WithSecure

WithSecure Elements Managed Detection and Response

2026-09-09

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: WithSecure Elements Security Center

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 WithSecure Elements Security Center. 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 to WithSecure Elements Security Center.

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 WithSecure Elements Security Center sign-in page 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: WithSecure Elements Security Center sign-in page.
   *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.

Before you begin, make sure that you have a Microsoft Entra account. If you are a new user, you must create one first.

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

1. Open the following link in the web browser: WithSecure Elements Security Center sign-in page.
   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 (FIDO2 specification)
- *Smartphones or other devices* that support the FIDO2 standard (FIDO2 specification)
- *Device biometrics*, fingerprint or facial recognition or Windows Hello from your device using WebAuthn (Web Authentication (WebAuthn) specification).

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.

You must already have another multi-factor authentication (MFA) method set up before you can use device biometrics.

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.

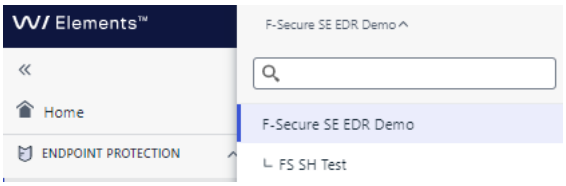
Move between the managed companies

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

Add a service partner account to your organization in WithSecure Elements.

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**.

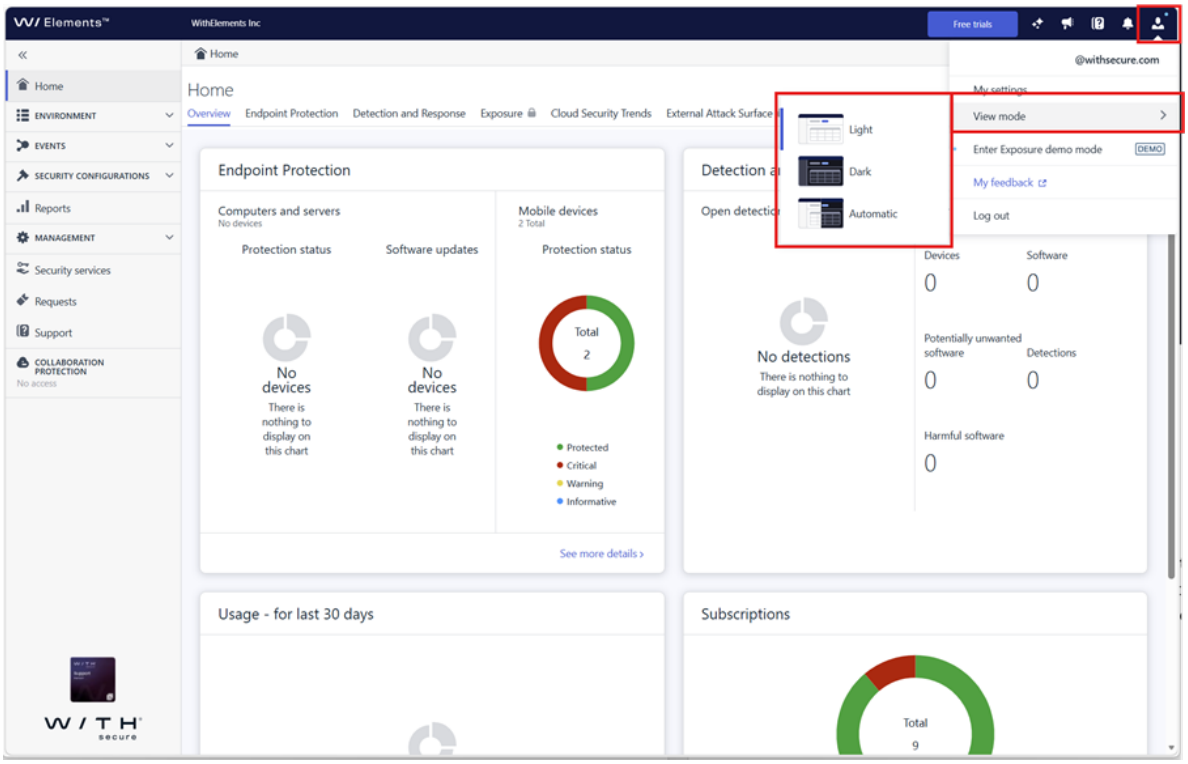
1.1.4 Change the view mode

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:

Option	Description
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.

Frequently asked questions

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 affects the Elements level, not only 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 WithSecure Elements Security Center sign-in page.
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 WithSecure Elements Security Center sign-in page.
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 WithSecure Elements Security Center sign-in page.
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 WithSecure Elements Connector documentation.

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.

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 new asset group.

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

WithSecure Managed Detection and Response overview

Topics:

- Key features

WithSecure Managed Detection and Response overview

WithSecure Managed Detection and Response (MDR) is a continuous 24/7 detection and response service, in which WithSecure's cyber security experts protect your IT environment by investigating and remediating cyber security attacks across your estate using data collected by WithSecure Elements Endpoint Detection and Response (EDR).

In today's digital landscape, safeguarding your network against cyber threats and intrusions is a challenging task. This is particularly true for incidents that occur beyond regular business hours. Effective cyber security measures demand extensive, around-the-clock monitoring and threat analysis. They also require skilled analysts who are ready at all times.

WithSecure Managed Detection and Response offers continuous monitoring, detection, and response. A response team authorized by you is equipped to take swift, decisive action against cyber threats. This keeps your digital environment secure at all times.

2.1 Key features

WithSecure Managed Detection and Response service offers the following key features.

Monitoring	The service provides continuous surveillance for suspicious activities within your IT infrastructure to ensure early detection of potential threats.
Investigation	The service thoroughly examines and identifies alerts about potential threats to determine their validity, distinguishing actual threats that require remediation from benign anomalies.
Escalation	The service ensures that verified threats are promptly escalated to the designated contacts or IT partners responsible for managing the environment.
Response	The service goes beyond the investigation of potential threats. It can take definitive actions, including containment and eradication of verified threats, and can act on your behalf when granted authorization.
Retainer	The service provides access to expert incident response resources who can assist you in the event of a significant cyber security incident.

Chapter 3

Getting started with WithSecure Elements MDR

Topics:

- Take the service into use

Getting started with WithSecure Elements MDR

Begin protecting your digital environment by deploying WithSecure Endpoint Detection and Response to endpoint devices.

WithSecure Endpoint Detection and Response is your first line of defense against cyber threats. It is designed to monitor and analyze activities across all endpoints — be it devices, computers, or servers. Endpoint sensors are crucial for in-depth data collection and analysis. They track the behavior and occurrences and identify any potential threats. When they detect anomalies, they generate alerts for further investigation.

WithSecure Managed Detection and Response builds upon these capabilities, offering advanced threat hunting and response services. Our specialized analysts will handle these alerts, ensuring comprehensive analysis and swift resolution of any detected issues.

Service Level Agreement (SLA) ensures prompt response times by during the threat investigation process. From the moment service detects potentially risky or unusual activity, WithSecure Threat Analysts will promptly start the investigation ensuring timely and effective threat management.

3.1 Take the service into use

You have to establish on-call support contacts and deploy WithSecure Elements Endpoint Detection and Response Agent to enable continuous monitoring and protection against cyber security threats.

Before you can use the service, set up on-call support contacts and deploy the Endpoint Detection and Response Agent to your devices.

1. Create a WithSecure business account if you do not already have one and log in to WithSecure Elements Security Center.
2. Deploy endpoint sensors on your 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.

   Install WithSecure Elements Endpoint Detection and Response Agent software across your network that identifies security threats. Once deployed on selected network devices, it collects data and sends it to WithSecure for comprehensive analysis.

   NOTE: For more information, see WithSecure WithSecure Elements Endpoint Detection and Response documentation.

3. Deploy your MDR license in WithSecure Elements Security Center.
   a) Go to **Management** > **Subscriptions** if you have "WithSecure MDR" present

      If you can see your WithSecure MDR subscription, continue to the next step.

   b) If you do not see the subscription on the list, select **Assign Subscription**.
   c) On the dialog that opens, enter your WithSecure MDR subscription code.
4. Turn on **Advanced Response** for MDR.
   a) In WithSecure Elements Security Center, go to **Security Configurations** > **Profiles**.
   b) In the profile editor, open **General Settings** and turn on **Integrations** > **Advanced Response**.
   c) Save the profile and repeat steps for each profile that is in use in the organization.
   d) Verify that adjusted profiles have been assigned correctly.
   e) Verify that advanced response is enabled on your active devices.

5. Add escalation contact information.

   To make sure that the service has continuous operational support, you must assign primary and secondary contact persons or groups, who must be readily available for on-call support at all times.

6. Activate automated actions.
   a) In WithSecure Elements Security Center, go to **Security Configurations** > **Automated actions**.
   b) Activate the automated action for **WithSecure MDR**.

3.1.1 Add contact information

To ensure continuous operational support, primary and secondary contact persons or groups must be assigned. These contacts must be readily available for on-call support at all times.

Follow these instructions:

1. Open WithSecure Elements Security Center.
2. Go to **Management** > **Subscriptions**.
3. On the **Subscriptions** page, select **WithSecure MDR** from the list.
   *The **Subscription information** page opens.*
4. On **Subscription information** page, add two incident response contacts by filling in the required fields.
   a) In **Timezone**, select the time zone of the contact person or group.
   b) Enter the **Full name** of the contact person or group.
   c) Add the **Country code** and **Phone number** of the contact person or group.

      WithSecure Threat Analysts will call this number if containment or remediation actions have not been pre-authorized.

   d) In **Available time**, specify when WithSecure Threat Analysts may contact this contact person or group.

      Make sure that either **Contact 1** or **Contact 2** is available at all times.

   e) Select **Save** after entering all contact information for both contacts.

Chapter 4

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.

4.1 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

4.2 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.

4.3 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.

4.3.1 Deploy manually using an EXE file

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

You 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.

4.3.2 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 73.

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.

4.3.3 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.

4.3.4 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:

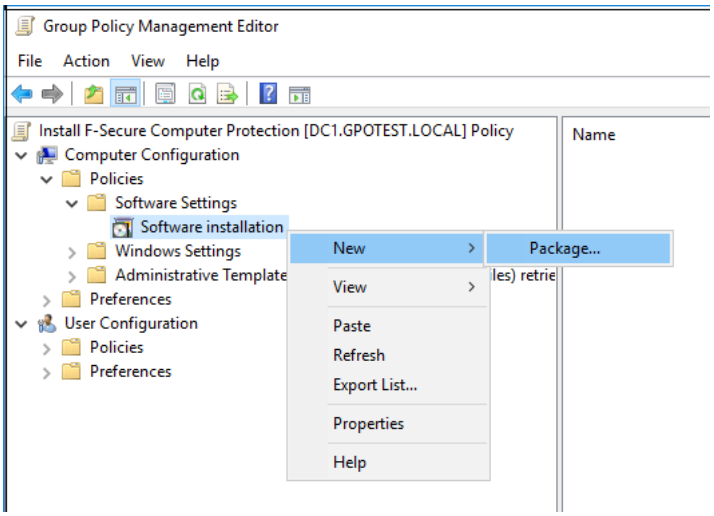
- An Active Directory environment.
- All target domain members need to have a Universal CRT installed. Normally, it comes with Windows updates and is present on regularly updated systems. If the installation fails to detect it, a corresponding error message is issued to the Windows Event Log of the target system. If you need to install or repair it manually, use this link: Visual C++ Redistributable (x86) installer.
- 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 73. 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.

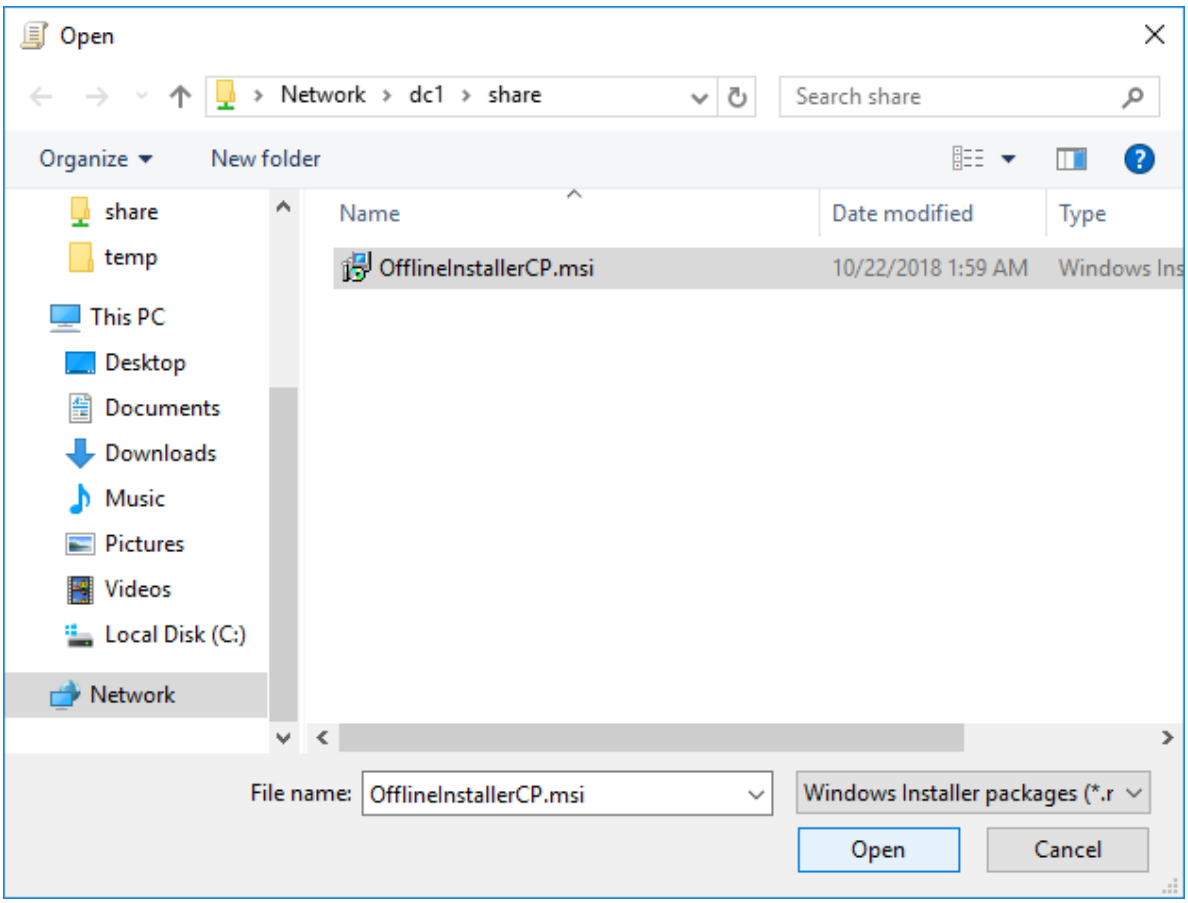
To install the product:

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

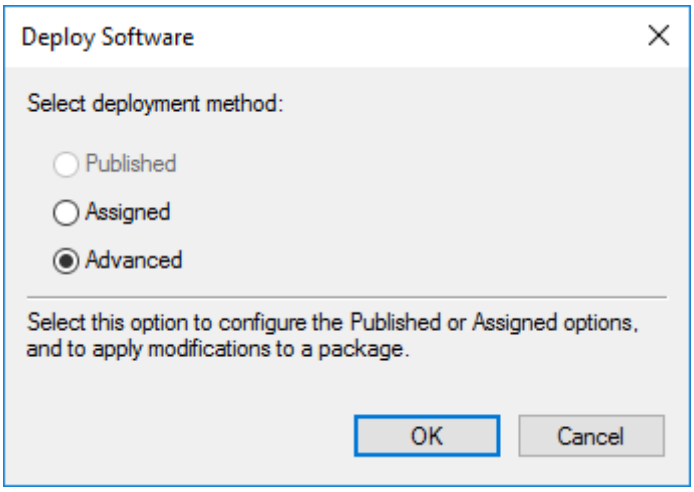
2. Open the Group Policy Management Console and create a new Group Policy Object that you link to the domain.
3. Navigate to **Computer Configuration** > **Policies** > **Software Settings** > **Software installation**.
4. Right-click the right pane and select **New** > **Package...**.



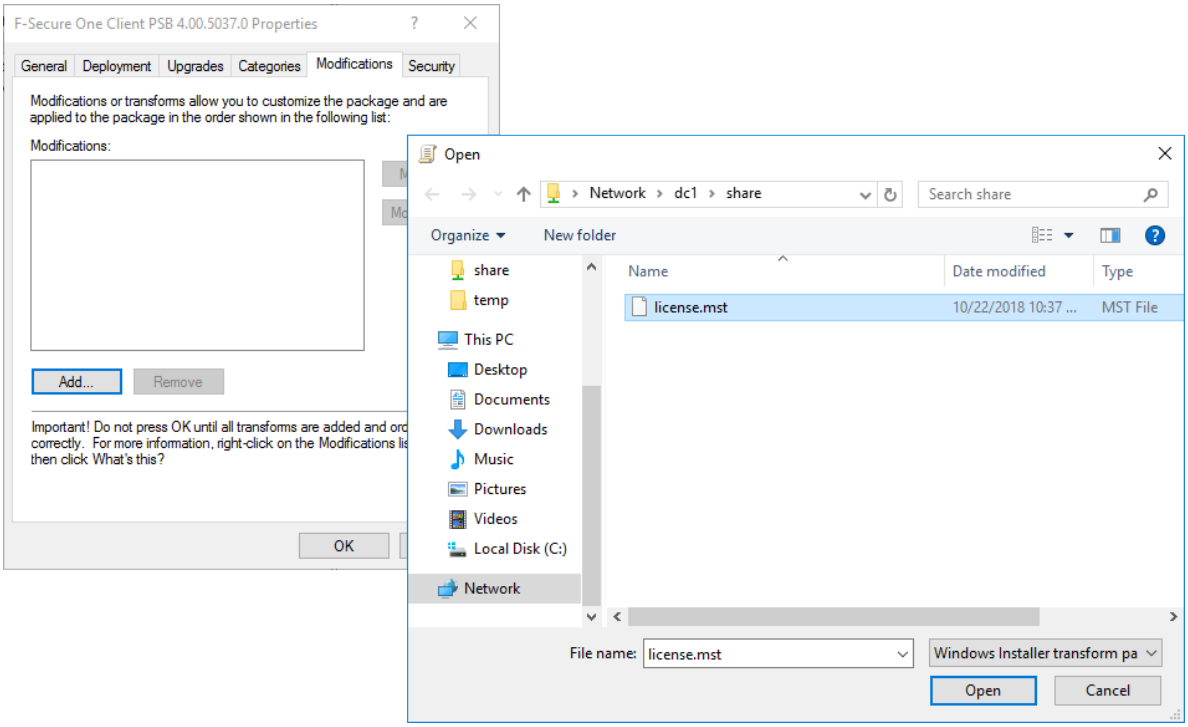
5. In the open file window, select `OfflineInstallerCP.msi` and then select **Open**.



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

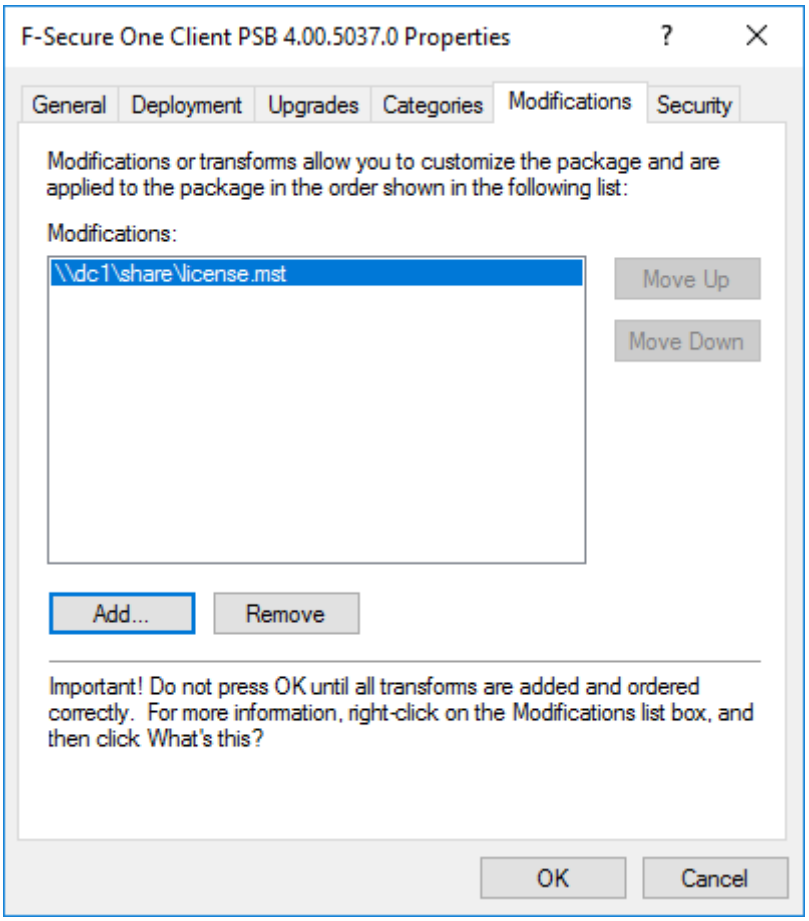


7. Go to the **Modifications** tab, and then select **Add...**.
8. In the open file window, select `license.mst` (the transform file from `FsMsiTool.exe` earlier), and then select **Open**. This adds the transform file path to the GPO settings.



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.

4.3.5 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: WithSecure Elements Agent offline installer 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.

Related reference
MSI properties on page 48
It is possible to configure MSI installers to adapt with special needs for your environment.

4.3.6 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: WithSecure Elements Agent installer.

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.

4.3.7 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.

4.3.8 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.

Related reference
MSI properties on page 48
It is possible to configure MSI installers to adapt with special needs for your environment.

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.

The device uses the specified profile when it is restored.

4.4 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.

4.4.1 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: the WebContentFilter page

```
<?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: the PrivacyPreferencesPolicyControl.Services page

```
<?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: the NotificationSettingsItem page

```
<?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.

4.5 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.

4.5.1 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.

4.5.2 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`.

4.5.3 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`.

4.6 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.

4.6.1 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.

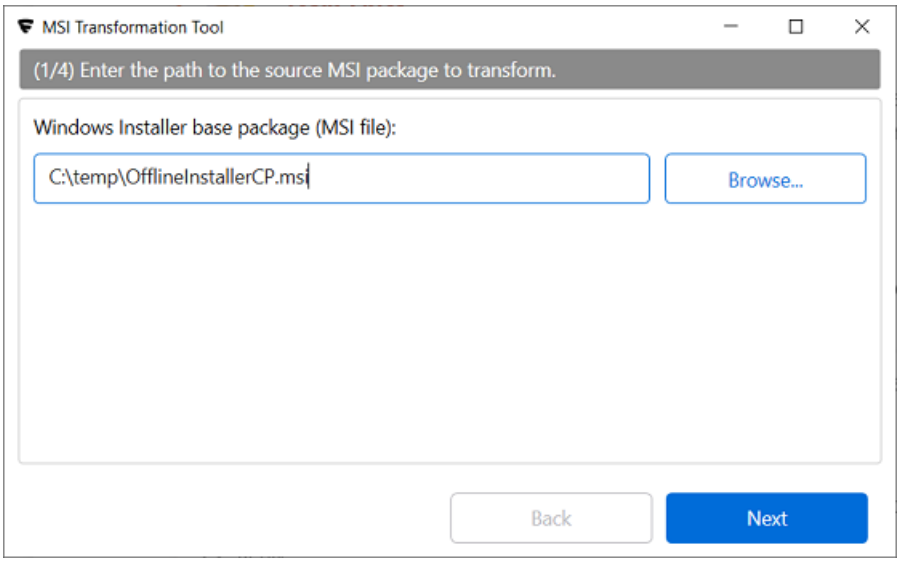
IMPORTANT: MSI files are valid for eight months. If you have downloaded an MSI file more than eight months ago, you need to download a new one.

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

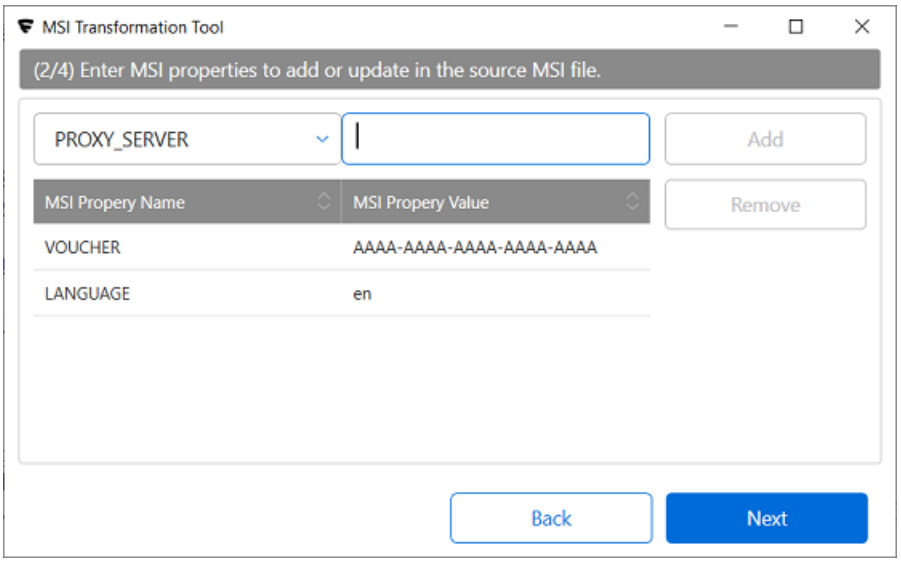
To use the MSI transformation tool:

1. Launch the MSI transformation tool.

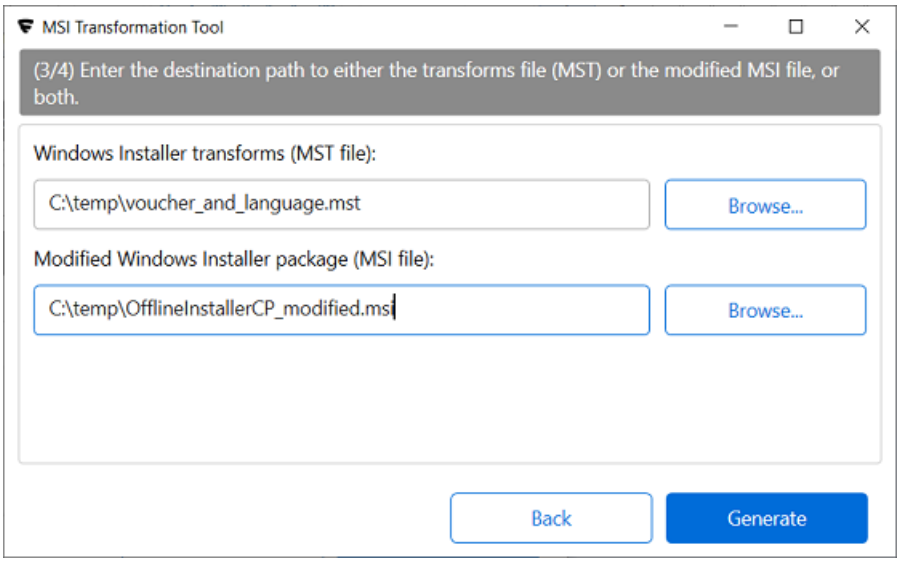
2. On the page that opens, specify the path to the MSI installer for Elements Agent, and select **Next**.



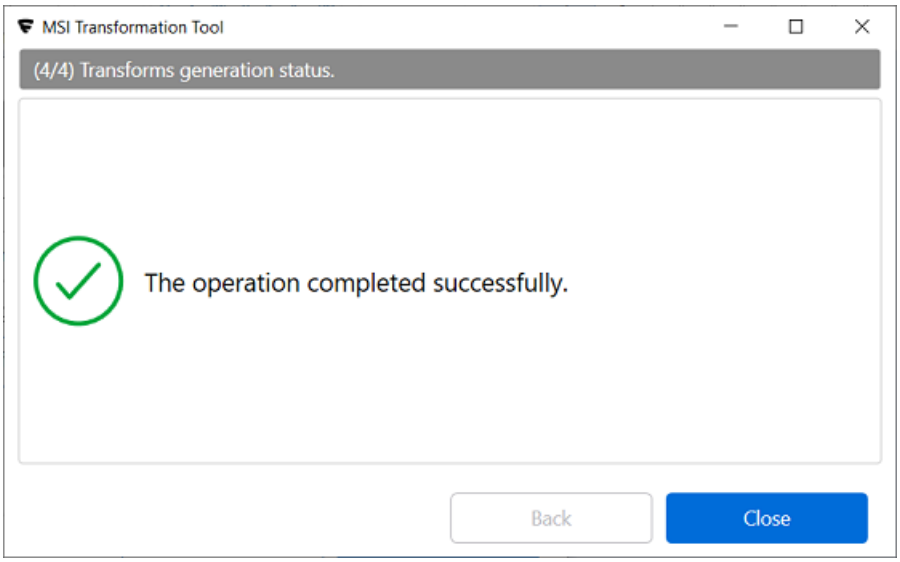
3. Specify one or more MSI properties you want to add, and select **Next**.



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



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



Related reference
MSI properties on page 48
It is possible to configure MSI installers to adapt with special needs for your environment.

4.6.2 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, profile assignment rules 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.

4.6.3 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 5

Using WithSecure Managed Detection and Response

Topics:

- Threat detection
- Incident escalation
- Incident response
- Incident response retainer

Using WithSecure Managed Detection and Response

Overview of threat detection and incident escalation processes for response actions, which align with your organization's security policies and regulatory requirements.

WithSecure Managed Detection and Response safeguards your organization against constantly evolving cyberattacks. It does this by providing continuous monitoring, detection, and rapid incident response.

WithSecure Managed Detection and Response enhances incident response. You can still access a comprehensive view of all Broad Context Detections through WithSecure Elements Security Center. This visibility allows your security team to review and validate detections. It also allows communication with WithSecure Threat Analysts during threat detection and escalation.

5.1 Threat detection

WithSecure Managed Detection and Response identifies and categorizes interconnected security incidents known as Broad Context Detections. Dynamic risk scoring helps the escalation of threat levels as new evidence emerges.

Broad Context Detections are series of interconnected incidents that may appear otherwise independent. They are designed for real-life, orchestrated, polymorphic attacks. They combine risk levels, information about affected hosts, and the current threat landscape to place incidents within a broader context.

When the solution detects a Broad Context Detection, it categorizes the risk as medium, severe, or high. This is based on the likelihood and impact of the security threat. These scores are derived from a variety of factors, including contextual identifiers, anomalies, telemetry patterns, and unusual activities. Risk scores are dynamic. They can escalate as new evidence of malicious activity is discovered. An initially low-risk detection can become high-risk if subsequent analysis reveals more severe threat indicators.

Specialized WithSecure Threat Analysts investigate and review these detections. This ensures an accurate assessment and an appropriate response for each detection.

NOTE: To preserve the integrity of the investigative process, Broad Context Detections in the WithSecure Elements Security Center are viewable but not modifiable. This applies during the initial threat detection phase.

WithSecure Managed Detection and Response provides ongoing updates on the status of Broad Context Detections under investigation. It also identifies detections that WithSecure Threat Analysts have conclusively resolved.

5.1.1 Threat investigation process

WithSecure Threat Analysts will promptly start the investigation process when the service detects potentially risky or unusual activity.

When the threat investigation process starts, WithSecure Threat Analysts conduct a more thorough analysis of the detection.

The Threat Investigation process looks at all Broad Context Detections (BCDs) for the target hosts, using both recent and historical data. This data is collected either automatically by the EDR agent on the host or through specific investigation tasks started by the Threat Analyst to help with the analysis.

The findings of each investigation are categorized as follows:

False positive	Harmless detections are classified as false positives and are not escalated further. Identical Broad Context Detections are automatically disregarded in the future to prevent unnecessary alerts.
Suspicious activity	Some activities may appear suspicious or risky but may have legitimate reasons. Such activities are monitored closely but do not require immediate escalation.
Accepted behavior	Some suspicious or risky activity can be accepted as legitimate behavior in the system.
Confirmed threat	When WithSecure Threat Analysts confirm a genuine threat, the incident status is updated to **Confirmed**. This classification escalates the incident and triggers a response from the designated contact person or group.

5.1.2 View Broad Context Detections

When WithSecure Managed Detection and Response identifies security incidents, they are displayed in the WithSecure Elements Security Center.

Follow these instructions to view Broad Context Detections:

1. In WithSecure Elements Security Center, select **Events** > **Broad Context Detections**

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

2. Choose the Broad Context Detection that you want to investigate from the list.

   The selected Broad Context Detection shows the risk level score, confidence, and criticality of the detection.

NOTE: To preserve the integrity of the investigative process, Broad Context Detections within the WithSecure Elements Security Center are viewable but not modifiable during the initial threat detection phase.

- Go to the **Analysis** tab to review the current analysis of the Broad Context Detection.
- Go to the **Comment** tab view your communication with WithSecure Threat Analysts. Select **Add comment** to add your comments to the Broad Context Detection.

NOTE: You receive an email notification whenever WithSecure Threat Analysts post a new comment to the Broad Context Detection.

5.2 Incident escalation

When analysts confirm a Broad Context Detection as a threat, incident, or suspicious activity, they escalate it based on severity.

For detections that do not require immediate action, WithSecure Threat Analysts add a comment to the Broad Context Detection.

TIP: Enable comment notifications in Elements Security Center to receive alerts when new comments arrive.

If the analysis confirms a threat or highly suspicious activity, WithSecure Threat Analysts notify the designated contacts.

5.2.1 Incident escalation process

When the service detects potentially risky or unusual activity, WithSecure Threat Analysts review the case.

The incident escalation follows this process:

1. When WithSecure Threat Analysts suspect that there is an incident or suspicious activity, an automated email notification is sent to the email addresses that are specified in the WithSecure Elements service settings.

   To view these incidents, in WithSecure Elements Security Center, select **Events** > **Broad Context Detections**, and then choose the Broad Context Detection that you want to investigate from the list. The status of the Broad Context Detection is **Waiting for customer**.

2. If the incident is deemed more serious, WithSecure Threat Analysts contact each of the designated phone numbers in priority order until a designated contact person is reached and alerted to the incident.
3. Communication with WithSecure Threat Analysts is available during the incident through the comments section of the Broad Context Detection in the WithSecure Elements Security Center.

5.3 Incident response

During the escalation of an incident, the WithSecure Threat Analysts start a thorough investigation into the Broad Context Detection. This process involves analyzing the scope and impact of the incident to understand its breadth and potential repercussions.

If authorized to do so, they can start incident containment actions to limit the spread of the threat. Later, they do remediation actions to remove the threat from the affected systems and to restore normal operations.

5.3.1 Supported response actions

WithSecure Threat Analysts employ a suite of incident response actions to conduct the necessary investigation, containment, and remediation processes.

Investigation

Investigation actions are critical for examining the environment and discerning the tactics, techniques, and procedures that the attacker is using. These actions focus on gathering all the possible evidence from endpoint devices to understand what activities have taken place.

Examples:

- Acquiring a forensics package and related system information.
- Securing a memory dump, as well as other vital data such as logs and temporary files.
- Enumerating active processes and services.

Containment

Containment actions are used to protect the network and to stop intruders and their harmful actions. They are used to stop attackers from stealing, altering, or destroying information and to stop the attack from spreading to other parts of the network.

Examples:

- Terminating malicious processes.
- Isolating compromised hosts from the rest of the network.

Remediation

Remediation actions are essential for preventing an attack from spreading and removing any malicious code. These actions cut off the affected part of the network and clean up any traces left by attackers, so preventing further unauthorized access.

Examples:

- Removing malicious files, directories, Windows registry keys and values.
- Eliminating compromised Windows Management Instrumentation (WMI) objects.

NOTE: For the full list of response actions, refer to the WithSecure Elements Endpoint Detection and Response administrator's guide.

5.3.2 Authorized response actions

WithSecure Threat Analysts can act without requesting your approval if you have authorized response actions beforehand, or if you give WithSecure Threat Analysts the permission to do so during the incident response.

Immediate investigation	When a potential threat is detected, WithSecure Threat Analysts promptly begin the investigation without waiting to get your permission. This expedited response entails executing investigation actions - such as retrieving forensic packages and additional relevant data - without the need for immediate approval. This ensures a swift response, mitigating the risk of further damage by the attackers.
Containment and remediation actions	Containment and remediation response actions can be either pre-authorized or explicitly approved. If WithSecure Threat Analysts do not receive an explicit approval and if pre-authorization is not in place, they will not conduct response actions on your behalf before your approval.
Communication	WithSecure Threat Analysts inform designated contact persons or groups about the direct results of any containment or remediation actions they take to handle a security issue. You then have to check how these actions - such as the isolation of a host from the network - may affect the broader system or your network infrastructure.

Pre-authorization

Pre-authorization determines whether WithSecure Threat Analysts can perform manual response actions on your devices and identities without waiting for your approval.

The **Manual actions** pre-authorization setting controls whether WithSecure Threat Analysts need your authorization before they perform a response action on a device or identity.

All actions	WithSecure Threat Analysts can perform any manual response action on the device or identity without requesting your authorization first.
None	WithSecure Threat Analysts can only investigate and offer guidance. For any other response action, they request your explicit approval.

You set the **Manual actions** value as an organization-wide default for each asset type, and you can override the default for individual or selected devices and identities. The organization defaults are:

Workstations	All actions
Servers	None
Users	All actions

Service principals	None

Set the organization default for pre-authorized actions

Set the organization-wide default **Manual actions** pre-authorization value for workstations, servers, users, and service principals.

The organization default determines the **Manual actions** pre-authorization value that applies to a device or identity unless you override it individually. Changing the organization default does not affect a device or identity that already has an individual override.

1. Open WithSecure Elements Security Center.
2. Go to **Management** > **Security services**.
3. On the **MDR for Endpoints** or **MDR for Identities (Entra ID)** card, select **Pre-authorized actions**.
   *The **Pre-authorized actions** page opens, showing the organization default settings.*
4. For each asset type that you want to change, select a **Manual actions** value.

All actions	Gives WithSecure Threat Analysts pre-authorized permission to perform any manual response action without requesting authorization.
None	Permits WithSecure Threat Analysts to only investigate, offer guidance, and request your explicit authorization before performing other response actions.

5. Select **Save**.

The new default applies to every workstation, server, user, or service principal that does not have an individual override.

Override pre-authorization for a device or identity

Override the organization default **Manual actions** pre-authorization value for one or more devices or identities.

Use the **Devices** view to override pre-authorization for workstations and servers, or the **Identities** view to override it for users and service principals. You can select one asset or several at once.

1. Open WithSecure Elements Security Center.
2. Go to **Environment** > **Devices** or **Environment** > **Identities**.
3. Select the checkbox for each device or identity that you want to override.
   *The **Actions** panel opens at the bottom of the page.*
4. Select **Pre-authorized actions**.
5. Under **Manual actions**, select **Override**, then choose the pre-authorization value (**All actions** or **None**) for the selected assets.
6. Select **Ok** on the **Devices** view, or **Update** on the **Identities** view.

The selected devices or identities use the overridden **Manual actions** value instead of the organization default.

Explicit approval

When the **Manual actions** pre-authorization setting is **None**, WithSecure Threat Analysts require your explicit approval for any containment or remediation actions.

You may grant approval over a phone call, ensuring a direct and immediate response. Alternatively, you can provide approval by posting a comment in the Broad Context Detection within the WithSecure Elements Security Center.

This process ensures that critical actions are taken with full awareness and consent, maintaining the integrity and stability of network operations.

5.4 Incident response retainer

When a cyber security incident qualifies as a *Major Incident*, WithSecure Threat Analysts provide further support by activating the Incident Response Retainer.

A *Major Incident* is declared under the following conditions:

- The incident has spread to at least two hosts within the network.
- A business-critical computer or a system that is vital for operational continuity is at risk.
- A host that does not have WithSecure Elements Endpoint Detection and Response protection is compromised by the security threat.

WithSecure Managed Detection and Response solution includes an Incident Response Retainer. This means that you have access to skilled WithSecure Incident Responders. Their goal is to keep your business operating during a major cyber security incident.

NOTE: If you need support beyond the scope of WithSecure Managed Detection and Response solution, we recommend the WithSecure Incident Response Retainer. This support includes extensive business impact assessments, in-depth device investigations outside the service coverage, and evaluations of third-party data (for example, firewalls).

5.4.1 First Response Package

The First Response Package provides support in the first 72 hours after a serious cybersecurity incident.

When Incident Response Retainer is activated, WithSecure Incident Responders provide immediate investigation and containment support. The support includes:

- An initial assessment of the incident's scope in the network.
- An estimate of the work needed to contain and fix the incident.
- A review of available data sources to determine the attack's full scope.
- Advice on containment.
- A root cause analysis to find what caused the incident.
- Other tasks related to preserving evidence, managing the incident, and communicating with stakeholders.

Incident Response Retainer includes one First Response Package: one prepaid day of incident-response work.

Glossary

Access Control

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

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.

Agent

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

Antivirus

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

Backdoor

An undocumented way of gaining access to a computer system.

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.

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.

Cloud Service

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

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.

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.

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).

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.

First Response Package

A predefined support package for immediate assistance during the first 72 hours of a major cybersecurity incident.

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.

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.

Incident Response Retainer

A service that provides pre-arranged access to cybersecurity experts to handle critical security incidents.

Lateral Movement

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

Lightweight Directory Access Protocol (LDAP)

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

Linux Authenticated Scanning

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

Malware

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

Managed Detection and Response (MDR)

Managed Detection and Response is a security service that combines threat monitoring, investigation, and response assistance delivered as an ongoing managed capability.

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.

Patch Management

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

Phishing

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

Privacy

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

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.

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.

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.

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.

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.

Sensor

Software that runs on monitored devices (hosts). The sensor monitors the device status and communicates with Elements Endpoint Detection and Response backend.

Service Partner

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

Severity

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

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.

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.

Tenant

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

Threat Detection

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

Threat Investigation Process

A threat investigation process is the structured analysis of detections and related evidence to determine whether suspicious activity is harmless, suspicious, or a confirmed threat and to guide escalation or response.

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.

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

A

B

C

D

E

F

G

I

J

K

L

M

N

O

P