Automatically protect newly-added drives** to automatically protect all the newly-added drives. If the setting is turned off, you must select in the table those newly-added drives that you want to be protected.

> **NOTE:** It can take up to 2-3 hours for WithSecure Elements Collaboration Protection to discover new OneDrive drives after they are added to the tenant.

   b) From the list of drives, select the user drives that you want to protect.

> **NOTE:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

> **NOTE:** The files that are shared via Teams chats are included in the OneDrive protection.

   c) To add protection for an existing unprotected drive on your account, select the drive from the list, and at the bottom of the page, select **Turn on protection**.
   The status of the drive changes to "Protected".

3.9 Set up Teams protection

Sets up protection for the files shared in Teams channels in a configured domain.

> **NOTE:** You can configure the protection for newly-added Teams assets in the **SharePoint** tab.

To set up protection for the channels:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **Teams** column.
3. In the page that opens, do the following:
   a) From the list of channels, select the channels that you want to protect.

   > **NOTE:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

   b) To add protection for an existing unprotected channel on your account, select the channel from the list, and at the bottom of the page, select **Turn on protection**.
   The status of the channel changes to "Protected".

The selected Teams channels are protected.

3.10 Restrict partner access

If your company is managing WithSecure Elements Collaboration Protection on its own, you may restrict the partner's access to your WithSecure Elements Security Center.

To restrict partner access:

1. Log in to WithSecure Elements Security Center.
2. On the sidebar, select **Management** > **Organization Settings** > **General**.
3. Under **Organization information**, select **Access Policies**.
   *The **Access Policies** pane opens.*
4. Under **Restrict Partner access**, turn the switch on.

   Turning on this setting restricts partner access to your organization. With restricted access, the partner cannot, for example, remove users from the company account, change the restricted company's access policies, or add administrators. The partner can, however, still view the company (in the scope selector) and see its administrators.

   In WithSecure Elements Security Center, the partner can no longer access Exposure Management and Collaboration Protection views.

Chapter 4
Administering the product

Topics:

- Manual application creation
- Check the overall status of the managed companies
- Managing cloud services
- Managing detections
- Managing compromised accounts
- Managing policies
- Managing quarantined items
- Managing system events
- Managing reports

Administering the product

Administering Elements Collaboration Protection covers the overall protection status, cloud services, detections, policies, quarantined items, and system events.

After you set up the portal, you administer Elements Collaboration Protection from Elements Security Center. You can view the overall protection status of all managed companies, connect and manage cloud services, and manage detections, policies, quarantined items, reports, and system events.

4.1 Manual application creation

You can create the application fully manually.

NOTE: If you want to create the application manually, refer to the Microsoft documentation for details.

The application must have at least the following properties:

Table 1: Required application permissions

API/Permission name	Type	Description
Azure Active Directory Graph		
Directory.Read.All	Application	Read directory data
User.Read	Delegated	Sign in and read user profile
Exchange		
full_access_as_app	Application	Use Exchange Web Services with full access to all mailboxes
Microsoft Graph		
Calendars.ReadWrite	Application	Read and write calendars in all mailboxes
Contacts.ReadWrite	Application	Read and write contacts in all mailboxes
Mail.ReadWrite	Application	Read and write mail in all mailboxes
User.Read.All	Application	Read all users' full profiles
Reports.Read.All	Application	Read all usage reports
Office 365 Management APIs		
ActivityFeed.Read	Application	Read activity data for your organization
ServiceHealth.Read	Application	Read service health information for your organization

NOTE: When more features and functionality are added to WithSecure Elements Collaboration Protection, you need to add more permissions. If you fail to add a permission, the product functionality becomes impaired and might stop working.

You must set the following redirect URLs in the application:

- https://portal.cp.f-secure.com/permission-request
- https://portal.cp.f-secure.com/cloud-services

4.2 Check the overall status of the managed companies

View the overall protection status of the companies you manage.

To view the overall status:

1. Select **Collaboration Protection** > **Dashboard** on the sidebar.
   The Dashboard view opens.
2. Check the Dashboard pane.

   The **Dashboard** pane keeps you informed on what takes place in the organizations that you manage. Based on the currently selected scope, it shows the overview of all companies or only the selected organization.

   NOTE: Using the drop-down menu at the top-right corner, you can select the time period for which you want to view the overall status.

   You can view the following information:

   Current detections — Shows the number of detections by their status and severity level from critical to low.

   Subscriptions — Shows the number of expired cloud service accounts, as well as those that expire within seven days and within 30 days.

   NOTE: This is shown only for Solution providers and Service partners.

   Item status — Shows the number of protected, unprotected, and unavailable mailboxes, sites, user drives, and channels in your organization as well as those that have errors or are unavailable.

   NOTE: As a Service partner or a Solution provider, you see the numbers per each organization that you manage.

   Top affected items — Shows the number and severity of detections and additional information in the top affected mailboxes, sites, user drives, and channels.

   Inbox rules — Shows the number of the scanned inbox rules and detected suspicious inbox rules. Selecting **View** opens the Detections view that shows you information on the found suspicious inbox rules.

   NOTE: Inbox rules are shown only on an organization level.

Protection trend	Shows the all-time average percentage of the unsafe content in the selected organization (the gray bar), the percentage of the unsafe content from the selected period (the dark blue bar) and from the period before the selected period (the light blue bar).
Cloud service protection status	The Exchange tab shows the total number of unsafe items (attachments and URLs) out of all the scanned items, and the amount of quarantined, deleted, and detonated items. The SharePoint, OneDrive, and Teams tabs each show the number of unsafe files and the amount of quarantined files.

4.3 Managing cloud services

The Cloud services page shows all the cloud services that have been added and set up for a chosen level (the partner level shows all the cloud services of the partner-managed companies).

You can add new services, assign new policies to existing cloud services, view the properties of and disconnect or remove existing cloud services.

The page shows you the overall status of each cloud service. The cloud service status can be as follows:

- Protected - The cloud service is fully protected. The protection is based on the assigned policy settings. The Exchange column shows the number of protected, unprotected, and unavailable mailboxes as well as the number of mailboxes in error state; the SharePoint column shows the number of protected, unprotected, and unavailable sites as well as the number of sites in error state; the OneDrive column shows the number of protected, unprotected, and unavailable user drives, and the number of drives in error state; the Teams column shows the number of protected, unprotected, and unavailable channels, and the number of channels in error state.
- Configure protection - The service is connected to Microsoft Exchange, SharePoint, OneDrive, or Teams but is not yet fully protected. You need to set up protection for the mailboxes, sites, user drives, or channels.

  NOTE: If real-time scanning under the Policy settings is turned off, the service has a "Connected" status.

- Connect - The cloud service is disconnected and not protected. Your attention is required.

  NOTE: You can connect a disconnected service by selecting **Connect** in the row of the could service or by selecting the cloud service and selecting **Connect...** at the bottom of the page.

- Authorize - Pending authorization - the cloud service is not yet connected, but waiting for authorization. The service is not protected and your attention is required.

  NOTE: A service in the authorization process needs appropriate permissions the grant of which can be started by selecting the cloud service and then selecting **Connect...** at the bottom of the page.

- Pending - the cloud service is not yet connected, but currently establishing a connection. The service is not protected during this process.

The page shows whether a cloud service is connected to Exchange, SharePoint, OneDrive, or Teams. It also shows the name of the policy that is in use for a given cloud service.

4.3.1 View cloud service properties

On the cloud service **Summary** page, you can view the properties of the selected cloud service.

To view cloud service properties:

1. On the sidebar, select **Collaboration Protection** > **Cloud services**.
2. Select the name of the cloud service whose details you want to view.
   *The **Summary** page opens. It shows the following:*
   - Name of the cloud service
   - Microsoft Office 365 domain
   - Exchange, SharePoint, OneDrive, and Teams status
   - Microsoft Azure Active Directory (tenant) and WithSecure (tenant) IDs
   - Subscription key
   - Date when the connection was created
   - Name of the assigned policy
   - Consent URL for Exchange, SharePoint, or OneDrive, or all of them
3. If you want to edit the name of the cloud service, enter the new name in the Name field, and select **Save**.
4. If the status of the cloud service is Disconnected or Pending, you can select **Copy URL**.

NOTE: The URL is used to start the connection for external cloud service administrators to grant permissions that are required for protecting the cloud service.

5. Select the **Exchange** tab.
   The Exchange page opens. It shows the setup for mailbox protection.
6. Select the **SharePoint** tab.
   *The **SharePoint** page opens. It shows the setup for site protection.*
7. Select the **OneDrive** tab.
   *The **OneDrive** page opens. It shows the setup for drive protection.*
8. Select the **Teams** tab.
   *The **Teams** page opens. It shows the setup for channel protection.*

4.3.2 Change the assigned policy for a deployed cloud service

Assigns a different policy to a cloud service that has already been deployed.

To change the assigned policy:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Cloud services**.
3. Select the cloud service for which you want to change the assigned policy.
4. At the bottom of the page, select **Assign policy...**, and from the drop-down menu, select a different policy.
5. Select **Assign** to confirm the action.

The assigned policy is changed for the selected cloud service.

4.3.3 Disconnect a cloud service

Disconnects a cloud service.

To disconnect a cloud service:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Cloud services**.
3. Select the cloud service that you want to disconnect.
4. At the bottom of the page, select **Disconnect...**.

NOTE: The **Disconnect** option is available only for cloud services the status of which is either Protected or Connected.

5. In the confirmation window, select **Disconnect** to confirm that you want to disconnect the selected cloud service.

The cloud service is disconnected and no longer protected.

4.3.4 Remove a cloud service

Removes a cloud service and its associated quarantined items, statistics, and detections.

To remove a cloud service:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Cloud services**.
3. Select the cloud service that you want to remove.
4. At the bottom of the page, select **Remove...**.
5. In the confirmation window, select **Remove** to confirm that you want to disconnect the selected cloud service.

The cloud service is removed from the WithSecure Elements Collaboration Protection service. When you remove a cloud service, all the quarantined items, dashboard statistics, and detections that are associated with the cloud service are also removed from the system.

4.3.5 Handle an expired or replaced subscription

When an expired subscription is replaced with a new one, reconnect the cloud service and assign the new subscription to restore protection.

When a subscription expires, a new subscription sometimes replaces it instead of extending the existing one. The cloud service that uses the expired subscription is then disconnected automatically. The WithSecure Elements Collaboration Protection portal shows a notification when this happens.

To restore protection:

1. Reconnect the cloud service to Microsoft Office 365.
2. Assign the new subscription to the reconnected cloud service.

Protection resumes after you reconnect the cloud service and assign the valid subscription.

4.4 Managing detections

Detections give you information about current security issues. You can manage detections by updating their status and by entering notes and comments about detections for other system users, which improves the daily management of detections.

Detections report current security issues found by Elements Collaboration Protection. From the portal you can filter detections, view their details, update their status, and add or view comments to coordinate handling with other users.

4.4.1 Filter detections

You can use filtering to find detections in the WithSecure Elements Collaboration Protection portal.

To filter detections:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Detections**.
   *The **Detections** page opens listing all the detections.*
3. From the drop-down menu, select a category for filtering the detections:
   - Status
   - Time from
   - Time to
   - Severity - available values:
     - Critical
     - High
     - Medium
     - Low
   - Type of threat - available values:
     - Harmful
     - Suspicious
     - Disallowed
     - Suspicious inbox rule
     - Breached domain account
   - User
   - SHA-1
   - Action taken - available values:
     - Deleted
     - None
     - No action taken
     - Passed
     - Quarantined
     - Subject modified
     - Error
   - Detonated in sandbox - available values:
     - Yes
     - No
   - Detection ID
   - Filename
   - Extension
   - Location
   - Cloud service source
   - Affected assets
   - Exchange
     - Sender

    - Subject
    - Inbox rule name
    - Item type (available values: Appointment, Contact, Contact group, Email message, Meeting message, Post item, Task)
    - URL
    - Email security threat
  - SharePoint
    - Item type (available value: SharePoint file)
  - OneDrive
    - Item type (available value: OneDrive file)
  - Teams
    - Item type (available value: Teams file)

4. In the field next to the category drop-down menu, enter or select a value, and select **Apply**.
5. To reset the selected filter category and the value, select **Clear all**.

NOTE: You can remove a filter by selecting **x** in the text box that appears under the drop-down menu once you have applied a filter.

6. From the drop-down menu on the right, select the cloud service for which you want to view the detections.

A list of the detections that match the filtering criteria you selected is shown.

4.4.2 View detections details

You can view the details of detections in the WithSecure Elements Collaboration Protection portal.

You can also view the quarantine items that are associated with the detections.

NOTE: Also, you can report as false positives any URLs that are marked as either suspicious or harmful in the URL section by selecting **Report as false positive** next to the URL which you want to report. The link is then sent to the WithSecure Tactical Defense team for evaluation.

To view detections details:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Detections**.
   *The **Detections** page opens listing all the detections.*
3. Select the name of the detection the details of which you want to see.
   *The **Detection details** page opens.*

The **Detection details** page shows the details of the selected detection, including its severity and status, affected user, the action taken on the item, the message headers, possible attachments, and URLs.

4.4.3 Update detection status

Updates the status of a detection.

To update the detection status:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Detections**.

*The **Detections** page opens.*

3. In the ID column, select the desired detection.
   *The **Detection details** page opens.*
4. Select a new status from the Status drop-down menu:
   - New
   - Acknowledged
   - In progress
   - Closed: Resolved
   - Closed: False positive
5. Select **Save**.

> **NOTE:** Alternatively, you can select the checkbox of the desired detection, and then at the bottom of the page, select **Update status**. From the drop-down menu that appears, select a new status and select **Update**.

4.4.4 Add comments

Adds a comment to a detection.

To add a comment:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Detections**.
   *The **Detections** page opens.*
3. Select the number in the **Comments** column in the row of the desired detection.
   *The **Comments** window opens.*
4. Enter your comment in the **Enter comment** box, and select **Save**.

4.4.5 View comments

Views the comments that have been added to a detection.

To view comments:

1. Select **Detections** on the sidebar.
   The Detections page opens.
2. In the Comments column, select the number in the row of a detection.

> **NOTE:** The number shows how many comments have been entered for the detection.

The Comments window opens showing who has left the comment, the date and time when the comment was left and the actual content.

4.5 Managing compromised accounts

WithSecure Elements Collaboration Protection detects compromised company email accounts in a domain early in the breach timeline.

Early detection gives the company administrators precious time to validate the user identity and take actions before the data becomes available for broader criminal audience.

A breached account gives an attacker a way into an organization. The attacker can then take maximum advantage by launching attacks such as internal phishing campaigns, ransomware attacks, or impersonation-based attacks. The attacks that use a breached account are hard to detect because they use a legitimate company user account. Detecting compromised accounts as soon as the breach information is available is the key to reclaiming those accounts. This means changing the password or using other security measures, such as multi-factor authentication, to avoid further exploitation of breached data.

As soon as you deploy the product to protect your organization's Microsoft 365 domain, it checks the domain's protected email addresses for possible breach information. It also notifies you if your company accounts have been compromised.

4.5.1 View compromised accounts

You can view the compromised accounts and their details in the WithSecure Elements Collaboration Protection portal

To view compromised accounts:

1. Open WithSecure Elements Security Center.
2. On the sidebar, select **Collaboration Protection** > **Compromised accounts**.

NOTE: If you see "N/A" in the MFA column in the Compromised accounts table view, you need to refresh the Cloud Service connection to see the MFA status. To refresh the connection, select **Cloud services** on the sidebar, select the cloud service and then select **Refresh** at the bottom of the page.

*The **Compromised accounts** page opens showing the following information:*

- The breached email account
- The domain name
- The number of breaches
- The date and time of the last password change
- Whether the breached email account has the multi-factor authorization (MFA) turned on

3. In the **Breaches** column, select the number.
   *The **Detection** view opens showing the date and time of the breach, its severity and status, the threat type, the cloud service, the user name, the number of comments, and the location.*
4. Select a detection in the ID column to see the detection details.
   *The **Detection details** page opens showing the following information:*
   - Breached domain account:
     - Severity
     - Status
     - Details
     - Affected user
     - Breach occurred
     - Cloud service
     - Breach detected
     - Action taken
     - Item type
     - Comments
   - Breach details:

- Breach title
- Breach type
- Password type
- Password change (at the time of the detection)
- Last password change
- Description

4.5.2 Remediation of compromised accounts

Ways to resolve a compromised account, based on its severity level.

There are different ways to resolve compromised accounts depending on their severity level.

Breached email address (severity level: low)

This low-level alert indicates that an email address or an email address and a non-crackable hashed password have been breached.

The primary concern here is that the email addresses that have been included in such a breach are being actively shared online by malicious actors. A likely attack scenario would be a spear-phishing campaign.

In a spear-phishing campaign, criminals send fraudulent emails claiming to be from reputable sources to induce unsuspecting individuals to reveal personal information or to open malicious links. We recommend that you carefully examine the links in emails and turn on the multi-factor authentication for your account, if not on yet.

Breached email address and password (severity level: medium)

This medium-level alert indicates that an email address and a plaintext password have been exposed in a data breach. The medium-level alert is generated in the following cases:

- If the user has changed their password after the breach and multi-factor authentication (MFA) is not turned on
- If the user has not changed their password after the breach, even though MFA is turned on

With this type of breaches, the primary concern is the password reuse. The password used for the breached service is compromised and actively shared in dark places. You must change the compromised password and never use it again. In addition, you should change all variations of the compromised password and never use them again. If an attacker has even a few characters of your password, they can crack the entire password. These types of breaches have impacted the most sophisticated users of major technology companies because of the password reuse. This is a serious concern and often overlooked. We highly recommend that you use a password manager so that all your passwords are unique and easily managed. We also recommend that you turn on multi-factor authentication for all your passwords, if it is not yet on.

Breached email address and password (severity level: high)

This high-level alert indicates that an email address and a plaintext password have been exposed in a data breach.

With this type of breaches, the primary concern is the password reuse. The password used for the breached service is compromised and actively shared in dark places. You must change the compromised password and never use it again. In addition, you must change all variations of the compromised password and never use them again. If an attacker has even a few characters of your password, they can crack the entire password. These types of breaches have impacted the most sophisticated users of major technology companies because of the password reuse. This is a serious concern and often overlooked. We highly

recommend that you use a password manager so that all your passwords are unique and easily managed. We also recommend that you turn on the multi-factor authentication for all your passwords.

Infected user (severity level: critical)

Given the source of this breach, a device that you have used has been infected with malicious software. The malicious software logs every keystroke. While your device is infected, changing your password does not solve the problem and is not recommended until the malicious software is removed. Also, while your device is infected, criminals capture every password that you use. We strongly suggest that you power off the infected device until a professional can analyze and remove the malicious software. Given that the malicious software could have been on your device for a long time, all passwords that you have used on this system are compromised. You must change all your passwords using a clean system.

We highly recommend that you use a password manager to simplify and speed up the process of protecting yourself in this situation. We also recommend that you turn on the multi-factor authentication for all your passwords.

4.6 Managing policies

WithSecure Elements Collaboration Protection uses policies to prevent security threats.

A policy defines how Elements Collaboration Protection scans and protects a connected cloud service. You configure separate settings for malware scanning, URL scanning, inbox rule scanning, compromised account protection, privacy, and notifications, and then assign the policy to the cloud services you want to protect.

4.6.1 Set up the General options

Sets up the general options — name, tags, and description — for a new policy.

To set up the general options:

1. In the Policy name field, enter a name for the new policy.
2. Optionally, add one or more tags and a description to make it easier to find the policy later.
3. Select **Save**.

The general options are saved to the policy.

Next, set up the privacy options.

4.6.2 Set up privacy options

Sets up privacy options that control data sharing with WithSecure for threat analysis, for a new policy.

To set up the privacy options:

1. In the General tab, select **Privacy**.
2. Select one or more of the following privacy options:
   - Select **Allow sending of non-personalized metadata with file submissions** to send non-personalized metadata together with files to support and enhance the threat analysis.
   - Select **Allow WithSecure to store suspicious executable files for further analysis** to save suspicious executable files to a long-term permanent storage where they are available for later analysis by WithSecure with automated and manual systems.
   - Select **Allow WithSecure to store suspicious non-executable files for further analysis** to save suspicious non-executable files to a long-term permanent storage where they are available for later analysis by WithSecure with automated and manual systems.

- Select **Allow data to be sent to third-party services used by WithSecure for threat analysis** to allow the sending of file content and metadata or only metadata. The data is used by WithSecure to improve quality of protection and threat analysis.

3. Select **Save**.

The privacy options are saved to the policy.

Next, set up the notifications.

4.6.3 Set up notifications

Sets up administrator and user notifications for a new policy.

To set up the notifications:

1. In the General tab, select **Notifications**.
2. In the **Recipient email addresses** field, specify the email addresses of the administrator users who want to receive detection and other administrator email notifications.
3. In the **Sender email address** field, specify the email address from which the detection and other administrator notifications are sent.
4. From the **User notifications based on severity** drop-down menu, select which notifications based on their severity are sent to users: All (Low, Medium, High, Critical); Medium, High & Critical; High & Critical; Critical.
5. Select **Save**.

The notification settings are saved to the policy.

Variables used in notification emails

Variables used in the user and administrator notification emails that are sent when harmful content or harmful URLs have been detected.

Variables used in user notifications about harmful content

Table 2: User notification variables for harmful content

Variable	Description
$ITEM-TO	To whom the item was sent
$ITEM-SUBJECT	The subject of the item
$ITEM-FOLDER	The folder in which the item was detected (for example, Inbox)
$ITEM-SENDER	The email address of the sender
$ITEM-DATETIME-SENT	The date and time when the harmful content was sent (UTC)
$TAKEN-ACTION	The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)

Variable	Description
$QUARANTINE-ID	The ID of the quarantined item (shown only if the Quarantine feature is turned on).
$AFFECTED-FILENAME	The name of the attachment in which harmful content was detected.
$AFFECTED-FILESIZE	The size (in bytes) of the attachment with harmful content
$ATTACHMENT-THREAT	The type of the threat that was detected in the attachment

Variables used in administrator notifications about harmful content

Table 3: Administrator notification variables for harmful content

Variable	Description
$USER-MAILBOX	The user mailbox in which harmful content was detected
$ITEM-FOLDER	The folder in which the item was detected (for example, Inbox)
$ITEM-SUBJECT	The subject of the item
$ITEM-SENDER	The email address of the sender
$ITEM-TO	The list of email addresses to which the item was sent
$ITEM-DATETIME-SENT	The date and time when the harmful content was sent at (UTC)
$TAKEN-ACTION	The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)
$PORTAL-LINK	The link to the portal
$QUARANTINE-LINK	A direct link to the item in the Quarantine view in the portal (shown only if the Quarantine feature is turned on).
$SECURITY-ALERT-LINK	A direct link to the Detections view in the portal
$QUARANTINE-ID	The ID of the quarantined item (shown only if the Quarantine feature is turned on).

Variables used in user notifications about harmful URLs

Table 4: User notification variables for harmful URLs

Variable	Description
$ITEM-TO	To whom the item was sent
$ITEM-SUBJECT	The subject of the item
$ITEM-FOLDER	The folder in which the item was detected (for example, Inbox)
$ITEM-SENDER	The email address of the sender
$ITEM-DATETIME-SENT	The date and time when the harmful content was sent (UTC)
$TAKEN-ACTION	The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)
$QUARANTINE-ID	The ID of the quarantined item (shown only if the Quarantine feature is turned on).
$AFFECTED-URL	The defanged or non-clickable URL that triggered the Security alert
$URL-THREAT	The specific threat or reason why the URL was detected

Variables used in administrator notifications about harmful URLs

Table 5: Administrator notification variables for harmful URLs

Variable	Description
$USER-MAILBOX	The user mailbox in which harmful content was detected
$ITEM-FOLDER	The folder in which the item was detected (for example, Inbox)
$ITEM-SUBJECT	The subject of the item
$ITEM-SENDER	The email address of the sender
$ITEM-TO	The list of email addresses to which the item was sent
$ITEM-DATETIME-SENT	The date and time when the harmful content was sent (UTC)

Variable	Description
$TAKEN-ACTION	The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)
$PORTAL-LINK	The link to the portal
$QUARANTINE-LINK	A direct link to the item in the Quarantine view in the portal (shown only if the Quarantine feature is turned on).
$SECURITY-ALERT-LINK	A direct link to the Detections view in the portal
$QUARANTINE-ID	The ID of the quarantined item (shown only if the Quarantine feature is turned on).
$AFFECTED-URL	The defanged or non-clickable URL that triggered the detection.
$URL-THREAT	The specific threat or reason why the URL was detected

4.6.4 Set up the Exchange general options

Sets up the Exchange general options for a new policy.

To set up the Exchange general options:

1. On the Policies page, select the policy that you just created.
   The General view opens.
2. Select the **Exchange** tab.
   The Exchange General view opens.
3. Turn **Real-time scanning** on to scan email messages and other Exchange items that are saved to user mailboxes.
4. Under **Trusted senders**, do the following to add trusted senders.
   a) Select **ON**.
   b) Select **Scan and create a low severity alert for trusted senders when harmful content detected** if you want the system to alert if harmful content is detected.

      NOTE: When this option is selected, no action is taken and the email items are passed through.

   c) In the **Trusted email sender addresses** field, add the email addresses of those senders whose email messages are not quarantined or deleted.
   d) In the **Trusted sender domains** field, add those sender domains that you consider trusted. Email messages coming from those domains not quarantined or deleted.
5. Under **Quarantine**, from the drop-down menu, select the amount of time after which you want old items to be automatically deleted.
6. Select **Save**.

The Exchange general options are saved to the policy.

4.6.5 Set up the SharePoint general options

Sets up the SharePoint general options for a new policy.

General options control whether SharePoint items are scanned in real time and how long quarantined items are kept before they're automatically deleted.

1. On the **Policies** page, select the policy that you just created.
   The General view opens.
2. Select the **SharePoint** tab.
   *The **SharePoint General** view opens.*
3. Turn **Real-time scanning** on to scan SharePoint items on the sites in your organization.
4. Under **Quarantine**, from the drop-down menu, select the amount of time after which you want old items to be automatically deleted.
5. Select **Save**.

The SharePoint general options are saved to the policy.

4.6.6 Set up malware scanning

Sets up malware scanning for a new policy.

To set up malware scanning:

1. Select of the following solutions for which you want to set up malware scanning:
   - Select **Exchange** > **Malware scanning**
   - Select **SharePoint** > **Malware scanning**
   - Select **OneDrive** > **Malware scanning**
   - Select **Teams** > **Malware scanning**
2. Turn **Malware scanning** on.

   NOTE: When on, malware scanning scans email messages for malware and other harmful content. It is available only when the real-time scanning is on.

3. Under **Scan files**, select which file types are scanned for malware and other harmful content: All; Included only; All except excluded.
   - If you selected the Included only option, in the **Included files** field, check the list of included file extensions and if needed, add a file extension that identifies the type of file that you want to be scanned for malware and other harmful content.

     NOTE: You can select

     to copy the email addresses to the clipboard or **Remove all** to empty the field.

   - If you selected the All except excluded option, in the **Excluded files** field, check the list of excluded file extensions and if needed, add a file extension that identifies the type of file to be excluded from scanning for malware and other harmful content.
   - Select **Scan inside archive (compressed) files** if you want to scan inside archived files.
   - Select **Sandbox detonation** if you want to send suspicious files to the Security Cloud to analyze the behavior of the file and decide whether it is clean or harmful.

4. Under **Disallowed file types**, do the following:
   a) Select **Configure file types**.
   *The **Malware scanning** page under the **General** tab opens.*

   NOTE: These malware scanning settings apply to Exchange, SharePoint, OneDrive, and Teams.

   b) Select one or more file types that you want the system to treat as harmful and take action based on the settings defined under **Action**.
5. Under **Action**, set up the following:
   - From the drop-down menu, select the action that the system takes if malware is detected:
     - for Exchange: Move malicious attachment into quarantine; Move whole item into quarantine; Delete malicious attachment; Delete whole item; Take no action.
     - for SharePoint: Quarantine; Delete item; Take no action
     - for OneDrive: Quarantine; Delete item; Take no action
     - for Teams: Quarantine; Delete item; Take no action

     IMPORTANT: The deleted items cannot be recovered; instead they are permanently removed.
   - Select **Notify the administrator** for the administrators to receive a notification when harmful content is found in user mailboxes.
   - Turn **Notify the user about detections with the following severities:** on for the users to receive a notification when harmful content is found in their mailbox.

     NOTE: Select **Change** if you want to change the severity level.

     NOTE: This option applies only to Exchange.
   - Select **Configure notification text** to go to the **Notifications** view. Under **Notifications for malware**, you can enter the text that you want to show in the notification or edit the current notification.

     NOTE: This option applies only to Exchange.
6. Select **Save**.

The malware scanning settings are saved to the policy.

4.6.7 Set up Exchange URL scanning

Sets up URL scanning for a new Exchange policy.

To set up URL scanning:

1. On the Policies page, select the policy that you just created.
   The General view opens.
2. Select **Exchange** > **URL scanning**.
3. Turn **URL scanning** on.

   NOTE: When on, URL scanning scans web links (URLs) in bodies of email messages and other Exchange items.

4. Under **Action**, set up the following:
   a) From the **Malicious URL** drop-down menu, select the action that the system takes if a malicious URL is detected: Move item into quarantine; Delete item; Modify the subject; Take no action.

   > **IMPORTANT:** The deleted items cannot be recovered, but they are permanently removed.

   > **NOTE:** If you select the 'Modify the subject' option, you can edit the message subject that is shown if a harmful link is detected. The default subject is "Malicious URL content".

   b) From the **Suspicious URL** drop-down menu, select the action that the system takes if a suspicious URL is detected: Move item into quarantine; Delete item; Modify the subject; Take no action.

   > **IMPORTANT:** The deleted items cannot be recovered; instead they are permanently removed.

   > **NOTE:** If you select the 'Modify the subject' option, you can edit the message subject that is shown if a harmful link is detected. The default subject is "Malicious URL content".

   c) Select **Notify the administrator** for the administrators to receive a notification when a harmful or suspicious URL is found in a user mailbox.
   d) Select **Notify the user about detections with the following severities:** for the users to receive a notification when a harmful or suspicious URL is found in their mailbox.

   > **NOTE:** Select **Change** if you want to change the severity level.

   e) Select **Configure notification text** to go to the **Notifications** view. Under **Notifications for malicious URL**, you can enter the text that you want to show in the notification or edit the current notification.
5. Turn **Trusted websites** on and set up the following:
   a) Select **Allow reporting of trusted websites to WithSecure** to improve the accuracy of URL detection. The product validates all email URLs against the one defined as a trusted in a policy.
   b) In the **Websites** field, enter addresses of trusted websites to specify the websites that you want to exclude from scanning, for example, `example.com` or `www.mywebpage.com`.

   If you specify a full URL, the system marks only a domain name as trusted: `http://foobar.example.com/?t=true` > `foobar.example.com`.

   > **NOTE:** If `http://foobar.example.com/?t=true` is defined as a trusted website in the Policy settings, the system processes the URLs as described below:
   >
   > - `www.alpha.foobar.example.com` - passes as trusted
   > - `http://example.com` - is sent for further analysis

   > **NOTE:** You can select
   >
   > to copy the website addresses to the clipboard or **Remove all** to empty the field.

6. Turn **Blocked websites** on and set up the following:

a) In the **Websites** field, enter addresses of blocked websites to specify the websites that you want to block, for example, `example.com` or `www.notmywebpage.com`.

If you specify a full URL, the system marks only a domain name as blocked: `http://foobar.example.com/?t=true` > `foobar.example.com`. Also, none of the subdomains of the blocked subdomain are allowed.

NOTE: You can select

to copy the website addresses to the clipboard or **Remove all** to empty the field.

NOTE: The Blocked websites setting has higher priority than the trusted one.

The Exchange URL scanning settings are configured for the policy.

Next, set up inbox rules scanning.

4.6.8 Set up Exchange inbox rules scanning

Sets up inbox rules scanning to detect suspicious inbox rules for a new Exchange policy.

To set up inbox rules scanning:

1. Select **Exchange** > **Inbox rules scanning**.
2. Turn **Inbox rules scanning** on.

NOTE: When on, inbox rules scanning detects suspicious inbox rules.

3. Select the inbox rules for which you want to turn detections on:
   - Suspicious rule name
   - Suspicious auto email moving
   - Suspicious email deletion
   - Suspicious auto auto-forwarding
4. Under **Action**, set up the following:
   - Select **Notify the administrator** for the administrators to receive a notification when a suspicious inbox rule is found in user mailboxes.
   - Select **Notify the user about detections with the following severities:** for the users to receive a notification when a suspicious inbox rule is found in their mailbox.
5. Select **Save**.

The Exchange inbox rules scanning settings are saved to the policy.

4.6.9 Set up the Exchange compromised accounts options

Sets up the Compromised accounts options for a new Exchange policy.

To set up the Compromised accounts options:

1. Select **Exchange** > **Compromised accounts**.
2. Turn **Compromised accounts** on.
3. Under **If an account is found as compromised**, set up the following:

- Select **Notify the administrator** for the administrator to receive a notification when an account has been detected as compromised.
- Select **Notify the user about detections with the following severities:** for the users to receive a notification when their email account has been detected as compromised.

NOTE: Select **Change** if you want to change the severity level.

NOTE: Even if a user email account has been part of a breach, it does not necessarily mean that the account users themselves have entered the email addresses to the breached site.

4. If you want to set up the user notification text, select **Configure user notification text**.
5. Select **Save**.

The Exchange compromised accounts options are saved to the policy.

4.6.10 Set up Exchange notifications

Sets up notifications for a new Exchange policy.

To set up Exchange notifications:

1. On the Policies page, select the policy that you just created.
   The General view opens.
2. Select **Exchange** > **Notifications**.
3. Under **Notifications for malware** and **Notifications for malicious URL**, you can edit the malware and malicious URL email templates for both user and administrator notifications.
4. Under **Notifications for compromised accounts**, based on the severity of the breach (critical, high, medium, or low), you can edit the subject and the text of the notification that is sent to users when their email account or password or both have been detected as part of a breach.
5. Under **Notification for released quarantine item**, you can edit the subject and text of the notification that is sent to users when items are released from the quarantine.
6. Select **Save**.

The Exchange notification settings are saved to the policy.

4.7 Managing quarantined items

Quarantine is a safe repository for items that may be harmful.

NOTE: Quarantined items cannot spread or cause harm to the company computers. The product can place harmful items in quarantine to make them harmless. You can release items from the quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in the quarantine removes it permanently from the cloud service.

In the WithSecure Elements Collaboration Protection portal, you can view the quarantined items, use filtering to find specific ones, and release or delete quarantined items.

4.7.1 Filter quarantined items

You can use filtering to find quarantined items by using different filtering criteria.

NOTE: By default, the Quarantine page is shown with the following Status filters applied: quarantined, failed, and recoverable failure,

To filter the quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, use any of the following criteria:
    - Quarantine ID - enter the quarantine ID of the quarantined message.
    - Status - select the status of the message. You can search for items that are quarantined, deleting, releasing, released, failed, or that have recoverable failure.
    - Time from - select from which date and time on you want to see the quarantined items.
    - Time to - select until which date and time you want to see the quarantined items.
    - Cloud service source: select one of the source options: Exchange, SharePoint, OneDrive, or Teams
    - Exchange
        - Message ID - enter the message ID of the quarantined message.
        - Sender - enter the email address of the message sender. You can only search for one address at a time, but you can widen the search by using the wildcards.
        - Mailbox - enter the email address of the message receiver.
        - Subject - enter the subject of the message to use it as a search criteria.
    - SharePoint
        - Site name - enter the name of the quarantined site.
        - Site URL - enter the URL of the quarantined site.
        - File name - enter the name of the quarantined file.
        - File location - enter the location of the quarantined file.
    - OneDrive
        - Drive name - enter the name of the quarantined drive.
        - Drive location - enter the location of the quarantined drive.
        - File name - enter the name of the quarantined file.
        - File location - enter the location of the quarantined file.
    - Teams
        - Site name - enter the name of the quarantined site.
        - Site location - enter the location of the quarantined site.
        - File name - enter the name of the quarantined file.
        - File location - enter the location of the quarantined file.
3. Select **Apply**.
4. From the drop-down menu on the right, select the cloud service that you want to view.

The page shows a list of items that were found based on your search criteria.

4.7.2 Delete quarantined items

You can delete quarantined items.

To delete quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, select the items that you want to delete from the quarantine.

NOTE: You can delete up to 200 items at a time.

3. At the bottom of the page, select **Delete**.

The selected items are gradually deleted one by one from the quarantine.

4.7.3 Release quarantined items

You can release items from the quarantine.

To release quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, select the items that you want to release from the quarantine.

NOTE: You can release up to 200 items at a time.

3. At the bottom of the page, select **Release**.

The selected items are gradually released from the quarantine.

Manually recover quarantined emails

Manually recovers quarantined emails after the Cloud Service has been deleted, using the EWS Editor tool.

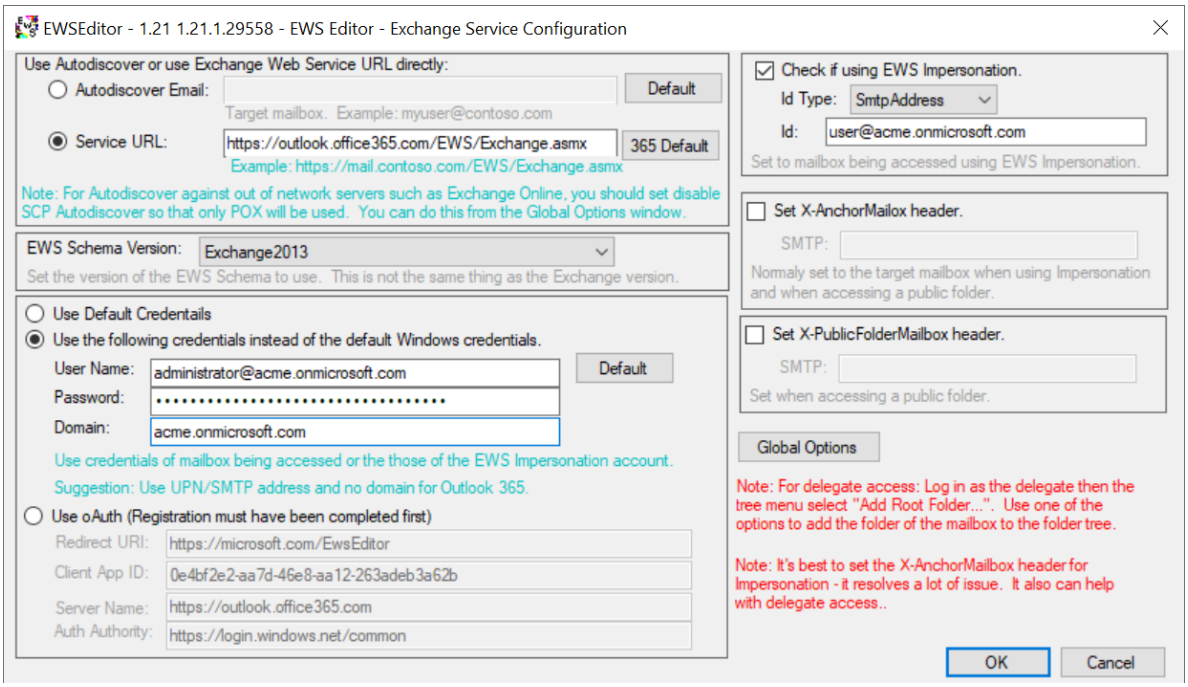
The best practice for managing quarantined items is to remove or release them from the quarantine before removing the Cloud Service. Once you have removed a Cloud Service, you no longer can manage any quarantined items for that Cloud Service via the WithSecure Elements Collaboration Protection portal.

NOTE: Creating a new Cloud Service with the same name or Azure AD connection does not grant access to old quarantined items.

After removing a Cloud Service, you can release the quarantined items for the user by using the EWS Editor tool at https://github.com/dseph/EwsEditor/releases as follows:

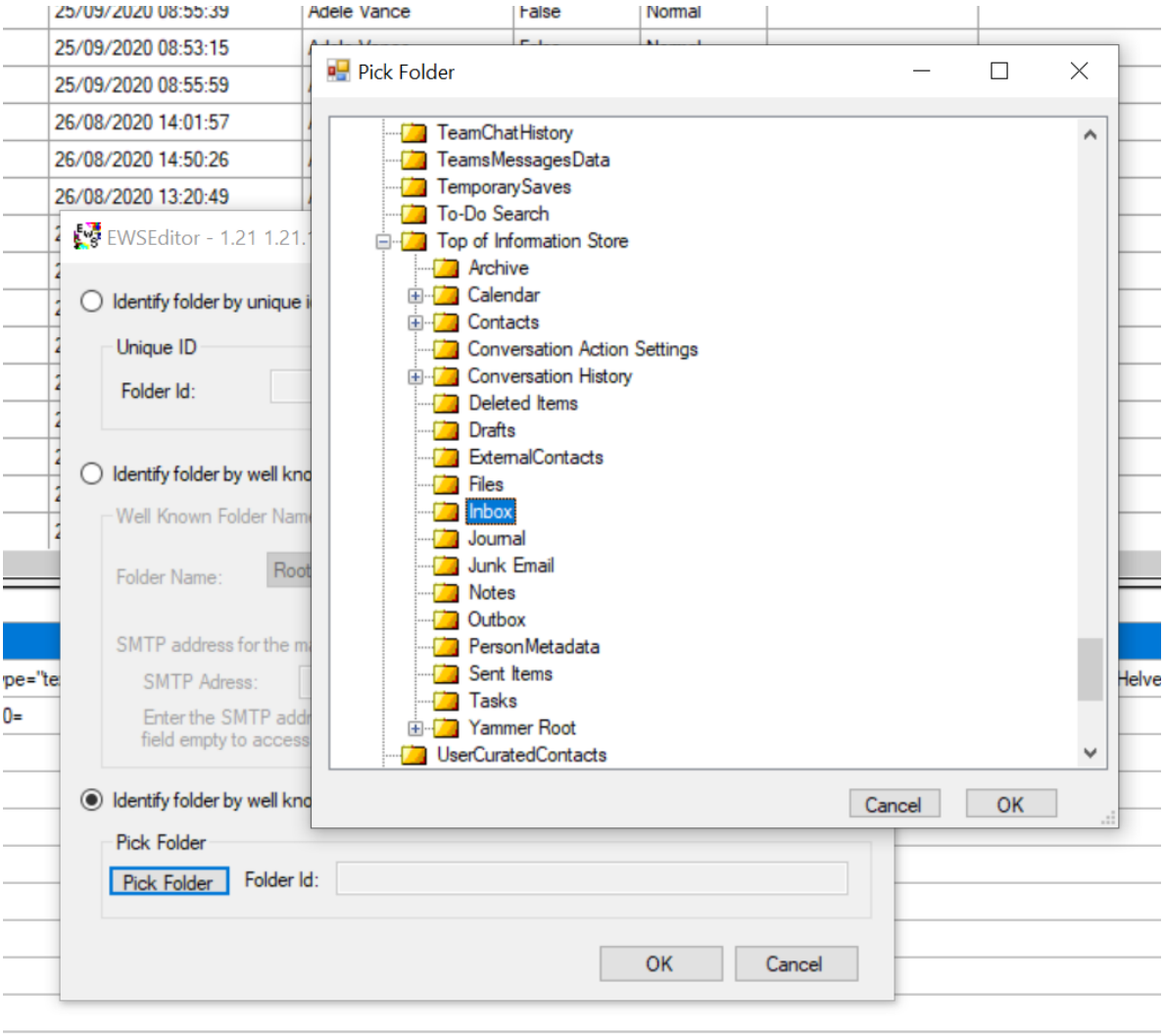
To manually restore quarantined items:

1. Use your administrator credentials to connect to Exchange and impersonate the user.



2. Select **OK**.
3. After configuring the connection, when asked if you want to add the mailbox root to the tree view, select **Yes**.
4. Double-click the **WithSecure Elements Collaboration Protection** folder inside the Root folder.
   A new window that contains all the Exchange items that have been quarantined opens up allowing you to delete or restore the quarantined items.
5. To restore an item, right-click the item and select **Move Item...**.
6. In the pop-up window that opens, select **Identify folder by well known name**.

7. In the pop-up window that opens, select **Identify folder by well known name** > **Pick Folder** to select the folder to which you want to restore the item. A good location would be, for example, the Inbox folder under Top of Information Store.



8. Select **OK** > **OK** to restore the item to the desired location.
9. Repeat the steps for any additional items that you want to release or remove.

4.8 Managing system events

System events help you understand changes in the state of your system resources or system health. Every action of adding, editing or deleting system resources generates a new system event.

System events record changes to your system resources and system health. Adding, editing, or deleting a system resource generates a new system event, and you can filter the event list to find specific events.

4.8.1 Filter system events

You can use filtering to find system events in the WithSecure Elements Collaboration Protection portal.

To filter system events:

1. Select **System events** on the sidebar.
   The System events page opens listing all the events.
2. From the drop-down menu, select one of the categories to filter the events:
   - Source

- Level
- Time from
- Time to

3. In the field next to the drop-down menu, select a value, and then select **Apply**.

   For the Source category, you can select one of the following values:

   - Provisioning service
   - Policy service
   - Quarantine service
   - Authorization service
   - Email scan service
   - Reporting service

   For the Level category, you can select one of the following values:

   - Information
   - Warning
   - Error
   - Critical

4. To reset the selected filter category and the value, select **Clear all**.

NOTE: You can remove a filter by selecting **x** in the text box that appears under the drop-down menu once you have applied a filter.

A list of the events that match the filtering criteria you selected is shown.

4.9 Managing reports

Scheduled reports give you information about the overall status of the WithSecure Elements Collaboration Protection portal. On the Scheduled reports page, you can switch a scheduled report task on or off in the Active column. If the scheduled task is switched off (that is, inactive), no report is generated.

Scheduled reports summarize the overall protection status of your Elements Collaboration Protection portal. You can generate, edit, view, clone, and delete report tasks, and switch each task on or off to control whether it produces a report.

4.9.1 Generate scheduled report tasks

You can use the portal to generate scheduled reports.

NOTE: Generated reports show the name of the user who created the scheduled task. To change the name, select

at the top right corner, and then select **Account settings**.

To schedule a report:

1. Select **Reports** on the sidebar.
   The Reports view opens.
2. Select **Add new**.
   *The **Scheduled report** screen opens.*
3. Enter the following information:

- Report name - give the report a name
- Organization - as a company administrator, you can only generate a report for your own company

  NOTE: As a partner, you can select the company for which you want to create the report.

- Frequency - select how often you want the report to be generated
- Timezone - select the timezone that is used in the report
- Contents - select which sections of the Dashboard you want to include in the report:
  - Detections by severity
  - Mailbox status
  - Top 10 affected mailboxes
  - Protection status
  - Protection trend
- Author name - the name of the user who created the scheduled report task.
- Summary (optional) - enter here text that you want to show in the beginning of the report

4. Select **Save**.
   The new schedule for generating a report is created.

4.9.2 Edit scheduled report tasks

Edits a scheduled report task.

To edit a scheduled report task:

1. Select **Reports** on the sidebar.
   *The **Reports** view opens.*
2. In the Action column, select

   next to the report that you want to edit, and then select **Edit**.
   The Scheduled report screen opens.
3. Make the changes to the report settings, and select **Save**.

4.9.3 Download and view reports

Downloads and views generated reports.

To view the reports:

1. Select **Reports** on the sidebar.
   The Reports view opens.
2. Select ⌄ next to the scheduled report task that you want to view.

   NOTE: The Reports available column shows if and how many reports are available.

3. Under **Reports ready to download**, select the report that you want to download and view. You can either open the report (PDF file) or save it on your computer.

   NOTE: The link shows the date of the report and in how many days the report expires.

4.9.4 Clone scheduled report tasks

Clones a scheduled report task.

To clone a scheduled report task:

1. Select **Reports** on the sidebar.
   *The **Reports** view opens.*
2. In the Action column, select
   
   next to the report that you want to edit, and then select **Clone**.
   The Scheduled report screen opens.
3. Enter a new name for the report and make any other changes, if needed.
4. Select **Save**
   The new scheduled report task was added.

4.9.5 Delete scheduled report tasks

Deletes a scheduled report task.

To delete a scheduled report task:

1. Select **Reports** on the sidebar.
   *The **Reports** view opens.*
2. In the Action column, select
   
   next to the report that you want to edit, and then select **Remove**.
3. In the window that opens, select **Remove**.
   The scheduled report is permanently removed and the action cannot be undone.

Chapter 5
Support

Support

If you cannot find answers to your questions in this guide, you can get more information from the our Help Center, Community forums and the support website.

In our User Guides, you can find user guides for all WithSecure products.

Our Community forums help you find more troubleshooting information and solutions for known issues.

Go to our Support request page for instructions on how to contact our technical support team.

Chapter 6

Offboarding Collaboration Protection

Topics:

- Remove a cloud service
- Remove permissions from the Azure portal

Offboarding Collaboration Protection

Offboarding WithSecure Elements Collaboration Protection removes the cloud service connection in WithSecure Elements Security Center and the granted permissions in the Azure portal.

To offboard WithSecure Elements Collaboration Protection, you remove the cloud service connection in WithSecure Elements Security Center and remove the permissions granted to the WithSecure application in the Azure portal.

6.1 Remove a cloud service

Removes a cloud service in WithSecure Elements Security Center.

Remove a cloud service when you no longer want it protected through the Elements Security Center.

1. In Elements Security Center, under **Collaboration Protection**, select **Cloud services**.
2. In the **Cloud** page, in the **Name** column, select a tenant.
3. From the action menu at the bottom, select **Remove cloud service**.
4. In the confirmation window, select **Remove** to confirm that you want to remove the selected cloud service.

6.2 Remove permissions from the Azure portal

Removes the granted permissions and the WithSecure Elements Collaboration Protection applications from the Azure tenant.

Before you remove these permissions, recover any quarantined items that you want to keep.

Removing these permissions revokes the Collaboration Protection applications' access to your Microsoft 365 tenant as part of offboarding the product.

1. Log in to portal.azure.com.
2. Search for `Microsoft Entra ID` and select it.
3. Select **Enterprise Applications**.

NOTE: Depending on for which applications you have configured protection, you may have 1-3 applications to remove.

4. Search for **WithSecure Elements Collaboration Protection for Exchange** and select it.
5. In the side bar, select **Manage** > **Properties**.
6. Select **Delete**.
7. Confirm by selecting **Yes**.
8. Repeat the search, delete, and confirm steps to remove the remaining two applications:
   - WithSecure Elements Collaboration Protection for OneDrive
   - WithSecure Elements Collaboration Protection for SharePoint and Teams

Appendix A

Specifying Microsoft Azure Active Directory tenant name and ID

Topics:

- Determine the tenant name of your Azure Active Directory and Office 365
- Locate the Microsoft Azure Active Directory tenant ID

Specifying Microsoft Azure Active Directory tenant name and ID

You need to specify the name and ID for the Microsoft Azure Active Directory tenant.

To connect Elements Collaboration Protection to your organization, specify the name and ID of your Microsoft Azure Active Directory tenant. You find both values in the Azure portal.

A.1 Determine the tenant name of your Azure Active Directory and Office 365

The Microsoft Azure Active Directory tenant name is the primary domain that was initially created for Microsoft Office 365.

To determine the tenant name:

1. Log in to Office 365 Admin Center as an administrator.
2. Under **Setup**, select **Domains** and find a domain that ends with `.onmicrosoft.com`.
   This is your Office 365 tenant name.

A.2 Locate the Microsoft Azure Active Directory tenant ID

Locates the Microsoft Azure Active Directory (AAD) tenant ID in the Office 365 Admin Center.

To locate the tenant ID:

1. Select **Azure Active Directory** in the navigation menu.
   The Azure Active Directory (AAD) administrator portal opens.
2. In the AAD administrator portal, select **Azure Active Directory**
3. Under Manage, select **Properties**.

The tenant ID is shown in the Directory ID box.

Appendix B

WithSecure Sample Validation Service Overview

Topics:

- Submit a file sample
- Submit an email sample
- Submit a URL sample
- Choosing the correct Sample Type

WithSecure Sample Validation Service Overview

This topic introduces WithSecure™ Sample Validation (formerly Submit a Sample) and highlights the service's purpose, features, and future updates.

WithSecure Sample Validation is a detection-quality–driven cybersecurity service integrated directly into the Elements Security Center. WithSecure's expert malware analysts deliver the service, with support from proprietary cloud technologies. The service provides high detection accuracy, consistency, and continuous improvement across all detection vectors.

More than a reactive security tool, Sample Validation actively improves detection performance by:

- Correcting false positives and false negatives
- Identifying detection gaps
- Strengthening overall security posture
- Providing expert human analysis, backed by malware analysis and threat research

Through this combination of automation, cloud intelligence, and analyst expertise, organizations gain deeper insight into emerging threats. The combination also improves the precision, speed, and reliability of detection, containment, and remediation.

B.1 Submit a file sample

Submit a file sample for validation in the Elements Security Center.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, you must first select the appropriate **Customer company** using the *scope selector* located at the top of the Elements portal. Once the correct customer company has been selected, you can proceed to the **Requests** page to create or view **Sample Validation requests**.

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **File**

   Make sure you selected the correct sample type for the file.

- File-Based False Positive: A clean file incorrectly detected as malware. For example, a company's internal tool flagged as a trojan.
- Potentially Unwanted Application (PUA): Legitimate software detected as unwanted. For example, a remote admin or adware-style installer used for business purposes.
- File-Based False Negative: A malicious file not detected by the product. For example, a ransomware executable encrypts data without being blocked.

6. Drag and drop the file or click **Browse** to upload the file
7. Open the **Request reason** drop-down menu and select one option:
   a. False Positive - Clean file was blocked
   b. False Negative - Malicious file not detected
   c. Potentially unwanted application detected
   d. Request whitelisting
8. Open the **Product name** drop down menu and select the product.
9. Add a short title for the request in the **Title** field.
10. Write down a description of the file or summary of concern.
11. Click **Create Request**.

The sample request is submitted to WithSecure.

B.2 Submit an email sample

Submit an email sample for validation in the Elements Security Center.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, you must first select the appropriate customer company using the scope selector located at the top of the Elements portal. Once the correct customer company has been selected, you can proceed to the **Requests** page to create or view **Sample Validation requests** .

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **Email**.

   Make sure you selected the correct sample type.

- Phishing False Positive: A legitimate email incorrectly marked as phishing. For example, vendor invoice emails flagged incorrectly.
- Phishing False Negative: A phishing email not detected. For example, a spoofed Microsoft 365 login email reaches the inbox.
- Email Attachment Not Detected: A malicious attachment is not detected by security products. For example, unexpected ZIP/Invoice file requiring a password mentioned in the email.
- Spam False Negative: Junk or promotional emails delivered to inbox. For example, promotional spam not filtered out.

6. Drag and drop the email file or click **Browse** to upload the email file
7. Open the **Request reason** drop-down menu and select one option:
   a. False Positive - Legitimate email was blocked
   b. False Negative - Phishing not detected
   c. False Negative - Spam not detected
   d. False Negative - Malicious email not detected
8. Open the **Product name** drop-down menu and select the product.
9. Add a short title for the request in the **Title** field.
10. Write down a description of the file or summary of concern.
11. Click **Create Request**.

The sample request is submitted to WithSecure.

B.3 Submit a URL sample

Submit a URL sample for validation in the Elements Security Center.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, you must first select the appropriate customer company using the scope selector located at the top of the Elements portal. Once the correct customer company has been selected, you can proceed to the Requests page to create or view Sample Validation requests .

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **URL**.

Make sure you selected the correct sample type.

- URL-Based False Positive: A safe website is blocked by mistake. For example, `https://partnerportal.company.com` blocked as phishing.
- URL Categorization: Request to update or correct the URL category. For example,reclassifying a corporate blog from "Unknown" to "Business."
- Unknown URL: A new or uncategorized domain requiring classification. For example, submitting `https://newvendor.io` for review.
- URL-Based False Negative: A harmful website is not blocked by the product. For example, `http://malicious-site.ru` remains accessible and serves malware.

6. Enter URL or IP address.
7. Open the **Request reason** drop-down menu and select one option:
   a. False Negative - Malicious URL not blocked
   b. False Positive - Trusted URL blocked
   c. CAT - URL has incorrect content category
   d. CAT - M - URL missing content category
8. Open the **Product name** drop-down menu and select the product
9. Add a short title for the request in the **Title** field
10. Write down a description of the file or summary of concern.
11. Select **Create Request**.

The sample request is submitted to WithSecure.

B.4 Choosing the correct Sample Type

Selecting the correct sample type when submitting a request ensures accurate analysis and faster resolution.

File Sample Type	**Choose this category when the issue involves a file from a device.**
File-Based False Positive	A clean file incorrectly detected as malware. For example: A company's internal tool flagged as a trojan.
Potentially Unwanted Application (PUA)	Legitimate software detected as unwanted. For example: A remote admin or adware-style installer used for business purposes.
File-Based False Negative	A malicious file not detected by the product. For example: A ransomware executable encrypts data without being blocked.
URL Sample Type	**Choose this category when the issue involves a URL, website, or IP address.**
URL-Based False Positive	A safe website is blocked by mistake. For example: `https://partnerportal.company.com` blocked as phishing.
URL Categorization	Request to update or correct the URL category. For example: Reclassifying a corporate blog from "Unknown" to "Business."
Unknown URL	A new or uncategorized domain requiring classification. For example: Submitting `https://newvendor.io` for review.
URL-Based False Negative	A harmful website is not blocked by the product.

URL Sample Type	**Choose this category when the issue involves a URL, website, or IP address.** For example: `http://malicious-site.ru` remains accessible and serves malware.
Email Sample Type	**Choose this category when the issue involves an email sample.**
Phishing False Positive	A legitimate email incorrectly marked as phishing. For example: Vendor invoice emails flagged incorrectly.
Phishing False Negative	A phishing email not detected. For example: A spoofed Microsoft 365 login email reaches the inbox.
Email Attachment Not Detected	A malicious attachment is not detected by security products. For example: Unexpected ZIP/Invoice file requiring a password mentioned in the email.
Spam False Negative	Junk or promotional emails delivered to inbox. For example: Promotional spam not filtered out.
Allowlisting Requests	**Choose this category for allowlisting tools, apps, or scripts.**
Request Whitelisting	Request to whitelist legitimate tools, scripts, or applications - often during development. May require temporary security exceptions. For example: WithSecure products block unsigned binaries, packers, automation scripts, or local dev servers, and adjustments are not feasible during early development stages.

Appendix C

Manual scanning of suspicious items

Topics:

- Manually scan suspicious Exchange items
- Manually scan suspicious SharePoint items

Manual scanning of suspicious items

You can force the scanning of suspicious emails and other items.

In addition to scheduled and real-time scanning, you can manually scan suspicious items when you want an immediate result. Manual scanning covers mailbox items and SharePoint files.

C.1 Manually scan suspicious Exchange items

Forces a manual scan of suspicious Exchange items by moving them to a dedicated folder.

To force the scanning of suspicious emails:

1. Create a new folder in the inbox called "manual scan".
2. Move any suspicious emails to the new folder.

The suspicious emails are automatically scanned. Depending on the action defined in the security policy, an action is taken, for example, the emails are quarantined or an email notification is sent.

C.2 Manually scan suspicious SharePoint items

Forces a manual scan of suspicious SharePoint items by moving them to a dedicated folder.

To force the scanning of suspicious items:

1. Create a new folder in the same location where the files that you want to scan are located.
2. Move any suspicious items to the new folder.

The items are automatically scanned. Within ten minutes, they are detonated and removed if detected as unsafe.

Glossary

Access Control

Access control is the practice of restricting and regulating who or what can view, use, or modify resources in a system, based on defined permissions and policies.

Active Directory (AD)

Active Directory (AD) is a Microsoft directory service that centralizes the management of network resources such as users, computers, and policies, providing authentication and authorization within a Windows domain network.

Agent

An agent is the client software installed on a managed device that enforces protection, reports device status, and communicates with the management service; more broadly, a program that acts on behalf of a user or another system.

Antivirus

Software that prevents, detects, and removes viruses and other malware.

Automation

Automation is the use of technology to perform tasks or processes with minimal human intervention, improving efficiency, accuracy, and scalability.

Backdoor

An undocumented way of gaining access to a computer system.

Breach

A breach is a security incident in which confidential or protected data is accessed, disclosed, or stolen by an unauthorized party.

Cloud Security

Cloud security is the set of policies, controls, and technologies that protect data, applications, and infrastructure hosted in cloud environments.

Cloud Service

A cloud service is an online service or workload that is connected to a platform for protection, monitoring, or administration.

Compromised Account

A compromised account is a user account that attackers have accessed, abused, or taken over without authorization.

Configuration Keys

Configuration keys are named settings used to preconfigure application behavior and feature values during deployment or device management.

Connector

A connector is a software or hardware component that enables communication and data exchange between two or more systems, applications, or devices.

Containment

Response actions that isolate affected hosts or accounts to stop an active attacker from spreading and to prevent the theft, alteration, or destruction of information.

Criticality

The possible impact that a detection would have in the customer environment, based on severity and the importance of affected hosts.

Custom Labels

A tagging feature in WithSecure Elements Security Center for organizing and managing devices.

Customer Company

A customer company is a customer organization that is created, managed, or serviced within a partner-managed platform or service structure.

Detection

A detection is an identified suspicious, malicious, or policy-relevant event, activity, or finding recognized by a security control or analysis system.

Direct Role Assignment

A direct role assignment grants a role to an individual account instead of granting access through group membership or another indirect path.

Discovery Scan

A discovery scan is a scan that identifies assets, systems, or targets present in a network or environment.

Email Sample

An email sample is an email message collected and submitted for security analysis, validation, or investigation.

Email Security Threat

A classification of security risks related to email communications, including phishing, malware attachments, and domain spoofing.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a security technology that continuously monitors endpoints to detect, investigate, and respond to suspicious activity and advanced threats.

Endpoint Protection

Endpoint protection is the set of security capabilities used to prevent, detect, and handle threats on endpoint devices such as workstations, servers, and mobile devices.

Entra ID

Microsoft's cloud-based identity and access management service (formerly known as Azure AD).

Exposure Management

Exposure Management is a security capability that identifies, prioritizes, and helps remediate weaknesses and exposures across assets, services, and environments.

False Negative

A false negative is a harmful file, message, URL, or activity that a security system incorrectly fails to identify as malicious or suspicious.

False Positive

A false positive is a legitimate file, message, URL, or activity that a security system incorrectly flags as malicious, suspicious, or otherwise harmful.

Federated Single Sign-On (FSSO)

A mechanism that allows users to authenticate once and access multiple applications across different domains without needing to log in again.

File Sample

A file sample is a file collected and submitted for security analysis, validation, or threat investigation.

Group Policy (GPO)

Group Policy (GPO) is a feature in Microsoft Windows that allows administrators to define security policies, user settings, and system configurations across multiple computers within a domain.

Harmful Content

Harmful content is files, applications, or web content that can damage data or compromise a device, such as malware or malicious websites.

IAM Role

An IAM role is an identity and access management role that defines a set of permissions which can be assumed by users, services, or workloads.

Identity and Access Management (IAM)

Identity and Access Management (IAM) is the framework of policies and technologies that ensures the right users have the appropriate access to resources, covering authentication, authorization, and the lifecycle of user identities.

Identity Management

Identity management is the discipline of creating, maintaining, and removing digital identities and their attributes so that users and devices can be reliably recognized across systems.

Identity Provider (IdP)

An Identity Provider (IdP) is a service that creates, stores, and manages digital identities, allowing users to authenticate and access multiple applications securely.

Inbox Rule Scanning

A security feature that analyzes mailbox rules for potential signs of compromise, such as unauthorized forwarding rules.

Incident

An incident is a security event or related set of events that indicates a compromise, policy violation, or other threat that requires investigation, containment, or remediation.

Lateral Movement

The process of moving through a network to access additional systems after an initial compromise.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an open protocol for accessing and managing directory information, such as users, groups, and devices, over a network.

Linux Authenticated Scanning

Linux authenticated scanning is a scan method that connects to Linux systems by using supplied credentials or keys to collect scan results and system information.

Malware

A program or a file that is developed for the purpose of doing harm. This includes computer viruses, worms and Trojan horses.

Manual Scanning

Manual scanning is a user-started security scan that runs on demand instead of running automatically on a schedule or in real time.

Membership

Membership is the state of belonging to a group, organization, directory, or other managed collection that affects visibility, access, or inherited permissions.

Mobile Device Management (MDM)

A security solution that enables IT administrators to remotely manage, monitor, and enforce security policies on mobile devices.

Multi-Factor Authentication (MFA)

A sign-in method that requires more than one form of verification before granting access to an account, so a leaked password alone is not enough to gain entry.

Offboarding

Offboarding is the controlled process of removing a product, integration, service connection, or granted permissions from an environment when it is no longer needed.

Patch Management

Monitoring the patch status of operating systems and third-party software and applying updates to close known vulnerabilities.

Phishing

In a phishing attack, an attacker sends a fraudulent message posing as a trusted sender to trick the recipient into revealing sensitive data such as credentials or financial information.

Potentially Unwanted Application (PUA)

A software program that may not be malicious but could introduce security risks, intrusive behavior, or unwanted advertisements.

Privacy

Privacy is the protection of a person's or organization's information from unauthorized collection, access, use, or disclosure.

Privacy Policy

A privacy policy is a published statement that describes how an organization collects, uses, discloses, and manages personal data.

Profile Assignment

Profile assignment is the process of applying a selected profile to a device, group, or target according to manual selection or assignment rules.

Quarantine

Quarantine is an isolated storage location or state where potentially harmful files, messages, or other items are held to prevent them from affecting systems or users while allowing later review, release, or deletion.

Quarantine ID

A unique identifier assigned to a file or email that has been isolated due to security concerns.

Quarantine Management

A security function that isolates potentially harmful files, emails, or applications for further review and prevents them from executing on the system.

Ransomware

A malicious program that prevents the user from accessing their data and/or device and demands a ransom to 'restore normal access'. The program may not actually restore normal access even if the ransom is paid.

Real-Time Protection

Real-time protection continuously scans files as they are accessed and blocks those that contain malware, providing always-on protection through real-time scanning.

Real-Time Scanning

Real-time scanning is continuous scanning that checks content or activity as it is accessed, saved, or processed.

Remote Monitoring and Management Integration (RMM)

Remote Monitoring and Management integration is the connection between a product and an RMM platform so status, data, or management actions can be exchanged.

Reputation Service

A service that puts files in context based on their age, frequency, and location to expose threats that could be otherwise missed.

Response Action

A response action is a manual or automated investigation, containment, or remediation step taken after suspicious or malicious activity is detected to gather evidence, reduce impact, or stop further spread.

Role Assignment

A role assignment is the grant of a role to a user, group, or other principal so it receives the permissions associated with that role.

Role-Based Access Control (RBAC)

A security model that restricts system access based on user roles and permissions to enforce the principle of least privilege.

Sample Validation

Sample Validation is a service for submitting suspicious files, URLs, or emails for expert analysis and tracking the results of the request.

Scan

A scan is a security check that examines a device, system, application, account, or other target for threats, vulnerabilities, suspicious activity, or policy-relevant findings.

Scan Node

A scan node is a host or service component that runs scans and reports their progress and results back to the management service.

Scan Templates

A scan template is a saved, reusable set of scan options that can be applied across multiple scans.

Scheduled Report

A scheduled report is a report that is generated automatically on a defined schedule and made available for review or delivery.

Scope Selector

A user interface component that can be used to broaden or narrow the scope of information that is displayed in the WithSecure Elements portals.

Security Administrator

A security administrator is a user account that manages security settings, access, or operational tasks according to the roles assigned to it.

Security Administrator Role

A role in the WithSecure Elements Security Center granting access to manage security configurations.

Security Cloud

Security Cloud is WithSecure's cloud-based threat analysis and reputation service that helps classify files, websites, and other security-relevant observations and deliver up-to-date protection against emerging threats.

Security Events

Security events are recorded security-related occurrences, detections, or actions that are shown for review, monitoring, or response.

Security Group

A security group is a collection of users that receives shared role assignments so its members inherit the same access permissions.

Security Policy

A set of rules that define how product settings are managed, protected and distributed. Primarily used in Policy Manager, but also appear in other admin-level corporate products.

Service Partner

A service partner is an organization or partner tier that manages services, customer organizations, or delegated operational responsibilities on behalf of others.

Severity

The possible impact that a cyber attack could have on the network environment based on how much damage the attack could do.

SharePoint Protection

SharePoint Protection is a Collaboration Protection capability that scans and protects content stored in a SharePoint deployment against malware and other threats.

Solution Provider

A Solution Provider is the top-level partner organization tier in the WithSecure Elements management hierarchy, which manages customer companies and delegates access to partner employees.

Spam

Spam messages are unsolicited email messages that are usually sent in bulk to a large list of recipients.

Subscription Key

A subscription key is a unique code that identifies and validates a subscription and is used to activate WithSecure products for an organization.

System Event Filtering

A security mechanism that processes and categorizes system events based on predefined criteria to reduce noise and focus on critical security insights.

Tenant

A tenant is an isolated instance of a multi-tenant cloud service — such as a Microsoft Entra ID directory — that belongs to a single organization and keeps its data, configuration, and users separate from other tenants.

Threat Detection

Threat detection is the process of identifying malicious activity, anomalies, or indicators of compromise within an environment so they can be investigated and stopped.

Threat Intelligence

Threat intelligence is evidence-based knowledge about existing or emerging threats — such as attacker tactics, indicators, and motivations — used to inform defensive decisions.

Trojan

A Trojan is malicious software that disguises itself as a legitimate program to trick users into running it, then performs harmful actions such as stealing data or opening a backdoor.

URL Sample

A URL sample is a submitted web address collected for security analysis, validation, or investigation.

User Invitation

A user invitation is the process or message used to add a new user or administrator to a service, organization, or managed scope.

Vulnerability

A flaw, loophole or unexpected behavior in a program or operating system that can be exploited by an attacker in order to perform unauthorized actions on the affected system / device.

Vulnerability Management

Vulnerability management is the continuous process of identifying, assessing, prioritizing, and remediating security weaknesses in systems and software.

Index

G

H

I

L

M

N

O

P

Q

R

S

T

U

V

W