WITH secure

Elements Endpoint Protection

2026-08-20

Contents

Chapter 1

Introduction to the WithSecure Elements solution

Topics:

- Using WithSecure Elements Security Center

Introduction to the WithSecure Elements solution

Overview of the WithSecure Elements solution and its offering.

WithSecure Elements in a nutshell

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

The WithSecure Elements offering

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

To highlight some of the main benefits:

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

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

Supported languages

The Elements Security Center supports the following languages:

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

Endpoint products support the following languages:

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

WithSecure Elements training

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

Accessing the WithSecure Elements Security Center

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

1.1 Using WithSecure Elements Security Center

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

This chapter describes the following tasks:

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

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

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

1.1.1 Get started with WithSecure Elements Security Center

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

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

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

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

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

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

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

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

1.1.2 Logging in

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

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

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

Log in to non-federated domains

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

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

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

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

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

Log in to federated domains

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

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

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

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

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

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

Multi-factor authentication

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

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

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

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

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

MFA methods

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

The methods include the following:

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

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

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

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

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

Choose multi-factor authentication

Chooses one or more multi-factor authentication methods.

Before you choose a multi-factor authentication method:

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

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

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

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

To choose one or more multi-factor authentication methods:

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

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

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

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

Remove a multi-factor authentication

Removes a multi-factor authentication method.

To remove a multi-factor authentication method:

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

Use device biometrics

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

To use device biometrics, do the following:

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

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

1.1.3 User management

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

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

About access rights

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

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

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

Access rights by role

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

Exposure Management – Exposure

Full editing Allows access to the following Exposure Management features:

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

- Management
- Cloud onboarding

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

Audit logs entry: cspm: admin

Exposure Management - Vulnerabilities

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

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

Audit logs entry: vm: administrator

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

Audit logs entry: vm: team_member

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

Audit logs entry: vm: readonly_team_member

Collaboration Protection

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

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

Audit logs entry: cpo365:admin

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

Audit logs entry: cpo: readonly

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

Audit logs entry: cpo365:quarantine_mgr

Collaboration Protection - Management

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

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

Audit logs entry: fusion_admin

Endpoint Protection

No access No access to Endpoint protection features including:

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

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

Endpoint Protection - Computers and mobiles

Full editing Allows the access to the following features:

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

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

Audit logs entry: epp: manage_computers_mobiles_only

or epp: manage_all

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

Audit logs entry: epp: manage_servers_only

or epp: readonly

Endpoint Protection - Servers

Full editing Allows the access to the following features:

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

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

Audit logs entry: epp: manage_servers_only

or epp_manage_all

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

Audit logs entry: epp: manage_computers_mobiles_only

epp: readonly

Extended Detection and Response - Toggle off

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

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

Extended Detection and Response - Broad Context Detections

Full editing Permission to manage:

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

Limited access to:

- Devices view
- Cloud view
- Subscription view

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

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

Audit logs entry: elements:xdr-incident-full

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

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-incident-read

Extended Detection and Response – Response

Execute responses Access to execute:

- response actions
- configure Automated actions

Limited access to Cloud view.

Audit logs entry: elements:xdr-response-full

List responses Access to review:

- executed response actions
- respective results available

Limited access to:

- Devices view
- Cloud view

Download response results requires the Execute Responses permission.

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-response-read

No access No access to execute or review:

- Response actions
- Automated actions

Extended Detection and Response – Event Search

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-event-search

No access No access to review event data.

Elements Administration

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

Move between the managed companies

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

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

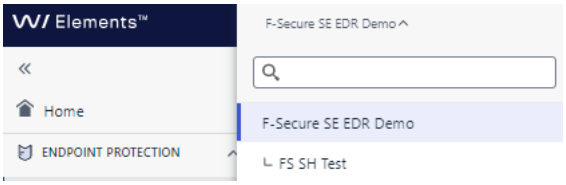
- Solution Providers (SoPs) manage Service Partners and groups of companies. They can access Elements Security Center to manage security and subscriptions for their directly managed companies, their Service Partners, and their Service Partners' companies.
- Service Partners (SePs) manage a group of companies.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

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

1. Select the

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

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

Elements Identity and Access Management (IAM) role

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

Overview

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

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

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

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

Benefits

The IAM role provides several benefits, including the following:

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

Claiming the IAM role

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

Elements IAM role properties

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

IAM administrators can do the following:

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

Acquiring the IAM role

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

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

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

Migration of IAM permissions

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

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

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

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

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

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

When IAM administrator candidate cannot be identified

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

Frequently asked questions about IAM roles

Answers to frequently asked questions about IAM roles.

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

Add a new administrator

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

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

To create an administrator account:

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

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

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

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

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

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

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

A new administrator account is created.

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

Add a new service partner

To create a service partner account:

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

The service partner account is created.

Edit or remove administrators

You can edit or remove administrators accounts.

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

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

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

The administrator account is deleted.

Create an API client

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

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

To create an API client:

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

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

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

A new API client is created.

Delete an API client

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

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

To delete an API client:

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

Recover your password

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

To recover your password:

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

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

Change your account details

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

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

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

To change your user name:

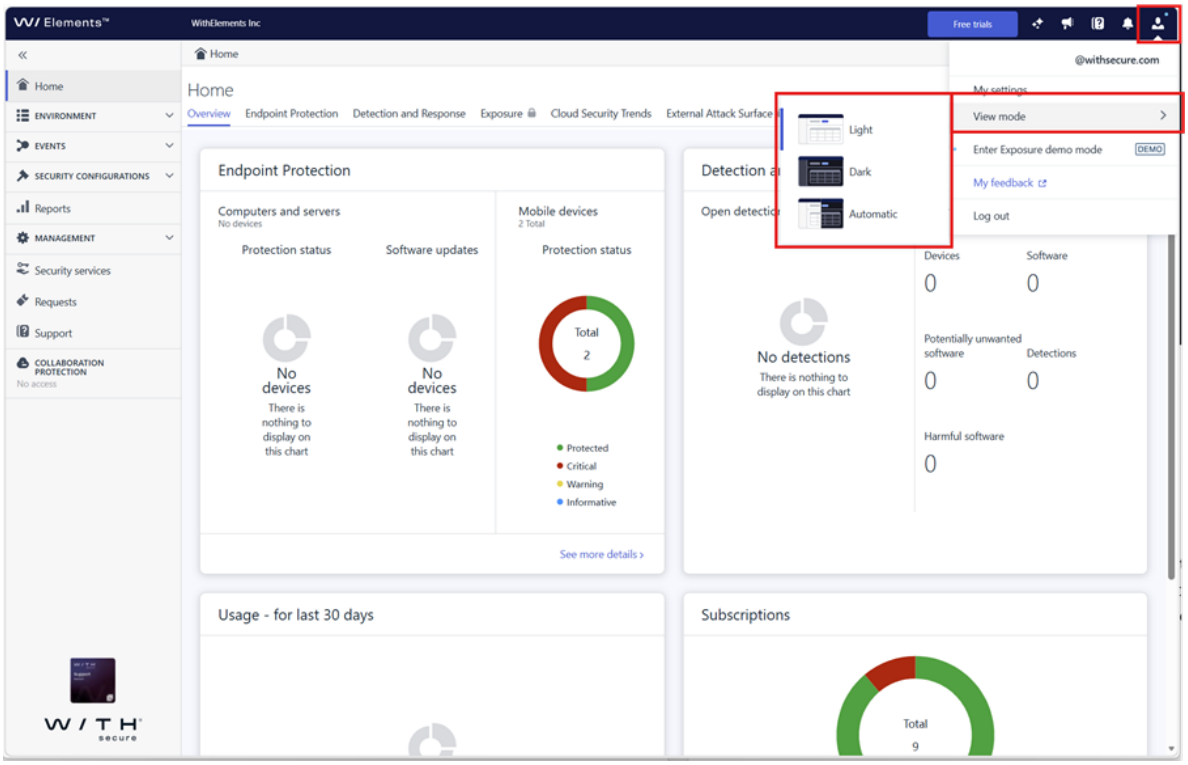
1. Select
   
   at the top-right corner, then select **My settings**.
2. Under **Details**, enter a new user name.
3. Select **Save**.

1.1.4 Change the view mode

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

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

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



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

1.1.5 Taking Elements products into use

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

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

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

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

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

Adding a customer company

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

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

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

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

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

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

Assign a subscription key for a customer company

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

You need to consider the following:

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

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

To assign a subscription key:

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

The new subscription key is added to the company account.

Order products for an existing customer company

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

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

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

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

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

*The **eOrdering** page is displayed.*

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

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

Order products for a new customer company

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

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

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

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

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

*The **eOrdering** page is displayed.*

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

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

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

View available product subscriptions

To view the available subscriptions:

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

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

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

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

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

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

Change the subscription key

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

To change the subscription key:

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

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

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

   The new subscription key is applied to the selected devices.

Upgrading your subscriptions

Options for upgrading your WithSecure Elements subscriptions.

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

Upgrading your subscriptions

You can upgrade your subscription in two ways:

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

You have the following options in upgrading your subscriptions:

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

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

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

1.1.6 Federated single sign-on

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

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

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

Prerequisites

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

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

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

Before implementing single sign-on (SSO)

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

Why is plus addressing problematic?

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

IMPORTANT:

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

How to avoid users losing access to remove federation?

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

How does SSO change the login process?

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

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

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

Global impact of SSO

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

Hierarchy-level considerations

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

Handling Microsoft Entra ID account removal

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

Set up federated single sign-on with Microsoft Entra ID

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

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

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

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

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

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

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

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

Link user identities

Links user identities in Elements Security Center for federated domains.

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

Make sure you have the following:

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

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

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

To link identities:

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

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

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

Remove federation from a domain

Removes single sign-on federation from a domain.

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

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

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

To remove federation:

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

1.1.7 Adding devices for management

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

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

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

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

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

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

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

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

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

Distributing WithSecure software

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

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

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

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

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

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

    NOTE: With all the Elements software (except for the Elements Connector), you can add devices by selecting the **Add new device** option and then choosing to send either one invitation or importing data from a CSV file to send multiple invitations.
  - By sending an installation email via a third-party MDM software.
- For installing WithSecure Elements Connector, see instructions at here.

Send an installation link via email

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

NOTE: The installation link is valid for 30 days.

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

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

1. Under **Environment**, select **Devices** on the sidebar.

   The **Add new device** option next to **Devices** is visible only at a company level. If the *scope selector* is set to show all customer companies, select the company you wish to manage.

   *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 **Add new device** option next to **Devices** is visible only at a company level. If the *scope selector* is set to show all customer companies, select the company you wish to manage.

   *The **Devices** page is displayed.*
2. Select

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

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

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

1.1.8 Enhancing device management with custom labels

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

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

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

Add device labels

You can add device labels in three different ways.

You can add device labels in the following ways.

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

Add device labels in one of the following ways:

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

1.1.9 Managing devices in Elements Security Center

How to manage the selected devices in WithSecure Elements Security Center

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

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

Managing asset groups

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

You can assign devices to asset groups in two ways:

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

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

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

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

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

Create asset groups

Creates an asset group at the company level.

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

1. Under **Management**, select **Organization Settings** > **General**.
2. Select **Create asset group**.
   *The **Create asset group** pane opens.*
3. Enter a name for the asset group.
4. (Optional) In the **Description** box, enter a description for the asset group.
5. Select **Save**.

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

Add devices to asset groups

Adds devices to one or more asset groups.

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

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

Remotely manage a device

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

To remotely manage a device:

1. Under **Environment**, select **Devices** on the sidebar.

   The **Add new device** option next to **Devices** is visible only at a company level. If the *scope selector* is set to show all customer companies, select the company you wish to manage.

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

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

   The instruction is sent to the selected device.

Automatically delete devices

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

NOTE: This feature does not apply to mobile devices.

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

To manage automatic deletion:

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

   NOTE: The minimum number of days is seven (7).
6. Select **Save**.

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

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

View devices based on the Active Directory structure

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

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

To view devices based on the Active Directory structure:

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

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

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

   NOTE: The Active Directory structure is built based on the data that is reported by company computers, so it may not be complete. A new Active Directory domain does not show in

> WithSecure Elements Security Center until WithSecure Elements EPP for Computers or WithSecure Elements EPP for Servers is activated in the computers in that domain.

Customize the Devices view

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

To customize the Devices view:

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

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

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

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

Request diagnostic data

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

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

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

To request diagnostic data:

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

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

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

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

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

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

1.1.10 Elements data recovery

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

No actions are required from you.

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

Chapter 2

Elements Endpoint Protection overview

Topics:

- Get started with WithSecure Elements EPP

Elements Endpoint Protection overview

WithSecure Elements provides security from computer and mobile endpoints to email and server levels.

With WithSecure Elements, you can easily install and manage Elements EPP, Elements Endpoint Detection and Response, and Elements Vulnerability agents.

Endpoint Protection comprises the following products:

- The **WithSecure Elements EPP for Computers** software offers protection for all Windows and Mac desktop computers.
- **WithSecure Elements EPP for Servers** is a security solution for Windows and Linux servers. The new WithSecure Elements EPP for Servers offers the most powerful protection for Windows Servers with the latest tools available.

NOTE: All server products can be used with the same subscription key. The subscription name for all server products is changed from Server Security to WithSecure Elements EPP for Servers to reflect the change.

NOTE: Both WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers use the same installer. They include a Premium version that incorporates additional ransomware protection with DataGuard and application-specific restrictions via Application Control.

- **WithSecure Linux Security** is a security solution for Linux servers.
- **WithSecure Elements Vulnerability Management** - is a vulnerability management solution that allows you to run network discovery and port scans, platform and service vulnerability scans, and web application scans.
- **WithSecure Elements Mobile Protection** offers proactive, full-coverage protection for Android and iOS devices. It fights off phishing attempts, prevents you from visiting harmful websites, blocks malware, detects potential vulnerabilities, and keeps your network traffic private when you connect to insecure networks like public WiFi.

WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers have many advanced features, for example:

- Software Updater - reduces threats by keeping the operating system and third-party software updated.
- DeepGuard - using its sophisticated technology, DeepGuard relies on heuristic, behavior, and reputation analysis to provide an exceptionally important layer of security.
- Device Control (WithSecure Elements EPP for Computers only) - prevents threats from accessing your system via hardware devices, such as USB sticks, CD-ROM drives, and web cameras. It also prevents data leakage, for example, by allowing read-only access.

WithSecure Elements Mobile Protection offers many advanced features, such as Network Gateway, protection against dangerous content, and more. Its 'Ultralight' technology ensures the impact on battery consumption and performance is minimal. You can use it with external MDM system, such as VMware Workspace ONE, IBM Security MaaS360, Ivanti Endpoint Management, and Microsoft Intune.

NOTE: For more information on using MDMs, see Elements Mobile Protection.

2.1 Get started with WithSecure Elements EPP

Gets started with WithSecure Elements Security Center by adding devices, creating an administrator account, and creating a profile.

You need a WithSecure Business Account to access WithSecure Elements Security Center, which is the unified management platform for managing all WithSecure Elements products. There are two scenarios:

- 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.

  TIP: If you have not received the email message, check your junk mail folder first.

- 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 https://elements.withsecure.com/self-register

This quick start guide walks you through getting started with WithSecure Elements in the Elements Security Center.

1. Use the Business Account credentials to log in to WithSecure Elements Security Center at https://elements.withsecure.com/
2. Add devices to your organization by sending an email invitation to install the product, or by downloading the installer for automated deployment.
3. Create an administrator account and fill in the administrator details.
4. Create your own profile, tailored to the specific security needs of your organization.
5. Assign the profile to devices.

Chapter 3

System requirements

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
`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

Service address	Protocol	Port	Region	Purpose
ew1-famp-prd-system-transfer.s3.ap-northeast-1.amazonaws.com	HTTPS	443	APAC	Response servers

Chapter 4
Deployment

Topics:

- Deployment methods for Windows
- Deployment methods for Mac devices
- Deployment methods for Linux devices
- Deployment methods for mobile devices
- Invite users by email

Deployment

The most common deployment methods and tools for installing WithSecure Elements software.

There is an ever-increasing number of different methods and tools for installing software on devices. Protecting your endpoint devices generally requires that WithSecure Elements Agent is installed and activated on your devices.

You can download the WithSecure Elements Agent installer for the WithSecure Computer Protection and WithSecure Server Protection software under **Management** > **Downloads** in WithSecure Elements Security Center.

NOTE: You cannot download the software package for WithSecure Elements Mobile Protection from Elements Security Center as it is deployed through the App Store (iOS) or Google Play (Android). Once you have downloaded the installer for the desired WithSecure Elements Endpoint Protection software and transferred it to the device to be protected, you can proceed to install it.

4.1 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.

4.1.1 Deploy manually using an EXE file

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

NOTE: Users must have administrator rights on the device.

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

To install the product:

1. Log in to WithSecure Elements Security Center.

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

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

   NOTE: The EXE file includes the subscription key.

*The **Download installer** page opens.*

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

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

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

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

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

Command-line parameters

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

Using parameters with .exe files

With .exe files this means adding the parameter as a command line argument, for example you can pass a subscription key as an argument to the installer and avoid the user having to enter it during installation in the following way:

```
installer.exe --voucher aaaa-bbbb-cccc-dddd-eeee --language en
```

For some exe parameters, both long (--language) and short options (-l) are available.

When installing the product using an `.exe` file, you can use the following command-line parameters:

--profile-id <id>	Sets the desired profile ID value. For example: `--profile-id 18062053`. 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 <id> **-l <id>**	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. For example: `C:\Users\<username>\\Downloads>installer.exe --language en`
--silent -s	Sets the silent installation flow. There are no dialogs for the user. EULT is assumed to be accepted. If there is an embedded keycode, it is automatically used by the software when it is installed. Otherwise, the software is left without a keycode (that is, in an expired initial state). If the installation requires restarting the computer, no dialog is shown about it, but the executable return code is 99 and it will automatically continue after the restart.

--voucher <subscription key> Sets the subscription key. The subscription key is handled as if it was embedded in the installer filename. If a subscription key exists in the filename and is also added to the command-line, the command-line overrides the filename subscription key. For example: `--voucher aaaa-bbbb-cccc-dddd-eeee`

--proxy <url> All requests are sent through this proxy when products are installed. Example: `--proxy http://proxy.local:3128`

--skip-sidegrade <skip options> EXE parameter: Allows you to specify a list of competitor products that should not be sidegraded during the installation. "*" skips all sidegrades.

You can also add [skip-reboot] before a conflict name to indicate that this sidegrade must not require restart (but will be sidegraded). Separate the values (sidegrade ID's or names) by "|":

- --skip-sidegrade "Sophos Cloud Endpoint|HitmanPro.Alert"
- --skip-sidegrade "HitmanPro.Alert|SG16|SG1"
- --skip-sidegrade "*" - do not sidegrade anything (including WithSecure products)
- --skip-sidegrade "[skip-reboot]*" - all conflicts are removed and restart is not required
- --skip-sidegrade "[skip-reboot]Sophos Cloud Endpoint|SG1" - Sophos Cloud Endpoint is uninstalled without a restart and SG1 is not detected as a conflict

--installation-tags <tags> Installation tags to be reported to a back-end portal (WithSecure Elements Endpoint Protection, WithSecure Elements Endpoint Detection and Response, WithSecure Elements Vulnerability Management), for example: `--installation-tags PSB=psb-tag1:psb-tag2:psb-tag3,RADAR=radar-tag1:radar-tag2:radar-tag3,department=accounting,role=secretary`

Currently, WithSecure Elements Security Center stores these tags from PSB=psb-tag1:psb-tag2:psb-tag3 to the "label" field as comma separated values. The maximum length of string is up to 255 characters. These tags cannot contain commas or colons.

--use_smbios_guid 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.

--use_ad_guid 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	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.
--skip-dotnet	Avoid installing .NET during installations. To handle .NET yourself, under Profiles > General settings > Automatic updates, turn off **Allow client to manage .NET** during product updates.
--connector-proxy <url>	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.

Commands for uninstalling the product

When uninstalling the product through Command Prompt, you may use the following command-line commands.

Uninstallation commands

IMPORTANT: You must turn off Tamper Protection before uninstalling the product, as it blocks all uninstallation attempts.

Table 2: Uninstall command examples

Exe file	Exe parameter	Explanation
fs_uninstall_32.exe	*[--silent]*	For `fs_uninstall_32.exe`, navigate to `C:\Program Files\F-Secure\PSB` directory or `C:\Program Files (x86)\F-Secure\PSB`. For silent mode, you can use the `--silent` parameter.

Exe file	Exe parameter	Explanation
msiexec	*/x {PRODUCT_CODE} [/qn]*	To find the product code, enter the following command in the PowerShell command line: `get-wmiobject Win32_Product | Format-Table IdentifyingNumber, Name`. For silent mode, you can use the `/qn` parameter.

NOTE: Optional parameters are in [square brackets].

4.1.2 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.

NOTE: To handle special cases with your installation, that is, how to pass parameters to the installer from the command line, see MSI properties on page 53.

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.

   For instructions on embedding properties to the MSI file, see MSI properties on page 53

   .

   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 55.

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.

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.

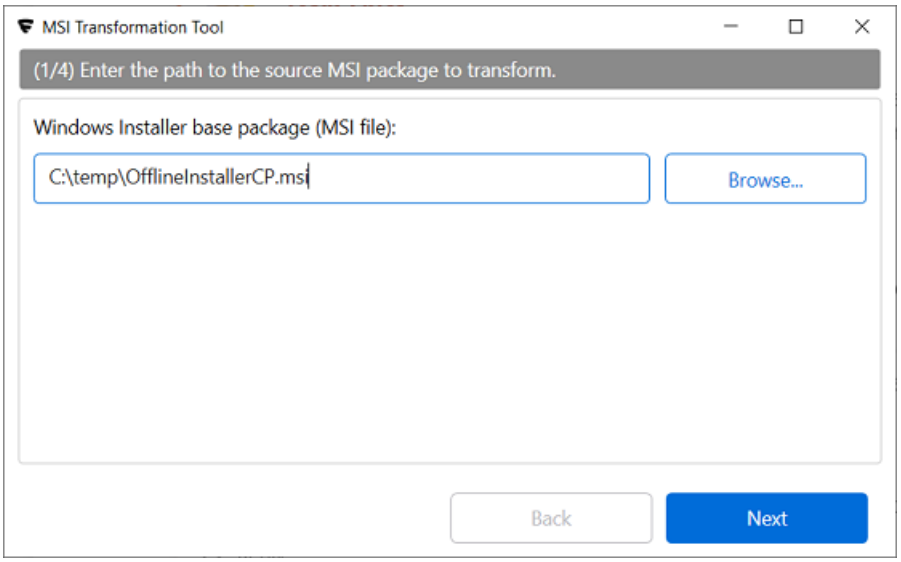
  IMPORTANT: MSI files are valid for eight months. If you have downloaded an MSI file more than eight months ago, you need to download a new one.

- Download the WithSecure MSI transformation tool (FsMsiTool_ui.exe) from the WithSecure download site.
- Get to know the available options in MSI properties on page 53.

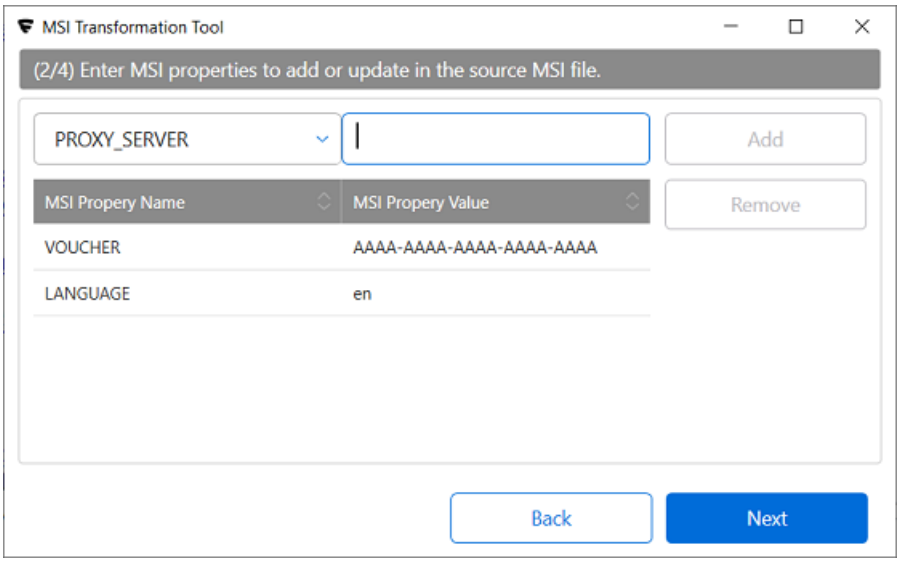
To use the MSI transformation tool:

1. Launch the MSI transformation tool.

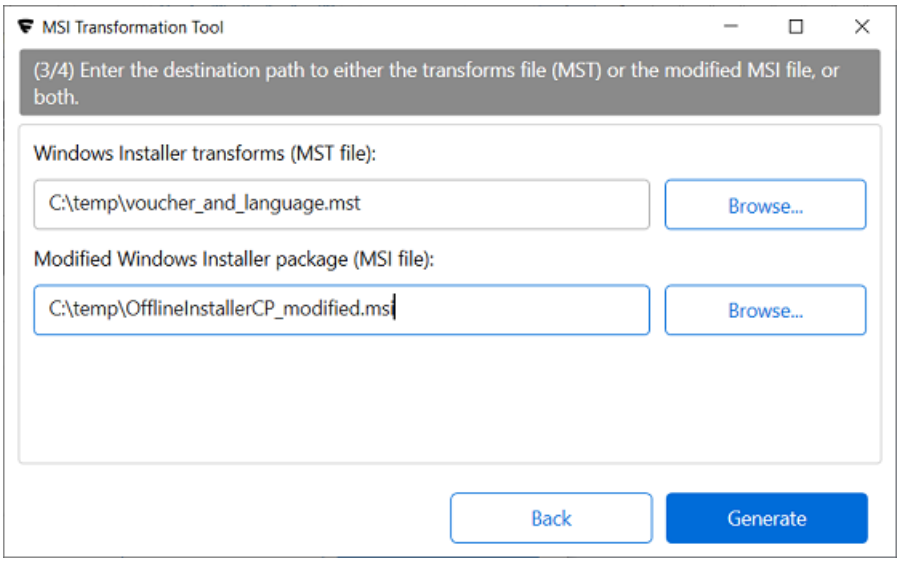
2. On the page that opens, specify the path to the MSI installer for Elements Agent, and select **Next**.



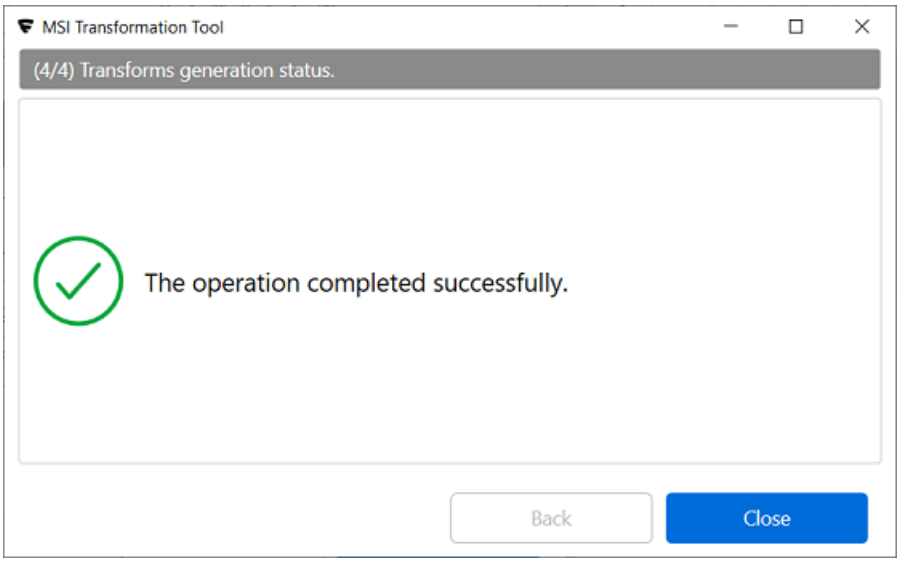
3. Specify one or more MSI properties you want to add, and select **Next**.



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



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



Related reference
Command-line parameters on page 49
It is possible to configure .exe installers to adapt with special needs for your environment.

4.1.3 Deploy via Active Directory GPO

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

For the installation, you need the following:

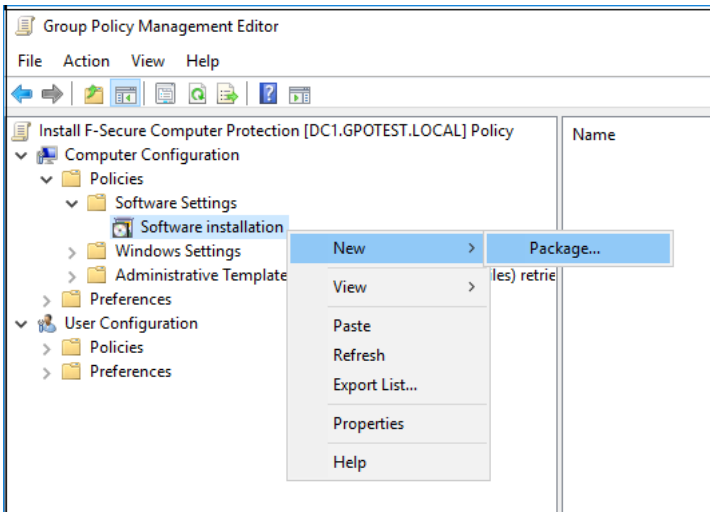
- An Active Directory environment.
- All target domain members need to have a Universal CRT installed. Normally, it comes with Windows updates and is present on regularly updated systems. If the installation fails to detect it, a corresponding error message is issued to the Windows Event Log of the target system. If you need to install or repair it manually, use this link: https://aka.ms/vs/16/release/vc_redist.x86.exe.
- All target domain members need to have a .NET Framework 4.7.2 installed for all the UI features to work properly.
- A customized MSI or MST file (recommended) that is prepared according to the instructions in Use the WithSecure MSI transformation tool on page 55. 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.

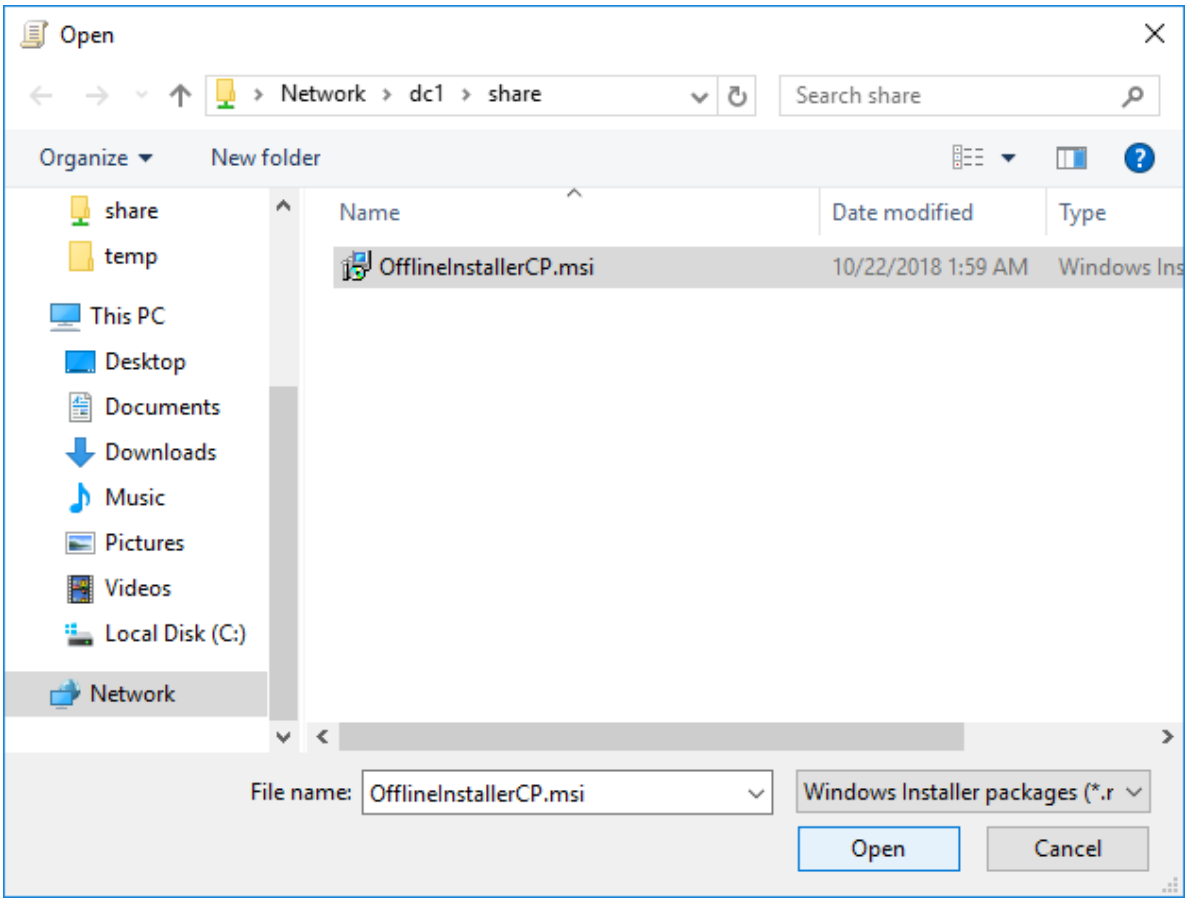
To install the product:

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**.

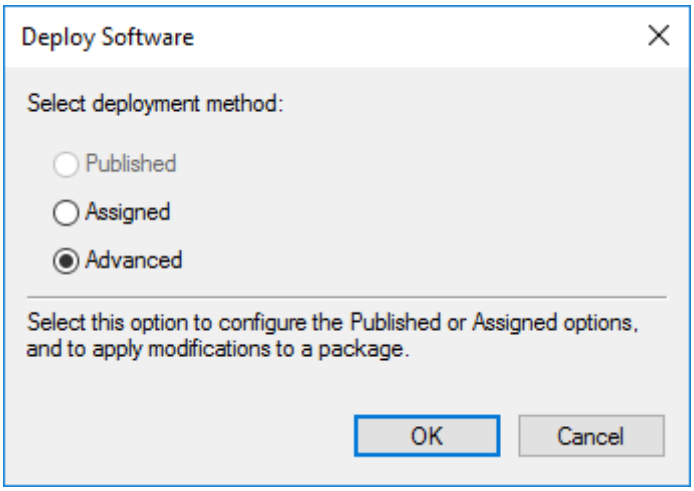
4. Right-click the right pane and select **New** > **Package...**.



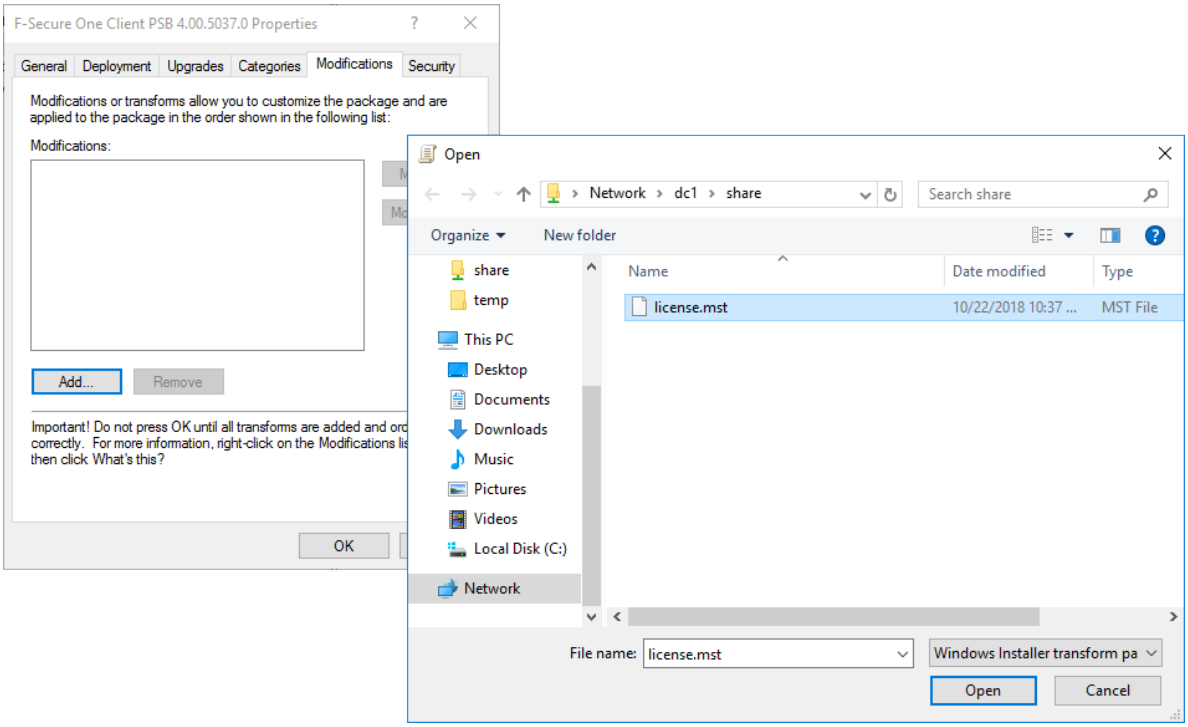
5. In the open file window, select `OfflineInstallerCP.msi` and then select **Open**.



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

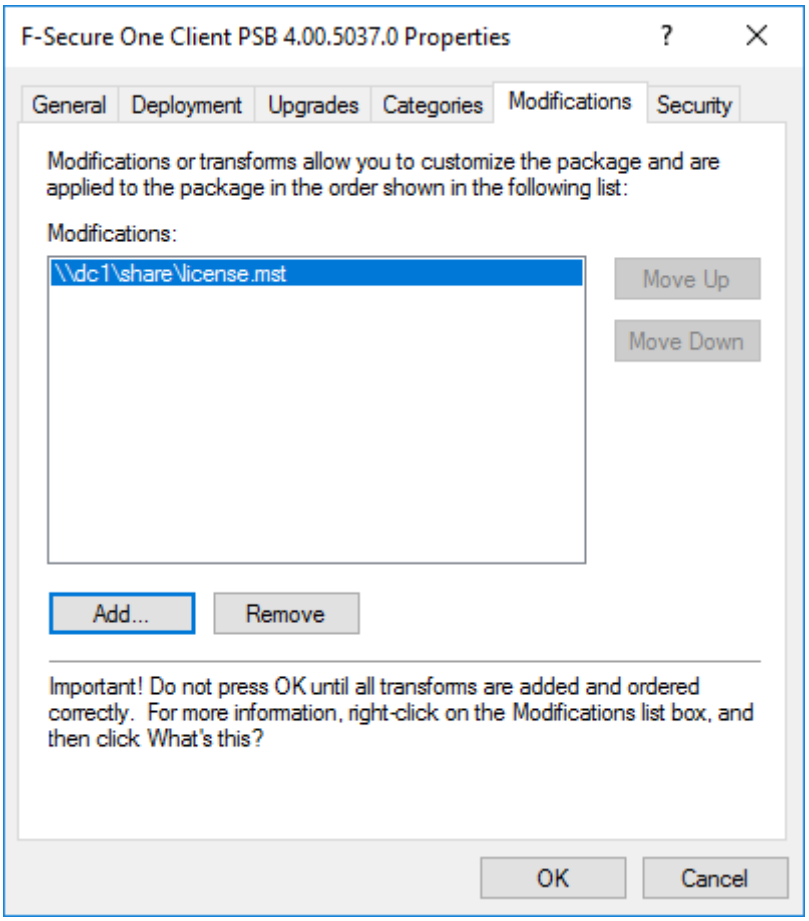


7. Go to the **Modifications** tab, and then select **Add...**.
8. In the open file window, select `license.mst` (the transform file from `FsMsiTool.exe` earlier), and then select **Open**. This adds the transform file path to the GPO settings.



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.

4.1.4 Deploying Elements Agent with Microsoft Configuration Manager

This deployment method is suitable for companies that use Microsoft Configuration Manager (SCCM/MECM) and want to distribute the WithSecure Elements Agent to managed Windows devices.

You can deploy the WithSecure Elements Agent MSI to managed Windows devices as a Configuration Manager application. The deployment procedure covers only the settings that are specific to this product.

NOTE: For general guidance on creating and deploying applications in Configuration Manager, refer to the Microsoft documentation.

The Configuration Manager deployment approach lets you control installation timing and target scope through your existing software distribution infrastructure. Once deployed, Configuration Manager can report on installation status across your device inventory.

IMPORTANT: The installer package must remain in the Configuration Manager client cache after installation. This is required for automatic updates of the WithSecure Elements Agent and for correct integration with Configuration Manager.

Deploy Elements Agent using Microsoft Configuration Manager

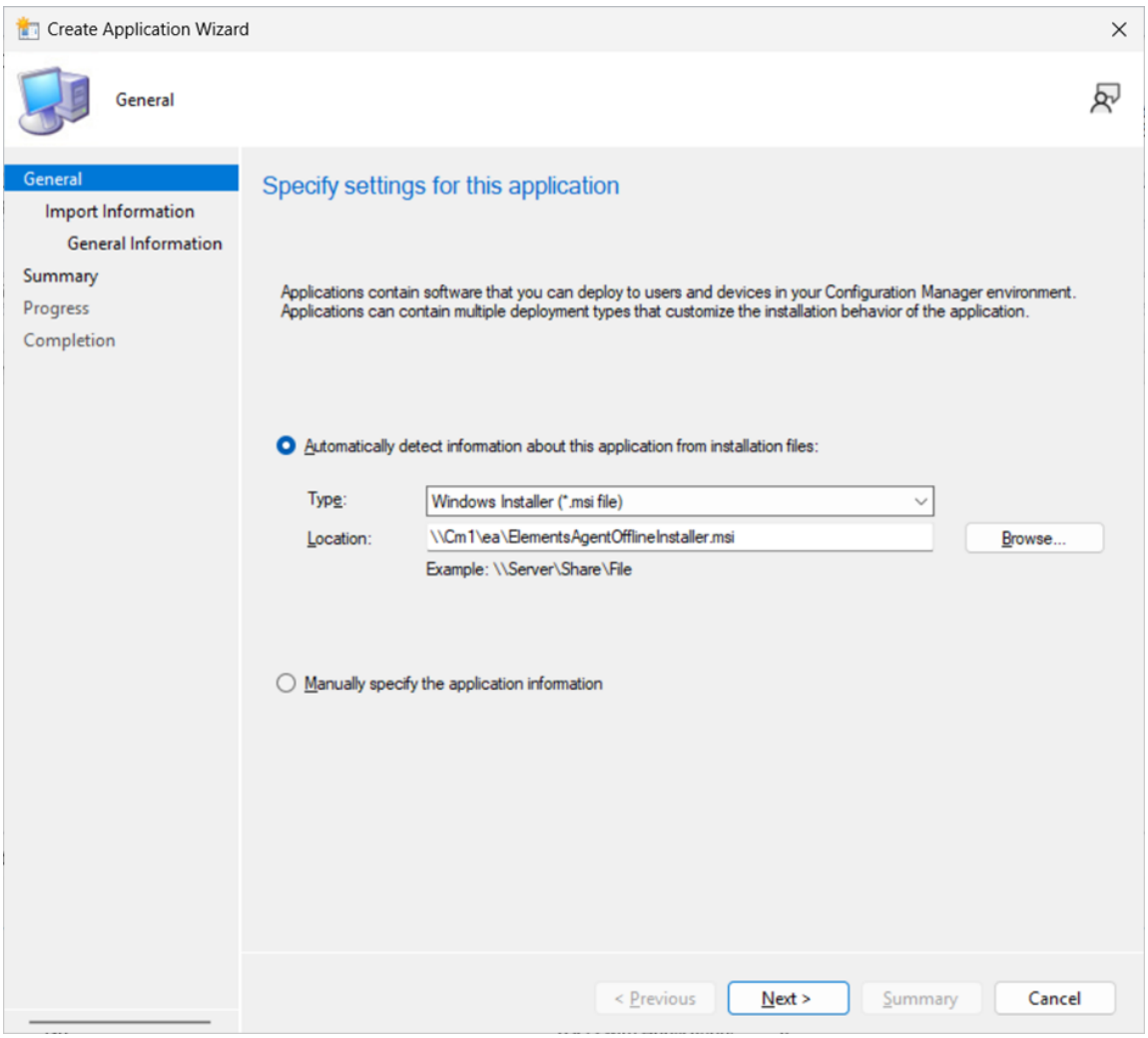
You can create a Configuration Manager application to deploy the WithSecure Elements Agent MSI to managed Windows devices.

- Download the Elements Agent installer (.msi) from WithSecure Elements Security Center and copy it to a network share that is accessible by the Configuration Manager site server.
- Save your subscription key somewhere easy to find - you will need it when you run the installation command.

> **NOTE:** The steps below cover only the settings that are specific to this product. For general guidance on creating and deploying applications in Configuration Manager, refer to the Microsoft documentation.

To create the application in Configuration Manager:

1. In the Configuration Manager console, start the **Create Application Wizard** and select **Windows Installer (*.msi file)** as the deployment type.
2. On the **General** page, configure the following settings:
   a) Set **Detection method** to **Automatically detect information about this application from installation files**.
   b) Set **Location** to the path of the `ElementsAgentOfflineInstaller.msi` on the network share.



3. On the **General Information** page, configure the following settings:

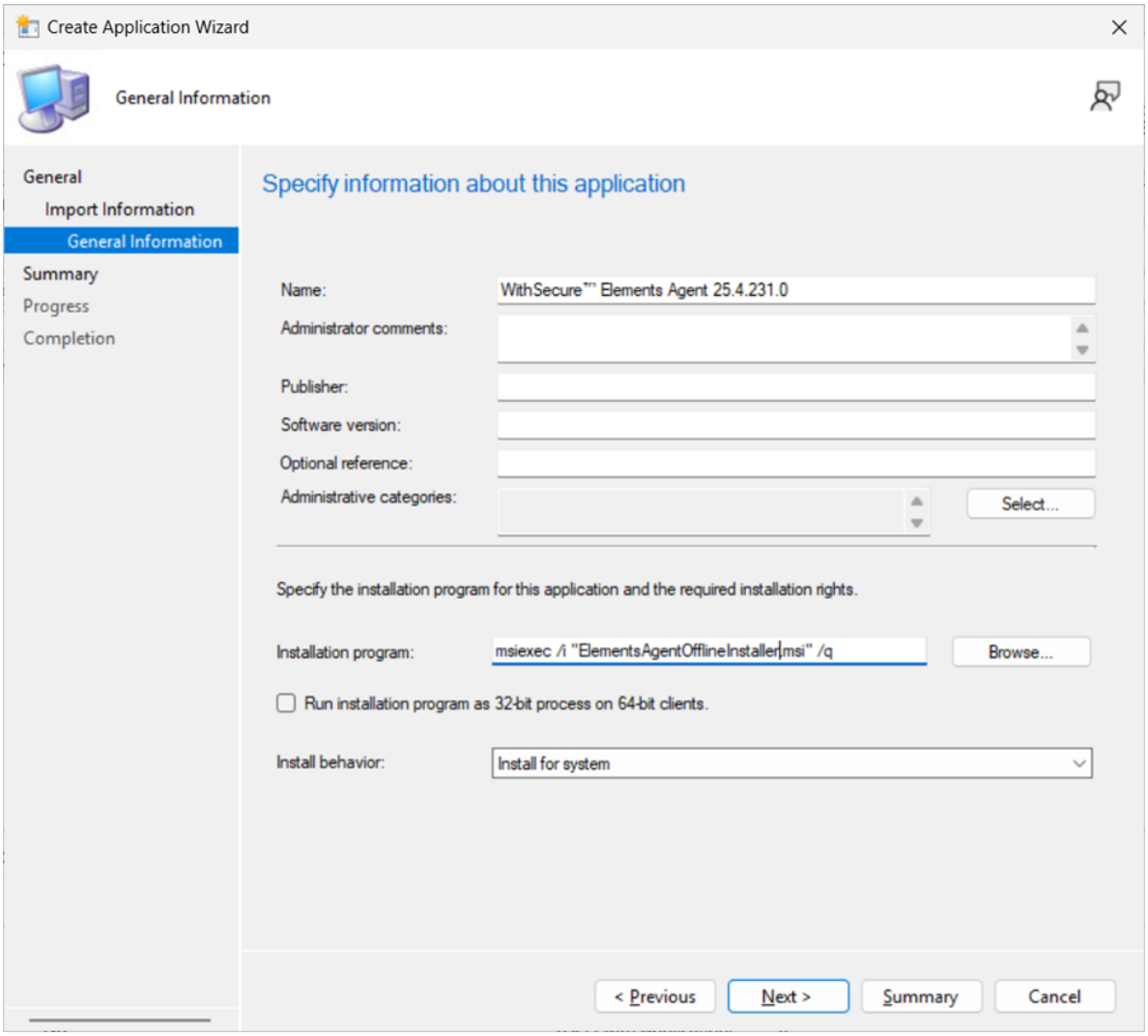
a) Set **Installation program** to the following command:

```
msiexec /i "ElementsAgentOfflineInstaller.msi" /qn VOUCHER="<your-key>"
```

NOTE: Replace `<your-key>` with the subscription key from Elements Security Center. The `/qn` switch suppresses all UI during installation. You can specify other supported MSI properties in this command line.

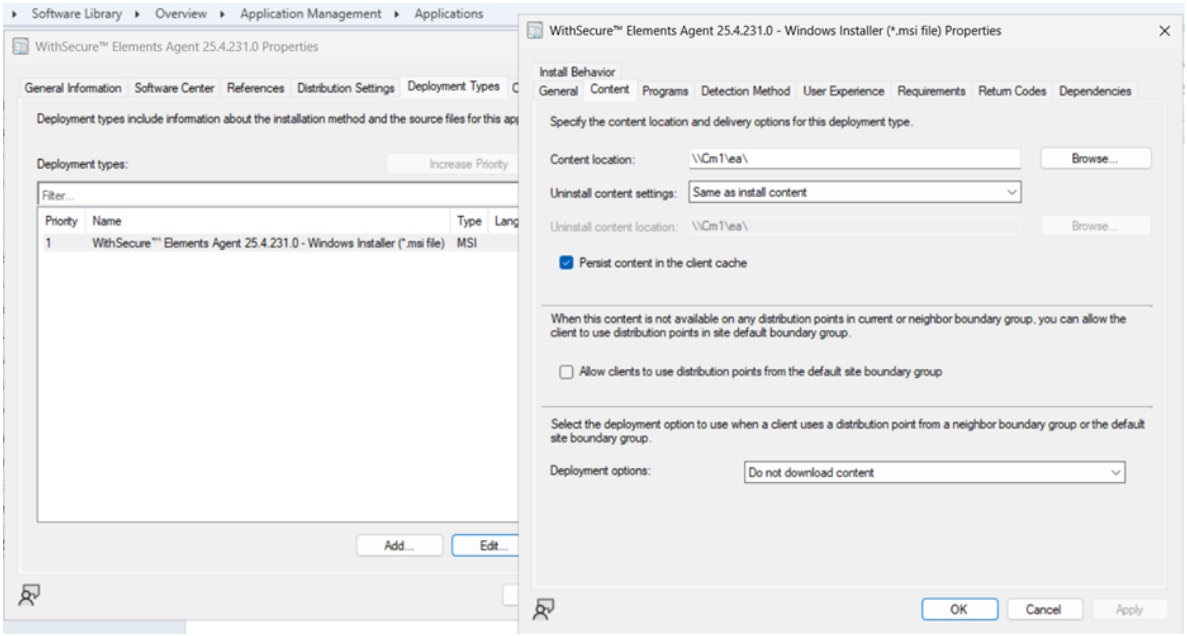
b) Set **Run installation program as 32-bit process on 64-bit clients** to **No**.

c) Set **Install behavior** to **Install for system**.



4. Complete the wizard to create the application.

5. Open the **Deployment Type** settings, go to the **Content** tab, and enable **Persist content in the client cache**.



IMPORTANT: Enabling **Persist content in the client cache** prevents Configuration Manager from removing the installer package from the client cache after installation. The presence of the installer in the local client cache is required for smooth automatic updates of the WithSecure Elements Agent and correct integration with Configuration Manager.

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

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

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

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

To install the product via Microsoft Intune:

1. Log in to the Microsoft Intune portal.
2. Select **Apps** > **All apps** > **Add**.
   *The **Select App type** pane opens.*
3. Under **Other** app types, select **Line-of-business app** > **Select**.
   *A page opens showing the **Add App** steps.*
4. In the **Add App** page, select **Select app package file**.
5. In the **App package file** pane, select the browse icon and select the MSI installer package that you downloaded earlier.
6. Select **OK** to add the app.

7. In the **App information** page, do the following:
   a) Next to **Ignore app version**, select **Yes** to make sure that Microsoft Intune will handle automatic upgrades correctly.
   b) Enter the details, such as the Publisher (WithSecure) and the command-line arguments for your app, for example, `VOUCHER=xxxx-xxxx-xxxx-xxxx-xxxx` (insert your subscription key).

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

   NOTE: You can find all the supported MSI properties.

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

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

4.1.6 Prepare the installer package for Intune

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

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

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

To prepare the installer package for Intune:

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

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

It creates a package called `ElementsAgentInstaller.intunewin`.

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

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

4.1.7 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.

4.1.8 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.

NOTE: If you want to use the MSI offline installer, you can use it with the UNIQUE_SIGNUP_ID=smbios or UNIQUE_SIGNUP_ID=adguid parameter. For more information, see MSI properties on page 53.

- The subscription key for the target company where the image is going to be used.

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

Prepare a golden image

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

To prepare a golden image:

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

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

NOTE: Alternatively, you can use `--use_ad_guid` instead of `--use_smbios_guid` to associate the device with Active Directory Computer GUID. You can also use other command line parameters that you can find in Deploy manually using an EXE file on page 48 and Deploy manually using an MSI file on page 52.

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.

IMPORTANT: Next, you must deploy a server from the golden image following the instructions in Deploy a server from the golden image on page 67.

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.

4.1.9 Setting up Browsing Protection via GPO

Sets up WithSecure Browsing Protection in Google Chrome, Microsoft Edge, and Mozilla Firefox using Windows Group Policies.

NOTE: These instructions are specific to Elements Endpoint Protection and for administrator users.

WithSecure Browsing Protection is a feature for web browsers. It provides support for secure connections (HTTPS) for the installed WithSecure security product.

NOTE: Support for non-secure connections (HTTP) is available without this feature.

This feature allows WithSecure to block unwanted web content, display rating icons, and enable SafeSearch mode for search engines when a secure connection is used. As an administrator, you can activate WithSecure Browsing Protection and enforce its use with Windows Group Policies.

Install the WithSecure browsing protection extension in Google Chrome

These instructions are Elements Endpoint Protection specific and intended for administrator users.

To install and turn on the browsing protection extension:

1. Download the latest Google Chrome group policy template ADMX files.

2. Copy the following Chrome administrative template files and the language folder of the language that is used in your system to the `C:\Windows\PolicyDefinitions` directory:

   `policy_templates/windows/admx/chrome.admx and google.admx`

3. Copy the files and the the language folder of the language that is used in your system also to your SYSVOL folder: `\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.

   For example: `\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`.

   NOTE: If you do not have the PolicyDefinitions folder, you need to create it.

4. Open the Windows Group Policy Management console (`gpmc.msc`) and either create a new group policy or edit your existing policy.

   NOTE: For more information, refer to Create and manage the Central Store for Group Policy Administrative Templates in Windows.

5. Go to `Computer Configuration/Policies/Administrative Templates/Google/Google Chrome/Extensions/Configure the list of Force-Installed apps and extensions` and edit the policy as follows:
   a) Select **Enabled** to turn the policy on.
   b) Under Options, select **Show...** and enter the following value:

   ```
   imdndkajeppdomiimjkcbhkafeeooghd
   ```

   NOTE: For more information, see how to set Chrome browser policies.

When the group policy is activated, WithSecure Browsing Protection is on and forced to be on.

Install the WithSecure browser protection extension in Microsoft Edge (Chromium)

These instructions are Elements Endpoint Protection specific and intended for administrator users.

NOTE: WithSecure Browser extension is installed from Google Store through Microsoft Group Policy Object (GPO). The device must be a member of a Microsoft Active Directory domain or this installation cannot be done.

To install and turn on the browser protection extension:

1. Use the Microsoft Edge policy file to do the following:
   a) Go to Microsoft Edge (Chromium) group policy template ADMX files.
   b) Select **Download Windows Policy** under the version and build of the browser and your operating system and then select **Accept and download**.
   c) Extract the cab file that you downloaded.
   d) From the extracted folders, copy to both the `C:\Windows\PolicyDefinitions` folder and your SYSVOL folder (`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`) the following files and folders:
      - The Microsoft Edge (Chromium) administrative template files:`msedge.admx` and `msedgeupdate.admx`
      - The language folder of the language that is used in your system

NOTE: If you do not have the PolicyDefinitions folder, you need to create it.

2. Open the Windows Group Policy Management console (gpmc.msc) and do one of the following:

NOTE: For more information, refer to Configure Microsoft Edge policy settings on Windows.

- Create a new group policy
- Go to `Computer Configuration/Policies/Administrative Templates/Microsoft Edge/Extensions/Control which extensions are installed silently` and edit the policy as follows:

  a. Select **Enabled** to turn the policy on.
  b. Under Options, select **Show...** and enter the following value:

```
aambijcigikmdoehgjhdepcpieghopdl
```

When the group policy is activated, WithSecure Browsing Protection is on and forced to be on.

Install the WithSecure browsing protection extension in Mozilla Firefox

These instructions are Elements Endpoint Protection specific and intended for administrator users.

NOTE: When you see a window asking you to activate the Browsing Protection extension for Mozilla Firefox, select **Allow**. The extension is activated automatically, but there is no way to prevent the window from appearing.

To install and turn on the browser protection extension:

1. Download the latest Mozilla Firefox group policy template ADMX files.
2. Extract the cab file and copy the following Mozilla Firefox administrative template files and the language folder of the language that is used in your system to the `C:\Windows\PolicyDefinitions` directory:

   `windows/mozilla.admx and firefox.admx`

3. Copy the files and the language folder of the language that is used in your system also to your SYSVOL folder:`\\yourdomainhere\SYSVOL\yourdomainhere\Policies\PolicyDefinitions\`.

   For example: `\\example.com\SYSVOL\example.com\Policies\PolicyDefinitions`.

NOTE: If you do not have the PolicyDefinitions folder, you need to create it.

4. Open the Windows Group Policy Management console (`gpmc.msc`) and either create a new group policy or edit your existing policy.
5. Go to `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Extensions to install` and edit the policy as follows:

   a) Select **Enabled** to turn the policy on.
   b) Under Options, select **Show...** and enter the following value:

```
https://download.withsecure.com/online-safety/ws_firefox_https.xpi
```

6. Go to `Computer Configuration/Policies/Administrative Templates/Mozilla/Firefox/Extensions/Prevent extensions from being disabled or removed` and edit the policy as follows:
   a) Select **Enabled** to turn the policy on.
   b) Under Options, select **Show...** and enter the following value: `ols_main@withsecure.com`.

When the group policy is activated, WithSecure Browsing Protection is on and forced to be on.

4.2 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.

4.2.1 Distribute using ssh

Distributes the product through ssh.

Before you start, download the `.mpkg` installer from **Management** > **Downloads** in WithSecure Elements Security Center. The `.mpkg` includes the subscription key.

Distributing using ssh has two parts: first you install the product and then run the `activator` tool to apply the subscription key.

1. Copy the `.mpkg` installer to the target machine using `scp` or another preferred way.
2. Connect to the target machine over `ssh` and run the silent installation command.

NOTE: For the command and options, see Installing the product automatically.

3. Over the same `ssh` session, run the `activator` tool at `/Library/WithSecure/bin/activator` with the desired configuration parameters.

NOTE: For the activation command and the available parameters, see Activating the subscription.

4.2.2 Distributing using MDM

There are different ways that you can use to distribute the product through Mobile Device Management (MDM) or another software distribution solution (for example, Munki).

You can manually activate and configure the product; you can use a custom package to activate and configure the product, or you can use one package to both install and activate the product .

Manually activate and configure the product

Distributes the product through MDM, then activates and configures it manually on each device.

Distribute the product through your MDM, then activate and configure it manually on each device.

1. Import the installation package into your MDM to allow the installation of the software on the Mac computers in your organization.
2. Execute the activator with the desired configuration parameters on the target computers using `ssh`.
3. Activate the computers.
4. Connect the computers to WithSecure Elements Security Center.

Use a custom package

Distributes the product through MDM using a custom package that handles activation and configuration.

Distribute the product through your MDM using a custom package that handles activation and configuration.

1. Import the installation package into your MDM to allow the installation of the product on Mac computers in your organization.
2. Create and import into your distribution software a custom macOS software package with activator call as follows:

NOTE: Create the package using the `pkgbuild` utility provided with macOS.

```
PROFILE_ID=<desired profile id>
TAGS=<desired installation tags>
ACTIVATION_KEY=<subscription key>

ACTIVATION_PACKAGE_SCRIPTS=./scripts
echo """#!/bin/zsh
/Library/WithSecure/activator \\
    --profile-id $PROFILE_ID \\
    --tags \"$TAGS\" \\
    --subscription-key \"$ACTIVATION_KEY\"
""" > ./$ACTIVATION_PACKAGE_SCRIPTS/postinstall
chmod +x ./$ACTIVATION_PACKAGE_SCRIPTS/postinstall
ACTIVATION_PACKAGE_IDENTIFIER=com.your-company.withsecure.elements.activation
pkgbuild \
    --nopayload \
    --scripts $ACTIVATION_PACKAGE_SCRIPTS \
    --identifier $ACTIVATION_PACKAGE_IDENTIFIER \
    "${ACTIVATION_PACKAGE_IDENTIFIER}.pkg"
```

NOTE: The `--nopayload` flag means that your package is not listed among the installed packages in macOS, which makes sense as it did not install any files into the system.

3. Create as many activation packages as you need.
4. Assign the packages to specific devices or device groups, depending on what your software distribution solution supports.

NOTE: The original installation package stays intact and keeps its designated signature. For macOS to validate your custom package, it needs to be signed and notarized.

Use a special product package

Distributes the product using a single package that both installs and activates it.

You can distribute the product with a single package that both installs and activates it.

Create a special product package from the installation package by running the prepare-installer.sh script with the following parameters:

```
prepare-installer.sh \
    /path/to/com.f-secure.macprotection.mpkg \
    /path/to/install-and-activate.pkg \
    "<Signing identity>" \
    "<profile id>" \
    "<installation tags>" \
    "<subscription key>"
```

NOTE: You can use the script as is or as an inspiration to create your own script that better suits your needs.

4.2.3 Use MDM profiles to set up the product

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

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

1. Generate MDM profiles for system preferences.

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

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

   Allow all WithSecure system extensions:

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

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

```
<key>RemovableSystemExtensions</key>
<dict>
<key>V928P8X763</key>
<array>
<string>com.withsecure.wsagent.wssystemextension</string>
</array>
</dict>
<key>PayloadDescription</key>
<string>Allows WithSecure System Extension</string>
<key>PayloadDisplayName</key>
<string>WithSecure System Extension</string>
<key>PayloadIdentifier</key>
<string>com.apple.system-extension-policy.213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadType</key>
<string>com.apple.system-extension-policy</string>
<key>PayloadUUID</key>
<string>213E79BF-4F5E-430D-AFED-D76EC62ACE96</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

Allow content filtering for WithSecure system extension:

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

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

<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">

<plist version="1.0">

<dict>

<key>PayloadContent</key>

<array>

<dict>

<key>UserDefinedName</key>

<string>WithSecure Firewall</string>

<key>PluginBundleID</key>

<string>com.withsecure.wsagent</string>

<key>FilterDataProviderBundleIdentifier</key>

<string>com.withsecure.wsagent.wssystemextension</string>

<key>FilterDataProviderDesignatedRequirement</key>

<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>

<key>FilterSockets</key>

<true/>

<key>FilterPackets</key>

<false/>

<key>FilterBrowsers</key>

<false/>

<key>FilterType</key>

<string>Plugin</string>

<key>PayloadDescription</key>

<string>Allow WithSecure Firewall to filter network traffic</string>

<key>PayloadDisplayName</key>

<string>WithSecure Firewall</string>

<key>PayloadIdentifier</key>

<string>com.apple.webcontent-filter.9FF6DE99-59E2-47A1-8918-CE259D92E785</string>

<key>PayloadType</key>

<string>com.apple.webcontent-filter</string>

<key>PayloadUUID</key>

<string>9FF6DE99-59E2-47A1-8918-CE259D92E785</string>

<key>PayloadVersion</key>

<integer>1</integer>

<key>PayloadOrganization</key>

<string>WithSecure Oyj</string>

</dict>
```

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

Grant full disk access for WithSecure processes:

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

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>PayloadDescription</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadDisplayName</key>
<string>Grant Full Disk Access to WithSecure processes</string>
<key>PayloadIdentifier</key>
<string>com.apple.TCC.configuration-profile-policy.F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadUUID</key>
<string>F8432F17-1ECD-420D-B3D0-2A35F0BB144E</string>
<key>PayloadType</key>
<string>com.apple.TCC.configuration-profile-policy</string>
<key>PayloadOrganization</key>
<string>WithSecure Oyj</string>
<key>Services</key>
<dict>
<key>SystemPolicyAllFiles</key>
```

```
<array>

<dict>

<key>Identifier</key>

<string>com.withsecure.wsagent</string>

<key>IdentifierType</key>

<string>bundleID</string>

<key>CodeRequirement</key>

<string>identifier "com.withsecure.wsagent" and anchor apple generic and certificate leaf[subject.OU]
 = "V928P8X763"</string>

<key>Allowed</key>

<true/>

<key>Comment</key>

<string>Grant Full Disk Access to WithSecure processes</string>

</dict>

<dict>

<key>Identifier</key>

<string>com.withsecure.wsagent.wssystemextension</string>

<key>IdentifierType</key>

<string>bundleID</string>

<key>CodeRequirement</key>

<string>identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate
 leaf[subject.OU] = "V928P8X763"</string>

<key>Allowed</key>

<true/>

<key>Comment</key>

<string>Grant Full Disk Access to WithSecure's System Extension'</string>

</dict>

</array>

</dict>

</dict>

</array>

<key>PayloadDisplayName</key>

<string>WithSecure Agent Profile</string>

<key>PayloadIdentifier</key>

<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>

<key>PayloadRemovalDisallowed</key>

<false/>

<key>PayloadType</key>

<string>Configuration</string>

<key>PayloadUUID</key>

<string>00000000-0000-0000-0000-000000000001</string>

<key>PayloadVersion</key>

<integer>1</integer>
```

```
</dict>
</plist>
```

Allow user notifications for WithSecure processes:

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

```
<?xml version="1.0" encoding="UTF-8"?>
<!DOCTYPE plist PUBLIC "-//Apple//DTD PLIST 1.0//EN" "http://www.apple.com/DTDs/PropertyList-1.0.dtd">
<plist version="1.0">
<dict>
<key>PayloadContent</key>
<array>
<dict>
<key>NotificationSettings</key>
<array>
<dict>
<key>AlertType</key>
<integer>2</integer>
<key>BadgesEnabled</key>
<true/>
<key>BundleIdentifier</key>
<string>com.withsecure.wsagent</string>
<key>CriticalAlertEnabled</key>
<false/>
<key>NotificationsEnabled</key>
<true/>
<key>ShowInLockScreen</key>
<true/>
<key>ShowInNotificationCenter</key>
<true/>
<key>SoundsEnabled</key>
<true/>
</dict>
</array>
<key>PayloadEnabled</key>
<true/>
<key>PayloadDescription</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadDisplayName</key>
<string>Allow notifications for WithSecure products</string>
<key>PayloadIdentifier</key>
```

```
<string>com.apple.notificationsettings.A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadType</key>
<string>com.apple.notificationsettings</string>
<key>PayloadUUID</key>
<string>A134E8B3-AE82-4AE9-8D39-F9976B5BEEE1</string>
<key>PayloadVersion</key>
<integer>1</integer>
<key>PayloadOrganization</key>
<string>WithSecure Corporation</string>
</dict>
</array>
<key>PayloadDisplayName</key>
<string>WithSecure Agent Profile</string>
<key>PayloadIdentifier</key>
<string>SAMPLE.00000000-0000-0000-0000-000000000001</string>
<key>PayloadRemovalDisallowed</key>
<false/>
<key>PayloadType</key>
<string>Configuration</string>
<key>PayloadUUID</key>
<string>00000000-0000-0000-0000-000000000001</string>
<key>PayloadVersion</key>
<integer>1</integer>
</dict>
</plist>
```

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

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

4.2.4 Creating MDM profiles for Microsoft Intune

When managing a network of devices, it is crucial to ensure that they all adhere to your organization's security standards.

Microsoft Intune simplifies this process through the use of MDM profiles. These profiles are packages of settings that control various aspects of device security and functionality.

This section explains how to create for Microsoft Intune MDM profiles with content filtering, notification, full-disk access, and system extension settings.

Create MDM profiles with content filtering settings

Creates an MDM profile that lets the network content filter component run without user approval prompts on managed macOS devices.

This profile lets the WithSecure network content filter component run without user approval prompts on managed macOS devices.

1. Log in to your Microsoft Intune portal.
2. Select **Devices** > **Manage devices** > **Configuration**
3. To create new policy, do the following:
   a) Select **Create New Policy**.
   b) Select **macOS** platform.
   c) As a profile type, select **Settings catalog**.
   d) Select **Create**.
4. Enter a name for the profile, and select **Next**.
5. In **Configuration settings** tab, select **+ Add settings**.
6. In the search bar, enter `Web content filter`.
7. Select **Web** > **Web Content Filter**, and select the following settings:
   - Filter Data Provider Bundle Identifier
   - User Defined Name
   - Filter Grade
   - User Name
   - Filter Sockets
   - Filter Packets
   - Plugin Bundle ID
   - Filter Data Provider Designated Requirement
   - Organization
   - Filter Type
8. Close the **Settings picker** window.
9. Enter the following values:
   - Filter Data Provider Bundle Identifier: `com.withsecure.wsagent.wssystemextension`
   - User Defined Name: `WithSecure Firewall`
   - Filter Grade: `firewall`
   - User Name: `WithSecure Element Content Filter`
   - Filter Sockets: `True`
   - Filter Packets: `False`
   - Plugin Bundle ID: `com.withsecure.wsagent`
   - Filter Data Provider Designated Requirement: `identifier "com.withsecure.wsagent.wssystemextension" and anchor apple generic and certificate leaf[subject.OU] = "V928P8X763"`
   - Organization: `WithSecure`
   - Filter Type: `Plug-in`
10. Select **Next**.
11. In the **Assignments** tab, add the groups, users, and devices to which you want to apply this profile configuration.

12. Select **Next**.
13. In the **Review + create** tab, select **Create**

Create MDM profiles with notification settings

Creates an MDM profile that lets alerts appear as persistent banners on managed macOS devices, without requiring manual notification approval.

This profile lets WithSecure alerts appear as persistent banners on managed macOS devices, without requiring the user to approve notifications manually.

1. Log in to your Microsoft Intune portal.
2. Select **Devices** > **Manage devices** > **Configuration**
3. To create new policy, do the following:
   a) Select **Create New Policy**.
   b) Select **macOS** platform.
   c) As a profile type, select **Settings catalog**.
   d) Select **Create**.
4. Enter a name for the profile, and select **Next**.
5. In **Configuration settings** tab, select **+ Add settings**.
6. In the search bar, enter `Notifications`.
7. Select **User Experience** > **Notifications**
8. Select the **Notification settings** option.
9. Close the **Settings picker** window.
10. Select **+Edit instance**.
11. Enter values for the following settings:

NOTE: Do not alter the default values of the other settings.

- Alert type: `Persistent Banner`
- Bundle Identifier: `com.withsecure.wsagent`

12. Select **Next**.
13. In the **Assignments** tab, add the groups, users, and devices to which you want to apply this profile configuration.
14. Select **Next**.
15. In the **Review + create** tab, select **Create**

Create MDM profiles with full-disk access settings

Creates an MDM profile that grants the agent full-disk access without requiring manual user approval on managed macOS devices.

This profile grants the WithSecure agent full-disk access without requiring manual user approval on managed macOS devices.

1. Log in to your Microsoft Intune portal.
2. Select **Devices** > **Manage devices** > **Configuration**
3. To create a new policy, do the following:
   a) Select **Create New Policy**.
   b) Select **macOS** platform.

c) As a profile type, select **Templates**, and then select **Device restrictions**.
d) Select **Create**.

4. Enter a name for the profile, and select **Next**.
5. In **Configuration settings** tab, select **Privacy preferences**.
6. Under **Apps and processes**, select **Add**, and enter and select the following values:
   - Name: `WithSecure Elements`
   - Identifier type: select **Bundle ID**
   - Identifier: `com.withsecure.wsagent`
7. Select **Next**.
8. In the **Assignments** tab, add the groups, users, and devices to which you want to apply this profile configuration.
9. Select **Next**.
10. In the **Review + create** tab, select **Create**

Import MDM profiles with system extension settings

Creates an MDM profile that lets the system extension load automatically on managed macOS devices, without requiring manual user approval.

This profile lets the WithSecure system extension load automatically on managed macOS devices, without requiring manual user approval.

1. Log in to your Microsoft Intune portal.
2. Select **Devices** > **Manage devices** > **Configuration**
3. To create new policy, do the following:
   a) Select **Create** > **New Policy**.
   b) Select **macOS** platform.
   c) As a profile type, select **Settings catalog**.
   d) Select **Create**.
4. Enter a name for the profile, and select **Next**.
5. In **Configuration settings** tab, select **+ Add settings**.
6. In the **Search** box, enter `System Extensions`.
7. Select **System Configuration** > **System Extensions**.
8. Select the **Allowed system extensions** option.
9. Close the **Settings picker** window.
10. Select **+Edit instance**.
11. Under **Allowed system extensions**, do the following:
    a) Next to the checkbox, enter the following: `com.withsecure.wsagent.wssystemextension`
    b) As a team identifier, enter `V928P8X763`
12. Select **Next**.
13. In the **Assignments** tab, add the groups, users, and devices to which you want to apply this profile configuration.
14. Select **Next**.
15. In the **Review + create** tab, select **Create**

4.2.5 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**.

System extension changes in macOS Sequoia

Starting with macOS Sequoia (15.x) users with administrator rights can turn off System Extensions via System Settings.

To prevent users from turning off specific System Extensions, you can apply a configuration profile to remove this ability via the System Settings UI.

IMPORTANT: You must scope the profile to devices with macOS Sequoia or later. If you scope the profile to an earlier version, the settings will not apply after upgrading.

Create non-removable system extensions from UI profile with Jamf

Creates a **non-removable system extensions from UI** configuration profile using Jamf for devices with macOS Sequoia or later.

In Jamf, create a configuration profile that prevents users from removing the WithSecure system extensions on managed devices.

1. Navigate to **Computers** > **Configuration Profiles** and create a **New** profile.
2. In the **General** category, give the new profile a descriptive name.
3. Select the **System Extensions** payload and then select **Configure**.
4. Enter a name in the **Display Name** field to help identify the profile, for example, `WithSecure UI Non-Removable`.
5. To prevent users from disabling an extension from the System Settings app, from the **System Extension Types** drop-down, select the **Non-removable system extensions from UI** option.
6. In the Team identifier field, enter the following: `V928P8X763`.
7. Select the **+Add** button.
8. Enter the following extension name: `com.withsecure.wsagent.wssystemextension`.
9. Select **Save** to the right of the text field.
10. In the **Scope** tab, select **Smart Computer Group** that contains devices with macOS Sequoia or later. If you do not have an existing smart group available, see Create a smart group for devices with macOS Sequoia or later.
11. Save the profile.
12. Deploy the configuration profile to the target devices.
13. Verify that the system extensions are non-removable in System Settings.
    The WithSecure system extensions are listed and cannot be turned off or removed.

Create a smart group for devices with macOS Sequoia

Creates a smart group for devices with macOS Sequoia.

IMPORTANT: These instructions apply only to macOS Sequoia (15.x) and later versions.

1. Log in to the Jamf portal.
2. Select **Computers** > **Smart Computer Groups** > **New**.
3. As the Display name, enter `macOS 15 or later`.
4. In the **Criteria** tab, select **Add**.
5. As the criteria, select **Operating System Version**.
6. From the **Operator** drop-down menu, select **greater than or equal** and enter `15` in the **Value** field.
7. Select **Save**.

4.2.6 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`.

Related reference
Installer parameters for macOS on page 90
Use these installer filename patterns and `activator` command-line options to configure WithSecure Elements Agent for Computers (Mac) at install time.

4.2.7 Install the product manually using an MPKG file

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

NOTE: Users must have administrator rights on the device.

Using this deployment method, you download the installer file and install the product.

To install the product:

1. Log in to WithSecure Elements Security Center at https://elements.withsecure.com.

   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 **WithSecure Elements Agent for Computers**, select **Download .mpkg**.

   NOTE: The `.mpkg` file includes the subscription key.

   *The **Download installer** page opens.*
4. Select the product that you want to install, and then select **Download**.
   The installation file is downloaded.
5. Locate the downloaded installation file (`.mpkg`) and double-click it to start the installation.
   *The **Install WithSecure Elements** wizard opens.*
6. Follow the instructions in the wizard.
7. When the installation is complete, in the **Summary** screen, select **Close**.

Related reference
Installer parameters for macOS on page 90

Use these installer filename patterns and `activator` command-line options to configure WithSecure Elements Agent for Computers (Mac) at install time.

4.2.8 Grant full disk access

Grants full disk access in macOS.

You need to allow WithSecure Elements Endpoint Protection with EDR for Mac and Client Security for Mac to scan your computer and to allow them to run.

1. Select the Apple icon in the top-left corner of your menu bar and then select **System Settings...**.
2. Select **Privacy & Security**.
3. Under **Privacy**, select **Full Disk Access**.
4. Turn on the **WithSecure Agent** option.

4.2.9 Allow the WithSecure system extension

Allows the WithSecure system extension in macOS.

After installation, macOS blocks the WithSecure system extension until you allow it.

1. After you have installed the product, the System Extension Blocked popup shows.
2. To allow the WithSecure system extension, in the popup, select **Open System Settings**.

NOTE: If you select **OK**, the popup closes. To continue, open **System Settings**.

3. Under **System software from application WithSecure Agent was blocked from loading**, select **Allow**.

The WithSecure system extension is allowed to load.

4.2.10 Allow WithSecure Agent notifications

Allows WithSecure Agent notifications.

To allow notifications:

1. After you have installed the product, the WithSecure Agent Notifications popup opens.
2. In the popup, select **Options** > **Allow**.

The WithSecure Agent can show notifications on the device.

4.2.11 Filter network content

Filters network content.

To filter network content:

1. From the Apple menu, open **System Settings**.
2. Select **Screen Time** > **Content & Privacy**.
3. Select **Store, Web, Siri & Game Center Content**.
4. Do one of the following to filter network content:
   - To automatically restrict access to many adult websites, from the **Access to Web Content** drop down menu, select **Limit Adult Websites**.

NOTE: By selecting **Customize**, you can add allowed or restricted websites.

- To limit access to specific websites, from the **Access to Web Content** drop down menu, select **Allowed Websites only**.

NOTE: By selecting **Customize**, you can add or remove allowed websites using the + and - icons. By selecting an allowed website from the list and then selecting the three dots icon, you can edit the website title or URL.

5. Select **Done**.

4.2.12 Checking that browser extensions are in use

Browsing protection requires browser extensions to be able to protect your web browsing, online banking and shopping, and to show you security information while you are browsing the internet.

Once you have installed the product on your computer, the product requires you to install and activate the browser extension for the web browser that you use.

The product installs the browser extension for Safari automatically, and the only thing you need to do is to make sure that the extension is turned on.

For Chrome, you need to install and enable the browser extension to be able to browse the internet safely. Also, the installation of the extension requires your permission to access information about the web addresses you visit. For more detailed information, see the related information.

Enable browser extension for Safari

You must enable the browser extension for Safari to be able to use the browser safely.

The product installs the browser extension automatically, and the only thing you need to do is to make sure that the extension is turned on.

To ensure that the browser extension for Safari is turned on:

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.
3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
5. In the pop-up window, select **Safari** and then **Enable**.
6. In the **Extensions** dialog, do the following:
   a) Make sure that **Browsing protection** is selected.
   b) Under **Private Browsing**, select **Allow in Private browsing**.
   c) Under **Permissions**, select **Allow on Every Website.**.

You can now use Safari to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: `https://unsafe[.]fstestdomain[.]com`. You should see the product block page.

Install and enable browser extension for Google Chrome

You need to install and enable the browser extension for Google Chrome to be able to use the Chrome browser safely.

To set up the browser extension for Google Chrome:

1. Select the product icon in the menu bar.
2. Select **Settings...** from the menu.

3. Open the **Secure Browsing** tab.
4. Select **Install browser extension**.
   *The **Browsing protection installation** window opens.*
5. From the drop-down, select **Chrome** and then **Install now**.
6. Select **Add to Chrome** > **Add extension**.

   Once the extension is installed, a user consent dialog opens. The browser extension requires your permission to access information about the web addresses you visit.
7. Select **Accept**.

NOTE: If you decline to grant the permission, you will not be able to use the extension and Browsing protection cannot block harmful websites nor show search result ratings. Also, the extension will be removed from the browser.

8. To complete setting up the extension, select **OK**.

You can now use Chrome to browse the internet safely.

To test that the browser extension is working, open the following test page in your browser: `https://unsafe[.]fstestdomain[.]com`. You should see the product block page.

4.2.13 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.
```

4.2.14 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.

Installer parameters for macOS

Use these installer filename patterns and `activator` command-line options to configure WithSecure Elements Agent for Computers (Mac) at install time.

Embedding parameters in the installer filename

You can embed a subscription key, activation token, profile ID, and release group into the installer package filename, so the values apply automatically during installation. The filename patterns work the same whether you use a `.pkg` or `.mpkg` installer package.

Table 3: Installer filename patterns

What you want to configure	Filename pattern
No subscription key or activation token	`ElementsAgentInstaller.pkg`
Subscription key	`ElementsAgentInstaller[<subscription-key>].pkg`
Activation token	`ElementsAgentInstaller[<activation-token>].pkg`
Subscription key + profile	`ElementsAgentInstaller[<subscription-key>][profile=<profile-id>].pkg`
Activation token + profile	`ElementsAgentInstaller[<activation-token>][profile=<profile-id>].pkg`
Subscription key + release group	`ElementsAgentInstaller[<subscription-key>][u-group=<group-id>].pkg`
Activation token + release group	`ElementsAgentInstaller[<activation-token>][u-group=<group-id>].pkg`
Subscription key + profile + release group	`ElementsAgentInstaller[<subscription-key>][profile=<profile-id>][u-group=<group-id>].pkg`
Activation token + profile + release group	`ElementsAgentInstaller[<activation-token>][profile=<profile-id>][u-group=<group-id>].pkg`

NOTE: If your software management tool does not accept square brackets, use a double underscore (__) around the subscription key instead, for example: `ElementsAgentInstaller__<subscription-key>__.pkg`.

NOTE: You can combine the profile and release-group parameters in any order within the brackets.

activator command-line parameters

The `activator` tool lets you set the same values using command-line options instead of the installer filename. It is distributed with WithSecure Elements EPP for Computers (Mac) versions 17.8.32555 and newer.

Table 4: activator command-line options

Parameter	Explanation
-p, --profile-id <profile-id>	Sets the ID of the profile to assign. For example: `--profile-id 123456`.
-t, --tags <tags>	Sets installation tags to report to WithSecure Elements Security Center. For example: `--tags "department=R&D,role=engineer"`.
-s, --subscription-key <subscription-key>	Sets the subscription key to activate.

Parameter	Explanation
-r, --release-group <release-group>	Sets the release group to use when checking for updates.
-h, --help	Shows command-line help.

4.2.15 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.

4.3 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.

4.3.1 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`.

4.3.2 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`.

4.4 Deployment methods for mobile devices

The most common deployment methods for mobile devices.

WithSecure Elements Mobile Protection can be deployed in mobile devices in the following ways:

- Inviting users by sending an installation email through WithSecure Elements Security Center
- Using an MDM

Deployment by inviting users

This method is suitable for small environments, educational institutions, and BYOD (Bring your own device) -environments.

NOTE: Users must have administrator rights on the device.

If you need to deploy the app to users who are remote, who do not know the subscription key, and who have administrative rights on their devices, using this installation method may be convenient. 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 Elements Endpoint Protection account.

Using this deployment method, you invite users by sending them an email message that contains a link to download WithSecure Elements Mobile Protection.

NOTE: The installation link is valid for 30 days.

The installer file has an embedded single-use installation token, which means that the subscription key remains hidden. This allows users to install the software on one device that will then appear in WithSecure Elements Security Center.

To install WithSecure Elements Mobile Protection on endpoint devices, you must add the new devices to Elements Security Center and enter user information such as email address and first and last name.

NOTE: Elements Security Center shows the first and last names if they have been added. If they have not been added, the system checks for email address and alias. If none of the information is available, the UUID is shown.

Deployment using MDM

Deploying WithSecure Elements Mobile Protection using MDM is perfect for organizations that want to provide additional security for their mobile devices on top of the basic security features that their existing MDM solution already provides. The solution greatly enhances security against malware, phishing, and data theft, among others.

WithSecure Elements Mobile Protection can be integrated with the following MDMs:

- Google Workspace Endpoint Management (for Android devices only)
- VMware Workspace ONE (formerly known as AirWatch)
- Microsoft Intune
- IBM Security MaaS360
- Ivanti Endpoint Management (formerly known as MobileIron Cloud)
- Miradore
- Samsung Knox (for Android devices only)

You can deploy WithSecure Elements Mobile Protection per profile enrollment, which means that if the end device has both personal and work profiles, you need to install the app on both profiles.

TIP: We strongly recommend that you test the enrolment on one device first.

NOTE: Variables are usually defined when WithSecure Elements Mobile Protection is configured on an MDM platform. The variables define whether the app is registered with an email address, username, or UUID. For example:

- If you do not configure the app, it uses the UUID, which shows under the device name in Elements Security Center.
- If you configure email addresses, they show under the device name in Elements Security Center.

Once you have configured the app on an MDM platform, you should not change it. If you do decide to change it, you need to first remove the devices from Elements Security Center and also remove the app from the MDM agent because it will create duplicates.

Automatic granting of diagnostic and data collection

When you activate WithSecure Elements Mobile Protection via an MDM profile, to have your diagnostic and data collection automatically granted, you need to add to your app configuration the following:

- Data collection: "data_usage_permission"
- Diagnostic collection: "diagnostic_usage_permission"

4.4.1 Install browser extension for Google Chrome

You need to install and enable the browser protection extension for Google Chrome to be able to use the Chrome browser safely.

NOTE: These instructions apply to Chrome OS. The Chrome browser on Android currently does not support browser extensions.

1. Open Google Chrome Browser.
2. From the three-dots menu at the top-right corner, select **Extensions** > **Manage extensions**.
3. In the Search box, enter `Browsing Protection by WithSecure`.
4. From the results, select the required extension.

After the installation is complete, the Chrome browser on ChromeOS starts to validate the URLs that you open using WithSecure Elements Mobile Protection which is installed in the Android container of ChromeOS.

4.4.2 Deployment using Google Workspace MDM

Deployment of WithSecure Elements Mobile Protection with Google Workspace MDM to Android devices.

To deploy the WithSecure Elements Mobile Protection app with Google Workspace, add and configure the app for managed Android devices, and enroll and protect Chromebooks.

Add the Android app to Google Workspace Endpoint Management

Adds WithSecure Elements Mobile Protection as an allowed app in Google Workspace MDM for Android devices.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

To add the product to Google Workspace MDM:

1. Log in to your Google Workspace Admin console.
2. On the Dashboard, select **Apps** > **Web and mobile apps**.
3. On the **Web and mobile apps** page, select **Add App** > **Add private Android app**.
4. On the **Managed Android apps** page, select **Search Play Store** and enter `mobile protection elements` in the search box.
5. Select the app and then select **Approve** > **Select**.
6. Under **User access**, select your preferred option and select **Continue**.
7. Under **Access method**, select your preferred options and select **Finish**.

The Android app is added to Google Workspace MDM.

Configure the Android app in Google Workspace

Configures the Android app in Google Workspace using a subscription key and registration key.

NOTE: Google Workspace does not support variables. However, the Registration key field accepts a subscription key as a variable in standard format. Therefore, enter the subscription key as is, but do not enter an email address. If you do, all your devices are shown with the same email address in WithSecure Elements Security Center. When you leave the email address empty, the devices that have WithSecure Elements Mobile Protection installed are shown with a Device UUID.

1. On the **Admin Console** page, under **Managed configurations**, select **Add managed configuration**.
2. On the Managed configuration page, enter a name for the configuration and do the following:
   a) In the Registration key field, enter the product subscription key.

      You can find the subscription key in the WithSecure Elements Security Center under **Management** > **Subscriptions** > **Subscriptions**.

   b) Enter your first and last name in the respective fields (optional).
   c) In the Alias field (optional), enter an alternate name.
   d) In the Email address field (optional), enter your email address.
   e) In the Environment field (optional), enter 2.
3. Select **Save**.

4.4.3 Deployment using VMware Workspace ONE MDM

Deployment of WithSecure Elements Mobile Protection with VMware Workspace ONE (formerly AirWatch) MDM on Android and iOS.

NOTE: This deployment does not include creating and configuring users and devices.

To deploy the WithSecure Elements Mobile Protection app with VMware Workspace ONE, add and configure the app for the iOS and Android devices that Workspace ONE manages.

Add the iOS app to VMware Workspace ONE MDM

Adds the WithSecure Elements Mobile Protection iOS app to VMware Workspace ONE MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

Adding the app to Workspace ONE lets you deploy and manage it on iOS devices enrolled in the MDM.

1. On the VMware Workspace ONE administration portal, go to **Resources** > **Apps**.
2. Select the **Public** tab.
3. Select **Add application**.
4. On the Add Application view, do the following:
   a) In the Managed by field, add you organization.
   b) From the Platform drop-down menu, select **Apple iOS**.
   c) In the Name field, enter the application name, for example, **WithSecure Mobile Protection**.
   d) Select **Next**.
   The Search page opens.
   e) From the Country drop-down menu, you can select your country, and click **Select**.
   The Add Application - WithSecure Mobile Protection view opens.
   f) On the view that opens, under **Name**, enter WithSecure Mobile Protection if its not detected by default and select **Save and assign**.

Next, you need to configure the iOS app.

Configure the iOS app in VMware Workspace ONE

Configures the WithSecure Elements Mobile Protection iOS app in VMware Workspace ONE MDM.

After adding the app to Workspace ONE, configure its assignment, restrictions, and automatic-activation settings before publishing it to devices.

1. Under **Assignment** > **Distribution**, enter the following:
   - Name - the name of the app (WithSecure Mobile Protection)
   - Description - a description for the assignment (optional)
   - Assignment groups - select the group to whom you want to assign the app, for example, **All devices**.
   - App delivery method - select the app delivery method: **Auto** or **On demand**.
2. Select the **Restriction** tab, and turn on the desired options.
3. Next , select the **Tunnel & Other Attributes** tab, and review the options.
4. Select the **Application Configuration** tab.
5. Turn on the **Send Configuration** option, and do the following:
   a) Next, select **Add** to add the configuration key and device identification details to allow for an automatic activation of the app.
   b) Under **Configuration Key**, enter values for the following configuration entries:
      - *fate_registration_key* - the subscription key
      - *first_name* (optional) - a name that makes it easier to identify the device inWithSecure Elements Security Center
      - *last_name* (optional) - a name that makes it easier to identify the device in WithSecure Elements Security Center
      - *email* - the user email address
      - *alias* (optional) - an alternate name for the user
   c) For entering any optional keys, select the icon next to **Insert Lookup Value** and select the respective variables. The fields are automatically filled when the application is deployed to user devices.
6. Select **Create**.
7. On the view that opens, select **Save**.
8. On the Preview Assigned Devices page, when you see your device that you added, select **Publish**.
9. On the main view, select **Devices List View**.

Your device shown on the list.

Add the Android app to VMware Workspace ONE MDM

Adds the WithSecure Elements Mobile Protection Android app to VMware Workspace ONE MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

Adding the app to Workspace ONE lets you deploy and manage it on Android devices enrolled in the MDM.

1. On the VMware Workspace ONE administration portal, go to **Apps and Books** and select **Native**.
2. Next, in the Public tab, select **Add application**.
3. On the Add Application page, do the following:
   a) From the **Platform** drop-down menu, select **Android**.
   b) In the **Source** field, select **Search App store**.
   c) In the **Name** field, enter `WithSecure Elements Mobile Protection`.
   d) Select **Next**.
4. In the Apps view, select **WithSecure Elements Mobile Protection**.
5. In the **WithSecure Elements Mobile Protection** view, select **Approve** > **Select**.
6. In the Edit Application view, select the **Terms of Use** tab.
7. From the **SDK** drop-down menu, select **MP strings@ WithSecure**.
8. Select **Save and assign**.

View the managed applications

Lists the managed applications in VMware Workspace ONE MDM.

The List View page shows which apps have been added to Workspace ONE, so you can confirm that the app was added successfully.

1. In the VMware Workspace ONE console window, select **Apps&Books** and then under **Applications**, select **List View**.
   The List View page opens
2. Select the **Public** tab.

   The WithSecure Elements Mobile Protection app appears in the Apps list on the VMware Workspace ONE administration portal.

Deploying Android Enterprise with VMware Workspace ONE

Deployment of WithSecure Elements Mobile Protection in the Android Enterprise context with VMware Workspace ONE.

To deploy the app in the Android Enterprise context with VMware Workspace ONE, set up Android Enterprise, add the app profiles, and add and configure the WithSecure Elements Mobile Protection app.

Set up Android Enterprise in VMware Workspace ONE MDM

Sets up the WithSecure Elements Mobile Protection Android app in the Android Enterprise context.

To deploy the app in the Android Enterprise context, the company must have Google Administrator account. All the users must have accounts there, either predefined or generated during the enrollment.

The domain administrator has to generate an EMM token and bind VMware Workspace ONE as an EMM provider.

To set up Android Enterprise:

1. Log into the VMware Workspace ONE administration portal.
2. Go to **Groups and Settings** and select **All Settings**.
3. In the Settings view, under **Devices and Users**, select **Android**.
4. Under **Android**, select **Android EMM Registration**.
5. Select the account icon at the top right corner and select **Manage your Google Account**.
6. Log in with your email and password.
7. On the Bring Android to Work page, select **Get started**.
   The Android EMM Registration page opens.
8. When the service account is set up, accept the settings in the **Enrollment Settings** and **Enrollment Restrictions** tabs.
9. Select **Save**.
   The settings are saved.

Add profiles in VMware Workspace ONE

Adds an SDK profile that controls how the app behaves on Android devices deployed through VMware Workspace ONE.

An SDK profile controls how the app behaves once it is deployed to Android devices through Workspace ONE.

1. On the VMware Workspace ONE administration portal, go to **Apps & Books** > **All Apps & Books Settings**
   The Settings page opens.
2. On the navigation pane, select **Settings and Policies** > **Profiles**.
   The Profiles view opens.
3. Select **Add Profile** > **SDK Profile** > **Android**
   The Add a New Android Profile page opens.
4. Select **General**.
5. Enter a name and description for the new profile.
6. Select **Save**.

Add the Android app

Adds the WithSecure Elements Mobile Protection Android app to VMware Workspace ONE MDM in the Android Enterprise context.

Add the WithSecure Elements Mobile Protection app to VMware Workspace ONE so it can be deployed to managed Android Enterprise devices.

1. On the VMware Workspace ONE administration portal, go to **Apps & Books** > **Applications** > **Native**.
   The List view opens
2. Select the **Public** tab, and then **Add application**.
3. In the Add Application view, do the following:
   a) From the **Platform** drop-down menu, select **Android**.
   b) Enter the application name: `mobile protection elements`.
   c) Select **Next**.
   *The **Apps** page opens.*
4. Select `WithSecure Elements Mobile Protection`.
5. In the WithSecure Elements Mobile Protection view, select **Approve** > **Select**.
   The Edit application view opens.
6. Select the **SDK** tab, and from the **Application Profile** drop-down menu, select **MP strings @ WithSecure**.
7. Select **Save and assign**.
   *The **WithSecure Elements Mobile Protection - Assignment** page opens.*
8. Select **Distribution** and do the following:
   a) In the Name field, enter a name for the distribution, for example, `alldevices`.
   b) In the Assignment groups, select your preferred device distribution group.
9. Next, select **Application Configuration** and do the following:
   a) In the **Registration key** field, enter the product subscription key.

   > **NOTE:** You can find the WithSecure Elements Mobile Protection subscription key in WithSecure Elements Security Center under **Endpoint Protection** > **Subscriptions**.

   b) In the First name (optional) field, enter **{FirstName}**
   c) In the Last name (optional) field, enter **{LastName}**
   d) In the Alias (optional) field, enter **{EnrollmentUser}**
   e) In the Email (optional) field, enter **{EmailAddress}**
   f) Select **Create**.
   *The **Assignments** tab opens.*
10. Select **Save**.
    *The **Preview Assigned Devices** page opens.*
11. Select **Publish**.

Configure the Android app in VMware Workspace ONE

Configures the WithSecure Elements Mobile Protection Android app in VMware Workspace ONE MDM in the Android Enterprise context.

To configure the Android app:

1. On the VMware Workspace ONE administration portal, select the **Edit Application** page.
2. Select the **Assignment** tab and define the assignment group.

3. Select **Send Application Configuration**.
4. Under **Configuration Key**, add values to the following configuration entries:

   > **NOTE:** The reseller provides you with the values.

   - fate_registration_key - the license key
   - first_name (optional) - a name that makes it easier to identify the user in WithSecure Elements Security Center
   - last_name (optional) - a name that makes it easier to identify the user in WithSecure Elements Security Center

   For the optional keys, select **Insert Lookup Value** and select respective variables. The fields are automatically filled when the application is deployed to user devices.
5. Fill the rest of the app settings under **Details and Assignment**, and select **Save and Publish** to add the app to **List View**.

Use certificates to register devices

Registers devices using a certificate.

> **NOTE:** You must have a subscription for WithSecure Elements Mobile Protection with External MDM to do this.

To register a device using a certificate:

1. Log in to WithSecure Elements Security Center with your company administrator account.
2. Under **Subscriptions**, select

   and then select **External MDM server configuration**
3. Download and save the certificate file.
4. On the VMware Workspace ONE administration portal, go to **Resources Profiles & Baselines** > **Add new Profile**.

   > **NOTE:** You can also use an existing profile to pre-configure the certificate.

5. Under **Credentials**, select **Add** to upload the certificate that you downloaded from WithSecure Elements Security Center.
6. Select **Save and publish**.
7. Assign the profile to your devices.

4.4.4 Deployment using Microsoft Intune MDM

Deployment of WithSecure Elements Mobile Protection with Microsoft Intune MDM, covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with Microsoft Intune, add and configure the app for the iOS and Android devices that Intune manages.

Deploying the iOS app with Microsoft Intune MDM

Deployment of the WithSecure Elements Mobile Protection iOS app with Microsoft Intune MDM.

To deploy the iOS app with Microsoft Intune, add the WithSecure Elements Mobile Protection app and configure its management settings for your managed iOS devices.

Add the iOS app to Microsoft Intune MDM

Adds the WithSecure Elements Mobile Protection iOS app to Microsoft Intune MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

Adding the app to Intune lets you assign and publish it to iOS devices enrolled in the MDM.

1. Log into your Microsoft Intune portal.
2. Select **Apps** > **iOS/iPadOS** > **Add**.
   *The **Select app type** pane opens.*
3. From the **App type** drop-down menu, select **iOS store app**, and then select **Select**.
4. In the **Add App** view, select **Search the App store**.
   *The **Search the App Store** pane opens.*
5. In the Search field, enter `WithSecure Mobile Protection`.
6. Select **WithSecure Elements Mobile Protection** > **Select**.
   The Add App view opens.
7. In the **App information** tab, select **Yes** to show WithSecure Mobile Protection as a featured app in the Company Portal, and select **Next**.
8. In the Assignments tab, under **Required**, select **Add all users**, and select **Next**.
9. In the **Review + create tab**, select **Create**.
10. When you are done, on the **Add App** blade, choose **OK**.

The WithSecure Elements Mobile Protection app has been added to Microsoft Intune MDM.

Next, add the app configuration policies.

Add the iOS app configuration policies

Adds WithSecure Elements Mobile Protection app configuration policies for managed iOS devices.

To create an app configuration policy:

1. Select **Apps**.
   *The **Apps overview** pane opens.*
2. Under **Policy**, select **App configuration policies**.

3. Select **Add** > **Managed devices**
   *The **Create app configuration policy** pane opens.*
4. In the **Basics** tab, do the following:
   a) In the **Name** field, enter WithSecure Mobile Protection.
   b) From the **Platform** drop-down menu, select **iOS/iPadOS**.
   c) Next to **Targeted app**, select **Select app**.
      The Associated app pane opens.
   d) Select **WithSecure Elements Mobile Protection**, and select **OK** > **Next**.

   *The **Settings** tab opens.*
5. Do the following:
   a) From the **Configuration settings format** drop-down menu, select **Use configuration designer**.
   b) For the value types, refer to Use the configuration designer on page 104
   c) Select **Next**.
      *The **Assignments** tab opens.*
   d) Under **Included groups**, select **Add all users** and select **Next**.
      *The **Review + create** tab opens.*
   e) Select **Create**.

The app configuration policy was created and assigned.

You need to install the app on an iOS device.

Use the configuration designer

You can use the configuration designer for apps on devices whether or not they are enrolled in Intune.

TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

The designer lets you configure specific configuration keys and values. You must also specify the data type for each value. For each key and value in the configuration, set:

- Configuration key - The key that uniquely identifies the specific setting configuration.
- Value type - The data type of the configuration value. Types include Integer, Real, String, or Boolean.
- Configuration value - The value for the configuration.

The following key and value is mandatory for WithSecure Elements Mobile Protection license activation.

Table 5: Mandatory configuration key

Key	Type	Description	Value	Notes
fate_registration_key	string	The registration or activation key that is used by the client	`ABCD-EFGH-IJKL-MNOP`	Example: The actual value is provided by the reseller.

End user is not able to switch VPN off from the WithSecure Elements Mobile Protection app nor disable individual protection features. Read more about the details and limitations with this feature from Keeping VPN switched on automatically.

The following optional keys help to identify devices on WithSecure Elements Security Center. Use Microsoft Intune dynamic variables to get suitable values.

Table 6: Optional device identification keys

Key	Type	Description
email	string	Specifies a user activation email
env	integer	Specifies the environment where the application is activated. For customers using production, set this value to "2"
data_usage_permission	Boolean	Set to true if the administrator allows data collection; otherwise, set to false
diagnostic_usage_permission	Boolean	Set to true if the administrator allows diagnostic collection; otherwise, set to false
create_vpn_profile	Boolean	Set to true to allow creation of the VPN profile; otherwise, set to false

Deploying the Android app with Microsoft Intune MDM

Deployment of WithSecure Elements Mobile Protection with Microsoft Intune MDM.

For MDM-managed devices, WithSecure Elements Mobile Protection supports silent activation, automatically granting all required system and feature permissions and deploying the VPN profile without user interaction. This provides a true zero-touch deployment experience, unlike standard deployments where users must manually approve each permission request and install the VPN profile.

Add the Android app to Microsoft Intune MDM

Adds the WithSecure Elements Mobile Protection Android app to Microsoft Intune MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

Adding the app to Intune lets you approve it in Managed Google Play and assign it to Android devices enrolled in the MDM.

1. Log into your Microsoft Intune portal.
2. Select **Apps** > **Android** > **Add**.
   *The **Select app type** pane opens.*
3. From the **App type** drop-down menu, select **Managed Google Play app**, and then select **Select**.
4. In the **Managed Google Play** view, in the Search field, enter `WithSecure Elements`.
   *The **Apps** view opens.*
5. Select **WithSecure Elements Mobile Protection**.

6. On the view that opens, select **Approve** > **Approve**.
7. In the **Approval settings** tab, select **Keep approved when app requests new permissions**, and select **Done**.
   *The **Managed Google Play** view opens.*
8. Select **Sync** at the top left corner.
   *The **Android Apps** view opens.*
9. Select **Refresh** and then select **WithSecure Elements Mobile Protection**.
   *The **WithSecure Elements Mobile Protection** view opens.*
10. Under **Manage**, select **Properties**.
    *The **WithSecure Elements Mobile Protection Properties** view opens.*
11. Next to **Assignments**, select **Edit**.
    *The **Edit Application** view opens.*
12. In the **Assignments** tab, do the following:
    a) Under **Required**, select **Add all users**.
    b) Select **Review + save**.
    c) In the **Review + save tab**, select **Save**.

The WithSecure Elements Mobile Protection app has been added to Microsoft Intune MDM.

Next, add the app configuration policies.

Add the Android app configuration policies

Adds WithSecure Elements Mobile Protection configuration policies for managed Android devices.

The app configuration policy pushes the subscription key and other activation values to the app so it can activate automatically on assigned Android devices.

1. Select **Apps**.
   The Apps overview pane opens.
2. Under **Policy**, select **App configuration policies**.
3. Select **Add** > **Managed devices**
   The Create app configuration policy pane opens.
4. In the **Basics** tab, do the following:
   a) In the **Name** field, enter WithSecure Mobile Protection.
   b) From the Platform drop-down menu, select **Android Enterprise**.
   c) From the Profile type drop-down menu, select either **Personally-Owned Work Profile Only** or **Fully-Managed, Dedicated, and Corporate-Owned Work Profile**.
   d) Next to **Targeted app**, select **Select app**.
      The Associated app pane opens.
   e) Select **WithSecure Elements Mobile Protection**, and select **OK** > **Next**.

   The Settings tab opens.
5. Do the following:
   a) Under **Configuration Settings**, from the Configuration settings format drop-down menu, select **Use configuration designer**.
   b) Select **+Add**.
   c) On the pane that opens at the right, select the following:
      - Registration key
      - Alias (optional)
      - Email address (optional)

- Environment (optional)

d) Select **OK**.

e) Select the value types and enter the configuration values for the following configuration keys:

- fate_registration_key: value type: **String**; configuration value: `[WithSecure Elements Mobile Protection subscription key]`.

NOTE: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Management** > **Subscriptions**.

- alias: value type: **String**; configuration value:`{{username}}`
- email: value type: **String**; configuration value: `{{mail}}`
- env: value type: **Integer**; configuration value: `2`

NOTE: The `env` configuration key and its value define where the VPN endpoint connects to.

f) Select **Next**.
*The **Assignments** tab opens.*

g) Under **Included groups**, select **Add all users** and select **Next**.
*The **Review + create** tab opens.*

h) Select **Create**.

The app configuration policy was created and assigned.

You need to install the app on an Android device.

Grant permissions to an app

Grants an app permission for silent activation.

Grant the required permissions so the app can activate silently on managed Android devices.

1. Log in to the Microsoft Endpoint Manager administrator center.
2. Select **Apps** > **App configuration policies** > **Add** > **Managed devices**.

NOTE: You can choose to add either managed devices or managed apps. For more information, see Apps that support app configuration.

3. On the **Basics** page, enter the following details:
   - Name - a name for the profile that is shown in the portal
   - Description - a description for the profile that is shown in the portal
   - Device enrollment type - the default option is **Managed devices**
4. Under **Platforms**, select **Android Enterprises**.
5. Next to **Targeted app**, choose **Select app**.
   *The **Associated app** pane opens.*
6. On the **Associated app** pane, select the managed app that you want to associate with the configuration policy, and select **OK**.
7. Select **Next** > **Add**.
   *The **Add permissions** pane opens.*
8. Select the permissions that you want to override.

NOTE: The granted permissions override the default app permissions policy for the selected apps.

9. Set a permission state for each permission. You can select from the following options:
   - Prompt - ask the user to accept or deny
   - Auto grant - automatically approve without notifying the user
   - Auto deny - automatically deny without notifying the user
10. Select **Review + save**.
    Your settings are saved.

4.4.5 Deployment using IBM MaaS360 MDM

Deployment of WithSecure Elements Mobile Protection with IBM MaaS360 MDM, covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with IBM MaaS360, add and configure the app for the iOS and Android devices that MaaS360 manages.

Deploying the iOS app with IBM MaaS360 MDM

Adding and deploying the WithSecure Elements Mobile Protection iOS app in IBM MaaS360 MDM.

To deploy the iOS app with IBM MaaS360, add the WithSecure Elements Mobile Protection app and distribute it to your users.

Add the iOS app to IBM MaaS360 MDM

Adds the WithSecure Elements Mobile Protection iOS app to IBM MaaS360 MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

The integration consists of the following:

- Adding the app to the MDM from Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

1. Login into the IBM MaaS360 administrator portal as an administrator.
2. Open the **Apps** view.
3. Select **Add** and then **iTunes App Store App** from the drop-down list.
4. In the **App Details** tab, search and select the **WithSecure Mobile Protection** app.

Adjust the app's category if necessary.

5. Open the **Policies and Distribution** tab and select the distribution methods and groups that you want to use.
6. Open the **Configuration** tab.

   The configuration contains the following mandatory attribute:

   - *fate_registration_key* - the license key

   You can use the firstName, lastName, email, and alias keys to add additional user data to the policy configuration.
7. Select **Add**.

The WithSecure Elements Mobile Protection app is in the **App** list.

Distributing the iOS app

The WithSecure Elements Mobile Protection iOS app is delivered to the users in a defined distribution group.

The WithSecure Elements Mobile Protection iOS app is delivered to users through a distribution group that you define in IBM MaaS360. Assign the users who should receive the app to that group.

Deploying Android Enterprise with IBM MaaS360 MDM

Deployment of WithSecure Elements Mobile Protection in the Android Enterprise context with IBM MaaS360 MDM.

To deploy the app in the Android Enterprise context with IBM MaaS360, configure Android Enterprise, then add, configure, and distribute the WithSecure Elements Mobile Protection app.

Configure Android Enterprise

Configures Android Enterprise in IBM MaaS360.

NOTE: Prior to enrolling devices, you need to configure Android Enterprise.

1. On the IBM MaaS360 administration portal, select **Setup** > **Services**.
2. Under **Mobile Device Management**, **Enable Android Enterprise Solution Set Enable via Managed Google Play Accounts (no G-suite for business)**, select **here**.
   *The **Confirm Android Managed Google Play Accounts Enablement** window.*
3. Select **Enable**.
4. In the **Security Check** window, enter your password and select **Confirm**.
   Google Play opens.
5. On the **Bring Android to work** page, select **Get started** and do the following:
   a) Enter the name of your business and select **Next**.
   b) On the Contact details page, enter your name, email, and phone number (optional), select **I have read and agree to the Managed Google Play agreement** option, and then select **Confirm**.
6. Select **Complete Registration**.
   You have completed the setup.

Next, you need to add the WithSecure Elements Mobile Protection app.

Add the WithSecure Elements Mobile Protection app to IBM MaaS360

Adds the WithSecure Elements Mobile Protection app to IBM MaaS360 MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

Adding the app to the App Catalog makes it available to distribute to enrolled Android devices.

1. On the IBM MaaS360 administration portal, select **Apps** > **Catalog**.
2. On the App Catalog page, select **Add** > **Android** > **Google Play App**.
3. In the Search box, enter `WithSecure Elements Mobile Protection`.
4. Select **WithSecure Elements Mobile Protection**, and select **Select**.
5. In the Approve Permission window, select **Approve** to add the app.

Next, you need to configure the app.

Configure the app

Configures the WithSecure Elements Mobile Protection app in IBM MaaS360.

Configuring the app supplies the subscription key and other activation values so it can activate automatically once installed on a device.

1. In the Add Google Play App window, in the **Configuration** tab, select **Configure App Settings** and do the following:
   a) In the Registration field, enter the product subscription key.

NOTE: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Endpoint Protection** > **Subscriptions**.

   b) Enter your first and last name in the respective fields (optional).
   c) In the Alias field (optional), enter an alternate name.
   d) In the Email address field (optional), enter your email address
   e) In the Environment field (optional), enter 2.
2. Select **Add**.
   *The **Security Check** window opens.*
3. Enter your password and select **Confirm**.
   The app was added.

Distribute the app

Distributes the app to the selected targets.

After configuring the app, distribute it to the devices, groups, or targets you want to protect.

1. On the App Catalog page, under **WithSecure Elements Mobile Protection**, select **View**.
2. On the page that opens, at the top-right corner, select **Distribute**.
   The Distribute App window opens.

3. From the Target drop-down menu, select one of the options:
    - Specific device
    - Group
    - All devices
4. Select **Distribute**.

4.4.6 Deployment using Ivanti Endpoint Management

Deployment of WithSecure Elements Mobile Protection with Ivanti Endpoint Management (formerly known as MobileIron Cloud MDM), covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with Ivanti Endpoint Management (formerly MobileIron), add and configure the app for the iOS and Android devices that it manages.

Deploying the iOS app with Ivanti Endpoint Management

Deployment of the iOS app with Ivanti Endpoint Management.

To deploy the iOS app with Ivanti Endpoint Management, add the WithSecure Elements Mobile Protection app, configure app management, and set any additional configuration keys.

Add the WithSecure Elements Mobile Protection iOS app to Ivanti Endpoint Management

Adds the WithSecure Elements Mobile Protection iOS app to Ivanti Endpoint Management.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

To add the iOS app to Ivanti Endpoint Management:

1. On the Ivanti Endpoint Management administration portal, go to the **Apps** page and select **Add**.
2. Select **App Store**.
3. Search for `WithSecure Elements Mobile Protection`.
4. Select the app and then select **Next**.
5. Check that the app description is correct, and select **Next**.
6. Configure the app distribution.
7. Select **Next**.

Configure iOS app management

Configures iOS app management.

TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

1. On the **Configuration** page, select **iOS Managed App Configuration** and then select **+**.
2. Under iOS 7+ Managed App Settings, do the following:
   a) Enter a name for this configuration, for example, `WithSecure Elements Mobile Protection license configuration`.
   b) In the **fate_registration_key** field, enter your WithSecure Elements Endpoint Protection license key.
3. Distribute this configuration to the relevant devices or device groups.
4. Configure any other necessary settings.
5. Select **Done**.

Additional configuration keys

The following Ivanti Endpoint Management variables can be used to help identifying devices on WithSecure Elements Security Center.

TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

NOTE: The key names are case sensitive.

Table 7: Additional configuration keys

Key	Value
fate_registration_key	`ABCD-EFGH-IJKL-MNOP`
email	`$(userEmailAddress)`
first_name	`$(userFirstName)`
last_name	`$(userLastName)`
alias	`$(userDisplayName)`

Deploying the Android app with Ivanti Endpoint Management

Deployment of the Android app with Ivanti Endpoint Management, including manual configuration of WithSecure Elements Mobile Protection using the subscription key.

To deploy the Android app with Ivanti Endpoint Management, add the WithSecure Elements Mobile Protection app and configure app management.

Add the WithSecure Elements Mobile Protection Android app to Ivanti Endpoint Management

Adds the WithSecure Elements Mobile Protection Android app to Ivanti Endpoint Management MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

> **NOTE:** WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

To add the Android app to Ivanti Endpoint Management:

1. In the Ivanti Endpoint Management MDM administration portal, go to **Apps** and select **Add**.
2. From the menu, select **Google Play**.
3. Search for `WithSecure Elements Mobile Protection`.
4. Select the app, and then click **Select**.
5. Check that the app category is correct.
6. Optionally, add app information in the Description box.
7. Select **Next**.
8. Select whether you want to delegate the app to all spaces, and select **Next**.
9. Select the preferred distribution group and press **Next**.

Next, you need to configure the app.

Manually configure the Android app management

Manually configures the Android app management.

Configuring app management manually lets you set the activation, permission, and installation options the app needs on managed Android devices.

1. Under **App Configurations** > **Managed Configurations for Android**, select the plus icon.
   *The **Configuration Setup** view opens.*
2. Do the following:
   a) Enter a name for the configuration.
   b) Under **Managed Configurations**, select **Auto-launch on install**.
   c) Make sure that **Only push settings with values defined** is selected.
   d) Next to **Registration key**, enter the subscription key.

   > **NOTE:** You can find the subscription key in WithSecure Elements Security Center.

   e) In the Email address field, enter `${userEmailAddress}` as a value.
   f) Select **Manage Permissions**.

*The **Select Permissions** window opens.*

g) Select all the options, and then click **Select**.

h) Under **Runtime Permissions**, go through all the drop-down menus, and select **Auto Grant**, and then select **Next**.
*The **App Configurations** page opens*

3. Next to **Install on device**, select the plus icon, and do the following:
   a) Enter a name for the configuration setup.
   b) Turn on **Device Installation Configurations**.
   c) Select the **App Update Mode** option, and from the drop-down menu, select **High Priority**.
   d) Select **Next**.
   *The **App Configurations** page opens.*
4. Next to **Promotion**, select the plus icon, and do the following:
   a) Enter a name for the configuration setup.
   b) Select **Featured List**.
   c) Select **Next**.
5. Next to **Delegated Device Permissions**, select the plus icon, and do the following:
   a) Enter a name for the configuration setup.
   b) Select **Manage App Configurations**.
   c) Select **Next**
6. Select **Done**.
   The WithSecure Elements Mobile Protection is added to the App Catalog.

Configure the Android app using certificates

Configures the Android app using certificates.

Certificates offer an alternative to registration keys for activating the app on managed Android devices.

1. On the **Ivanti Endpoint Management** administration portal, go to the **Configurations** page and select **Add**.
2. Select **Certificate**.
3. Enter a name for the certificate.
4. Upload the WithSecure Elements certificate for WithSecure Elements Mobile Protection.

NOTE: You can find the certificate in WithSecure Elements Security Center.

5. Select **Next**.
6. On the next page, select the preferred option for deploying the certificate, and then select **Done**.

NOTE: The certificate must be deployed to the device, manually or automatically, to activate WithSecure Elements Mobile Protection.

Android Enterprise deployment with Ivanti Endpoint Management

Deployment of WithSecure Elements Mobile Protection in the Android Enterprise context with Ivanti Endpoint Management.

To deploy the WithSecure Elements Mobile Protection app in the Android Enterprise context with Ivanti Endpoint Management, add and configure the app for your managed Android devices.

Add the WithSecure Elements Mobile Protection app to Ivanti (Android Enterprise)

Adds the WithSecure Elements Mobile Protection app to Ivanti Endpoint Management in the Android Enterprise context.

Adding the app to Ivanti (Android Enterprise) sets up Google Play integration and configures the app so it can activate automatically once distributed to managed devices.

1. In theIvanti Endpoint Management administration portal, select **Admin** > **Google** > **Android Enterprise**.
   The Android Enterprise page opens.
2. Under **Begin Recommended Setup**, select **Authorise Google**.
3. Select **Complete sign-up**.
4. Select **Apps** > **App Catalog**, and select **+Add**.
   The Add App wizard opens.
5. In the Choose view, from the drop-down menu, select **Google Play**.
6. In the Search the Google Play store... box, enter `WithSecure Elements Mobile Protection`.
7. Select the app and then select **Approve** > **Approve**.
8. Select **Done** > **Select** > **Next**.
9. In the Describe view, select **Next**.
10. In the Delegate view, select **Next**.
11. In the Distribute view, select you preferred option and select **Next**
12. In the Configure view, next to **Managed Configurations for Android**, select the plus icon.
    The Configuration Setup page opens.
13. In the Name field, enter a name, and under **Managed Configurations**, do the following:
    a) In the Registration key field, enter the product subscription key.

    NOTE: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Management** > **Subscriptions**.

    b) Enter your first and last name in the respective fields (optional).
    c) In the Alias field (optional), enter an alternate name.
    d) In the Email address field (optional), enter your email address.
    e) In the Environment field (optional), enter 2.
14. Under **Distribute this App Config**, select **Everyone with App**, and select **Next**.
15. On the App Configurations page, select **Done**.
    *WithSecure Elements Mobile Protection is shown on the **App Catalog** page.*

4.4.7 Deployment using Miradore MDM

Deployment of WithSecure Elements Mobile Protection with Miradore MDM, covering Android and iOS devices.

NOTE: This deployment does not include creating and configuring users and devices.

To deploy the WithSecure Elements Mobile Protection app with Miradore, add and configure the app for the iOS and Android devices that Miradore manages.

Add the iOS app to Miradore MDM

Adds the WithSecure Elements Mobile Protection iOS app to Miradore MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

> **NOTE:** WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

1. In the Miradore administration portal, select **Management** > **Applications** from the left pane menu.
2. In the Actions menu, select **Add** > **iOS application**.
   The Add application wizard opens.
3. In the Add application wizard, do the following:
   a) In step 1, select **App Store** and then **Next**.
   b) In step 2, enter the following details:
      - Name: `WithSecure Elements Mobile Protection`
      - App Store ID: `1549210826`
      - App Store country: Choose the country that you want to use
      - Package name: `com.f-secure.mobileprotection`
      - Description: Enter any description that you want to use.
      - Select **Remove application when device is unenrolled**.
   c) Select **Create**.
   d) In step 3, make sure the information is correct and select **Close**.

Configure the iOS app in Miradore

Configures the WithSecure Elements Mobile Protection iOS app in Miradore MDM.

> **TIP:** By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

1. In the Miradore administration portal, double-click the `WithSecure Elements Mobile Protection` entry on the Application list.
2. Go to the **Configuration** tab and select **Add new**.
   The Create configuration setting view opens.
3. Add the following values for the first setting:
   - Setting: `fate_registration_key`
   - Data type: `String`
   - Value: Enter your subscription key

4. Select **Add** to add the new setting to the configuration.
   After you have configured this mandatory setting, you can add optional settings.
5. To add user details, select **Add new** and use the following values:

TIP: User details can help you to identify devices.

Table 8: Configuration keys

Key	Type	Description
email	string	Specifies a user activation email
env	integer	Specifies the environment where the application is activated. For customers using production, set this value to "2".
data_usage_permission	Boolean	Set to true if the administrator allows data collection; otherwise, set to false
diagnostic_usage_permission	Boolean	Set to true if the administrator allows diagnostic collection; otherwise, set to false
create_vpn_profile	Boolean	Set to true to allow creation of the VPN profile; otherwise, set to false

Add the Android app to Miradore MDM

Adds the WithSecure Elements Mobile Protection Android app to Miradore MDM.

Miradore MDM can provide the license information to the app either by using an XML file or the Install Referrer service of the Google Play store. Select the method that you want to use before you start adding the app to the MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

NOTE: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

1. In the Miradore administration portal, select **Management** > **Applications** from the left pane menu.
2. In the **Actions** menu on the right, select **Add** > **Android application**.
   The Add application wizard opens.
3. In the Add application wizard, do the following:

a) In step 1, select **Google Play store** and then **Next**.
b) In step 2, enter the following details:
   - Name: `WithSecure Elements Mobile Protection for Android`
   - Package name: `com.fsecure.mp.ucf`
   - Description: Enter any description that you want to use.
   - Notification to user: Enter any information that you want users to see.
   - Add shortcut to home screen: Select to create a shortcut to the app.
c) Add the following information to the **Install referrer** field:
   - If you want to use the Install Referrer service to deliver the license information, use the install referrer string that can be found from WithSecure Elements service. Look for **Google Play download URL** with the WithSecure Elements Mobile Protection activation string. Copy the latter part of the string, starting from utm-medium. If you want to send additional information to the app, you can add extra elements to the activation string.

4. Select **Create**.
5. In step 4, make sure the information is correct and select **Close**.

4.4.8 Deployment using Jamf Pro MDM

Deployment of WithSecure Elements Mobile Protection using Jamf Pro MDM to iOS and iPadOS devices.

To deploy the WithSecure Elements Mobile Protection app with Jamf Pro, buy the app licenses, then configure the app, notifications, and the Safari browsing-protection extension for your managed iOS and iPadOS devices.

Buy licenses for your devices

Buys licenses for your devices.

The WithSecure Mobile Protection app is free from the App Store. To distribute the app via the Jamf Pro MDM, you need to buy Volume Purchase Program (VPP) licenses for the devices on which you want to install the WithSecure Mobile Protection app. This amount must be equal to the amount of the WithSecure Mobile Protection licenses that you have bought from WithSecure.

To buy the required licenses:

1. Log in to the Apple Business Manager portal.
2. Go to **Apps and Books** and search for WithSecure Mobile Protection.
3. Under **Buy Licenses**, enter the amount of WithSecure Mobile Protection licenses that you have bought from WithSecure, and select **Get**.

   The purchase is synchronized with your Jamf Pro within 15 minutes.

Configure the app for iOS and iPadOS devices

Configures the With Secure Mobile Protection app for iOS and iPadOS devices in Jamf Pro MDM.

TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

To configure the app:

1. Log in to Jamf Pro.

2. Select **Devices** > **Mobile Device Apps** > **WithSecure Mobile Protection** > **Edit**.
3. In the General tab, configure the following:
   a) Under **Distribution Method**, choose your preferred method.
   b) Select the **Automatically force app updates** option.
   c) To prevent users from removing WithSecure Mobile Protection, we recommend turning off the **Allow users to remove app (iOS 14 or later)** option.
4. In the **Managed Distribution** tab, select **Assign Content Purchased in Volume**.

   To prevent users from removing WithSecure Mobile Protection, we recommend turning off the **Allow users to remove app (iOS 14 or later)** option.

   NOTE: "Location" must match the VPP location where you bought the WithSecure Mobile Protection app.

5. In the **App Configuration** tab, do the following:
   a) Copy the following configuration into the **Preferences** box:

```
<dict>
 <key>fate_registration_key</key>
 <string>ENTER-THE-SUB-KEY-HERE</string>
 <key>email</key>
 <string>$EMAIL</string>
 <key>alias</key>
 <string>$USERNAME</string>
 <key>env</key>
 <string>2</string>
</dict>
```

   NOTE: Replace "ENTER-THE-SUB-KEY-HERE" with your WithSecure Mobile Protection subscription key. You can find your subscription key for WithSecure Mobile Protection in WithSecure Elements Security Center.

   NOTE: The "alias" key helps you identify devices in the WithSecure Elements Security Center. If you prefer a different value for "alias", Jamf offers other variables to consider. Refer to "Managed App Configuration Variables" in the Jamf Pro User Guide for more details. However, if you prefer to not use an alias, you may remove that key and the associated string from your configuration as this is an optional setting.

   b) Configure the scope to include the devices on which you want to install With Secure Mobile Protection.

Configure notifications for the app

You can configure how notifications are shown via a Configuration Profile.

NOTE: Configuring notifications for the devices is optional.

To configure notifications for WithSecure Mobile Protection:

1. In Jamf Pro, select **Devices** > **Configuration Profiles** > **New**.
2. In the Name field, enter `WithSecure Mobile Protection Notifications`.
3. Select **Notifications payload** > **Add**, and do the following:
   - **App Name**: `WithSecure Mobile Protection`
   - **Bundle ID**: `com.f-secure.mobileprotection`

Configure the alert settings to your organizations preferences, and then scope the policy to match.

4.4.9 Deployment using Samsung Knox

Deployment of the WithSecure Elements Mobile Protection app with Samsung Knox to Android devices.

> **NOTE:** This deployment does not include creating and configuring users and devices.

To deploy the WithSecure Elements Mobile Protection app with Samsung Knox, add and configure the app for your managed Android devices.

Deploying the Android app with Samsung Knox

Deployment of the Android app with Samsung Knox.

To deploy the Android app with Samsung Knox, add and configure the WithSecure Elements Mobile Protection app for your managed Android devices.

Add the Android app to Samsung Knox

Adds the WithSecure Elements Mobile Protection Android app to Samsung Knox.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

> **NOTE:** WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides

To add the Android app to Samsung Knox:

1. Log in to your Samsung Knox console.
2. Select **Application**.
   The Application page opens.
3. Select **Add**.
4. On the Select Application Type screen, select **Android platform** > **public Managed Google Play**, and then select **OK**.
5. On the Add Application page, enter `WithSecure Elements Mobile Protection` and search for the application.

   > **NOTE:** To change the country of the selected platform, select the check box next to **Set Country** and then select the country.

6. In the search results, first select the application that you want to add and then **Select**.
7. Edit the following imported information, if necessary:
   - Name - enter the name of the application

- Category - select the category for the application. By selecting **Manage category**, you can add or edit the application categories.
- Description - enter a description for the application

8. Choose one of the following options to continue:
   - Select **Save & Assign** to save the information and proceed to assign the application by selecting **Continue**.
   - Select **Save** to save the information and return to the application list. You can assign this application later.

Assign and configure the Android app

Assigns and configures the Android app.

IMPORTANT: When you assign a profile to a parent organization, its sub-organizations inherit the profile. However, sub-organizations do not inherit Applications and Contents.

To assign and configure the Android app on Samsung Knox:

1. Select **Application**.
   The Application page opens.
2. Select **WithSecure Elements Mobile Protection** and then select **Assign**.
   The Assign Application page opens.
3. Configure the following assignment settings:
   - Target device - you can select one of the following options: **Android Enterprise**, **Android Legacy**, or **Android Enterprise + Legacy**.
   - Installation area- shows the designated installation area
   - Installation type - select one of the available options:
     - **Manual** - allows device users to install the application manually
     - **Automatic (Removable)** - sets the application to be installed automatically. Device users are allowed also to manually remove the application.
     - **Automatic (Non-Removable, Android Management API only)**
   - Auto-run after installation (Non-Android Management API) - you can select to set the application to start immediately after installation.
   - Auto update model - the available options are **Default update**, **High Priority**, and **Postponed (90 days)**.
4. Next to Managed Configuration, select **Set configuration** and do the following:
   - In the Managed configuration field, enter a descriptive name, for example, `Work`.
   - In the Registration key field, enter the WithSecure Elements Mobile Protection subscription key.
   - In the Alias field, enter the following: `$username$`.
   - In the Email address field, enter `$emailaddress$`.
   - In the Environment field, enter `2`.

NOTE: Registered devices to WithSecure Elements will be shown with Email Address when you configure the value `$ emailaddress$`.

5. Select **Save** to save the changes.
6. Under Target, select the group to which you want to assign the application.

4.5 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 **Add new device** option next to **Devices** is visible only at a company level. If the *scope selector* is set to show all customer companies, select the company you wish to manage.

   *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.*

   > **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:** 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.

4.5.1 Install and activate the app on Android devices

Instruct the users to follow these steps to install the app on their Android devices.

> **NOTE:** In the following steps, "you" refers to end users.

You receive an email from your administrator instructing you to install the app. The email contains a link for installing the app on one device and a link to activate your license.

To install the app:

1. Open the invitation email.
2. Select the link next to Android.
   You are redirected to Google Play Store where you can download and install the WithSecure Mobile Protection app.
3. After you have installed the app on your device, go back to the installation email and select **Activate for Android** to activate the subscription.

NOTE: The activation link is valid for 29 days, but you can only use the link once. If you log in to the app using the username and password that are provided in the email, but you do not manage to activate the license, you can try using the activation link. If you, however, first select the activation link and, for some reason, it does not work, you can no longer manually enter the credentials.

   The WithSecure Mobile Protection app opens.
4. When asked, select **Allow** to give the app the required permissions.

NOTE: The app needs permission to access your photos, media, and files to be able to scan for harmful items.

The app is installed and activated on the Android device.

4.5.2 Install and activate the app on iOS devices

Instruct the users to follow these steps to install WithSecure Elements Mobile Protection on their iOS devices.

NOTE: In the following steps, "you" refers to end users.

You receive an email from your administrator instructing you to install the app. The email contains a link for installing the app on one device and a link to activate your license.

To install the app:

1. Open the invitation email.
2. Select the link next to iOS.
   You are redirected to AppStore where you can download and install the WithSecure Mobile Protection app.
3. After you have installed the app on your device, go back to the installation email, select **Activate for iOS** to activate the subscription.

NOTE: The activation link is valid for 29 days, but you can only use the link once. If you log in to the app using the username and password that are provided in the email, but you do not manage to activate the license, you can try using the activation link. If you, however, first select the activation link and, for some reason, it does not work, you can no longer manually enter the credentials.

   The WithSecure Elements Mobile Protection app opens.
4. When asked, select **Allow** to give the app the required permissions.

NOTE: The app needs permission to notify you about important events.

The app is installed and activated on the iOS device.

Chapter 5
Managing profiles

Topics:

- Assigning settings to clients
- Administering profiles
- Controlled Updates
- Managing profiles in Elements EPP for Computers and Elements EPP for Servers (Windows)
- Managing profiles in Elements EPP for Computers (Mac)
- Managing profiles in WithSecure Elements EPP for Linux
- Managing mobile device profiles

Managing profiles

Profiles are collections of security settings you apply to the workstations, servers, and mobile devices in your account.

You can control what users can do with the security settings on a computer, or on a mobile device that has WithSecure Elements Mobile Protection installed. Profiles are a collection of settings that can be applied to devices. You can use them for certain groups of users or devices, such as:

- Novice users: A profile for novice users may restrict their rights to change their security settings.
- Computer type: laptop or desktop computer. A profile for a laptop computer is designed to protect users when they access the Internet from unsafe locations, such as cafes with free Internet access. A profile for a desktop computer is designed to protect access to the Internet from a fixed location.

NOTE: A predefined default profile is assigned automatically if no other profiles are defined. Predefined profiles are designed to bother users as little as possible.

We recommend that you create your own profiles with stricter settings than the predefined ones. You can use an existing profile as a basis for a new profile.

In a more secure profile setup, for example, settings are locked, tamper protection is on, files cannot be run from an external USB storage, and users cannot uninstall products.

5.1 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.

5.1.1 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.

5.1.2 Specify profile ID during Elements Agent installation

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

To specify the profile ID:

1. Copy the profile ID from the profile settings as follows:
   a) Under **Security configurations**, select **Profiles**, and then select a profile.
   b) Edit the profile that you want to be assigned.
   c) Copy the profile ID that is shown at the top of the profile settings.

2. If you install the Elements Agent from command line or from a script, you can add the parameter to the command by substituting the number in the example with what you see in your own profile:

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

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

```
PROFILE_ID=117525
```

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

5.1.3 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.

5.2 Administering profiles

Profiles define configuration settings that can be applied to endpoints. Managing profiles allows administrators to standardize security policies across multiple devices efficiently.

Profiles are collections of predefined settings that control how endpoints behave and enforce security policies. By using profiles, you can:

- Apply consistent configurations to multiple clients.
- Simplify policy updates and reduce manual configuration errors.
- Export and import profiles for reuse across environments.

5.2.1 Set a default profile for a group in Active Directory

You can set a default profile for a group based on its location in an Active Directory hierarchy.

You can set and specify a default profile for any group in the Active Directory hierarchy. If you do not set a default profile, the device that you add inherits the default profile from the parent group.

When you add a new device to WithSecure Elements EPP, the system automatically receives information about the Active Directory structure from the new the device.

NOTE: A default Active Directory profile is assigned only to new devices that are added to WithSecure Elements Security Center. If you turn off the **When a device changes its AD group, automatically assign the profile of that AD group to that device** setting and the location of a device in the AD hierarchy changes, the device profile does not change; if you turn on the setting and the device location changes, the device profile is updated with the new AD default

profile within ten minutes. If the setting is off and you apply a profile manually, when the location of a device in the AD hierarchy changes, the device profile remains as is.

To set a default profile for an Active Directory group:

1. Go to **Profiles** and select **Default profiles**.
2. Under **Active Directory**, go to the Active Directory group whose default profile you want to change.
3. In the **Menu** column, select **Change**.
   *The **Change default profile** window opens.*
4. From the drop-down menu, select a default profile, and select **Change**.

NOTE: You can select a profile separately for WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers.

5.2.2 Edit profiles

When you edit an existing profile, the changes that you make are enforced on all the computers with that profile.

To edit a profile:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select one of the tabs.
3. Select the profile that you wish to edit.
4. Select **Save and Publish** to save your changes to the current profile.

NOTE: If you want to use the edited settings in multiple profiles, select **Save and Publish to multiple profiles**. However, note that only switchable (on/off) settings are saved when you publish your changes to multiple profiles.

The changes you made to the profile settings are applied to all the devices with the selected profiles.

5.2.3 Export profiles

In WithSecure Elements Security Center, you can export a profile as a JSON file.

To export a profile:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Open the profile that you want to export.
3. At the top-right corner, select , and then select **Export profile**.
   You can store the exported profile or edit it with a JSON editing tool.

5.2.4 Import profiles

You can import a profile to another profile in WithSecure Elements Security Center.

NOTE: You can import not only already exported Elements Endpoint Protection profiles but also other exported files. You can, for example, import a profile that was exported from WithSecure Policy Manager.

To import a profile:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Open the profile to which you want to import the already exported profile.
3. Select
   
   ,
   and then select **Import profile**.
   The profile is imported to the selected profile in a JSON file. All the changed settings are highlighted.
4. Review the changes and do one of the following:
   - Select **Save and publish** to save the changes.
   - Select **Cancel** to reject the changes.

5.2.5 Remove a profile

When you remove a profile, it is deleted from WithSecure Elements Security Center.

The removed profile is not deleted from the actual device.

To remove a profile:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select next to the profile that you want to delete.
3. Select **Delete profile** and then select **OK**.

   CAUTION: Deleting a profile is permanent. Make sure that you selected the correct profile.

   The profile is deleted from Elements Security Center.

5.2.6 Assign profiles

Assign a security profile to the devices you manage.

To assign a profile:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the devices to which you want to assign a profile.
3. At the bottom of the page, select **Assign profile**.
4. From the drop-down menu, select the profile that you want to use.
5. Select **Assign**.

The selected profile is assigned to the selected devices.

5.2.7 Compare profiles

You can select profiles to compare and copy values from one profile to another.

To compare profiles:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Computers** or **For Windows Servers** tab.

3. Select ••• next to the profile that you want to compare, and then select **Compare and edit profiles**.
4. On the **Select profiles to compare** page, select one or more profiles to compare, and then select **Next**.
   A page opens with a table that shows those settings that are different in the selected profiles. The differences are bolded.

   NOTE: Only two profiles are visible at a time. If you selected more, from the drop-down menus at the top of the page, you can select which of the selected profiles you want to compare.

5. To copy values from one profile to another, use the right and left arrows.

5.2.8 Prevent users from changing computer profile settings

You can choose to lock or unlock each setting separately or all the settings at the same time to prevent users from changing them.

NOTE: A profile is 'read only' if it has a black lock next to it. It means that you cannot, for example, change a setting to be edited by an end user.

To lock the profile settings:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a custom profile that you want to lock or unlock.
   *The **Profile** page opens.*
3. Select ••• at the top-right corner and then select one of the following options:

Table 9: Lock and unlock options

Lock all settings	Locks all the settings that have a lock symbol displayed beside them on the current page. After this, the users cannot change these settings.
Unlock all settings	Unlocks all the settings that have a lock symbol displayed beside them on the current page. After this, the users can change these settings.

5.2.9 Managing tables

You can export data from a table in the selected profile and replace it with or import it to the same table or to another, similar table in another profile in WithSecure Elements Security Center.

These options allow you to customize the tables, export the data, edit the data in the exported file in a text editor, and upload it to the same or another profile.

NOTE: You can only import the exported data into a similar table. If you export data from the Application control exclusion rules table in one profile, you can import the data only to the Application control exclusion rules table either in the same or another profile. You cannot import it, for example, to a DeepGuard protection rules table.

Export data from tables

Exports data from a table to a `.JSON` file.

To export data from a table:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the desired profile.
3. On the **Profile** page, select the relevant setting, and make sure the setting is turned on.
   To export data, for example, from the Exclusion rules table, select **Application control** > **Exclusions**. The **Exclusion rules** table opens.
4. At the top right corner of the table, select ··· and then select **Export to file (JSON)**.

   NOTE: If the ··· icon is not visible, make sure the relevant setting is on.
5. Save the exported `.json` file.

   NOTE: You can edit the exported file in a text editor before importing it to the same or another profile.
6. Select **Done**.

Import data to tables

Imports data to a table in the selected profile.

When you use the **Import from file (JSON)** option, the already existing entry in the table is not updated or deleted, only the new entry is added.

NOTE: You can import the exported data only into a similar table. If you export data, for example, from the **Application control exclusion rules** table in the selected profile, you can import the data only to another Application control exclusion rules table, either in the same or another profile. You cannot import it, for example, to the DeepGuard protection rules table.

To import data:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the desired profile.
3. On the **Profile** page, select the relevant setting, and make sure the setting is turned on.
   To import data, for example, to the Exclusion rules table, select **Application control** > **Exclusions**. The **Exclusion rules** table opens.
4. At the top right corner of the table, select ··· and then select **Import from file (JSON)**.

   NOTE: If the ··· icon is not visible, make sure the relevant setting is on.
5. Navigate to the exported `.json` file, and import it.

NOTE: When you import data from a `.json` file, non-unique values may not be imported or they are imported only partially. In the latter case, the application indicates that you need to complete the values that were not imported. In such a case, we recommend that you use the **Replace from file (JSON)** option.

6. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

Replace data in tables

Replaces data in a table with the values from a `.json` file.

When you select **Replace from file (JSON)**, all the existing values in the table are deleted and replaced with the values in the `.json` file.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the desired profile.
3. On the **Profile** page, select the relevant setting.
   To replace data in, for example, the Exclusion rules table, select **Application control** > **Exclusions**. The **Exclusion rules** table opens.
4. Make sure the setting is turned on.
5. At the top right corner of the table, select and then select **Replace from file (JSON)**.

NOTE: If the icon is not visible, make sure the relevant setting is on.

6. Navigate to the exported `.json` file and replace the data in the table.
   All values in the table are deleted and replaced with the data in the imported `.json` file.
7. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

5.3 Controlled Updates

Controlled Updates lets you control when devices update to new WithSecure Elements agent versions, instead of updating as soon as they are released.

By default, devices update to new WithSecure Elements agent versions automatically, as soon as WithSecure releases them. With Controlled Updates, you decide when and how devices receive these updates instead. You can:

- Update manually, on your own schedule.
- Update automatically, but only during times that you define.
- Test updates on a small group of devices before they reach your whole fleet.

Controlled Updates is supported on Windows, macOS, and Linux devices. Whichever mode you choose, the upgrade itself is silent and works the same way as a regular update.

Update modes

The **Access to client software** setting in the profile editor determines how devices receive updates. It has three modes:

Automatic updates — Devices update automatically as new versions are released. This is the default mode. It has two submodes:

- **Generally available** — Devices receive updates as WithSecure rolls them out to the general public. This is the default submode.
- **Early** — Devices receive updates before the general release: agent and engine updates arrive about one week early, and security definition updates arrive about two hours early.

> **IMPORTANT:** We recommend assigning a small, representative group of devices to Early, so that you catch problems before they reach your whole fleet.

Controlled updates - Manual — Devices stay on the release group version that you choose, until you change the profile to point to a different version.

Controlled updates - Scheduled — Devices move to the latest available release group automatically, but only during a schedule that you define.

> **NOTE:** Each device profile has its own **Access to client software** setting. Create separate profiles for different groups of devices, for example a pilot group using **Early** and a production group using **Controlled updates - Scheduled**.

> **NOTE:** Controlled Updates applies to the agent software and engine components. Security definition updates continue to update on their own schedule and are not affected by the update mode, except in **Early** submode, which also delivers definitions ahead of the general release.

Choosing the right mode

Table 10: Update mode by goal

Goal	Recommended mode
Stay current automatically with minimal effort	**Automatic updates - Generally available**
Validate updates before they reach your whole fleet	**Automatic updates - Early**, on a pilot group of devices
Keep devices on a known, stable version and update at your own pace	**Controlled updates - Manual**
Move to each new release automatically, but only at predictable times	**Controlled updates - Scheduled**

5.3.1 Release groups

A release group is a validated bundle of WithSecure Elements agent components, published on a quarterly cadence.

WithSecure publishes a new release group on the second Tuesday of the second month of each quarter: February, May, August, and November.

Each release group has an incremental version number. The number identifies the release group's order, not the month it was published. When you set **Access to client software** to **Controlled updates - Manual**, you select which release group version the devices in that profile use. Devices stay on that version until you change the profile to point to a different release group.

NOTE: To see the release group version currently installed on a device, check the device inventory in the Elements Security Center.

Release group retirement

WithSecure retires older release groups after a set support period. After a release group reaches its end-of-support date, devices on that version must upgrade, regardless of the profile setting.

IMPORTANT: One month before a release group's end-of-support date, WithSecure warns you with a host issue in the **Endpoint Protection** dashboard.

5.3.2 Update schedule

An update schedule defines when devices set to Controlled updates - Scheduled check for and install the latest release group.

An update schedule controls timing only. It does not control which version devices install. Whatever release group is the latest available when the check runs is the one that devices install.

When you configure the schedule, you set a recurrence, for example weekly or monthly, and a one-hour time window during which the check runs.

NOTE: If a device is offline when its scheduled check time arrives, it checks the next time it comes online, rather than waiting for the next scheduled interval.

How the check works

1. The device checks WithSecure's distribution infrastructure for the latest available release group.
2. If that release group is newer than the one currently installed, the device upgrades to it.
3. If no newer release group is available, the device stays on its current version until the next scheduled check.

Example

You set the schedule to the first day of each month. WithSecure publishes release group version 2 on the second Tuesday of May. On June 1, the device checks, finds version 2, and upgrades to it. If version 2 had not been published yet by June 1, the device would stay on version 1 and check again on July 1.

5.4 Managing profiles in Elements EPP for Computers and Elements EPP for Servers (Windows)

Profile management in WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers software.

A profile is a bundle of settings that you assign to the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers clients on Windows. This section describes how to create a profile and configure its settings, including scanning, browsing protection, the firewall, device control, and automated tasks.

5.4.1 Create a new computer profile

You can create profiles that can be assigned to specific computers.

To create a new profile:

1. Log in to WithSecure Elements Security Center.
2. Under **Security Configurations**, select **Profiles**.
   *The **Profiles** page opens.*
3. Select the **For Windows Computers** or **For Windows Servers** tab, and then select **Create a profile**.

   > **NOTE:** Alternatively, select ⋯ and then **Clone profile** to use one of the default security profiles as a basis.

   *The **Profile for Windows Computers** or **Profile for Windows Servers** page opens.*
4. Enter a name and description for the new profile, and select a type for the new profile.
5. Make desired changes to the settings, and then select **Save and Publish**.

   > **NOTE:** You can also configure the profile as the default for a specific device type or based on Active Directory group membership.

   The new profile is created.

5.4.2 Configuring general settings for Windows

General settings control global behavior of the Windows endpoint client, including user interface visibility, integration features, BitLocker management, licensing notifications, and user permissions.

The General settings contain configuration options that define how the endpoint protection client behaves on managed devices. These settings let you control:

- Feature availability
- User interaction with the client application
- Integration with operating system security capabilities

These options are typically configured during policy creation. They apply to all Windows devices that are assigned to the policy.

Configure access to client software for Windows

Configure how Windows devices receive new WithSecure Elements agent versions.

The **Access to client software** setting controls how Windows devices receive new WithSecure Elements agent versions. Choose **Automatic updates**, **Controlled updates - Manual**, or **Controlled updates - Scheduled**, depending on how much control you want over update timing.

To configure access to client software:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers** or **For Windows Servers** tab.
3. Select one of the profiles.
4. From the menu on the left, select **General settings**.
5. In the **Define access to client software** dropdown, select a mode.
   - **Automatic updates** updates the device automatically as new versions are released.

- **Controlled updates - Manual** keeps the device on a release group version that you choose.
- **Controlled updates - Scheduled** updates the device automatically, but only during a schedule that you define.

6. If you selected **Automatic updates**, choose a submode: **Generally available** or **Early**.

   Early devices receive updates before the general release: agent and engine updates arrive about one week early, and security definition updates arrive about two hours early.

   IMPORTANT: We recommend assigning a small, representative group of devices to **Early**, so that you catch problems before they reach your whole fleet.

7. If you selected **Controlled updates - Manual**, select the release group version to assign to this profile.
8. If you selected **Controlled updates - Scheduled**, set the recurrence, day, and one-hour time window for the update check.
9. Select **Save Profile** to apply your changes.

Integrate EDR sensor on Windows

Configure settings to integrate the EDR sensor on Windows endpoints.

Follow these steps to enable and configure the EDR sensor using WithSecure Elements Connector.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows** tab.
3. Choose the profile you want to edit.
   *The **Profile for Windows** page opens.*
4. From the menu on the left, select **General settings**.
5. Turn on **EDR sensor** to enable endpoint detection and response on devices with an EDR subscription.

   NOTE: We strongly recommend to keep this setting turned on. If disabled, EDR will not detect or alert on attacks against the endpoint.

6. Turn on **Advanced response** if you want to activate the advanced response module in EDR.

   With Advanced response, you can access detailed system information that may include sensitive data. Before turning this feature on, you should ensure that its use complies with applicable worker privacy legislation and any relevant customer or contractual requirements.

   NOTE: By using this feature, you confirm that you are legally permitted and have obtained all necessary consents under applicable law.

7. Turn on **WMI provider** if you want external tools or scripts to query the WithSecure Elements Agent status through Windows Management Instrumentation (WMI).

   If you do not use monitoring or management tools that rely on WMI queries, leave this setting off.

8. Select **Save profile** to apply your changes.

Manage BitLocker on Windows

Configure BitLocker management options to collect recovery keys and turn on disk encryption on managed devices.

Use the BitLocker management settings to control disk encryption and recovery key collection on Windows devices.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows** tab.
3. Choose the profile you want to edit.
   *The **Profile for Windows** page opens.*
4. From the menu on the left, select **General settings**.
5. Turn on **Collect BitLocker recovery keys** to collect all BitLocker recovery keys that are available on the device.

   NOTE: Confirm that the device reports the recovery keys in the management portal.

6. In **BitLocker protection**, select which disks BitLocker protection is on.
   - **No changes**: No changes are made to BitLocker settings on the device.
   - **System only**: BitLocker protects only the system disk.
   - **All fixed**: BitLocker is turned on for all fixed disks in the system.
7. Turn on **Request to set a PIN code for extra protection** for additional device protection.

   The PIN adds an additional layer of protection by requiring the a PIN when the system starts.

The BitLocker settings apply to the devices that use this profile.

Set up license expiration notifications

You can set up notifications about license expiration.

To set up the notifications:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Computers** or **For Windows Servers** tab.
   *The **Profiles** page opens.*
3. Select the profile that you want to edit.
4. Under **General settings**, go to **License expiration**.
5. Under **Show notifications**, turn the notifications on.
   When this setting is on, users see notifications about expiring or expired licenses.
6. Under **Days before license expiration**, enter how many days before the license expiration you want to show a notification.

   NOTE: If you enter a negative value, a notification is shown after the license has expired.

7. In the **A customized message about license expiration** field, you can enter a message that you want to show to users before their license expires.

> **NOTE:** You need to keep the message as short as possible for it to show properly in the notification area.

Manage security features on Windows

Control whether users can uninstall the WithSecure Elements Agent or turn off security features on the device.

Use these settings to control whether users are allowed to uninstall the product or turn off its security features.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows** tab.
3. Choose the profile you want to edit.
   *The **Profile for Windows** page opens.*
4. From the menu on the left, select **General settings**.
5. Select **Allow user to uninstall the product** to control whether users can uninstall WithSecure Elements Agent.

   If this setting is turned on, users can uninstall the agent from the device. If a password is configured, they must enter the password to uninstall the product.

   > **IMPORTANT:** We recommend that you keep this setting turned off to prevent users from removing the agent.

6. Select **Allow users to turn off all security features** to control whether users can turn off WithSecure security features.

   If this setting is turned on, users can turn off the WithSecure protection features on the device.

   > **IMPORTANT:** We strongly recommend that you keep this setting turned off to ensure that security features remain active.

7. Specify a password in the **Password** field.

   This setting is optional. If a password is configured, users must enter the password to perform restricted actions such as uninstalling the product or turning off security features.

   If no password is specified, users can perform these actions without authentication if the settings are turned on.

The uninstallation and security-feature settings apply to the Windows devices that use this profile.

5.4.3 Configuring communication settings for Windows

Communication settings control how Windows endpoint clients connect to the service, download updates, and route network traffic through proxy servers or WithSecure Elements Connectors.

Communication settings define how managed Windows endpoint clients connect to the service infrastructure. These settings determine whether clients connect directly to cloud services or route traffic through configured proxy servers or WithSecure Elements Connectors.

You can use these options to align endpoint communication with organizational network policies. This is especially useful in environments where outbound internet access must be controlled or routed through specific gateways.

Configure proxy settings

Configure how Windows endpoint clients route network traffic through an HTTP proxy and how updates are downloaded.

Follow these instructions to configure proxy settings for Windows clients:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Communication**.
4. Go to **Communication settings**.
5. Select **Use HTTP proxy** to route client communication through a proxy server.

   When HTTP proxy is in use, all connections made by product components use an HTTP proxy. If the proxy cannot be reached, the client automatically falls back to a direct connection.

   This setting also applies to standalone Endpoint Detection and Response agents.

   NOTE: Using the proxy from the user's browser settings requires a user to be logged in. The proxy configuration can also be changed by the user. As the proxy is selected from a logged-in user and cannot be detected if no user is logged in, we do not recommend using proxy settings from user browser configuration for servers.

6. Select **Prefer connection through proxy** if you want clients to prioritize proxy connections.

   By default, clients use the connection method that succeeded during the last connection. If the proxy fails, the client may switch to a direct connection and continue using it until it becomes unavailable.

   This setting forces the client to attempt using the proxy for every connection.

7. Select **Hide proxy configuration** to hide proxy settings from the local client interface.

   When hidden, the proxy configuration panel is not visible in the local user settings interface on endpoint devices.

8. Select **Use HTTPS to download updates** to download updates over encrypted connections.

   HTTPS improves privacy and helps meet certain compliance requirements. However, HTTPS traffic cannot be cached by proxies, which may increase network traffic in environments where update caching is used.

The proxy settings apply to the Windows computers that use this profile.

Configure Software Updater communication settings

Configure how Software Updater connects to update services using an HTTP proxy or a WithSecure Elements Connector.

Software Updater communication settings determine how the Software Updater component connects to update services. You can configure the component to use a dedicated HTTP proxy or route traffic through a WithSecure Elements Connector.

1. Under **Security Configurations**, select **Profiles** on the sidebar.

*The **Profiles** page opens.*

2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Communication**.
4. Select **Use HTTP proxy** to configure Software Updater to use an HTTP proxy.

   When using HTTP proxy, Software Updater attempts to connect to update services through the configured HTTP proxy. If the proxy cannot be reached, Software Updater automatically falls back to a direct connection.

5. Select **Use WithSecure Elements Connector** to route Software Updater traffic through Elements Connector.

Use WithSecure Elements Connector with a Computer profile

WithSecure Elements Connector is provided by WithSecure to minimize the bandwidth usage while downloading updates to WithSecure Elements EPP for Computers clients.

This proxy caches GUTS2 updates -- the malware signature database. If Elements Connector is not available, WithSecure Elements EPP for Computers clients automatically fall back to accessing GUTS2 directly.

To configure WithSecure Elements Connector and use it with WithSecure Elements EPP for Computers profiles:

1. Download the latest version of WithSecure Elements Connector.
2. Install WithSecure Elements Connector for your platform:
   - For Windows: Follow these instructions, Installing Elements Connector on Windows.
   - For Linux: Follow these instructions, Installing Elements Connector on Linux.
3. Configure a profile to use WithSecure Elements Connector:
   a) Under **Security Configurations**, select **Profiles**.
   b) Select the profile that you want to edit.
   c) Under **General**, edit the **WithSecure Elements Connector** setting and specify the address of the Connector server that you installed.

   NOTE: By default, WithSecure Elements Connector uses port 80 . To use HTTPS address/port, follow the Configuring Elements Connector as a proxy instructions to configure TLS certificates. Make sure the port is not blocked by the Windows firewall.

   d) If you want to use Software Updater, open the **Software Updater** tab, edit the **WithSecure Elements Connector** setting and specify the address of the Connector server that you installed. Also select an appropriate value for the **Use WithSecure Elements Connector** setting.

   NOTE: By default, WithSecure Elements Connector uses TLS and port 443. Follow the Configuring Elements Connector as a proxy instructions to configure TLS certificates. Make sure the port is not blocked by the Windows firewall.

   e) If the endpoint computers do not have direct internet connection and you want to use Elements Connector as an ultimate proxy, open the **General** tab and specify the address of the Connector server that you installed under **Manually defined proxy address** (Windows profiles) or **Remotely managed proxy address** (Mac profiles).

NOTE: The ultimate mode extends the HTTP host interface (port 80 by default). Make sure the port is not blocked by the Windows firewall.

4. After you have assigned the profile, verify it on the client:
   a) Right-click the client from its tray icon and select **Check for updates**.
   b) When the **Settings** window opens, check that WithSecure Elements Connector address value is specified in the **Connection** > **Update server** field.
   c) Select **Check now**.

      The check should run without any errors.

5.4.4 Configuring scanning settings for Windows

Scanning settings define how the endpoint protection client detects and handles malware, manages removable media scanning, and applies global exclusions across security scans.

Scanning settings control how the Windows clients monitor files and system activity for malicious content. These settings determine how threats are detected, how removable storage devices are handled, and how scan notifications are presented to users.

Configure common scanning settings on Windows

Configure how Windows endpoint clients monitor malware, handle removable media, and show notifications.

Common scanning settings control how the endpoint client monitors system activity for malware and how scanning-related behavior is applied on managed devices. These settings affect malware detection behavior, removable media handling, user notifications, and disk space usage during scanning.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Scanning settings**.
4. Under **Common scanning**, configure the **Malware monitoring mode**.

   The malware monitoring mode determines how the client handles detected threats.

NOTE: In modes other than **Block**, the Windows Elements Agent does not actively protect the operating system and only reports detected threats.

- Select **Block (recommended)** to block harmful items automatically.

  This is the default mode. If a harmful item is detected, it is handled according to the configured product settings.

- Select **Allow** to monitor activity without blocking malware.

  Malware is not blocked in this mode. Monitoring all processes and actions may affect computer performance.

NOTE: This option should be used for testing purposes only.

- Select **Allow (Enhanced Threat Detection)** to monitor activity with enhanced detection.

Malware is not blocked in this mode. Enhanced monitoring analyzes all processes and system actions and may significantly reduce system performance.

NOTE: This option should be used for testing purposes only.

IMPORTANT: We strongly recommend that you keep the default **Block** mode unless instructed otherwise by WithSecure Support.

5. Configure **Action when USB storage device is plugged in**.

   This setting controls how the client reacts when a USB storage device is connected to the computer.

   - **Do nothing**: The client does not perform any scan when a USB storage device is connected.
   - **Ask user to scan USB**: Users are prompted to start a scan of the connected USB storage device.
   - **Silently scan USB**: The USB storage device is scanned automatically without notifying the user.
   - **Scan USB and show result to user**: The USB storage device is scanned automatically and the user is notified about the scan result.
   - **Force scan USB and show result to user**: The USB storage device is scanned automatically and the result is shown to the user. Users cannot bypass the scan.

6. Under **Show notifications**, select which users can see client notifications such as restart requests, detected threats, and error notifications.
7. Set the **Maximum size of temporary files** used during scanning.

   This setting defines how much disk space the scanning platform can use to store temporary files when analyzing archives and other complex files.

NOTE: If the available disk space is insufficient or the unpacked file exceeds the configured limit, the scan fails.

Set up scanning exclusions

Configure exclusions that prevent selected files, folders, and file hashes from being included in security scans.

Global exclusions define files, folders, and SHA-1 or SHA-256 checksums that are excluded from all security scans and protection measures. Use exclusions only when necessary because excluded content is not covered by WithSecure protection.

NOTE: This does not apply to EDR sensor scanning.

IMPORTANT: Exclude files or folders only if absolutely necessary. For example, excluding `C:\` excludes the entire default system drive and all its folders, subfolders, and files from all security measures.

To set up scanning exclusions:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*

3. Select **Scanning settings**.
4. Under **Global exclusions from all security scans**, select **Hide exclusions from clients** if you do not want users to see exclusions in the Elements Agent or in scanning reports.

   When hidden, the list of configured exclusions is hidden from the client user interface and from scan reports shown to users.

5. Add the required entries under **Global exclusions**.

   You can exclude folders, files, and SHA-1 or SHA-256 checksums. All configured exclusions apply to all security scans and protection measures.

   You can use wildcards (*) and system environment variables in paths.

   NOTE: Folder exclusions must end with a backslash (\).

   - **File path** excludes a specific file, for example `C:\Program Files (x86)\Microsoft Office\root\Office16\OUTLOOK.EXE`.
   - **Folder path** excludes a folder and all its subfolders and files, for example `C:\Program Files (x86)\Microsoft Office\`.
   - **Wildcard path** excludes matching paths, for example `C:\Program Files*\Microsoft*`.
   - **Environment variable path** excludes a path that uses a system environment variable, for example `%ProgramFiles%\Java`.
   - **SHA-1 or SHA-256 checksum** excludes a file by its checksum, for example `3395856ce81f2b7382dee72602f798b642f14140`.

The scanning exclusions apply to the Windows computers that use this profile.

Configure quarantine settings on Windows

Configure how quarantined or blocked items can be released and how long items are retained in quarantine.

Quarantine settings control how the endpoint client manages files that have been blocked or placed in quarantine. You can allow users to restore quarantined items, protect the release action with a password, and configure automatic cleanup of old quarantined items.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Scanning settings**.
4. Under **Quarantine**, select **Allow users to release blocked and quarantined items** if users should be able to restore quarantined or blocked files.

   When this setting is on, users can release quarantined items or allow blocked items from the client interface.

5. Set a **Password for releasing blocked or quarantined items** if you want to restrict this action.

   When a password is defined, users must enter the password before they can release quarantined items or allow blocked items.

   If no password is configured, users can perform the action without additional authentication.

6. Select **Delete old Quarantine items automatically** to clean up quarantined files automatically.

When selected, items that are stored in quarantine are automatically removed after the configured retention period.

7. Set **Days to keep items in Quarantine**.

   This value defines how long quarantined items are retained before they are automatically deleted.

   The allowed range is `1 to 1095 days`.

The quarantine settings apply to the Windows computers that use this profile.

Set up Tamper Protection

Configure tamper protection to prevent unauthorized modification of the endpoint protection client and optionally exclude specific applications from generating tamper protection events.

Tamper Protection prevents unauthorized applications or users from modifying WithSecure services, processes, files, and registry entries on managed devices.

To set up the tamper protection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **Computer Protection for Windows** or **Server Protection** tab.
   *The **Profiles** page opens.*
3. Select the profile that you want to edit.
4. Under **Scanning settings**, scroll down to **Tamper Protection**.
5. Select **Turn on Tamper Protection**.

   When selected, tamper protection prevents external applications or users from controlling WithSecure services, processes, files, or registry entries.

6. Select **Add exclusion** to add entries to **Exclude tamper protection events** if certain applications should not generate tamper protection events.

   You can exclude specific applications from generating tamper protection events to reduce the number of tamper protection events that are generated in environments where trusted applications frequently interact with protected components.

   Unauthorized access attempts are still blocked, but no event is sent.

   You can use wildcards (`*`) and system environment variables in the application path.

   - **Application path** excludes a specific application from generating tamper protection events.
   - **Wildcard path** excludes multiple applications that match the specified path pattern.
   - **Environment variable path** excludes applications using system environment variables in the path.

The Tamper Protection settings apply to the devices that use this profile.

Scan archive files

You can set manual scanning to check compressed archive files.

Archive scanning can scan files inside compressed `ZIP`, `7Z`, `JARARJ`, `LZH`, `TAR`, `TGZ`, `GZ`, `CAB`, `RAR`, `BZ2`, `R??` , and `0??` archives.

NOTE: This is a default list and it can change in the future. As an administrator, you can change the list in WithSecure Elements Security Center.

NOTE: Archive scanning uses the same maximum temporary file size setting as other scanning operations.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Computers** or **For Windows Servers** tab.
3. Select the name of the profile that you want to edit.
4. Under **Manual scanning**, make sure that **Scan inside compressed files (ZIP, RAR,´...)** is turned on.
5. The archive scanning settings are listed under Included extensions. To change the settings, do the following:
   a) Under **Files to scan**, from the drop-down menu, select **Files with the following extensions**.
   b) Under **Included extensions**, edit the extensions list.
   c) Select **Save and publish**.

5.4.5 Configuring real-time scanning for Windows

Real-time scanning continuously monitors system activity and file operations to detect and block malicious or suspicious content before it can affect the endpoint.

Real-time scanning provides continuous protection by monitoring files, processes, and system activity on managed devices. When real-time scanning is on, the endpoint protection client analyzes files as they are accessed, executed, or transferred. Supported channels include web traffic and network drives.

You can configure:

- How threats are detected
- How suspicious behavior is handled
- How the protection engine interacts with operating system security features

Use AntiMalware Scan Interface

AntiMalware Scan Interface (AMSI) integration allows the operating system to use the WithSecure protection engine to scan scripts and other supported content.

AntiMalware Scan Interface (AMSI) integration allows the operating system to use the WithSecure protection engine to analyze scripts and other potentially malicious content before execution.

For example, Windows uses AMSI to scan PowerShell scripts and Microsoft Office VBA macros using the installed antimalware solution.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Select **Enable AMSI**.

   When the setting is selected, supported applications and operating system components can submit scripts and other content to the WithSecure protection engine for security analysis before execution.

Configure file scanning settings

Configure how real-time scanning handles infected files, scans network drives, and analyzes file types.

File scanning settings define how the endpoint protection client scans files during real-time protection. You can configure how different threat types are handled, control scanning behavior for network drives and file types, and turn on cloud-based analysis to improve threat detection.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Select **Action on infection** to determine how the client handles objects that are detected as infected:
   - **Decide action on infection automatically** selects the action automatically, without asking you.
   - **Rename** renames the infected object so that it cannot run, without deleting it.
   - **Delete** deletes the infected object.
   - **Disinfect** removes the malicious code from the infected object and keeps the cleaned file.
   - **Quarantine** moves the infected object to quarantine.
   - **Ask after scan** waits until the scan finishes, then asks you to choose an action for each detection.
   - **Block** blocks access to the infected object without deleting it.
5. Select **Action on riskware** to determine how the client handles objects classified as riskware:
   - **Delete** deletes the riskware object.
   - **Quarantine** moves the riskware object to quarantine.
   - **Ask after scan** waits until the scan finishes, then asks you to choose an action for each detection.
   - **Block** blocks access to the riskware object without deleting it.
6. Select **Action on spyware** to determine how the client handles objects classified as spyware:
   - **Delete** deletes the spyware object.
   - **Quarantine** moves the spyware object to quarantine.
   - **Ask after scan** waits until the scan finishes, then asks you to choose an action for each detection.
   - **Block** blocks access to the spyware object without deleting it.
7. Select the scanning behavior for **Scan network drives** to control how files located on network drives are scanned during real-time scanning.
   - **Scan on every file access** scans files whenever they are opened, modified, or otherwise accessed.
   - **Scan on execute** scans files only when they are executed, such as when an application is started.

   NOTE: Scanning files on a network drive on every file access can significantly reduce performance.
8. Select **Scan files only with specific extensions** if you want to limit scanning to specific file types.

   When selected, the scanning engine analyzes only files with extensions defined by the protection engine. This list is managed automatically.

   NOTE: You can still exclude additional file extensions using the **Excluded extensions** setting.
9. Select **Upload suspicious samples to WithSecure Security Cloud**.

When selected, suspicious files that are not recognized by the local protection engine may be uploaded to the WithSecure Security Cloud for further analysis.

If a document could contain user data, only file parts that cannot contain personal information are uploaded.

NOTE: We strongly recommend keeping this setting on because it helps detect zero-day malware and reduces false positives.

10. Select **Protect hosts file**.

    This setting enables protection for the system `Hosts` file.

    When the hosts file is protected, the file can still be edited. However, if the product detects redirects that could interfere with product functionality, the changes are reverted to a clean version of the file.

11. Select **Exclude files with the following extensions** to skip scanning specific file types.

    Use the **Excluded extensions** list to define file extensions that should not be scanned.

    Enter file extensions without a leading period, for example `JPG` instead of `.JPG`. Separate multiple extensions with a space.

Configure exclusions

Configure exclusions that prevent specific files, folders, processes, or threat categories from being scanned by real-time protection.

You can use exclusion settings to prevent selected files, folders, processes, or specific threat categories from being scanned by real-time protection. Exclusions may be required for trusted applications or specialized workloads that interact with protected files.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Select **Allow to exclude objects** to use object exclusions.

   When selected, you can define files and folders that are excluded from real-time scanning.

5. Add excluded entries under **Excluded objects**.

   Specify the full path to a file or folder that should be excluded from scanning. Wildcards (*) and system environment variables can be used in paths.

   NOTE: Folder exclusions must end with a backslash (\).

   - **File path**, for example `C:\Program Files\Application\app1.exe`, excludes the specified file.
   - **Folder path**, for example `C:\Folder1\`, excludes all files in the specified folder.
   - **Wildcard path**, for example `C:\Program Files (x86)\Microsoft*`, excludes all files and folders that match the wildcard pattern.
   - **Environment variable path**, for example `%ProgramFiles%\Java\`, excludes files using a system environment variable.

6. Select **Allow to exclude processes** to use process exclusions.

When selected, you can exclude specific processes from real-time scanning.

NOTE: Excluded processes are not monitored and may introduce security risks.

7. Add excluded entries under **Excluded processes**.

   Specify the full path to the process that should be excluded from scanning. System environment variables can be used in the path.

   - **Process path**, for example `C:\Program Files\Application\app1.exe`.
   - **Environment variable path**, for example `%ProgramFiles%\Application\app1.exe`.

8. Select **Exclude all riskware** to skip scanning for all riskware.
9. Select **Exclude all spyware** to skip scanning for all spyware.
10. Select **Allow to exclude riskware/spyware** to use custom exclusions for specific detections.

    When selected, you can define specific riskware or spyware detections that should be excluded from real-time scanning.

11. Add excluded entries under **Excluded riskware/spyware**.

    Specify the name or a substring of the detection name to exclude it from scanning. Wildcards (*) are supported.

The real-time scanning exclusions apply to the Windows computers that use this profile.

Configure web traffic scanning

Configure HTTP web traffic scanning and define applications that are excluded from web traffic inspection.

Web traffic scanning analyzes files transferred over HTTP connections to detect and remove malicious content before it reaches the endpoint. You can turn on web traffic inspection, control what types of content are scanned, and exclude specific applications from scanning when necessary.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Select **Enable web traffic scanning**.

   This setting turns on scanning of web traffic over HTTP connections.

5. Select how web traffic is scanned and whether detected malware is removed automatically:

   This setting determines what types of web content are scanned and whether detected malware is removed automatically.

   - **Scan web traffic and remove found malware** scans web traffic and automatically removes detected malicious files.
   - **Only the included extensions** scans only files that match the extensions defined by the protection engine.

6. Add entries to **Applications excluded from Web traffic scanning** if certain applications should bypass web traffic inspection.

   Use this list to exclude specific applications from web traffic scanning. Each entry defines an application using its SHA-1 hash.

- **Enabled** turns the exclusion rule on or off.
- **Application SHA-1** identifies the application to exclude. Generate the 40-character SHA-1 hash using a SHA-1 calculator.

  NOTE: When the application is upgraded, you must calculate a new hash.

- **Notes** can be used to store the name of the application or other identifying information. This field is not visible to users.

The web traffic scanning settings apply to the Windows computers that use this profile.

Set up DeepGuard

DeepGuard provides extra security layers with both behavior-based and access control protection.

DeepGuard continuously monitors all running applications to detect abnormal behavior or harmful changes to the system.

IMPORTANT: Keep DeepGuard enabled at all times. It provides essential protection against advanced threats, such as ransomware.

When DeepGuard is active, the following protections are enabled:

- Exploit protection
- Ransomware protection
- Heuristic analysis
- Behavior monitoring

To configure DeepGuard:

1. Turn on DeepGuard:
   a) Under **Security Configurations**, select **Profiles**.
   *The **Profiles** page opens.*
   b) Select the used profile.
   c) Open **Real-Time Scanning**.

   NOTE: Make sure that Real-time scanning is on.

   d) Turn **DeepGuard** on.
2. Under **DeepGuard settings**, select **Block rare and suspicious files**.

   This setting allows DeepGuard to block rare or suspicious files based on behavioral analysis and reputation information.

   Turning this feature on improves detection of suspicious programs and provides additional protection against zero-day attacks.

   NOTE: In environments that use uncommon or internally developed software, this setting may occasionally generate false positives, but we strongly recommend keeping it enabled.

3. Add entries to **Protection rules** if you need to trust or block specific applications.

   Protection rules allow you to exclude trusted applications from DeepGuard scanning or explicitly block them. Use this feature only when necessary, because DeepGuard provides critical protection against advanced threats such as ransomware.

TIP: If DeepGuard blocks an application that you trust, add it as a trusted application in **Protection rules**, then submit the file to Sample Validation so that the detection can be corrected.

- **Enabled** turns the protection rule on or off.
- **Application SHA-1/SHA-256** identifies the application using its SHA-1 or SHA-256 hash. Generate the hash using a hash calculator.

  NOTE: When the application is upgraded, you must calculate a new hash value.
- **Notes** can be used to store the application name or other identifying information. This field is not visible to end users.
- **Trusted** defines how DeepGuard handles the application.

  If application is trusted, DeepGuard allows all operations for the application.

  If application is not trusted, DeepGuard always prevents the application from running.

4. Add rules to exclude applications from DeepGuard scanning when necessary.

NOTE: We recommend that you exclude applications only when it is absolutely necessary.

NOTE: If you exclude an application, also the files it accesses are ignored.

5.4.6 Configuring manual scanning for Windows

Manual and scheduled scanning settings define how endpoint devices are scanned for malware on demand or at scheduled intervals.

Manual and scheduled scanning provides additional protection by scanning files and system areas for malicious content outside of real-time protection. You can configure scheduled scans to run automatically at defined intervals and control how manual scans behave when they are run.

Set up scheduled scanning

Configure how often scheduled scans run and define the conditions and performance settings used during scheduled scanning.

Scheduled scanning allows the endpoint protection client to automatically scan the system for malware at defined times. You can configure scan frequency, start time, system conditions, and performance settings to balance protection and system impact.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Manual scanning**.
4. Under **Scheduled scanning**, select the **Scan frequency** and the days when the scheduled scan runs.

   This defines how often scheduled scans run and which days of the week scans are performed.

5. Configure the scheduled scan start time under **Start scanning**.

   Specify the time when the scheduled scan begins by defining the hour and minute.

6. Set **Start scan after system is idle for**.

   Scheduled scanning starts only after the computer has been idle for the specified period.

7. Select **Run scanning as low priority** if you want scanning to use fewer system resources.

   Running scans with low priority reduces system impact but increases the time that is required to complete the scan.

8. Select **Scan inside compressed files** if you want the scan to analyze archive contents.

   When selected, the scanning engine analyzes files inside archives such as ZIP, 7Z, and RAR.

   NOTE: Disabling this setting may reduce detection capability because malware can be hidden inside compressed files.

9. Select **Scan only known file types during scheduled scanning** to limit scanning to high-risk file types.

   When selected, scanning focuses only on file types that are commonly associated with malware, such as executables and scripts.

   NOTE: Limiting scans to known file types improves performance but may reduce detection coverage.

10. Select **Skip a scheduled scanning while the device is running on battery** if you want scans to run only when the device is connected to power.
11. Select **Show notifications to user**.

    Turn off this setting to hide scheduled scanning notifications from users.

The scheduled scanning settings apply to the Windows computers that use this profile.

Set up manual scanning

Configure how manual scans use system resources, handle detected threats, and define which files are included or excluded from scanning.

Manual scanning settings define how on-demand scans are performed. These settings control scan priority, threat handling behavior, scanning scope, and exclusions.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Manual scanning**.
4. Under **Manual scanning**, configure **Scanning priority**.

   This defines how much system resources manual scanning can use.

   - **Normal priority** runs the scan using normal system resources.
   - **Background** runs the scan with reduced resource usage. This option minimizes performance impact but may increase the time required to complete the scan.

5. Select **Action on infection** to define how the product handles objects that are detected as infected during manual scanning:

   - **Clean** removes the malicious code from the infected object and keeps the cleaned file.
   - **Delete** deletes the infected object.

- **Rename** renames the infected object so that it cannot run, without deleting it.
- **Ask after scan** waits until the scan finishes, then asks you to choose an action for each detection.
- **Quarantine** moves the infected object to quarantine.
- **Report only** reports the detection without taking any action.

6. Select **Scan inside compressed files** if you want to analyze files contained in archives.

   When selected, the scanning engine analyzes files located inside archive formats such as ZIP files.

7. Select **Scan inside mailbox files** if you want to scan email mailbox files.

   When selected, the scanner analyzes supported mailbox file formats. The default action for threats detected inside mailbox files is **report only** to avoid the risk of corrupting mailbox data.

   Supported mailbox formats include:

   - BSD mbox format
   - Netscape/Mozilla mailbox
   - Eudora mailbox
   - Pegasus mailbox
   - Outlook mailbox

8. Under **Files to scan**, select whether to scan all files or only specific file extensions.

   You can scan all files or limit scanning to specific file extensions. Even when scanning all files, you can exclude selected file extensions using the exclusion settings.

9. Specify file types to scan in **Included extensions** if scanning is limited to specific extensions.

   Enter file extensions without the leading period, for example `EXE` instead of `.EXE`. Separate multiple extensions with a space.

10. Select **Exclude files with the following extensions** to skip scanning certain file types.

    The file extensions defined in **Excluded extensions** are not scanned during manual scanning.

11. Specify excluded file types in **Excluded extensions**.

    Enter file extensions without the leading period, for example `EXE` instead of `.EXE`. Separate multiple extensions with a space.

12. Select **Enable excluded objects** to enable file and folder exclusions.
13. Add entries under **Excluded objects**.

    Specify the full path of files or folders that should be excluded from scanning. Wildcards (`*`) and system environment variables can be used in paths.

    NOTE: Folder exclusions must end with a backslash (`\`).

    - **File path**, for example `C:\Program Files\Application\app1.exe`.
    - **Folder path**, for example `C:\Folder1\`, excludes all files in the folder.
    - **Wildcard path**, for example `C:\Program Files (x86)\Microsoft*`.
    - **Environment variable path**, for example `%ProgramFiles%\Java\`.

The manual scanning settings apply to the Windows computers that use this profile.

5.4.7 Configuring browsing protection for Windows

Browsing protection settings control how Windows endpoint clients monitor and filter web traffic to block malicious, suspicious, or unwanted web content.

Browsing protection helps protect users from web-based threats. It analyzes visited websites, filters web content, and prevents access to harmful or inappropriate resources.

You can configure browsing protection to:

- Block dangerous websites
- Enforce safe search behavior
- Control access to specific categories of web content

Set up Browsing Protection

Configure general browsing protection behavior, including user access to blocked pages, browser extension reminders, SafeSearch enforcement, and event reporting.

Browsing protection common settings control how blocked pages are handled, how users are notified about browser protection extensions, and what information is included in security events related to blocked websites.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Browsing Protection**.
4. Select **Allow user to continue to blocked pages**.

   When selected, users with administrative rights can bypass the warning page and continue to a blocked website.

   NOTE: We recommend keeping this turned off.

   NOTE: For the **Allow this website** link to appear in the browser when a page has been blocked, the **Web site exceptions** must be on and the **Allowed/Denied sites** tables must be in the edit mode.

5. Select **Remind user to activate browser extensions**.

   When selected, users receive a reminder to install the Browser Protection extension if it is missing or to activate it if it is installed but disabled in a supported browser.

6. Select **Enforce SafeSearch mode**.

   This setting enforces SafeSearch strict mode in supported search engines to filter adult or inappropriate content from search results.

   NOTE: The browser extension must be installed and activated for this feature to work correctly.

7. Select **Include the blocked URLs in all security events**.

When selected, the URL of a blocked website is included in related security events that appear in the **Security events** view.

NOTE: Regional legislation about monitoring user web activity may restrict the use of this feature. Ensure that enabling this setting complies with applicable local laws and organizational policies.

8. Select **Include the blocked malicious URLs in all security events**.

   When selected, the malicious URL of a blocked website is included in related security events visible in the **Security events** view.

NOTE: Regional legislation about monitoring user web activity may restrict the use of this feature. Ensure that enabling this setting complies with applicable local laws and organizational policies.

9. Specify the **Sample submission URL**.

   This URL is displayed to users on the block page and can direct them to a custom page with instructions for submitting URLs for analysis.

   The URL must include the protocol, for example: `https://example.com/SampleSubmission`.

Use reputation based browsing on Windows

Reputation-based browsing blocks websites that are suspicious or known to be malicious.

To turn on reputation-based browsing on Windows endpoints:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows** tab.
3. Select the profile that you want to edit.
   *The **Profile for Windows** page opens.*
4. From the menu on the left, select **Browsing Protection**.
5. Turn on **Enable reputation-based browsing** to filter websites.
6. Under **Reputation-based browsing**, you can turn on the following:
   - **Block access to websites rated as harmful**
   - **Block access to websites rated as suspicious**
   - **Block access to websites rated as prohibited**
   - **Block trackers found on websites**
   - **Block access to recently created domains**
7. Select **Show link reputations on search results** to shows reputation-based information for search results.

NOTE: The browser extension must be installed and activated.

Control web content

Turn on web content control to block websites based on their content categories.

Use Web content control to restrict access to websites based on predefined content categories, such as illegal content, hate, gambling, or file sharing. This can be used to enforce acceptable use policies and reduce exposure to risky or inappropriate web content.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Browsing Protection**.
4. Under **Web content control**, select **Enable web content control**.

   When selected, the product blocks access to websites based on their content category.

NOTE: Selecting the **Unknown** category blocks access to websites whose reputation has not yet been determined. These are typically less popular or newly created websites that have not been widely visited.

Filter content types

Turn on content type filtering and configure filters that block downloads based on internet media types or file names.

Content type filtering lets you block specific types of web content based on internet media types or file extensions. This helps prevent users from downloading potentially dangerous file types such as executable files, scripts, or other high-risk content.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Browsing Protection**.
4. Under **Content type filtering**, select **Enable content type filtering**.

   When selected, the product blocks web content based on the rules defined in the **Content type filters** list.

5. Add or edit rules in **Content type filters**.

   This list defines which types of content are blocked. You can turn suggested filters on or off, and add new filters by selecting **Add Content Type Filter**.

   If **Filter safe sites** is disabled, filtering is applied only to sites that are unknown or considered unsafe by the Security Cloud.

   - **Active** enables or disables the filter rule. Disabled rules are ignored.
   - **Filter safe sites** applies the filter to all websites. If disabled, the filter applies only to unknown or unsafe websites.
   - **Content type** specifies the internet media type to block. Wildcards (`*`, `?`) are supported. For example: `application/*zip*`.
   - **Filename/extension** specifies space-separated file names or extensions to block. Wildcards are supported. For example: `*.exe *.do? viewcard*.asp.scr`.
   - **Description** stores a description of the filter rule for administrative reference.

Configure web site exceptions

Configure website exception rules that always allow or block access to specified domains.

With website exceptions, you can define domains that are always allowed or always blocked regardless of their reputation. These rules can be used to ensure access to trusted services or to block specific websites.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Browsing Protection**.
4. Select **Enable web site exceptions**.

   When enabled, the lists of **Allowed sites** and **Denied sites** are used to override normal browsing protection behavior.

   Users can always access sites listed in **Allowed sites**, while access to sites listed in **Denied sites** is always blocked.

5. Select **Block everything except allowed sites** if you want to allow access only to explicitly permitted websites.

   When enabled, all websites are blocked except those listed in **Allowed sites**.

6. Select **Disable referrer-based allowance** to enforce stricter filtering rules.

   When enabled, pages are no longer allowed based on their referrer. Normally, pages loaded from approved referrers are allowed to ensure that content embedded in allowed websites works correctly.

   NOTE: Enabling this setting may cause embedded content or linked resources on some websites to load incorrectly or not appear at all.

7. Select **Send security event about access to denied site**.

   When enabled, a security event is generated whenever a user attempts to access a site listed in **Denied sites**.

   If disabled, no event is generated for denied site access attempts.

8. Add entries to **Allowed sites** or **Denied sites**.

   Use these lists to define domains that should always be allowed or always blocked.

   - **Address** specifies the domain name. Examples: `www.example.com` or `example.com`. Using the root domain applies the rule to all subdomains.
   - **Notes** can be used to store additional information about the domain or rule.

Use connection control

Configure connection control to protect sensitive online sessions and restrict network activity from untrusted applications.

Connection control protects sensitive web sessions, such as online banking, by restricting network activity from untrusted applications. When in use, the feature monitors connections to sensitive websites and applies additional security restrictions to prevent unauthorized access or data leakage.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*

2. Select **For Windows Computers**, and then select a profile.
   *The **Profile for Windows Computers** opens.*
3. From the menu on the left, select **Browsing Protection**.
4. Add entries to **Allowed sites** or **Denied sites**.

   Use these lists to define domains that should always be allowed or always blocked.

   - **Address** specifies the domain name. Examples: `www.example.com` or `example.com`. Using the root domain applies the rule to all subdomains.
   - **Notes** can be used to store additional information about the domain or rule.

5. Under **Connection control**, select **Enable connection control**.

   When selected, the connection control detects when users access sensitive websites such as online banking sites (HTTPS only) or other defined services that handle confidential information.

6. Select **Do not block active connections for untrusted apps**.

   This setting controls how existing network connections from untrusted applications are handled when connection control is activated.

   - When this setting is on, existing active connections continue to work normally.
   - When this setting is off, active internet connections of untrusted applications stop working when they are refreshed.

   NOTE: New connections from untrusted applications are always blocked.

7. Select **Clear clipboard when done** to remove clipboard content after a protected session.

   When selected, the clipboard is cleared after the user finishes a protected session, such as an online banking session. This helps prevent sensitive information from remaining in the clipboard.

8. Select **Block command-line and scripting tools**.

   When selected, the connection control blocks network connections started by command-line and scripting tools during protected sessions.

9. Select **Block remote access**.

   When selected, the connection control blocks remote access tools while a protected session is active.

   Supported tools may include applications such as Remote Desktop, TeamViewer, LogMeIn, and VNC.

10. Add entries to **Connection control sites** if you want to define additional protected websites.

    Adding a site to the list allows you to mark it as a sensitive service. When users access these sites, the connection control activates enhanced protection for the session.

5.4.8 Firewall configuration

When Windows Firewall is on, its user and network rules are applied to the devices.

WithSecure Firewall profiles provide an additional security layer on top of the Windows Firewall user rules and other domain rules. The WithSecure firewall profiles or rules are not applied if Windows Firewall is off. Therefore, we recommend that you always keep firewall on.

NOTE: Domain rules may override these rules.

> **NOTE:** If you use GPO or 3rd party firewall, in most cases you need to turn off WithSecure firewall profiles (the **Apply WithSecure firewall profiles** setting) to avoid conflicts. "Use Windows Firewall" should match the case-specific settings configured for the GPO or 3rd party firewall.

> **IMPORTANT:** You can turn on **Allow other rules** if you want to allow also those firewall rules that are not created by WithSecure. If you turn off this option, only WithSecure firewall rules are applied to the current profile. We strongly recommend that you keep this option turned on.

You have an option to use a different firewall profile for different sites. You can change the firewall profile between an office network and an outside network using customizable rules. You can do this by going to **WithSecure firewall profile**, selecting **Automatic selection** from the drop-down menu, and then adding a rule. These rules are used to automatically select a firewall profile based on the configuration.

Add a rule

Add a rule to a firewall profile to allow or block network traffic.

To add a rule:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. From the left pane, select **Firewall**.
   *The **Firewall** page opens.*
4. Select the profile that you want to edit or to which you want to add a new rule.
   In the Firewall rules table, you can see the rules that have been created for the selected firewall profile.

   > **NOTE:** The order of the rules has no effect, but block rules override allow rules.

5. Do one of the following:
   - To add a new rule, select **Add rule** at the top of the table.
   - To edit an existing rule, select the row to edit it.

     > **NOTE:** We do not recommend that you delete rules, but rather deactivate those that you feel are not needed.

6. Enter values for the rule or edit the existing ones in the following fields:
   - Give the new rule a name and add a description.

     In the Action and direction column, select either to allow or block incoming or outgoing traffic.

     In the Attributes column, do the following:
     - Select a protocol.
     - Enter the local and remote IP addresses.

       > **NOTE:** You can leave these empty unless you want to allow a specific IP address or range.

     - Enter the local port number to allow traffic to come through this specific port
     - Enter the remote port number to allow traffic to come from specific port.
     - Enter the service name.

- Enter the application path.
- Select the interface type.

NOTE: You can add more than one port number (separated with a comma) or a range of ports (for example, 0-65535).

NOTE: For automatic profile selection rules, go to **Network location settings**. You can add one or more rules to assign a specific firewall profile when you, for example, need to take your laptop out of the office network range.

The new rule appears in the Firewall rules table for the selected firewall profile.

Set up alerting for firewall rules

Sets up alerts for firewall rules that block traffic.

NOTE: Alerting only works when you select "block" as the action for the rule.

To set up firewall rule alerts:

1. Log in to WithSecure Elements Security Center.
2. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
3. Select the **For Windows Computers** tab, and then select the profile that you want to edit.
4. Select **Firewall**.
5. Select the WithSecure firewall profile for which you want to set up alerts.
6. Define the alert as follows:
   a) Make sure the switch in the **Active** column is on.
   b) From the top drop-down menu, select **Block** as the rule action.
   c) From the middle drop-down menu, select either **In** or **Out** for the traffic direction.
   d) From the bottom drop-down menu, select **Send alert**.

Adding a firewall rule to a network isolation profile

When you isolate a computer from a network, a strict set of firewall rules are applied to prevent the computer from connecting to the internet.

NOTE: The isolated computer retains its device profile, including its firewall profile. The isolation rules are applied but not shown in the profile editor.

By default, the firewall profile turns off all network connections and allows only WithSecure processes. It turns off all other firewall rules for the selected devices. Also, it blocks the DNS resolution for all non-allowed DNS addresses to prevent possible information leakage through DNS queries. An isolated device has no internet connection, thus it cannot be accessed from outside or used to search the internet.

As an administrator, you can add extra rules to the firewall profile used by the device if you need to provide extra access. For example, you can allow remote access to the device so that a support engineer could access it and investigate issues.

NOTE: Extra rules are usually "Allow" rules, because everything is already blocked by default.

NOTE: The isolation rules replace the firewall rules of the current firewall profile when the computer is isolated. When network isolation is removed, the previous firewall profile is applied.

The **Allowed domains** field below the Firewall rules table allows you to specify the domain for which you want to allow the isolated device to connect.

NOTE: Only the domains in the **Allowed domains** field are resolved by DNS.

The network isolation feature works even if the firewall is turned off in the WithSecure Elements Endpoint Protection profile settings. The network isolation mode forces the firewall and the network isolation profile on. However, if the GPO settings on a device force the firewall off, the network isolation mode does not turn it on.

Allow unknown connections

Allows unknown inbound and outbound connections in the firewall profile.

By default, the **Allow unknown inbound connections** and **Allow unknown outbound connections** settings are turned off. When they are off, the firewall blocks unknown traffic. You can use automatically selected profiles, select a predefined WithSecure firewall profile, or customize a profile to suit your needs. If no rule exists that blocks or allows this traffic, the default rule is used, which means that first the WithSecure firewall general settings are applied, and then the rules from the firewall rules table. If no other rules match, then the fallback settings are applied.

NOTE: Fallback settings are per profile.

For example, if you turn **Allow unknown connections** on and delete all the firewall rules, everything is allowed. If you turn **Allow unknown connections** off, everything is blocked. When there are no firewall rules, all traffic is unknown and therefore blocked. You can add rules to allow certain traffic and the rest will be blocked. Alternatively, by turning on **Allow unknown connections** you can allow everything and by creating a set of block rules, you block certain traffic and allow everything else.

To allow unknown connections:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. From the left pane, select **Firewall**.
   The Firewall page opens.
4. Select the profile that you want to edit.
5. Under **Fallback settings**, do one of the following:
   - **Allow unknown inbound connections** - when this setting is on, it allows unknown inbound connections to the computer. We recommend that you keep this setting turned off.
   - **Allow unknown outbound connections** - when this setting is on, it allows unknown outbound connections from the computer. We recommend that you keep this setting turned off.
6. Save and publish your changes:
   - To save the changes to the current profile, select **Save and Publish**.
   - To save the changes to multiple profiles, select **Save and Publish to multiple profiles**.

5.4.9 Using Device control

Device control blocks certain hardware devices for protection. It prevents malware from spreading to the network from external devices such as USB storage devices and DVD/CD-ROM drives. When a blocked device is plugged into the client computer, Device control can turn it off to prevent access to it.

This section describes how to set up Device control, block devices, exclude devices using a device mask, and find a device ID.

Set up Device control

You can set restrictions on how users can access USB devices (for example, web cams and hard disks) and whether removable mass storage devices are allowed to execute installers.

To set up Device control:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. From the menu on the left, select **Device control**.
4. Turn **Device control** on.

NOTE: If Device control is on, all devices that are connected to the computer are visible on the device page under **Connected devices**.

5. Under **Removable mass storage devices**, you can turn on one of the following options:
   - Allow write access - when this option is off, users cannot copy files to a removable mass storage device. Removable mass storage devices can only read data.
   - Allow executables to run - when this option is off, executing files from removable mass storage devices is prevented.

Exclude devices using a mask

You can exclude devices to which you do not want to apply any device access rules.

If you want to exclude, for example, all USB devices, instead of entering full device IDs, you can use a mask "USB*" to filter the devices.

To exclude devices using a mask:

1. To find device IDs, under **Environment**, select **Devices**.
   *The **Devices** page opens.*
2. Select the desired device.
   The device details page opens.
3. Select the **Connected devices** tab.
4. In the **Filter by device ID** field, enter a mask, for example, "USB*".
   The page shows all the devices with a device ID starting with "USB\".
5. Confirm that the list includes all the devices that you want to exclude.
6. Under **Profiles**, select the desired profile, then select **Device control**
7. Under **Device filtering rules**, in the Rules table, select **Add rule**.
   An empty row appears.
8. Add a new rule with a mask, for example, *USB*".
9. Select **Save and Publish**.

All devices with an ID starting with "USB*" that are found in the Rules table are excluded from the list of connected devices.

Block hardware devices

You can block the access to devices with predefined rules.

By default, rules do not block any devices. To block devices, follow these instructions.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. From the menu on the left, select **Device control**.
4. To add a device access rule, do the following:

   Under **Device access rules**, you can add or remove rules to control the devices and allow or block access to them.

   a) Select **Add rule**.
   b) Enter the device name and its hardware ID.
   c) For **Access to device**, select either **Allow** or **Block**.

      A device that has **Access to device** set to **Block** cannot be accessed, when the rule is set as active.

   d) Select **Publish** to publish the new rule.

Find the hardware ID for a device

You can use the hardware ID with blocking rules.

Follow these instructions to find the hardware ID with Windows Device Manager:

1. Open Windows **Device Manager** in the client computer.
2. Find the correct device in the list.

   TIP: Expand the device type to see all the devices.

3. Right-click the device and select **Properties**.
4. Go to the **Details** tab.
5. Select one of the following IDs from the drop-down menu and write down its value:

   - Hardware IDs
   - Compatible IDs
   - Device class guid
   - Parent ID

   NOTE: For external storage devices, this is the only ID that includes the unique serial number of the device.

   NOTE: By right-clicking the item, you can open the context menu and copy the ID.

5.4.10 Scheduling automated tasks

With automated tasks, you can schedule tasks to run automatically on devices at a specific time.

You can set up automated tasks in the WithSecure Elements Security Center profile editor. Using a selected profile, you can schedule, for example, the following:

- Running a quick scan for malware
- Scheduled scanning for malware
- Scanning for malware in folder
- Allowing product updates
- Scanning for missing software updates
- Upgrading the client application
- Installing all missing software updates
- Installing all security updates
- Installing critical security updates
- Installing critical and important security updates
- Forcing shutdown
- Forcing shutdown, if required
- Forcing restart
- Forcing restart, if required
- Forcing hibernation
- Locking workstation

In scheduling automated tasks, you can use macros, such as @daily, @midnight, @monthly, @away, or @lock. You can use @away to schedule a task that runs when the user is away for a given amount of time (minutes). For example, selecting "Quick malware scan" or "Lock workstation" and "@away 30" means that a quick malware scan is run or the workstation gets locked when the user is away for 30 minutes. Similarly, you can schedule to automatically lock a workstation daily at a certain time by selecting the Lock workstation task and @daily <hours>. By using "@lock", you can schedule a task to run as soon as a computer is locked.

You can also use CRON expressions.

NOTE: For information on and examples of CRON expressions, see WithSecure Elements Security Center.

NOTE: To make sure that the devices do not overload your infrastructure, task starting times are randomized to a precision of one hour.

NOTE: If you turn on the switch in the **Never skip** column in the Automated tasks table, the task is run as soon as possible even if it could not be run at the scheduled time. Otherwise, the task will be skipped.

The following gives some examples on how to set up automated tasks.

Schedule scans on Windows

Set the product to scan viruses and other harmful applications at regular times.

To schedule a scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.

*The **Profiles** page opens.*

2. Select the desired profile.
3. Select **Automated tasks**.
4. Make sure automated tasks are on.
5. Select **Add task**.
6. In the Type column, select **Scheduled scan for malware**.
7. In the Schedule column, select how often you would like the scheduled scanning to run.
8. (Optional) In the Description box, enter a description for the selected scan.
9. In the start when available column, make sure the switch is on.
10. Select **Save and publish**.
    Your changes are saved and published to the current profile.

Set up a task to update the product at a specific time

Create an automated task to update the product, for example, every Saturday at 12:00.

NOTE: With this task, you can control when a product is updated. You can schedule it, for example, for a maintenance weekend, to prevent the updated at other times.

To set up a task to update the product at a specific time:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile for which you want to create an automated task.
3. Open **Automated tasks**, and make sure it is on.
4. Select **Add task** above the Automated tasks table, and do the following:
   a) From the Type drop-down menu, select **Allow WithSecure Elements Agent update**.
   b) In the Schedule field, enter the following CRON expression: `* * 12 ? * 6`.

NOTE: For more details on how to use CRON expressions, see the related help section in WithSecure Elements Security Center.

The product checks for new updates every Saturday between 12:00 and 13:00.

NOTE: One hour is a constant period for this type of an automated task to guarantee enough time for the product to check for new updates and perform upgrade if an update package is available.

Set up a task to install missing critical and other security updates

Create automated tasks to install missing critical and other security updates at specific times.

For installing missing critical security updates, for example, every day and other security updates, for example, once a week, you need to create two automated tasks in the profile editor.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile for which you want to create an automated task.
3. Open **Automated tasks**, and make sure it is on.

4. To create a task for installing critical security updates every day, select **Add task** above the Automated tasks table, and do the following:
   a) From the Type drop-down menu, select **Install critical security updates**.
   b) From the Schedule drop-down menu, select **@daily**.

   NOTE: In the Description field, you can add a description for the new task (optional).

5. To create a task for installing other security updates once a week, select **Add task** and do the following:
   a) From the Type drop-down menu, select **Install all security updates**.
   b) From the Schedule drop-down menu, select **@weekly**.

After you created these two automated tasks, the product installs critical security updates every day at a random time and other security updates on a specific day at a random time.

NOTE: Randomization is used to reduce the network load.

Set up a task to scan for missing security updates

Create an automated task to scan for missing security updated every day.

NOTE: If you create a task to scan for missing updates, you can turn off **Scan automatically for missing updates** on the Software updater page.

NOTE: Tasks to install missing software updates scan also for missing updates. If you install updates every day, a separate task for scanning is not needed.

To create an automated task to scan for missing security updates:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile for which you want to create an automated task.
3. Open **Automated tasks**, and make sure it is on.
4. Select **Add task** above the Automated tasks table, and do the following:
   a) From the Type drop-down menu, select **Scan for missing updates**.
   b) From the Schedule drop-down menu, select **@daily**.

The product scans for missing security updates every day at random time.

NOTE: If a device is off when the task is scheduled to run, the task will run automatically once the device is on again if you have turned on the "Start when available" option.

Set up a task to scan for malware

Create an automated task to scan monthly for malware.

To create an automated task to scan for malware:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile for which you want to create an automated task.
3. Open **Automated tasks**, and make sure it is on.

4. Select **Add task** above the Automated tasks table, and do the following:
   a) From the Type drop-down menu, select **Scan for malware**.
   b) From the Schedule drop-down menu, select **@monthly**.

The product scans for malware every month at a random time.

5.4.11 Set up network locations

With network locations, you can control the settings when devices are connected to the network in the selected network location.

You can, for example, set up network locations and rules so that when a device is at home, Software Updater and firewall are on, but when at the office, both Software Updater and firewall are off. For this, you need to add two locations and create four rules.

To set up network locations and rules:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile for which you want to set up the network locations and create the rules.
3. Select **Network location settings**, and make sure it is on.
4. Under **Locations and rules**, select **Add location**, and do the following:
   a) In the Name column, enter a descriptive name for the location, for example, **At home**.
   b) In the Triggers column, from the Type drop-down menu, select **My network**.
   c) In the Value field, enter the network mask, for example, `10.0.0.0/24`.

   NOTE: A location can have multiple triggers, but it must have at least one.

   d) Select **Add trigger**.
   e) From the Type drop-down menu, select **DHCP server IP address**.
   f) In the Value field, enter the DHCP server IP address.

   The new location will be active when both triggers are active.
5. To add another location, select **Add location** and do the following:
   a) In the Name column, enter a descriptive name for the location, for example, **At the office**.
   b) In the Triggers column, from the Type drop-down menu, select **Default gateway IP address**.
   c) In the Value field, enter the default gateway IP address.

   NOTE: You can raise or lower the priority of a location. A location with a higher priority is processed before a location with a lower priority. For example, if you have a network location "At home" set to "Always" and another location "At the office" set to "Default gateway IP address", it is important that the "At home" location has a lower priority. Otherwise, the device location "At home" takes always precedence over the "At the office" location.

6. To create a rule, select **Add rule** above the Rules table, and do the following:
   a) In the Location column, from the drop-down menu, select the location where the rule is applied, in this example, **At home**.
   b) In the Setting column, from the drop-down menu, select one of the product feature that is turned on or off by the rule, in this example, **Software updater**.
   c) In the Value column, make sure the switch is turned **on**.
7. To create another rule, select **Add rule**, and do the following:

a) In the Location column, from the drop-down menu, select **At home**.
b) In the Setting column, from the drop-down menu, select **Firewall**.
c) In the Value column, make sure the switch is turned **on**.

8. Repeat the last two steps to create two more rules for the location "At the office":
   a) For the first rule, in the Setting column, select **Software updater** and in the Value column, turn the switch **off**.
   b) For the second rule, in the Setting column, select **Firewall** and in the Value column, turn the switch **off**.

NOTE: For a rule to be applied, the location must be active.

5.4.12 Protect files against ransomware

Restores files and system settings that the product automatically reverted during a suspected ransomware attack.

If the product detects changes to files or system settings that could be caused by a ransomware attack, it automatically reverts the changes and stores them in the quarantine. If the changes are valid and not caused by a ransomware, you can restore the automatically reverted changes from the quarantine.

To allow the product to automatically protect your files against ransomware:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Computers** or **For Windows Servers** tab, and then select the profile that you want to edit.
3. From the menu on the left, select **Rollback** and do the following:
   - Turn on **Rollback**.
   - Turn off **Allow and report mode**.
   - Turn on **Allow to restore reverted files**.

NOTE: We recommend first keeping the Allow and report- mode turned on for a week. If there are no false positives, then you can turn off the Allow and report- mode and turn on the **Allow to restore reverted files** setting to restore the files from the quarantine.

NOTE: By default, the Allow and report-mode is on. In this mode, the product detects the changes that ransomware has done, but it does not revert them. The changed files are automatically restored only after you turn off the Allow and report-mode.

The changed files and system settings are restored.

Remove locally excluded paths

Using WithSecure Elements Security Center, you can remotely remove from a local exclusion list exclusions that can be considered risky for your organization.

To remove one or more locally excluded paths:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the name of the device whose excluded paths you want to remove.
   The device details page opens.

3. From the action menu at the bottom, select **Remove locally excluded paths**.
   A list of excluded paths is shown.
4. Select one or more excluded paths that you want to remove.
5. Select **Remove**.

The selected locally excluded paths are removed.

5.4.13 Managing profiles in the Premium products

WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers have also the WithSecure Elements EPP for Computers Premium and WithSecure Elements EPP for servers Premium variants.

They include advanced security features. The first advanced security feature is DataGuard, which provides extra layer of protection against threats, such as ransomware.

Using DataGuard

The WithSecure Elements EPP for Computers Premium and the WithSecure Elements EPP for Servers Premium subscriptions add the WithSecure DataGuard feature that protects specific locations and prevents unexpected applications from modifying data.

NOTE: DataGuard is available only in the Premium versions of the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers software. If you do not have a Premium subscription, the DataGuard feature is grayed out.

DataGuard is an added functionality that strengthens DeepGuard and monitors user content folders. The folders can be discovered automatically, and exceptions can be added manually. Trusted applications are allowed to access the folders and change them. DataGuard is especially useful in case of a new Ransomware managing to avoid all the security layers provided by WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers.

IMPORTANT: DeepGuard must be turned on for DataGuard to function.

Set up DataGuard

You can define the folders that DataGuard protects on managed computers, and add trusted applications that you do not want DataGuard to block.

When DataGuard is turned on, untrusted applications and malware (including ransomware) cannot modify files in folders that you define as protected.

To use DataGuard:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. Under **DataGuard**, turn on **DataGuard advanced behavioral blocking** to use DataGuard.
4. Turn on **Discover monitored user data folders automatically** if you want DataGuard to automatically check for folders that contain documents, pictures, or other end user content.
5. Under **Manually included folders** and **Manually excluded folders**, you can add to or exclude folders from the DataGuard protection on end user computers as follows:
   - Under **Manually included folders**, select **Add path**.

NOTE: When you add a path, the specified path and all its subfolders are added. If you, for example, add C:\Documents, DataGuard monitors all files and folders under C:\Documents.

- Under **Manually excluded folders**, select **Add path**.

NOTE: When you exclude a path, the specified path and all its subfolders are excluded. If you, for example, exclude C:\Documents, DataGuard stops monitoring all files and folders under C:\Documents.

6. Turn on **Access control** to define which are the trusted applications that can have access to change the files and folders that DataGuard protects.
   - If you want DataGuard to automatically find trusted applications, turn on **Discover trusted applications automatically**
   - If you want to manually add trusted applications, under **Manually added trusted applications and folders**, select **Add path**.

NOTE: When you add a path, the specified path and all its subfolders are added. If you, for example, add C:\Documents, DataGuard monitors all files and folders under C:\Documents.

Add a vault

Adds a vault in DataGuard that restricts which applications can write to a folder.

A vault is a folder where only applications that are configured for that vault are able to write, create, or rename files and sub-folders. Vaults allow you to create specific rules to lock down certain locations. For example, if you want to create sub-folders in a vault using Windows Explorer, you need to add `%windir%\explorer.exe` to the list of trusted applications. Or if you want to make sure that only an SQL server executable file can modify the files of an application that uses a local database, create a vault to allow it.

Each vault offers the possibility of monitoring. Whenever an application tries to access files in a vault, a DataGuard log is created in Security Events.

To add a vault:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the profile you want to edit.
   The Profile page opens.
3. From the menu on the left, under **Premium**, select **DataGuard**.
4. Scroll down to **Vaults**, and select **Add a vault**.
5. In the **Path to the vault** field, enter the path.
6. Select **Add a trusted application**.
7. In the **Path to the application** field, enter a path to the application that you want to be able to access the vault.

NOTE: To add more trusted applications, select **Add a trusted application**.

8. Select **Save and Publish**.

Tips for using DataGuard

These tips help you set up DataGuard protected folders and allowed locations on Windows.

If a program runs from Program Files, it is not blocked; if the same program runs from `AppData\Local` for example, it is blocked by DataGuard. Therefore, we recommend that in Windows you install software programs under Program Files. Windows has built-in security measures that make it harder for malware distributors to get into that location.

If a user asks you to allow an unsafe location and you allow it, then DataGuard allows everything in that specific location after that. This also applies to certain file names. For example, if a file in one location is replaced with another file that has the same name, DataGuard allows that file automatically.

When turned on, DataGuard automatically checks folders that contain user content such as documents. You can also manually add folders for DataGuard to check. Even though you can add paths based on individual user requests, we recommend that you use environment variables for Windows. For example, instead of adding `c:\user\JohnSmith`, use an environment variable `%HOME%`.

Application control

Application control prevents execution and installation of applications, and prevents them from running scripts.

NOTE: Application control is available only in WithSecure Elements EPP for Computers Premium and WithSecure Elements EPP for Servers Premium.

Application Control reduces the risks that malicious, illegal, and unauthorized software pose in the corporate environment. It provides the following features:

- Security: Pre-configured security rules designed by WithSecure penetration testers cover attack vectors that are used to breach into corporate environments.
- Policy enforcement: Based on a simple rule editor, policy enforcement helps the administrator define which applications are blocked, allowed, or monitored.
- Central visibility to all the cases where rules have been triggered under Security Events

Use Application control

With Application control, you can set restrictions on which applications can run.

To use Application control:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. In the **Profile** page that opens, select **Application control**.
4. Turn **Application control** on or off.

   NOTE: By default, the Application control is on.

5. Under **Global rule**, select one of the options:
   - Allow all applications - if none of the exclusion rules block an application, installer, or script, it is allowed.
   - Block all untrusted applications - if none of the exclusion rules allow an application, installer, or script, it is blocked.
   - Allow and monitor all applications - if none of the exclusion rules block an application, installer, or script, it is allowed but its behavior is monitored and, if need be, reported.

NOTE: Global rule defines the last rule that is applied to all applications.

6. Save and publish your changes to the current profile or to multiple profiles.

NOTE: If you selected to save and publish to multiple profiles and you close the window without saving the changes, the changes are not applied to the current profile.

Your changes are applied to the selected profiles.

Add application control rules

You can add your own application control rules.

You can add rules and top rules. The rules are applied in a priority order - they are checked from top to bottom in the table. The decision to allow or block an application is made by the first-match rule. If none of the rules match, then the global rule is used.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
   *The **Profile** page opens.*
3. From the menu on the left, select **Application control**.
4. Depending on what kind of rule you want to add, select either **Add a new top rule** or **Add a new rule**.
5. Enter a name for the rule.
6. From the Event drop-down menu, select the event that triggers the rule.
7. From the Action drop-down menu, select **Allow**, **Block**, or **Allow and monitor**.
8. Enter a description for the rule.
9. Do the following to add one or more conditions that activate the new rule:
   a) Select **Add condition**.
   b) From the attribute drop-down menu, select an attribute.
   c) From the condition drop-down menu, select a condition for the attribute.
   d) Enter a value for the condition.

Using attributes and conditions in rules

The following table explains the attributes that you can select to match the condition values.

Table 11: Exclusion rule attributes

Selected attribute	Description
Target	Values of the actual application. For example, **Target file name** is the actual file that you want to block.
Parent	Values of the process that launches the application. For example, **Parent file name** is the file that launches the application that you want to block.
Installer	Values of the installers (MSI installer packages).

NOTE: For example, if you want to block Internet Explorer, `iexplore.exe` is the target and `explorer.exe` (Windows Explorer) is the parent.

The following table explains how different conditions work with the values that you enter.

Table 12: Exclusion rule conditions

Selected condition	Description
is equal to	The value must be exactly the same as the selected attribute, for example, `iexplore.exe`.
is not equal to	The value may be anything except the selected attribute.
is less than	The numeric value may be anything less than the selected attribute.
is greater than	The numeric value may be anything greater than the selected attribute.
is less or equal to	The numeric value may be anything less than or exactly the same as the selected attribute.
is greater or equal to	The numeric value may be anything greater than or exactly the same as the selected attribute.
contains	The selected attribute must contain the value, for example, `explore`.
starts with	The selected attribute must start with the value, for example, `ie`.
ends with	The selected attribute must end with the value, for example, `explore.exe`.

NOTE: To find information about what each parameter contains, go to **Profiles** > **Application control** and select the help icon next to **Application control rules**. It describes the condition values per each condition type. For example, the Target file size is shown in bytes of the started application or loaded module.

Note also the following when adding conditions to a rule:

- If you use attribute `Target SHA1` or `Parent SHA1` in the rule condition, you have to use **Application start** as the event type.
- If a dynamic link library (.dll) is blocked and you want it to be allowlisted by Application Control, you have to use the **Module load** event type in the rule. In a case like this, you cannot therefore use attribute `Target SHA1` nor `Parent SHA1` in the rule.
- Attributes `Target file names mismatch` and `Parent file names mismatch` kick in when the binary filename is different from the "Original filename" found under file Properties > Details.

Example: Prevent a vulnerable version from running

To use Application control to prevent vulnerable applications from running, for example, to block an unpatched version, use a Target file version attribute.

For example, a program had a vulnerability that was patched in version 1.2.4. To block any version older than 1.2.4 from running, do the following.

1. Create the following exclusion rule:
   a) Give the rule a name: `Block an unpatched program`.
   b) From the Event drop-down menu, select `Application start`.
   c) From the Action drop-down menu, select `Block`.
2. Add the first condition to the exclusion rule:
   a) From the attribute drop-down menu, select `Target file description`.

   NOTE: To find the file description, right-click the file in the File Explorer and select Properties.

   b) From the condition drop-down menu, select `contains`.
   c) In the Value field, enter the name of the unpatched program as it appears in the File description. For example, "Internet Explorer".

   NOTE: As "Internet Explorer" is in the Target file description, the program is blocked regardless of the file name or its location.

3. Add the second condition to the exclusion rule:
   a) From the attribute drop-down menu, select `Target file version`.
   b) From the condition drop-down menu, select `is less or equal to`.
   c) In the Value field, enter `1.2.3.*.*`.

   NOTE: The condition for the target file version is "less or equal to 1.2.3.*.*" The asterisk indicates that only major and minor fields are used in the comparison.

Application control event types

The event types you can select for an application control rule, and when each one is triggered.

Table 13: Application control event types

Event	Description
Application start	Triggers when an executable file or script is launched.
Module load	Triggers when a DLL is about to get loaded into a process.
Installer start	Triggers when `msiexec.exe` is launched with some MSI package as a command line parameter.
File access	Triggers when a file is accessed.

Event	Description
Application start and Module load	A combination of the two event types. Triggers when an executable file or script is launched and a DLL is about to get loaded into a process.

Submitting Custom Indicators of Compromise

By submitting custom Indicators of Compromise (IOCs), you can create detection rules based on file hashes, IP addresses, or hostnames, and define how the system should respond when these are detected.

IOCs help your organization stay aligned with modern cybersecurity standards. You can create custom detections and automated responses that fit your specific environment. You can also take a more proactive approach to defense by using threat data from trusted sources such as knowledge-sharing communities, threat intelligence publications, and your own internal investigations.

Create IOC detection rules

Create custom Indicators of Compromise (IOC) rules so the platform automatically detects or blocks file hashes, IP addresses, or DNS hostnames you flag as threats.

You can define and manage custom IOC rules through the security platform interface. The platform supports three types of IOCs:

- File hashes (SHA1 or SHA256)
- IP addresses
- DNS hostnames

For each IOC type, you can configure the system to generate a detection, block the threat, or perform both actions. By default, both detection and blocking are enabled.

NOTE: File hash-based rules are supported on Windows systems and do not depend on any specific network protocol. IP address-based rules are also supported on Windows and apply only to outbound TCP traffic. For DNS hostnames, the platform supports plain DNS queries on Windows, but does not support DNS over HTTPS (DoH).

Follow these steps to add custom Indicators of Compromise (IOCs) with the profile editor.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile that you want to edit.
   The profile editor opens.
3. Open the **Application Control** tab.
4. Add a new IOC Rule.
   a) In the **Event Type** field, select **IOC - Hash** for a hash-based IOC, or **IOC - IP** for an IP-based IOC.
   b) In the **Condition** field, enter the SHA1 or SHA256 hash value, or the IP address, depending on the selected IOC type.
   c) In the **Rule Name** field, enter a custom name that helps you easily identify and track the rule later.
   d) In the **Rule Description** field, provide a short explanation that will appear in the detection context when the rule is triggered.
   e) Select the appropriate **Severity** level for the rule: **Severe**, **High**, or **Medium**, based on the potential impact of the IOC.
   f) In the **Action Type** field, choose what should happen when the IOC is detected: **Generate detection**, **Block**, or **Generate detection and block**.
5. Save and publish changes.

When a custom IOC is triggered, the platform generates a Broad Context Detection (BCD). These BCDs function like standard detections and can start email alerts, populate dashboards, and appear in incident timelines, providing full visibility into the event.

Once your IOC rules are configured, you can save and publish them to apply across all profiles in your organization. This ensures consistent enforcement of your custom threat intelligence throughout your environment.

Detecting system events

System event detection is an advanced security feature that comes with the WithSecure Elements EPP for Computers Premium and the WithSecure Elements EPP for Servers Premium subscriptions.

Recognizing potentially risky activities may sometimes be challenging because the data is spread out over multiple locations. System event detection allows you to recognize security-related Windows Event log entries directly in WithSecure Elements Security Center. These events are potential indicators of something that might be going on. We recommend that you investigate them further to find out whether there is no valid reason for them.

The following events are turned on by default:

- **Event ID: authentication failure ("An account failed to log in")** - it is common for authentications to fail, but if there are suddenly several authentication attempts targeting a single user or an endpoint device, it could indicate that an attacker is submitting multiple credentials for user accounts to gain access to an endpoint device.
- **Event ID: user locked ("A user account was locked out")** - this indicates that a user account has been locked because of multiple failed authentication attempts. Repeated events are a strong indicator of a script error or an attack in progress.

  NOTE: The actual number of attempts is defined in the GPO user-lockout-threshold.

- **Event ID: audit log cleared ("Audit log was cleared")** - once attackers gain access to a device, they might attempt to hide their tracks by clearing audit logs. In such an event, you should make sure that it was not caused by a legitimate action.

NOTE: Several events that are turned off by default. Generally, these are events that might interest a professional security operations control team that wants to collect relevant data into a SIEM or SOAR solution. Such events are indirect indicators of activities and for that reason, they are turned off by default.

Set up system event detection

Selects the Windows system events that WithSecure Elements Agent monitors and sends to Security Events.

To set up system event detection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Servers** or **For Windows Computers** tab, and then select the profile that you want to edit.
   *The **Profile** page opens.*
3. From the menu on the left, select **System event detection**.
4. In the **Active** column, turn on the switch for those events that you want the product to monitor.
5. Select **Save and Publish**.

Device drive encryption

Elements Endpoint encryption gives you an overview of the state of encryption on your devices and the tools to manage them.

Encryption is an essential tool in ensuring the confidentiality of your data. By encrypting your devices, you make sure that if they are lost or stolen, a third party is unable to access the data stored on them. You can view the disk encryption status in the Device details, the Compliance view of the device list, and under the Device reports.

NOTE: Encrypting a drive with Elements Endpoint encryption requires a Windows 10 or newer operating system. Also, the device must have a Trusted Platform Module (TPM) version 2 or higher. You can find information about your device's TPM version on the left-side menu in the Device details page.

Recovery keys are an important part of managing disk encryption. If valid users get locked out of their devices or you need to restore data from an encrypted drive using a different device, you need the recovery key to access the data. There are many tools to collect these keys, but it is important that you use one of them. WithSecure Elements Endpoint Protection can collect recovery keys for you, if needed. you can find the setting in the **General** tab under **Profiles**.

NOTE: For collecting recovery keys, you need a Windows device with Elements Endpoint Protection installed and a disk that was encrypted using BitLocker with "recovery password protector". After turning on the feature, we recommend verifying that recovery keys were successfully collected and that the keys are visible in WithSecure Elements Security Center.

Encrypt a device drive

Turning drive encryption on or off is an advanced security feature that comes with the WithSecure Elements EPP for Computers Premium and the WithSecure Elements EPP for Servers Premium subscriptions.

You must have a Windows device with Elements Endpoint Protection installed and a disk that was encrypted using BitLocker or FileVault.

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the device whose drive you want to encrypt.
3. From the action menu at the bottom of the page, select **System drive encryption** > **Encrypt drive**, and then select one of the following:
   - Encrypt only the used disk space (faster and the best for new PCs and drives)
   - Encrypt the entire drive (slower but the best for PCs and drives that are already in use)
4. Select **Encrypt**.

5.4.14 Server Share Protection

Server Share Protection is a security feature that comes with the WithSecure Elements EPP for Servers subscriptions.

Server Share Protection helps you protect shared files against ransomware that runs on remote clients. It identifies ransomware even when the malicious files and processes are not on the host. It monitors the actions that take place in those user sessions that are working with shared files or folders. While monitoring, it also backs up all the changed files. Server Share Protection can identify cases where ransomware impersonates a user and encrypts files. Upon detecting ransomware, it blocks the user from making further

changes for a defined time (by default 30 minutes), reverts all the changes that were already made, and restores the filesystem to its original state.

NOTE: If a user makes changes to files but no ransomware is detected, Server Share Protection does not revert any changes.

You can exclude shared folders and users. Server Share Protection does not monitor the excluded folders and users. If a user is currently blocked and you exclude them, they are allowed to access shared files again.

Turn on Allow and report mode

In the Allow and report mode, Server Share Protection monitors and identifies ransomware attacks.

NOTE: It does not, however, block anything or revert any changes.

You can view the possible detections and their details under **Events** > **Security Events**.

We recommend that you have this mode on as a part of your testing when you first take the Server Share Protection feature into use. Turning the mode on does not protect you, but when it is on, you can use it to identify false positives, for example, if you have a valid script that, from the detection point of view, behaves like ransomware.

NOTE: When this mode is on, encrypted files are not restored.

To turn on the Allow and report mode:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Servers** tab, and then select the profile that you want to edit.
   The Profile for Windows Servers opens.
3. From the menu on the left, select **Server Share Protection**.
4. Turn on the **Allow and report mode** setting.
5. Select **Save and Publish**.

Prevent a user from temporarily accessing shared files or folders

When this setting is on and Server Share Protection detects ransomware, you can define for how long (in minutes) you want to prevent a user from accessing shared files and folders.

To define for how long a user is blocked:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Servers** tab, and then select the profile that you want to edit.
   The Profile for Windows Servers opens.
3. From the menu on the left, select **Server Share Protection**.
4. In the **Block user access (minutes)** field, enter the time.

NOTE: The default time is 30 minutes.

5. Select **Save and Publish**.

Exclude shared folders

Excludes a shared folder from Server Share Protection monitoring.

Server Share Protection monitors shared folders and allows you to restore files that ransomware has changed via the network. If there is a shared folder you do not want to be monitored, you can add it to the excluded folders.

NOTE: You can only exclude a shared folder as a whole, not just of one its subfolders.

To exclude a shared folder:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Servers** tab, and then select the profile that you want to edit.
   The Profile for Windows Servers opens.
3. From the menu on the left, select **Server Share Protection**.
4. Select **Excluded folders**, and then select **Add excluded folder**.
5. Enter the path to the shared folder that you want to exclude.
6. Select **Save and Publish**.

Exclude users

Excludes users from Server Share Protection monitoring and file-edit blocking.

When you exclude users, they are not monitored or blocked even if malware is detected. They are also allowed to edit files in the shared folders.

You can add either a username in a fully qualified format `domain_name\user_name` or a user SID (security identifier).

NOTE: The username or user SID must be the one that is used on the Windows server.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Windows Servers** tab, and then select the profile that you want to edit.
   The Profile for Windows Servers opens.
3. From the menu on the left, select **Server Share Protection**.
4. Select **Excluded users**, and then select **Add user**.
5. Enter either a username or a user SID.

NOTE: The username or user SID must be the same as is used on the Windows server.

6. Select **Save and Publish**.

5.4.15 Restart Elements Agent from Elements Security Center

Using WithSecure Elements Security Center, you can restart **Elements Agent** on a selected device without having to restart the whole system.

To restart **Elements Agent** from Elements Security Center:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the device that you want to restart.

3. From the action menu at the bottom, select **Restart** > **Restart WithSecure Elements Agent**.

Elements Agent restarts on the selected device.

5.5 Managing profiles in Elements EPP for Computers (Mac)

Profile management in WithSecure Elements EPP for Computers (Mac) software.

A profile is a bundle of settings that you assign to the WithSecure Elements EPP for Computers clients on Mac. This section describes how to create a profile and configure its settings, including updates, real-time scanning, scheduled scans, scanning exclusions, browsing protection, and the firewall.

5.5.1 Create a new computer profile

You can create profiles that can be assigned to specific computers.

To create a new profile:

1. Under **Security configurations** > **Profiles** > **For Mac**, select 
   next to an existing profile, and select **Clone profile**.
   *The **Profile for Mac** page opens.*
2. Enter a name and description for the new profile, and select a type for the new profile.
3. Make desired changes to the settings, and then select **Save and Publish**.
   The new profile is created.

5.5.2 Allow uninstallation

Only when this setting is turned on can users uninstall the product on their computers.

To allow uninstallation:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab.
3. Select one of the profiles.
   *The **Profile for Mac** page opens.*
4. From the menu on the left, select **General settings**.
5. Turn **Allow user to unload the product** on.

5.5.3 Turn on Early access

Turns on the Early access setting so the device receives the latest product version before general availability.

After you have assigned to a device a profile that has **Early access** turned on, the device receives the latest product version before they are published for general availability and released to channels for a silent upgrade. The upgrade still happens silently and is identical to the regular update.

NOTE: We reserve up to two weeks for a new version to be available in Early access before we push the new version to all client software. We may keep the early access stage to a minimum, if a release contains urgent vulnerability fixes.

IMPORTANT: We strongly recommend that you turn this setting on to be able to test new and upcoming features.

To turn the Early access setting on:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab.
3. Select one of the profiles.
   *The **Profile for Mac** page opens.*
4. From the menu on the left, select **General settings**.
5. Turn the **Early access to client software** setting on.
6. Select **Save and Publish**.

5.5.4 Automatic update settings

In the WithSecure Elements profiles, you can set how you want the product to handle the automatic updates.

WithSecure Elements Security Center has the following options for setting up HTTP proxy connections:

- Don't use proxy
- HTTP Proxy from System preferences
- Use remotely managed HTTP proxy

NOTE: If you select this option, you need to specify the proxy address in the **Remotely managed proxy address** field.

You can set the in-house GUTS2 server addresses for the product to fetch updates from them. The product tries to download the updates first from the local server, if it is set up and available. If not, the product downloads updates from the global WithSecure server, if you have turned on the **Fallback to global WithSecure updates server** option under **Security Configurations** > **Profiles** > **General settings**. For each server, the product goes through the allowed HTTP proxies options in the following order: **Use remotely managed HTTP proxy**; **HTTP Proxy from System preferences**; **Don't use proxy** (direct connection without HTTP proxy).

5.5.5 Set up real-time scanning

This setting turns on real-time malware scanning for all items that end users access.

To set up real-time scanning:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab, and then select a profile.
   *The **Profile for Mac** page opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Set the following real-time scanning options:
   a) Turn **Real-time scanning** on.

NOTE: We strongly recommend keeping this setting turned on.

   b) Make sure that **Security Cloud (ORSP)** is turned on.

NOTE: *Security Cloud* collects security data on unknown applications and web sites and on malicious applications and exploits on web sites. We strongly recommend keeping this setting turned on.

c) Make sure **XFence** is turned off.

NOTE: XFence is an advanced feature and we currently recommend keeping it off for typical installations.

5.5.6 Schedule scans on Mac

Set the product to scan viruses and other harmful applications at regular times.

To schedule a scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select a profile.
3. Select **Manual scanning** > **Scheduled scanning**.
4. Turn scheduled scanning on.
5. Select how often you would like the scheduled scanning to run:
   - Daily - scan every day
   - Weekly - scan on selected days during the week
   - Monthly - scan every month
6. Under **Start scanning**, select one of the options:
   - Hour - select the hour when the scan will start. You should select a time when you expect to not be using the computer.
   - Minute - select the minutes when the scan will start.

5.5.7 Set up scanning exclusions

Set the product to exclude files or folders from scanning.

NOTE: The Exclude folders and files feature applies only to client versions 17.7 and newer.

To set up scanning exclusions:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select **For Mac**, and then select a profile.
   *The **Profile for Mac** opens.*
3. Select **General settings**.
4. Under **Exclude folders and files from all security scans**, select the **Add exclusion** link.
5. In the Path column, add a path to the file or folder that you want to exclude.
   Folders and files that are in the specified path are excluded from all security scans and measures, and are not protected by WithSecure. This applies to any subfolders within the designated folders. For example, `/Users/*/folder-to-exclude/*` excludes everything that is found in "folder-to-exclude" for all the users.

IMPORTANT: Use this only for files or folders that absolutely must be excluded from scanning. For example, if you exclude "/*" from scanning, the whole system volume and all folders, subfolders, and files in it are excluded from all security measures.

5.5.8 Set up browsing protection

Browsing protection secures visits to banking sites (Connection control) and prevents access to blocked sites (Web content control)

To set up browsing protection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab, and then select a profile.
   *The **Profile for Mac** page opens.*
3. From the menu on the left, select **Browsing protection**.
4. Set the following browsing protection options:
   a) Turn **Browsing protection** on.

NOTE: We recommend keeping this setting turned on.

   b) You can turn on **Web content control**.

NOTE: This setting blocks web sites based on their content, for example, "hate" or "illegal". "Unknown" blocks access to sites whose reputation is unknown, typically because they are not popular and not as accessed as most sites.

   c) Make sure **Connection control** is turned on.

NOTE: This setting alerts users when they have a secure connection to online banking sites and other defined sites that handle sensitive information. We recommend keeping this setting turned on.

5.5.9 Turn on Mac firewall

Keep the Mac firewall turned on to block intruders from accessing your computer.

NOTE: By default, Apple Firewall is on in the product. You can change it in the Elements profiles.

To make sure that the firewall is on:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab, and then select a profile.
   *The **Profile for Mac** page opens.*
3. From the menu on the left, select **Firewall**.
4. From the Apple firewall drop-down menu, select one of the options:
   - On - turns Apple firewall on
   - Off - turns Apple firewall off
   - Externally managed - No changes are done to the Firewall settings if they are externally managed

NOTE: Running `/usr/libexec/ApplicationFirewall/socketfilterfw` on a managed Monterey device produces the following message: "Firewall settings cannot be modified from command line on managed Mac computers." If you see that message, select **Externally managed** as the Apple firewall option.

5.5.10 Using WithSecure app-layer firewall profiles

With WithSecure app-layer firewall profiles, you can control incoming and outgoing network traffic using application-specific rules.

NOTE: WithSecure firewall is referred here as WithSecure app-layer firewall.

In the profile editor, you can switch **WithSecure Firewall** on or off, edit the firewall profiles, and create, export and import firewall rules.

NOTE: Currently, you can configure WithSecure app-layer firewall profiles only in WithSecure Elements Security Center.

What is WithSecure app-layer firewall

WithSecure app-layer firewall allows you to control incoming and outgoing network connections for a particular client device, which helps in securing network traffic. You can define these settings for a set of applications that belong to a specific category or apply them to a specific application. With a pre-defined set of rules called firewall profiles that are configurable, you can allow or block incoming or outgoing network connections for a specific set of applications. By defining specific firewall rules for a specific application, you can also allow or block network traffic for that application.

Using macOS firewall, you can allow or block incoming connections for a specific application or all applications. F-Secure firewall offers you a wider set of possibilities, for example, you can choose to allow or block both incoming and outgoing connections. You can specify it for a single application or a set of applications that belong to a specific category, such as signed applications.

What is the Trusted by WithSecure setting?

You can use this setting to allow or block incoming and outgoing connections for all allowed applications that are signed by vendors or developers trusted by WithSecure.

Add firewall rules

You can add new rules to firewall profiles.

To add a firewall rule:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab.
3. Select the profile that you want to edit.
4. Select **Firewall**.
5. Select the WithSecure firewall profile for which you want to add a rule.
6. Under **Firewall rule for WithSecure profile**, select **Add rule**, and do the following:
   a) Make sure the switch in the **Active** column is on.
   b) Enter a name and a description for the rule.
   c) From the top drop-down menu, select the action for the rule (either **Allow** or **Block**).
   d) From the middle drop-down menu, select the traffic direction.

Table 14: Firewall rule directions

Direction	Explanation
In/Out	The traffic will be allowed or blocked to and from your computer in both directions. Examples of applications using this direction: Messengers with Audio/Video calls capabilities and torrent clients.
In	The traffic will be allowed or blocked if coming from the defined remote hosts or networks to your computer. Examples of applications using this direction: server applications, such as sshd (ssh server), ScreenSharing (vnc server), Apache, and Nginx.
Out	The traffic will be allowed or blocked if going from your computer to the defined remote hosts or networks. Examples of applications using this direction: client applications, such as, web browsers, wget, curl, ftp clients, ssh clients, and vnc clients.

e) From the bottom drop-down menu, select the action for alerts (either **No alert** or **Send alert**).

f) Under **Attributes**, enter one or more signing identifiers.

The signing identifier is a unique identifier embedded in the application signature. It usually matches a bundle identifier, for example, `com.apple.Safari`.

NOTE: When entering more than one identifier, you can use a comma to separate them. Alternatively, you can use a wildcard (*) as the last character, for example, `com.google.Chrome*` or `com.apple.Safari,com.google.Chrome*`

g) Enter one or more team identifiers.

The team identifier is a unique identifier assigned by Apple to a vendor that provides applications for macOS, for example, `APPLE` or `EQHXZ8M8AV`. When entering more than one identifier, you can use a comma to separate them: `APPLE,EQHXZ8M8AV`

Export and import firewall rules

You can export firewall rules to or import it from a .json file.

To export or import firewall rules:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mac** tab, and then select the profile that you want to edit.
3. Select **Firewall**.
4. Next to the Firewall rules table, select ⋯.
5. Depending on what you want to do, select one of the options:

- To export rules, select **Export to file (JSON)**, and then either open or save the FirewallRules.json file.
- To import rules, select **Import from file (JSON)**, and then select the .json file from which you want to import the rules.
- To replace rules in the table, select **Replace from file**, and then select the .json file to replace.

Obtain Signing and Team Identifiers

You can use the Apple `codesign` utility to get a Signing and a Team Identifier for your application.

NOTE: The `codesign` utility is included in all the supported macOS versions.

To obtain identifiers for your application:

1. Locate the application path.
2. Open `Terminal.app`.
3. Enter the following command and press **Enter**:

   ```
   codesign -dv "<path to application>"
   ```

4. In the output, look for the Identifier and TeamIdentifier fields.

```
Executable=###
Identifier=<Signing Identifier>
Format=###
CodeDirectory ###
Signature size=###
Timestamp=###
Info.plist entries=#
TeamIdentifier=<Team Identifier>
Runtime Version=###
Sealed Resources version=###
Internal requirements ###
```

For some applications that Apple provides, the TeamIdentifier value is not set:

```
Executable=###
Identifier=com.apple.###
Format=###
CodeDirectory ###
Signature size=###
Timestamp=###
Info.plist entries=#
TeamIdentifier=not set
Runtime Version=###
Sealed Resources version=###
Internal requirements ###
```

In those cases, you can use the following Team Identifier:

```
APPLE
```

NOTE: Make sure that the identifier has the "com.apple." prefix.

Examples

Google Chrome

- The application path: `"/Application/Google Chrome.app"`

- The `codesign` command:

```
codesign -dv "/Applications/Google Chrome.app"
```

- The `codesign` output:

```
Executable=/Applications/Google Chrome.app/Contents/MacOS/Google Chrome
Identifier=com.google.Chrome
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20500 size=1789 flags=0x12a00(kill,restrict,library-validation,runtime) hashes=47+5
 location=embedded
Signature size=9043
Timestamp=11 Feb 2020 at 4.12.31
Info.plist entries=36
TeamIdentifier=EQHXZ8M8AV
Runtime Version=10.14.0
Sealed Resources version=2 rules=13 files=60
Internal requirements count=1 size=204
```

NOTE: In this codesign output, the Signing Identifier is "com.google.Chrome" and the Team Identifier is "EQHXZ8M8AV"

Apple Safari:

- The application path: "`/Applications/Safari.app`"
- The `codesign` command:

```
codesign -dv "/Applications/Safari.app"
```

- The `codesign` output:

```
Executable=/Applications/Safari.app/Contents/MacOS/Safari
Identifier=com.apple.Safari
Format=app bundle with Mach-O thin (x86_64)
CodeDirectory v=20100 size=321 flags=0x2000(library-validation) hashes=3+5 location=embedded
Signature size=4547
Info.plist entries=41
TeamIdentifier=not set
Sealed Resources version=2 rules=13 files=2227
Internal requirements count=1 size=64
```

NOTE: In this codesign output, the Signing Identifier is "com.apple.Safari". The Team Identifier is not set, but because it is a built-in Apple application (that is, the identifier has the "com.apple." prefix), you can use "APPLE".

5.6 Managing profiles in WithSecure Elements EPP for Linux

Profile management in WithSecure Elements EPP for Linux software.

A profile is a bundle of settings that you assign to the WithSecure Elements EPP for Linux clients. This section describes how to create a profile and configure its settings, including connection settings, automatic updates, real-time and scheduled scanning, tamper protection, and integrity checking.

5.6.1 Create a new computer profile for Linux

You can create profiles that can be assigned to specific computers.

To create a new profile:

1. Under **Security configurations** > **Profiles** > **For Linux**, select
   
   next to an existing profile, and select **Clone profile**.
   *The **Profile for Linux** page opens.*
2. Enter a name and description for the new profile, and select a type for the new profile.
3. Make desired changes to the settings, and then select **Save Profile**.
   The new profile is created.

5.6.2 Configure proxy settings for Linux

Configure proxy settings for Linux Protection updates and Security Cloud (ORSP) connections.

Use these steps to configure proxy settings for Linux systems to enable updates and secure connectivity.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then select a profile.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **General**.
4. Specify the proxy settings for updates and Security Cloud connectivity:

   Configure proxy settings for Linux Protection updates (product and malware definitions) and Security Cloud (ORSP).

   a) Turn on **Use HTTP proxy** to use proxy for updates and Security Cloud connectivity.
   b) Enter the HTTP proxy host address in the **HTTP proxy host** field.

      Accepted formats: `domain.com`, `127.0.0.1`, `localhost`.

   c) Enter the HTTP proxy port number in the **HTTP proxy port** field.

      Valid range: `0–65535`.

   d) Enter the username for proxy authentication in the **HTTP proxy username** field.
   e) Enter the password for proxy authentication in the **HTTP proxy password** field.
5. Select **Save Profile** to apply your changes.

5.6.3 Use WithSecure Elements Connector

Configures WithSecure Elements Connector settings in a Linux profile.

To use WithSecure Elements Connector:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab.
3. Select one of the profiles.
   *The **Profile for Linux** page opens.*
4. From the menu on the left, select **General settings**.
5. In **WithSecure Elements Connector**.

   Accepted formats: `domain.com`, `127.0.0.1`, `localhost`.

   You can specify multiple connectors separated by a semicolon, for example:
   `http://myconnector.local; http://myproxy2.com:8080`

When multiple connectors are specified, the client uses the first one and switches to the next if the first connector becomes unavailable.

6. Select **Save Profile** to apply your changes.

5.6.4 Set up automatic updates

Configure automatic updates for WithSecure products and malware definitions on Linux.

These settings control how the managed software handles WithSecure product and malware definition updates. Follow these steps to enable and configure automatic updates for Linux systems.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then choose the profile you want to edit.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **General**.
4. Turn on **Enable automatic updates** to download and install updates automatically.
5. In **Apply updates**, choose when updates are installed.
   - **On arrival**: Install updates immediately after they are downloaded.
   - **Once**: Install updates at a specific date and time. Set both the date and the time of day for installation.
   - **On schedule**: Install updates on a recurring day and time. Specify the day of the week and the time of day for installation.
6. Turn on **Send alerts after update** to notify administrators when updates are applied.
7. Turn on **Use HTTPS to download updates** to secure update downloads over HTTPS.

NOTE: Using HTTPS enhances privacy and meets compliance requirements for certain certifications. However, this may increase network traffic when using proxies, because HTTPS traffic cannot be cached by proxy servers.

8. Select **Save Profile** to apply your changes.

5.6.5 Configure access to client software for Linux

Configure how Linux devices receive new WithSecure Elements agent versions.

The **Access to client software** setting controls how Linux devices receive new WithSecure Elements agent versions. Choose **Automatic updates**, **Controlled updates - Manual**, or **Controlled updates - Scheduled**, depending on how much control you want over update timing.

To configure access to client software:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab.
3. Select one of the profiles.
   *The **Profile for Linux** page opens.*
4. From the menu on the left, select **General settings**.
5. In the **Define access to client software** dropdown, select a mode.
   - **Automatic updates** updates the device automatically as new versions are released.
   - **Controlled updates - Manual** keeps the device on a release group version that you choose.

- **Controlled updates - Scheduled** updates the device automatically, but only during a schedule that you define.

6. If you selected **Automatic updates**, choose a submode: **Generally available** or **Early**.

   Early devices receive updates before the general release: agent and engine updates arrive about one week early, and security definition updates arrive about two hours early.

   IMPORTANT: We recommend assigning a small, representative group of devices to **Early**, so that you catch problems before they reach your whole fleet.

7. If you selected **Controlled updates - Manual**, select the release group version to assign to this profile.
8. If you selected **Controlled updates - Scheduled**, set the recurrence, day, and one-hour time window for the update check.
9. Select **Save Profile** to apply your changes.

5.6.6 Integrate EDR sensor on Linux

Configure settings to integrate the EDR sensor on Linux endpoints.

Follow these steps to enable and configure the EDR sensor using WithSecure Elements Connector.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab.
3. Choose the profile you want to edit.
   *The **Profile for Linux** page opens.*
4. From the menu on the left, select **General settings**.
5. Turn on **EDR sensor** to enable endpoint detection and response on devices with an EDR subscription.

   NOTE: We strongly recommend to keep this setting turned on. If disabled, EDR will not detect or alert on attacks against the endpoint.

6. Turn on **Advanced response** if you want to activate the advanced response module in EDR.

   With Advanced response, you can access detailed system information that may include sensitive data. Before turning this feature on, you should ensure that its use complies with applicable worker privacy legislation and any relevant customer or contractual requirements.

   NOTE: By using this feature, you confirm that you are legally permitted and have obtained all necessary consents under applicable law.

7. Select **Save profile** to apply your changes.

5.6.7 Protect against unwanted changes

Tamper protection safeguards WithSecure services, processes, files, and registry entries from unauthorized changes by end users or third-party applications.

To use tamper protection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab.

3. Select one of the profiles.
   *The **Profile for Linux** page opens.*
4. From the menu on the left, select **General settings**.
5. Make sure that **Allow user to turn off all security features** is turned off.

   If this setting is turned on, users can turn off all WithSecure security features.

   NOTE: We strongly recommend keeping this setting turned off to prevent users from disabling protection at any time.

6. Select **Save Profile** to apply your changes.

5.6.8 Set up real-time scanning for Linux

Perform real-time malware scans on files and folders whenever users open or modify them.

Follow these steps to configure real-time scanning for Linux endpoints.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then choose the profile you want to edit.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Turn on **Real-time scanning** to enable continuous malware scanning for accessed files.

   Real-time scanning ensures that all files that are defined in the scan configuration are checked when they are accessed.

   NOTE: We strongly recommend keeping this setting turned on.

5. Make sure that **Use Security Cloud (ORSP)** is turned on to check file reputation online.

   Security Cloud (ORSP) verifies unknown files against WithSecure Security Cloud for enhanced protection.

   NOTE: We strongly recommend keeping this setting turned on.

6. Specify which files are scanned during real-time scanning:
   a) Specify **Files and folders to scan** using full absolute paths.

      Directories include all subdirectories recursively.

      NOTE: By default, this field is empty, which means that nothing is scanned.

   b) Specify **Files and folders excluded from scanning** when necessary.

      Use this only for files or folders that absolutely must be excluded from scanning.

      CAUTION: Be careful when excluding paths. For example, excluding the root directory (/) removes all protection.

   c) Add paths to **Trusted applications** for processes that must bypass scanning.

      Any files opened by trusted applications are not scanned.

CAUTION: Be careful when adding trusted application paths. For example, adding the root directory (/) excludes all applications from all security measures.

d) Turn on **Scan only executables** if you want to limit scanning to executable files only.

e) Turn on **Scan for potentially unwanted applications** to detect potentially unwanted applications. These are programs that may not be classified as malware but can negatively affect system performance or security.

7. Specify how archives are handled during real-time scanning:

a) Turn on **Scan inside archives** to check files within compressed packages.

b) Turn on **Treat encrypted archives as unsafe** to block encrypted archives.

c) Set **Scan archive up to nesting level** to define maximum depth for scanning.

d) Turn on **Treat archives that exceed the maximum nesting level as unsafe** to block deeply nested archives.

8. Choose actions for real-time scanning detections.

a) Select an action for malware: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

b) Select an action for potentially unwanted applications: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

c) Select an action for suspicious files: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

9. Select **Save profile** to apply all changes.

5.6.9 Set up manual scanning for Linux

Configure on-demand (manual) malware scanning for Linux endpoints.

To set up manual scanning:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then select a profile.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **Manual scanning**.
4. Choose which files are always excluded from the manual scanning.

a) Select **Add path** to choose paths to exclude from manual scanning.

Enter the full absolute path of the file or folder you want to exclude. All subfolders within the specified directory are also excluded for all users.

CAUTION: Be careful when excluding paths. For example, excluding the root directory (/) excludes all files from all manual scans.

b) Turn on **Scan for potentially unwanted applications** to detect potentially unwanted applications. These are programs that may not be classified as malware but can negatively affect system performance or security.

5. Configure how archives are handled during manual scanning.
   a) Turn on **Scan inside archives** to check files within compressed packages.
   b) Turn on **Treat encrypted archives as unsafe** to block encrypted archives.
   c) Set **Scan archive up to nesting level** to define maximum depth for scanning.
   d) Turn on **Treat archives that exceed the maximum nesting level as unsafe** to block deeply nested archives.
6. Choose actions for manual scanning detections.
   a) Select an action for malware: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

   b) Select an action for potentially unwanted applications: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

   c) Select an action for suspicious files: **Do nothing**, **Rename**, or **Remove**.

NOTE: Access is blocked regardless of the chosen action.

7. Select **Save Profile** to apply your changes.

5.6.10 Schedule scans for Linux

Set the product to scan viruses and other harmful applications at regular times.

Scheduled scans use the same configuration as manual scans.

To schedule scans:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then select a profile.
   *The **Profile for Linux** page opens.*
3. Select **Manual scanning**.
4. Under **Scheduled scanning**, select the days when you want the scan to run.
5. Set the start time in **Time of day**.

   Enter the time in 24-hour format: `HH:mm (00:00 - 23:59)`
6. Select **Save Profile** to apply your changes.

The scheduled scan settings apply to the Linux devices that use this profile.

5.6.11 Set up scanning exclusions for Linux

Define which files, folders, and processes to exclude from real-time scanning on Linux.

To set up scanning exclusions:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*

2. Select the **For Linux** tab, and then select a profile.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **Real-time scanning**.
4. Turn **Real-time scanning** on.

   This setting turns on real-time malware scanning for all objects, defined in the files and folders to scan -setting, that end users access.

   NOTE: We strongly recommend keeping this setting turned on.

5. Make sure that **Use Security Cloud (ORSP)** is turned on.

   This setting turns on checking the reputation of unknown files with the WithSecure Security Cloud.

   NOTE: We strongly recommend keeping this setting turned on.

6. Choose which files are scanned during the real-time scanning.
   a) Specify the **Files and folders to scan** using full, absolute paths.

      Folders and files specified here are included to Real-time Scanning, so they are covered by WithSecure protection. Use the full, absolute path names of individual files or directories. The listed directories also include subdirectories recursively.

      NOTE: By default, this field is empty, which means that nothing is scanned.

   b) Specify the **Files and folders excluded from scanning**.

      Folders and files specified here are excluded from Real-time Scanning, so they are not covered by any WithSecure protection. This includes any subfolders within the designated folders for all users.

      IMPORTANT: Use this only for files or folders that absolutely must be excluded from scanning. For example, if you exclude / from scanning, the whole system volume and all folders, subfolders, and files in it will be excluded from all security measures.

   c) Add paths to **Trusted applications**.

      List of paths to trusted applications and processes. Any files that are opened by these applications and processes are not scanned, regardless of their location.

      IMPORTANT: Use this only for applications and processes that absolutely must be trusted. For example, if you add / here, all applications and all files will be excluded from all security measures.

   d) Turn on **Scan only executables** to scan only executable files.

      This setting allows to scan only executable files.

   e) Turn on **Scan for potentially unwanted applications**.

      This setting turns on scanning of potentially unwanted applications.

7. Choose how to handle archives in real-time scanning
   a) Turn on **Scan inside archives** to scan files inside archives.

      Enable scanning files inside archives.

b) Turn on **Treat encrypted archives as unsafe** to handle encrypted archives as malware.

Encrypted archives will be handled as malware.

c) Set **Scan archive up to nesting level** to the maximum nesting level to scan.

Set max nesting level to scan archive.

d) Turn on **Treat archives that exceed the maximum nesting level as unsafe**.

Archives that exceed the maximum nesting level will be handled as malware.

8. Choose actions for real-time scanning
   a) Select the **Action for malware**: **Do nothing**, **Rename**, or **Remove**.

   Choose action for malware: **Do nothing**, **Rename**, **Remove**.

   NOTE: Access will be blocked regardless of chosen action.

   b) Select the **Action for potentially unwanted applications**: **Do nothing**, **Rename**, or **Remove**.

   Choose action for PUA(potentially unwanted application). Note: Access will be blocked regardless of chosen action.

   c) Select the **Action for suspicious files**: **Do nothing**, **Rename**, or **Remove**.

   Choose action for suspicious files.

   NOTE: Access will be blocked regardless of chosen action.

9. Select **Save Profile** to apply your changes.

5.6.12 Set up integrity checking for Linux

Integrity Checking protects the system from unauthorized modifications by verifying files against a trusted baseline.

Integrity Checking relies on a known good configuration. Turn it on only when you are sure the system is in a trusted state. With Integrity Checking, you create a baseline of system files to protect. Any modified files outside this baseline can be blocked for all users.

To configure Integrity Checking:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Linux** tab, and then select a profile.
   *The **Profile for Linux** page opens.*
3. From the menu on the left, select **Integrity checker**.
4. Turn on **Check the integrity of the files** to enable file integrity verification.
5. (Optional) Turn on **Integration with apt package manager**.

   Turning on the integration with apt package manager temporarily disables integrity checking during apt package installation, updates, or removal. After changes, the baseline is automatically updated.
6. (Optional) Turn on **Integration with DNF package manager**.

   Turning on the integration with DNF package manager temporarily disables integrity checking during DNF package installation, updates, or removal. After changes, the baseline is automatically updated.
7. Configure Integrity Rules

Add rules to create a baseline for specific files or directories.

- Integrity is verified only for files in specified directories.
- Adding new files does not break the baseline, new files are ignored until you update the baseline.
- Disabling and re-enabling the profile regenerates the baseline.

a) Add a **Path** to include in integrity checking.
b) In **Exclusions**, specify file name patterns to exclude from integrity checking in the selected path.
c) Set **File write** permission: choose **Allow** or **Deny**.

   Deny prevents writing to the file.

d) Set **File read** permission: choose **Allow** or **Deny**.

   Deny prevents reading from a tampered file.

e) Select the file attributes to include in the integrity baseline.

   If **File read** is set to **Deny**, reading is blocked when any of these attributes change:

   - **Access mode**: Prevents reading if access mode changes.
   - **Owner**: Prevents reading if file owner changes.
   - **Group**: Prevents reading if group changes.
   - **Size**: Prevents reading if file size changes.
   - **Modification time**: Prevents reading if modification timestamp changes.

8. Select **Save Profile** to apply your changes.

5.7 Managing mobile device profiles

Information on how to manage mobile device profiles in WithSecure Elements Security Center.

A profile is a bundle of settings that you assign to WithSecure Elements Mobile Protection devices. This section describes how to create a profile and configure its settings, including VPN, browsing protection, malware protection, scheduled scans, and website and app exceptions.

5.7.1 Create a new mobile device profile

You can create profiles that can be assigned to specific mobile devices.

To create a new profile:

1. Log in to WithSecure Elements Security Center.
2. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
3. Select the **For Mobile** tab.
4. Select

   next to an existing profile, and select **Clone profile**
   *The **Profile for Mobile** page opens.*
5. Enter a name and description for the new profile, and select a type for the new profile.
6. Make desired changes to the settings, and then select **Save and Publish**.
   The new profile is created.

5.7.2 Turn on Network Gateway

Network Gateway keeps mobile phone apps safe by checking their internet traffic for threats and blocking malicious requests.

To turn on Network Gateway:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab, and then select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
3. Under **Network Protection**, turn on **Network Gateway**.

NOTE: You can select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.

4. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

5.7.3 Send activation reminders for browser plugins

You can choose to send users reminders to install or activate Browsing protection plugin.

NOTE: This applies only to iOS devices.

When this setting is on, users get reminders to install the Browser protection plugin, if it is missing or activate it for the supported browser, if it is installed but not activated.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
4. From the left pane, select **Network Protection**.
5. Turn on **Remind user to activate browser plugin**.
6. Select **Save and Publish**.
   Your changes are saved and published to the selected profile.

5.7.4 Turn on reputation-based browsing

Reputation-based browsing blocks websites that are suspicious or known to be malicious.

To turn on reputation-based browsing:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
4. Under **Network Protection**, turn on **Reputation-based browsing**.
5. Under **Reputation-based browsing**, you can turn on the following:
   - **Block access to websites rated as harmful**
   - **Block access to websites rated as suspicious**
   - **Block access to websites rated as prohibited**

- **Block trackers found on websites**
- **Block access to recently created domains**

NOTE: Select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.

6. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

5.7.5 Select web content to block

You can select the types of web content that you want to block.

Web content control blocks websites based on their content.

NOTE: Turning on the Unknown category blocks access to websites whose reputation is unknown.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
4. From the menu on the left, select **Network Protection**, and scroll down to **Web content control**.
5. Turn on **Web content control**.
6. Select next to **Web content control**.
   The list of web content categories opens.
7. In the **Disallowed** column, turn on the categories that you want to block for mobile devices.
8. In the **Alert** column, turn on the categories for which you want a security event to be sent.

NOTE: If you turn on **Block everything except allowed sites**, it overrides your selections in the **Web content control** table.

9. Select **Save and Publish**.

5.7.6 Allow and block websites

You can add websites to the allowed and denied websites list.

To allow or block websites:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the desired profile.
   *The **Profile for Mobile** page opens.*
4. From the menu on the left, select **Network Protection**, and scroll down to **Website exceptions**.
5. Under **Web site exceptions**, do the following:
   a) To allow a website, under **Allowed sites**, select **Add site** and enter the website URL in the **Address** field.

b) To block a website, under **Denied sites**, select **Add site** and enter the website URL in the **Address** field.

NOTE: You can enter a description in the **Notes** field.

5.7.7 Show blocked website URLs in security events

You can turn on this settings if you want the security events to contain detailed information about the blocked URLs.

NOTE: When this setting is turned off, only malicious URLs are shown in the security events.

IMPORTANT: The local legislation governing the monitoring of users' web activity may restrict your ability to turn on this feature. It is your responsibility to fully understand how your local laws relate to this feature and make sure that you adhere to them.

To include information about blocked URLs:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
4. Under **Network Protection**, scroll down to **Include the blocked URLs in all security events** and turn it on.

Detailed information about the blocked URLs is included in the security events.

5.7.8 Show blocked malicious website URLs in security events

You can turn on this settings if you want the security events to contain detailed information about the blocked malicious URLs.

NOTE: When this setting is turned off, only blocked URLs are shown in the security events.

IMPORTANT: The local legislation governing the monitoring of users' web activity may restrict your ability to turn on this feature. It is your responsibility to fully understand how your local laws relate to this feature and make sure that you adhere to them.

To include information about blocked malicious URLs:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
4. Under **Network Protection**, scroll down to **Include the blocked malicious URLs in all security events** and turn it on.

Detailed information about the blocked malicious URLs is included in the security events.

5.7.9 Add app exceptions

You can add apps as trusted applications that connect to the internet directly, bypassing the protection of Network Gateway.

NOTE: This applies only to Android devices.

To add an app exception:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the desired profile.
   *The **Profile for Mobile** page opens.*
4. From the menu on the left, select **Network Protection**.
5. Under **App exceptions**, select **Add applications** and do the following:
   a) Make sure that the switch in the **Active** column is on
   b) In the **Description** column, enter the app name.
   c) In the **App name (ID)** column, enter the application ID as it appears in the Google Play Store.
6. Select **Save and Publish**.

5.7.10 Turn on malware protection

When on, malware protection scans files and applications.

NOTE: This applies only to Android devices.

To turn on malware protection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
4. From the left pane, select **Malware Protection**.
5. Turn on **Malware Protection**.

NOTE: Select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.

6. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

5.7.11 Turn on metered scan

A metered network connection has a limit on how much data can be used.

You can allow scanning over metered connections. Exceeding the limit may incur extra costs.

NOTE: This applies only to Android devices.

To turn on metered scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
4. From the left pane, select **Malware Protection**.
5. Turn on **Metered scan**.
6. Select **Save and Publish**.
   Your changes are saved and published to the current profile.

5.7.12 Select action on infections

You can select an action for infected objects.

NOTE: This applies only to Android devices.

To select an action:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
4. From the menu on the left, select **Malware Protection**.
5. From the **Action on infections** drop-down menu, select the desired action for infected objects:
   - Delete - this option automatically removes the infected objects from your device
   - Ask after scan - you need to manually remove the infected objects from your device

5.7.13 Schedule scans on mobile devices

Set your device to scan and remove malware and other harmful applications automatically periodically to make sure that your device is secure.

NOTE: This applies only to Android devices.

To schedule a scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
   *The **Profile for Mobile** page opens.*
4. From the menu on the left, select **Malware Protection**, and scroll down to **Scheduled scanning**.
5. Turn on **Scheduled scanning**.
6. Select the arrow next to **Scheduled scanning**.
   *The **Scan frequency** drop-down menu appears.*
7. From the drop-down menu, select how often you want to scan your device automatically.

Option	Description
Daily	Scan your device every day.

Option	Description
Weekly	Scan your device on selected days of the week. Select the weekday from the list.
Every four weeks	Scan your device on a selected weekday at four-week intervals. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday.
Monthly	Scan your device on a selected weekday every month. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday.

8. Select **Save and publish**.
   Your changes are saved and published to the current profile.

Chapter 6
Monitoring security

Topics:

- Device operations
- Monitoring device security
- View security events
- Scan Active Directory for unprotected devices
- Isolate devices from network
- Remove devices
- Using third-party RMM tools

Monitoring security

With WithSecure Elements Security Center, you can monitor the security status of all protected computers and mobile devices.

As a Solution Provider or Service Partner, you can choose to view devices in either Organizational or List view. The Organizational view shows all the devices per companies, whereas the List view lists all the devices under the administration of a selected Solution Provider or Service Partner.

NOTE: You can add new devices or import mobile devices only in a Company view.

You can view detailed information about the status of a particular device, including:

- Most recent updates to the malware and browsing protection on the device
- License key used for the device, and length of remaining subscription period
- A history of blocked malware, harmful sites and tracking attempts

6.1 Device operations

The operations you can run on a selected device from WithSecure Elements Security Center, such as scanning, assigning a profile, isolating, or uninstalling.

Available device actions

You can also send instructions to a particular device to perform certain actions, such as:

- Send (a full) status update - request a status update from one or more devices to make sure Elements Security Center has the latest status information.
- Install software updates - select software updates in different categories to be installed in selected devices
- Scan (for malware or updates) - remotely trigger a manual scan on one or more devices.
- Assign profile - assign a profile to selected devices
- Manage labels - add, replace, or remove a label to selected devices
- Change subscription - change the existing subscription for the selected devices
- Remove device - remove one or more devices from the system
- Network isolation - isolate one or more devices from the network, for example, in case of a network attack.

  IMPORTANT: You should use this option with the utmost caution.

  NOTE: You can isolate a device also through Elements Security Center.

- Restart system - restart the system automatically. Users cannot stop the device from restarting but they have five minutes to save all the data.
- System drive protection - encrypt or decrypt a system drive
- Diagnostic operations - select 'Request diagnostic file' to send a request to users to allow diagnostic data to be uploaded to WithSecure. For privacy reasons, the users are asked for their acceptance. You can also select to turn on debug logging and select the time after which it will automatically turn off.
- Send the device a message - send a message to the selected devices. All logged-in users see the message.

- Turn off security features - select a security feature to turn off (firewall, DeepGuard, real-time scanning, resource protection), or turn off all security features
- Uninstall - uninstall the software from a device. Uninstalling frees up the subscription and deletes all information about the device from the system

6.2 Monitoring device security

You can use WithSecure Elements Security Center to monitor the security status of all protected computers and mobile devices.

NOTE: You can use the *scope selector* to select the level of information detail you wish to display in Elements Security Center. You can use it to switch between:

- A broad overview of all your customer companies OR
- A detailed view of information related to a selected company

6.2.1 View the device security overview

You can see an overview the security status of all devices registered to your WithSecure Elements Security Center on the **Home** page.

To view the security status of registered devices:

1. Select **Home** on the sidebar.

   The **Home** page is displayed.

   The Home page has the following tabs:

   - **Overview** shows the following:
     - Endpoint Protection
     - Detection and Response
     - Collaboration Protection
     - Usage for last 30 days
     - Subscriptions
   - **Endpoint Protection** shows the following:
     - Workstations protection status
     - Servers protection status
     - Software updates status
     - Mobiles protection status
     - Issues - a list of issues to be addressed (the item type, severity, and the number of affected devices)
   - **Detection and Response** shows the following:
     - Devices at risk
     - Overview
     - Open detections by risk
     - Detections by status
     - Detections by category
     - OS by number of devices
   - **Exposure** (requires an Exposure Management subscription) shows the following:

- Coverage
- Organization exposure risk
- Highest impact recommendations
- Exposure risk by category
- Assets with the highest exposure risk

- **Cloud Security Trends** (requires an Exposure Management subscription) shows the following:
  - Number of findings
  - Number of scanned resources
  - Finding with tags
  - Findings severities
- **External Attack Surface** (requires an Exposure Management subscription) shows the following:
  - Total asset count
  - Recently found assets
  - Assets over time

NOTE: Without an Exposure Management subscription, the **Exposure**, **Cloud Security Trends**, and **External Attack Surface** tabs show the **Request trial** button and links instead of their widgets.

2. To display more detailed **Company status** information for the selected company on the **Home** page, select the company in the *scope selector*.

6.2.2 Filter devices

You can use filtering to find devices in WithSecure Elements Security Center.

To use filtering:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. From the Filter drop-down menu, select a category for filtering the devices.
3. From the Value drop-down menu, select the desired value for the selected category.

NOTE: For example, if you select **Connectivity status** as the category and **Connected** as the value, you will see all the devices that are currently connected.

TIP: You can use the search function together with filtering.

4. Select **Apply**.
5. To reset the selected filter category and the value, select **Clear filters**.

NOTE: You can remove a filter by selecting the X next to the filter.

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

6.2.3 Search for mobile devices

You can use various search criteria to find mobile devices.

The mobile device search uses the following information to match your search string:

- Device UUID
- Device name
- Labels
- Last user
- UPN
- IP address
- Subscription key

To search for a mobile device:

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

   TIP: You can use also the filtering function when searching for devices.
3. Enter your search string in the **Search** field.
   The list of mobile devices shows the devices that match your search string.

6.2.4 Viewing a device's protection status

You can find more information about each individual device added to your WithSecure Elements Endpoint Protection account, including its protection status, subscription details, device information, installed software and statistics.

Each device added to WithSecure Elements Endpoint Protection has a details view that shows its protection status, subscription details, device information, installed software, and statistics.

View more details of a device's protection status

On the Devices page, you can view different details of device protection status.

To view more details of a specific device:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. On the Devices page, select the **Computers**, **Mobile devices**, **Connectors**, or **Unmanaged devices** tab.
   *A table is shown containing details of devices matching the selected type. The **Overall status** view is shown by default.*
3. To change the view to show other device details, select the arrow next to the **View drop-down** list.
   A menu opens listing the available views.
4. Select one of the available views to see additional information about the devices

   For computers, the following views are available:

   - Overall status
   - Configuration details
   - Compliance
   - Hardware info
   - Needing reboot

- Running out of space
- All fields
- EDR status
- Vulnerability management

For mobile devices, the following views are available:

- Protection overview
- All fields

For Connectors, the following view is available:

- Connector all

The table is updated to show the selected information.

6.2.5 View device security posture

You can review your devices' compliance with security recommendations on the **Device Security Posture** page.

To view security recommendations for your devices:

1. In WithSecure Elements Security Center, select **Device Security Posture** under **Environment** on the sidebar.
   *The **Device Security Posture** page is displayed. The **Security recommendations** panel shows how many recommendations your devices are **Compliant** and **Non compliant** with, followed by a table of individual recommendations.*
2. Review the table columns to assess your devices' security posture.

   The table shows the following columns:

   - **Security recommendation** - the name of the recommended security setting.
   - **Status** - whether your devices are compliant or non-compliant with the recommendation.
   - **Devices** - the number of devices affected by the recommendation.
   - **Profiles** - the number of profiles affected by the recommendation.
   - **Supported** - the platforms that the recommendation is supported on.

   You can filter the table by **Security recommendation** or **Supported OS**.

3. Select a recommendation to view more information.
   A panel opens showing a description of the setting, the potential risk if it is not resolved, and links to related vendor documentation.
4. Resolve a recommendation by updating the setting that it describes.

   Some recommendations, such as **User is allowed to uninstall client without password in the profile**, are resolved by updating the corresponding setting in a profile. Others, such as **Minimum password length is not defined or less than 8 characters**, are resolved by changing an operating system-level setting, such as a Group Policy setting.

6.3 View security events

Use the **Security Events** page to review all detected security events in your system and take appropriate actions.

To view security events:

1. Use the scope selector to select the company for which you want to view the security events.
2. Open the **Security Events** page.

In the sidebar, under **Events**, select **Security events**.

The **Security Events** page displays the following information:

- **Time** - The timestamp when the security event was detected.
- **Severity** - Indicates the criticality of the event (low, medium, high).
- **Source** - The origin of the event.
- **Device** - The name or identifier of the device where the event was detected.
- **Description** - A summary of the event.
- **Acknowledged** - Shows whether the event has been reviewed.

3. To view event details, select the

icon next to the event.

The **Details** view opens. It includes:

- **Incident ID** - A unique identifier for the security event.
- **Risk** - Assessed threat level.
- **Resolution** - Action taken to resolve the event.
- **Fingerprint** - Unique hash of the detected file or threat.
- **Initial detection timestamp** - Time of the detection.
- **Username** - User account under which the event occurred.
- **Client timestamp** - Time recorded by the client device.
- **Transaction ID** - Identifier for event processing.
- **Device UUID** - Unique identifier of the device.

4. Take action on the event:

Open **Menu** next to the event to choose one of the following actions:

- **Acknowledge** - Mark the event as reviewed.
- **Show all target events** -View all events related to the same target.
- **Show similar events** - Display events with similar characteristics.
- **Delete from quarantine** - Permanently remove the quarantined file.
- **Restore to the original location** - Return the quarantined file to its original location.
- **Report a possible false positive detection** - Notify WithSecure about a detection that may be incorrect to improve future threat detection accuracy.
- **Exclude the file by full path** - Prevent future detections of the file based on its full path.
- **Exclude the file by hash** - Prevent future detections of the file based on its unique hash value.

6.3.1 Filter security events

You can filter the security events shown in the **Security Events** page.

To filter security events:

1. Under **Events**, select **Security Events** on the sidebar.
   *The **Security Events** page opens.*
2. From the drop-down menu, select **Device type**.
3. From the **Select value** drop-down menu, select one of the following filtering options
   - Active Directory Organizational Unit

NOTE: This option is available only in the company level.

- Device Label
- Device type
- Device UUID
- Event ID
- Source
- Target
- Time
- URL

4. From the **Select value** drop-down menu, select one of the options.

NOTE: You can also enter a search term in the drop-down menu.

NOTE: You can see security event details by selecting the arrow in front of the relevant event.

5. Select **Apply**.
   The Security events table shows the filtered events.

6.4 Scan Active Directory for unprotected devices

Scans your company Active Directory for devices not yet managed by WithSecure.

Unprotected devices are computers or servers in your company Active Directory that are not yet managed by WithSecure. Unprotected devices are either new ones or devices that have been permanently deleted from WithSecure Elements Security Center.

When the scan starts, Elements Security Center automatically selects one or more devices that run the scan operation on each Active Directory node. These devices are WithSecure-managed devices that are listed on the **Devices** page. For scan operations, Elements Security Center always selects devices that have contacted it recently.

Information about unprotected devices is useful especially for troubleshooting. For example, if scanning fails, the reason can be found in one of the devices. If you want to run the operation by other devices, you need to start a new scan.

To scan for unprotected devices:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the **Unmanaged devices** tab.
3. Select **Start scan**.
   The system scans your company's Active Directory for any unprotected devices. When the scan is complete, the top of the page shows the node name and the device that was used for the scanning. The unprotected devices are listed below in the table showing the following information:

   - DNS name
   - Date when the device was created in an Active Directory
   - Date of the last login
   - Active Directory comment
   - Operating system
   - Active Directory Organizational Unit
   - Active Directory GUID
   - Comments

- Status
- Column with the

  icon with the following options: Mark as trusted, Comment

NOTE: The list of unprotected devices is cleaned up in 24 hours after the scan is finished.

NOTE: To add an unprotected device to Elements Security Center, you need to manually install WithSecure Elements Agent on it.

4. If you trust a device even when it is not protected with WithSecure Elements Agent, you can mark it as trusted. To do this, select

   on the row of the device.
5. Select **Mark as trusted**.
6. You can also leave a comment about the unprotected device. To do that:
   a) Select

      on the row of the device, and then select **Comment**.
   b) Enter your comment, and select **Save**.

6.5 Isolate devices from network

You can isolate one or more devices from the network.

NOTE: Network isolation does not apply to mobile devices.

To isolate a device from the network:

NOTE: Use network isolation with caution and only in case of a network attack.

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select the devices that you want to isolate from the network.
3. From the action menu at the bottom of the page, select **Network isolation** > **Isolate from network**.
   The selected devices are isolated from the network.
4. To connect an isolated device back to the network, select **Network isolation** > **Release from network isolation**.

When you release a device from isolation, it can communicate with the network again.

6.6 Remove devices

Removes devices from WithSecure Elements Security Center, freeing up the subscription seat.

Removing a device frees up the subscription. If a device that has been removed from WithSecure Elements Security Center becomes active again and if there are free seats in the subscription, the device is shown

again in WithSecure Elements Security Center If there are no free seats in the subscription, the device is not shown in Elements Security Center and the device is not protected.

If you check the **Block device from returning** option, the device is moved to a blocklist.

NOTE: You can add the device back again by selecting the

icon next to **Devices** and then the **Manage removed devices** option from the drop-down menu. When the device reconnects and if there are free seats in the subscription, the device is shown again in the device list.

To remove devices:

1. Under **Environment**, select **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Select one or more devices that you want to remove from Elements Security Center.

NOTE: Make sure that you selected the correct devices before you remove them.

3. From the action menu at the bottom of the page, select **Remove device**.
4. Do one of the following:
   - To remove the selected devices, select **Remove device**.
   - To move the selected devices to a blocklist, select **Block device from returning**, and select **Remove device**.

Depending on your selection, the selected devices are either removed from Elements Security Center or moved to a blocklist.

NOTE: By using **Restore devices from blocklist** under **Management** > **Subscriptions**, you can add back a device that you have moved to the blocklist. In that case, the device will reappear in the device list when it reconnects and if there are free licenses in the subscription.

6.7 Using third-party RMM tools

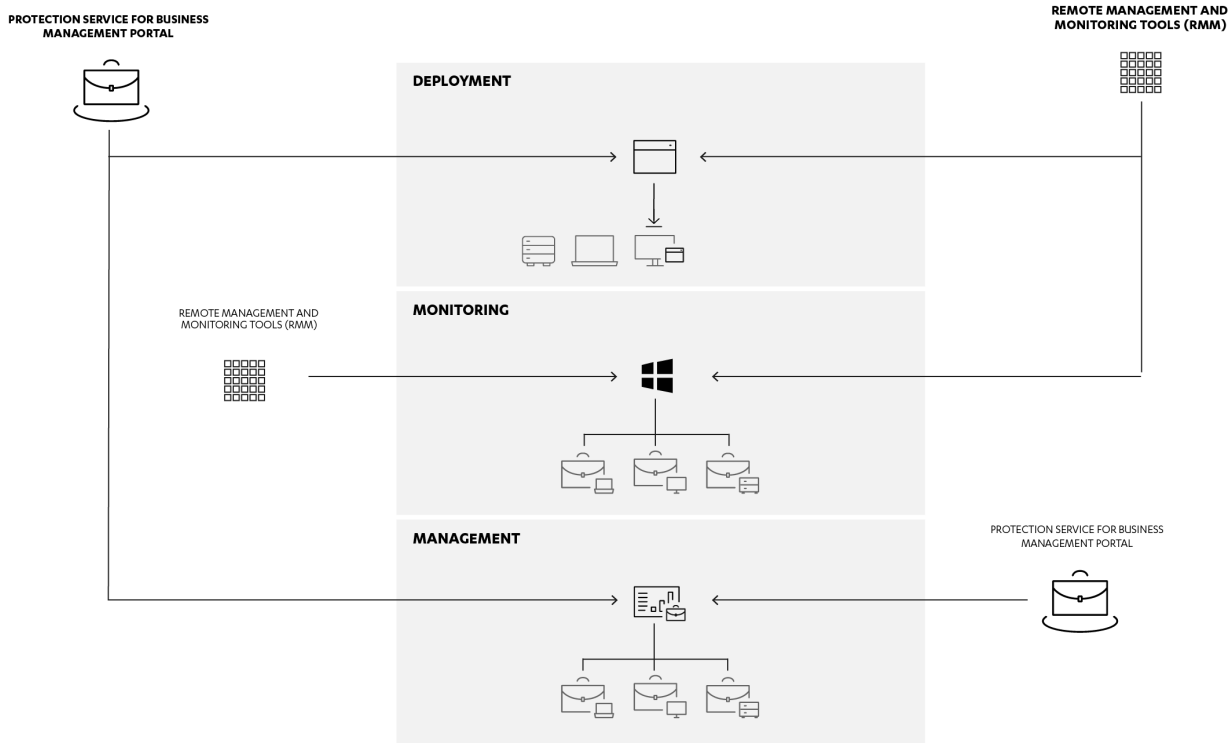
WithSecure Elements EPP supports the integration of third-party Remote Monitoring and Management (RMM) tools.

NOTE: The current version of WithSecure Elements EPP supports Datto, Kaseya, and SolarWinds RMM tools. Use the Windows Management Instrumentation (WMI) API with other RMM tools.

You can deploy, monitor, and manage your system using WithSecure Elements Security Center. If you, however, want to use RMM tools, you can do the following:

- Deploy the MSI packages and monitor your system through the RMM tools, and manage the system through Elements Security Center.
- Deploy and manage your system through Elements Security Center, and monitor the system through the RMM tools.

NOTE: You can manage your system only through Elements Security Center.



6.7.1 Integration with Kaseya RMM for Windows computers

The Kaseya portal can monitor and manage WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers through a set of pre-created agent procedures.

WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers can be monitored and managed from the Kaseya portal through a set of pre-created agent procedures.

You can download the pre-created agent procedures from the WithSecure download site.

After you import the procedures, the following agent procedures are available. You can use Kaseya standard means to schedule some or all of them, depending on your needs.

CheckProductInstalled Detects whether the WithSecure Elements EPP for Computers or WithSecure Elements EPP for Servers software is installed. If the product is not installed, an alert is issued. The procedure is called by all other procedures because the product installation is required for them to work.

CheckWmiProviderEnabled Detects whether a WMI Provider module is on. If the module is off, an alert is issued. This procedure is called by all other procedures (except for CheckProductInstalled) because the WMI Provider module is required for them to work.

NOTE: You can turn the WMI Provider on in WithSecure Elements Security Center in the Profile settings.

CheckLicenseStatus Verifies the subscription status of a product. If a subscription is expired or it is not installed, an alert is issued.

CheckDefinitionsAreUpToDate Checks whether antivirus definitions are updated. If the definitions are more than seven days old, an alert is issued. This may indicate problems with Internet connection or other failures.

CheckConnectivityToManagementPortal	Checks the connectivity to Elements Security Center. If the successful connection to it was more than 24 hours ago, an alert is issued. This may indicate problems with Internet connection or other failures.
RunFullComputerScan	Runs a full computer scan. If any infected objects are detected, an alert is issued.
CheckRealTimeScanning	Checks whether real-time scanning is on. If it is off, an alert is issued.
CheckDeepGuard	Checks whether the DeepGuard module is on. If it is off, an alert is issued.
CheckFirewall	Checks whether the Firewall module is on. If it is off, an alert is issued.
CheckBrowsingProtection	Checks whether the Browsing Protection module is on. If it is off, an alert is issued.
CheckSoftwareUpdater	Checks whether the Software Updater module is on. If it is off, an alert is issued.

Import agent procedures

Import the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers installation and monitoring procedures into the Kaseya portal.

To import agent procedures:

1. Log in to the Kaseya portal.
2. Open the **Agent Procedure** module.
3. Under **Manage Procedures**, select **Schedule/Create**.
4. In the pane on the right, right-click **Shared**.
5. From the menu that opens, select **Import Folder/Procedure** to specify the XML file (`Kaseya_F-Secure.xml`) that you want to upload.

6.7.2 Install the Kaseya agent on remote Mac computers

Installs the Kaseya agent on a remote Mac computer.

To manually install the Kaseya agent to a remote computer:

1. Log in to the Kaseya portal.
2. Select **Agent** > **Packages** > **Manage Packages** to download the agent package.

NOTE: The full filename for a Macintosh agent install package is `KcsSetup.app`. The package is downloaded as a `KcsSetup.zip` file that contains the `KcsSetup.app` inside a folder called Agent.

3. Select the `KcsSetup.zip` file to expand it.
4. Select the Agent folder.
5. Select the `KcsSetup.app` file to execute it.
6. Install the WithSecure Elements EPP for Computers (Mac) software using a Kaseya agent procedure, as described in Install WithSecure Elements EPP for Computers (Mac).

Install WithSecure Elements EPP for Computers (Mac)

Installs WithSecure Elements EPP for Computers (Mac) using a Kaseya agent procedure.

To install WithSecure Elements EPP for Computers (Mac) using a Kaseya agent procedure:

1. Upload the PKG file by navigating to the Agent Procedure module.
2. Select **Schedule / Create** > **Manage Files**.
3. Upload the file on the server.

NOTE: Only the files stored on the server can be sent to the agents via scripts.

4. To create new agent procedures, select **Agent Procedures** > **Schedule/Create** > **New Procedure**.

NOTE: Kaseya provides limited agent procedure modules for OS X.

NOTE: You can use the `writeFile` module to write the PKG file to a location in the remote machine. To install the package, use the `installPKG` module. For example:

```
writeFile("F-Secure_PSB_Mac_Installer[License key].pkg", "/tmp/ F-
Secure_PSB_Mac_Installer[License key].pkg", "Mac OS X", "Halt on Fail")
installPKG ("/tmp/ F-Secure_PSB_Mac_Installer[License key].pkg", "Mac OS X", "Halt on
Fail")
```

5. To execute or schedule an agent procedure, select the newly created agent procedure from the list of agent procedures.
6. Select the target devices.
7. Select either Schedule Agent Procedures or Run Now.

6.7.3 Integration with Kaseya RMM for Linux computers

The Kaseya portal can install and monitor WithSecure Linux Protection through a set of pre-created agent procedures.

Kaseya lets you install and monitor WithSecure Linux Protection on the Linux computers you manage. This section describes how to import the agent procedures, install the software, and install it remotely through the Kaseya portal.

You can download the pre-created agent procedures from the WithSecure download site.

Import agent procedures

Imports the WithSecure Linux Protection installation and monitoring procedures using the Kaseya portal.

To import agent procedures:

1. Log in to the Kaseya portal.
2. Open the **Agent Procedure** module.
3. Under **Manage Procedures**, select **Schedule/Create**.
4. In the pane on the right, right-click **Shared**.
5. From the menu that opens, select **Import Folder/Procedure** to specify the XML-file (`Kaseya_F-Secure_Linux_Procedures.xml`) that you want to upload.

Agent procedures

The following agent procedures are available for checking the WithSecure remote client status and reporting it to the Kaseya RMM portal.

- *CheckProductInstalledForLinux* - detects whether the WithSecure Linux Protection software is installed. If the product is not installed, an alert is issued. The procedure is called by all other procedures because the product installation is required for them to work.

- *CheckLicenseValidForLinux* - verifies the subscription status of a product. If the product is switched off, an alert is issued. If the subscription is expired or it is not installed, an alert is issued. The procedure is called by all other procedures (except for `CheckProductInstalledForLinux`) because the product needs to be active for feature checks to work.
- *CheckRealTimeScanningForLinux* - checks whether the real-time scanning is on. If it is off, an alert is issued.
- *CheckIntegrityCheckingForLinux* - checks whether the integrity checking is on. If it is off, an alert is issued.
- *CheckDatabaseUpToDateForLinux* - checks whether the antivirus definitions are up to date. If the definitions are more than seven days old, an alert is issued. This may indicate a problem with internet connection or other failures.

NOTE: Depending on what you need, you can use the Kaseya standard means to schedule some or all of these procedures.

Install the Kaseya agent on remote computers

Installs the Kaseya agent on a remote computer.

To install the Kaseya agent:

1. In the Kaseya portal, select **Agent** > **Packages** > **Manage Packages** to download the agent package (`KcsSetup.sh`).
2. Run the downloaded file.

Install WithSecure Linux Protection

Installs the WithSecure Linux Protection software using the Kaseya portal.

To install WithSecure Linux Protection:

1. In WithSecure Elements Security Center, open the **Downloads** page.
2. Under Linux, select **Generic** to download the `linuxsecurity-installer.tar` archive.
3. Extract the `linuxsecurity-installer` file from the tar archive.
4. To create an agent procedure to install the software on the remote device, do the following:

NOTE: Kaseya provides limited agent procedure modules for Linux.

a) Open the **Agent Procedure** module to upload the extracted installer file to the Kaseya portal.
b) Select **Schedule/Create** > **Manage Files**.
c) Upload the file to the server.

NOTE: Only the files that are stored on the server can be sent to the agents via scripts.

d) Use the sample agent procedure as a basis for your software installation procedure.
Edit the `Install Linux Protection (edit before use)` procedure to include your subscription key for WithSecure Linux Protection and to correct the path to the uploaded installer.

NOTE: Make sure that the remote device has dependencies (specific to your distribution) installed for WithSecure Linux Protection before you actually install the product. You can use the `executeShellCommand` or `executeShellCommandToVariable` statement to add

the installation of the necessary packages to the sample procedure. For more information, see the Linux Protection documentation.

e) To schedule the execution of an agent procedure, select the agent procedure from the list of available procedures.
f) Select the target devices.
g) Select either **Schedule Agent Procedures** or **Run Now**.

6.7.4 Integration with SolarWinds MSP RMM for Windows computers

You can manage the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers software using SolarWinds MSP.

For more information, see the SolarWinds MSP official documentation at:
https://secure.n-able.com/webhelp/NC_11-0-0_en/Content/Help_20/Services/FSecure/Services_FSecureCentralMgmt.htm and
https://secure.n-able.com/webhelp/NC_11-0-0_en/Content/Help_20/Automation/Policies/F_Secure/pol_FSecure_AV_Protection.htm.

6.7.5 Integrate with SolarWinds MSP RMM for Mac computers

Manages the WithSecure Elements EPP for Computers (Mac) software using SolarWinds MSP.

Installing the product on remote devices using MSP N-Central:

1. Log in to the MSP N-Central.
2. Download the macOS agent to remote macOS devices.

NOTE: Make sure that the devices are available in the **All Devices** view and the **Remote Control** option is active for the selected remote devices.

NOTE: You also need to have the following available:

- the product subscription key
- the package for WithSecure Elements Agent for Computers (Mac), locally or in the network share

3. Use **Remote Control** to copy the WithSecure Elements Agent for Computers (Mac) package to the remote devices.
4. Run a Mac script task to execute the install_mac_client.sh script in the remote devices.

NOTE: Executing the script requires administrator privileges. This script accepts the following command line arguments: the package path on the remote device, the package name, and the product subscription key.

```
sh install_mac_client.sh -p /Users/Shared/F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg
 -n F-Secure_PSB_Mac_Protection.B20766.C20766.mpkg -k 4T16-E2VW-U2U9-J5V8-9Z0F
```

Import custom services for reporting

Instructions on how the WithSecure remote client reports its status to the SolarWinds RMM portal.

To import custom services:

1. Make sure that the WithSecure Elements EPP for Computers (Mac) software is installed in the remote computer.
2. Select **Administration** > **Service Management** > **Custom Services** > **Import**.
3. Browse and import all the xml files that contain the custom services for reporting.

NOTE: The xml files are available from the following link: https://download.withsecure.com/PSB/RMM/Solarwinds/Solarwind_F-Secure_Custom_services_for_Mac

4. To add the custom services for monitoring, do the following:
   a) Go to **Views** > **All devices** to select the device that monitors these custom services.
   b) Then select **Device Details** > **Monitoring** > **Add**.
   You can see all the custom services that you imported earlier.
   c) Add each of these custom services.
   d) Apply the changes.

The services are updated and you can see a report of all the individual settings of the WithSecure client on the remote machine. Based on the status of each setting, the report shows either a failure or a warning if the expected behavior does not match.

Available custom services for Mac computers

Depending on the requirements, you can import the relevant custom service.

- WithSecure AV Database status for Mac - displays the database status. If the database is not up to date, a warning is shown.
- WithSecure AV Firewall Management for Mac - displays the status of the system firewall. If firewall is off, a warning is shown.
- WithSecure AV Protection status for Mac - displays the status of the real-time scanning. If real-time scanning is off, an error is shown.
- WithSecure AV Safari Extension for Mac - displays if Safari Extension is turned on. If turned off, a warning is shown.
- WithSecure AV Virus Protection for Mac - displays the status of virus protection, for example, "license expired", "OAS disabled", "OAS malfunction", or "old updates".
- WithSecure Browsing Protection status for Mac - displays the status of browsing protection. If turned off, a warning is shown.

6.7.6 Integration with SolarWinds MSP RMM for Linux computers

WithSecure Linux Protection on managed Linux devices can be monitored through SolarWinds MSP N-Central.

Monitoring a Linux device and the status of the WithSecure Linux Protection software in it requires that SolarWinds's own Linux agent is running on the device. You can find the installation instructions in the Install a Linux agent section of the N-Central User Guide.

NOTE: Automating the installation of the WithSecure Linux Protection software on remote devices is not possible due to limited Linux device support in MSP N-Central. The installation

instructions of the WithSecure Linux Protection software are available in the Linux Protection installation guide.

Import custom services for reporting

Reports the WithSecure remote client status to the SolarWinds RMM portal.

To import custom services

1. Make sure that you have installed the WithSecure Linux Protection software on the remote computer and turned on the rmmd service.
2. Select **Administration** > **Service Management** > **Custom Services** > **Import**.
3. Browse and import all the xml files that contain the custom services for reporting.

NOTE: The xml files are available from the following link: https://download.withsecure.com/PSB/RMM/Solarwinds/SolarWinds_F-Secure_Custom_Services_for_Lir

4. To add the custom services for monitoring, do the following:
   a) Go to **Views** > **All devices** and select the device that monitors these custom services.
   b) Select **Device Details** > **Monitoring** > **Add**.
   You can see all the custom services that you imported earlier.
   c) Add each of these custom services.
   d) Apply the changes.

The services are updated and you can see a report of all the individual settings of the WithSecure client on the remote machine. Based on the status of each setting, the report shows either a failure or a warning, if the expected behavior does not match.

Available custom services

Depending on the requirements you can add the relevant custom services for monitoring.

The following are the available custom services for Linux computers:

- WithSecure AV database status for Linux - displays the database status. If the database is not up to date, a warning is shown.
- WithSecure AV Integrity checking protection status for Linux - displays the status of the integrity checking. If integrity checking is off, an error is shown.

NOTE: The feature is considered to be off also when there are no file paths added for integrity checking.

- WithSecure AV license status for Linux - displays the status of the product license. If the license is not valid, an error is shown.
- WithSecure AV product status for Linux - displays the status of the product's master-switch. If the product has been turned off, an error is shown.
- WithSecure AV real-time protection status for Linux - displays the status of the real-time scanning. If real-time scanning is off, an error is shown.

NOTE: The feature is considered to be off also when there are no directories included for scanning.

Turn on RMM upstream reporting

After installing WithSecure Linux Protection, turn on the RMM upstream reporting service so that the device reports its status to SolarWinds MSP.

After you have installed WithSecure Linux Protection, turn on the RMM upstream reporting service.

As a root user, run the following command:

```
/opt/f-secure/linuxsecurity/bin/setup-rmmd.sh install
```

When you no longer need the service, remove it by running the command with the uninstall option.

6.7.7 Integration with Datto RMM for Windows computers

Information about the components that you can use to install and manage WithSecure Elements EPP for Computers using the Datto platform.

The Datto's online components repository (ComStore) contains the following WithSecure components:

Deploy WithSecure Elements Agent [WIN]	Use this scripting component to install WithSecure Elements EPP for Computers on target computers. You need provide a valid license keycode and choose the correct region from the list when you run it.
WithSecure Elements Agent Tasks [WIN]	Use this scripting component to run tasks on endpoints that have WithSecure Elements EPP for Computers installed. Available tasks include a full computer scan and installing security updates (critical, important, or all updates).
WithSecure Elements Agent Monitor [WIN]	Use this monitoring component to check the current status. You can check whether WithSecure Elements EPP for Computers is installed, the current license status, statuses of different protection components, antivirus definitions age, and any missing critical updates. You can turn each check either on or off.

For more details of all the components, see their descriptions in the Datto RMM management portal. Every configuration variable includes a help text.

Latest versions of these components are also available from the following link:
https://download.withsecure.com/PSB/RMM/Datto/Components_For_Datto_RMM.zip

6.7.8 Integration with Datto RMM for Mac computers

WithSecure Computer Protection for Mac can be installed and monitored on managed Mac computers through the Datto RMM platform.

Datto RMM lets you install and monitor WithSecure Computer Protection for Mac on the Mac computers you manage. This section describes how to install the software through Datto RMM and how to monitor its status.

Install WithSecure Elements EPP for Computers (Mac)

Installs WithSecure Elements EPP for Computers (Mac) using the Datto platform.

To install the product:

1. In the Datto portal, from the **Components** menu, under **Actions**, select **New Component**.
2. From the **Category** drop-down menu, select **Applications**.
3. In the Name field, enter the **WithSecure Elements EPP for Computers (Mac)** .
4. In the **Description** box, enter a description for the application (optional), and select **Save**.
   *The **Component Application** page opens.*

5. From the **Install command** drop-down menu, select **Unix (Linux, Mac OSX)** and enter the following command:

```
InstallerBaseName=$(ls -d ElementsAgent*.mpkg)
installer -pkg "$InstallerBaseName" -target /
if [ $? -ne 0 ]; then
     echo "$InstallerBaseName installation failed"
else
     echo "$InstallerBaseName installation was successful"
fi
```

NOTE: The script covers the following cases:

- Installing the product with a license key embedded in the filename.
- Installing the product without a license key embedded in the filename; activate the product using the activator tool as described in Activating the subscription.

6. Select **Add file...** and then select the **WithSecure Elements EPP for Computers (Mac)** installer with the embedded key in the package name.
7. Select **Save**.
   The installer file is uploaded to the new component.
8. From the **Sites** menu, select **Sites** and under either Managed or OnDemand, select **Devices**.
9. Under **Actions**, select **Schedule a job**.
10. Enter a name for the scheduled job.
11. In the **Schedule** section, select **Immediately**.

NOTE: To select another option, select **Click to change...**.

12. Next, under **Component Name**, select **Add component**.
    The page that opens shows the component that you just created.
13. Select the component and select **Save**.

Monitor the product

Monitors WithSecure Elements EPP for Computers (Mac) using the Datto platform.

To monitor the product:

1. From the **Components** menu, under Actions, select **New Component**.
2. From the **Components** menu, under **Categories**, select **Device monitors**.
3. In the Name field, enter the **WithSecure Elements EPP for Computers (Mac)** .
4. In the **Description** box, enter a description (optional), and select **Save**.
   *The **Component Monitor** page opens.*
5. From the **Install command** drop-down menu, select **Unix (Linux, Mac OSX)** and enter the following command:

```
InstallerBaseName=$(ls -d ElementsAgent*.mpkg)
installer -pkg "$InstallerBaseName" -target /
if [ $? -ne 0 ]; then
     echo "$InstallerBaseName installation failed"
else
     echo "$InstallerBaseName installation was successful"
fi
```

NOTE: The script covers the following cases:

- Installing the product with a license key embedded in the filename.
- Installing the product without a license key embedded in the filename; activate the product using the activator tool as described in Activating the subscription.

6. Select **Add file...** and then select the **WithSecure Elements EPP for Computers (Mac)** installer with the embedded key in the package name.
7. Select **Save**.
   The installer file is uploaded to the new component.
8. From the **Sites** menu, under either **Managed** or **OnDemand**, select **Sites**.
9. On the page that opens, select the device that you want to monitor.
10. Select
    
    ,
    and then select **Monitor**.
11. On the right side of the page, select the **Monitors** option.
    The device page opens.
12. Select **Add a monitor...**.
13. On the **Add monitor** page, from the drop-down menu, select **Component Monitor**, and then select **Next**.
14. From the **Run the component monitor** drop-down menu, select the component that you just created, and select **Next** > **Next**.

    Alerts are generated when one of the components is turned off in the device, for example, Real Time Scanning, Firewall, or Browsing Protection.

6.7.9 Integration with Datto RMM for Linux computers

WithSecure Linux Protection can be installed and monitored on managed Linux computers through the Datto RMM platform.

Datto RMM lets you install and monitor WithSecure Linux Protection on the Linux computers you manage. This section describes how to install the software through Datto RMM and how to monitor its status.

Install WithSecure Linux Protection

Installs WithSecure Linux Protection using the Datto platform.

To install WithSecure Linux Protection:

1. Download the latest generic WithSecure Linux Protection software installer from WithSecure Elements Security Center.
2. In the Datto portal, from the **Components** menu, under Actions, select **New Component**.
3. From the **Category** drop-down menu, select **Applications**.
4. In the Name field, enter the **Deploy WithSecure Linux Protection [LIN]** .
5. In the **Description** box, enter a description for the application (optional), and select **Save**.
   *The **Component Application** page opens.*
6. From the **Install command** drop-down menu, select **Unix (Linux, Mac OSX)** and enter the script from the following file in the text field: `deploy_f-secure_linux_protection.sh`.

> **NOTE:** You can download the deployment script at https://download.withsecure.com/PSB/RMM/Datto/deploy_f-secure_linux_protection.sh.

7. Edit the script to include installation of the dependencies before the actual installation step, when needed.
8. Check the needed dependencies in the Linux Protection dependencies guide.
9. Edit valid subscription key to the script.
10. Select **Add file...** and then select the **WithSecure Linux Protection** installer.
11. Select **Save**.
    The installer file is uploaded to the new component.
12. From the **Sites** menu, under **Managed**, select **Devices**.
13. Check the devices where you want to do the installation.
14. Select
    
    to schedule a job:
    a) Enter a name for the scheduled job.
    b) In the **Schedule** section, select **Immediately**.

    > **NOTE:** To select another option, select **Click to change...**.

    c) Under **Component Name**, select **Add component**.
    The page that opens shows the component that you just created.
    d) Select the component and select **Save**.
    e) Select **Save** to launch the job.

Monitor WithSecure Linux Protection

Monitors WithSecure Linux Protection using the Datto platform.

To monitor WithSecure Linux Protection:

1. Download the pre-made Linux monitoring component from the following link:
   https://download.withsecure.com/PSB/RMM/Datto/F-Secure_Linux_Protection_Monitor_LIN.cpt
   It contains the following component: `F-Secure Linux Protection Monitor [LIN]`. Use this monitoring component to check the current status and whether WithSecure Linux Protection is installed and enabled. You can also check the current license status, statuses of different protection components, and the antivirus definition age. You can turn individual checks either on or off.

   > **NOTE:** For more details on the component, see its descriptions in the Datto RMM management portal.

   Every configuration variable includes a help text.
2. Import the component file (.cpt) in the **Components** page of the Datto portal.
3. Create a Component Monitor using the imported component as follows:
   a) From the Sites menu, under Managed, select **Devices**.
   b) On the page that opens, select the device that you want to monitor.
   c) Select the icon, and then select **Monitor**.
   d) On the right side of the page, select the **Monitors** option. The device page opens.
   e) Select **Add a monitor...**.

f) On the **Add monitor** page, from the drop-down menu, select **Component Monitor**, and then select **Next**.

g) From the Run the component monitor drop-down menu, select the component that you just imported.

h) Adjust the monitor parameters as needed, and then select **Next** on each page to complete the creation.

   Alert is generated when one of the components is turned off in the device, for example, Real Time Scanning or Integrity checking. The first failing check will generate an alert. The alert needs to be resolved before a new alert is generated for the same device from one monitor.

Chapter 7
Alerting and reporting

Topics:

- Use the Notification Hub
- Protection status overview
- Security events report
- Create customized email reports on security events
- Audit Log

Alerting and reporting

The **Reports** section tracks metrics to help you gauge the security status of the computers and mobile devices registered to your WithSecure Elements Security Center account.

On the **Reports** section, you can do and view the following:

- In the My report tab, you can add widgets to create your own reports, including EDR Broad Context Detection reports
- Configure alerts and scheduled custom email reports that are delivered to specified email addresses
- Dashboard in the pre-configured system view provides information on devices, software updates, and security events
- View vulnerability notifications

7.1 Use the Notification Hub

The Notification Hub is a central place in WithSecure Elements Security Center where you can view and manage important product messages.

The Notification Hub replaces most banner-based announcements and shows messages such as critical issues and outages, warnings and operational updates, and general informational announcements. A bell icon in the top-right corner indicates when there are new, unseen notifications.

To view and manage notifications:

1. Select
   
   in the top-right corner of **Elements Security Center**.
   *The **Notification** panel opens, showing all new notifications in the **Unread** tab.*
2. Review the notifications in the panel.
3. Mark notifications as read to keep track of new and past messages.

NOTE: Read notifications remain available in the Read tab for future reference. However, some notifications, such as scheduled maintenance notifications, are removed shortly after the event ends and will no longer appear in the Read tab.

7.2 Protection status overview

The charts in the **Devices** tab under **Reports** provide an overview of the infection activity and protection status of registered computers.

The charts show the following information:

- **Computer protection status** - shows the number of the computers that are protected and have no issues that affect their security; the computers that have **non-critical** issues; the devices that have **critical issues**, and the computers that have not connected to the server for more than two weeks
- **Windows devices by client version** - shows the number of Windows devices based on the client version that is installed on them
- **Mac devices by client version** - the number of Mac devices based on the client version that is installed on them
- **Linux devices by client version** - the number of Linux devices based on the client version that is installed on them

- **Mobile devices by client version** - the number of mobile devices based on the client version that is installed on them
- **Connector devices by client version** - the number of Connector devices based on the client version that is installed on them
- **Most popular computers by manufacturer** - the number of computers based on the computer manufacturer
- **Computers by operating system** - the number of computers based on the operating system that they have
- **Mobile devices by operating system** - the number of mobile devices based on the operating system that they have
- **Password policy: minimum length** - the number of devices based on the length of password that is set for them
- **Computers by drive encryption status** - the number of computers based on their drive encryption status (enabled or disabled)
- **Computers by default browser** - the number of computers based on the default browser that is used on them
- **Computers by account lockout threshold** - the number of computers on which the account lockout threshold is and is not configured

All the charts provide a summary of the activity from the last 28 days.

7.2.1 Export CSV reports

You can export reports in a CSV file on computers, mobile devices, and the software updates installed on them.

You can also use the *scope selector* to display a customer company and export reports on the devices and the software update installations of the selected company.

1. Select **Devices** on the sidebar.
2. Select
   
   .
   A menu opens.
3. Select one of the following reports:
   - Export found computers report

     NOTE: For example, from the Profile filters drop-down menu, you can select one of the profile filtering options, and then select to view the devices to which the selected profile is assigned. On the Devices page, you can then select the **Export found computer report** option to export only those devices that were found based on your filtering (or search) results.
   - Export all computers report
   - Export all software update operations
   - Export all mobiles report

   The report is downloaded to the browser's default download location. You can then either open or save the report.

7.3 Security events report

The charts in the Security events tab on the Reports page provide an overview of the security events.

The charts show the following information:

- **Top computers by blocked infections** - the names of the top computers that have blocked infections, as well as the total number of blocked infections over the last 30 days.
- **Top infections** - the names and number of the top ten infections over the last 30 days. You can select the name of an infection to open a web browser page that displays details about the infection from the WithSecure Labs Threat Descriptions database. By selecting the bar, you can open the Security events page.
- **Infections handled by real-time scanning** - the number of infections handled by real-time scanning per day, and the total infections handled over the last 30 days.
- **Infections handled by manual and scheduled scans** - the number of infections handled by manual and scheduled scans per day, and the total infections handled over the last 30 days.
- **Top computers by tampering attempts** - the names of the top computers by the number of times they were a target for tampering attempts over the last 30 days.
- **Top websites blocked by Reputation-based browsing** - the URLs of the top websites that were blocked and the number of times they were blocked by Reputation -based browsing over the last 30 days.
- **Top Application Control rules** - the top Application Control rules that blocked an application and the number of times an application was blocked based on that rule over the last 30 days.
- **Top computers accessing blocked websites** - the names of the top computers and the number of times they tried to access a blocked website over the last 30 days.
- **Top sources** - the names of the top sources that triggered security events and the number of the events that each source triggered over the last 30 days.
- **Web Content Control - top blocked categories** - the names of the top web content categories blocked over the last 30 days.
- **DataGuard - top blocked applications** - the top applications to which DataGuard blocked access over the last 30 days.
- **Device Control - top rules-blocking devices** - the top Device Control rules that blocked a device and the number of times a device was blocked based on that rule over the last 30 days.
- **Tamper Protection - top alert types** - the most common Tamper Protection alert types and the number of times each alert type was triggered over the last 30 days.
- **System Events - top event types** - the number of top system events by their type over the last 30 days.

7.4 Create customized email reports on security events

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

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

To create a custom view:

1. Under **Events**, select **Security Events**.
2. Apply filters to specify which security events you want to include in the email reports.
3. Open the **View** drop-down menu in the top-right corner.
4. Select **Save as** and enter a name for your custom view.
5. Select **Save**. The custom view appears under **My views**.

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

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

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

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

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

11. Select **Save**.

7.5 Audit Log

In the **Audit Log** page, you can view and filter events about profiles.

The **Audit Log** page shows the following columns:

- **Timestamp** - the date and time when the event occurred.
- **Description** - free-form text describing the event, for example an administrator login that includes the IP address, user agent, and authenticated user.
- **Target** - the object that the event affected, such as a profile or a device.
- **Transaction ID** - the unique identifier of the event.

You can filter the events by the following:

- Action
- Administrator
- Device UUID
- Organization
- Profile name
- Timestamp
- Transaction ID

By default, the **Audit Log** page shows events from the last 14 days. You can also filter the events by time range. You can select to see events that took place before or after the date that you select.

For example, an administrator login entry has a description such as `Administrator login from IP 203.0.113.5 using Mozilla/5.0, authenticated as jane.doe@example.com`.

Audit Log entries are kept for as long as your organization's data retention settings allow.

Chapter 8

Keeping third-party software up to date

Topics:

- View available software updates
- Install software updates individually or by category
- Install software updates automatically
- Scan a device for missing software updates
- View and install software updates on a specific device
- Configure an HTTP proxy for Software Updater
- Configure WithSecure Elements Connector for Software Updater
- Using Software Updater and Windows Server Update Service to install Microsoft updates

Keeping third-party software up to date

You can manage and install software updates for the computers in your network.

Software vendors will periodically issue updates for their software, usually to include improvements to their features or to release fixes for security issues that were discovered after the last update. It is important to have the latest software updates installed on the workstations in your network, because many updates fix security vulnerabilities in installed products.

NOTE: You can find the list of vendors included in WithSecure Software Updater.

With WithSecure Elements Security Center, you can install software updates for selected programs onto computers and mobile devices registered to your account. You can configure the profile editor to automatically install security updates to computers. You can also check the status of software updates and install missing software updates manually when needed.

NOTE: Software Updater is unable to update running applications. Therefore, we recommend to turn on the **Force close running applications** option (in the action menu that opens when you select an update under **Patch Management**) to make sure that all software updates can be installed.

NOTE: We recommend that you keep the registered devices current with the latest available software updates to make sure that the devices are fully protected.

8.1 View available software updates

You can view the details of all missing updates that are available for download and installation in WithSecure Elements Security Center.

In addition to missing updates, the **Patch Management** page shows also installation logs.

To view the details:

1. To view missing updates:
   a) Under **Environment**, select **Patch Management** on the sidebar.
   *The **Patch Management** page opens.*
   a) Select the **Missing Updates** tab.
2. To view installation logs:
   a) Under **Environment**, select **Patch Management** on the sidebar.
   *The **Patch Management** page opens.*
   a) Select the **Installation Logs** tab.

8.2 Install software updates individually or by category

You can install software updates on a selected device by choosing all updates, individual updates by a vendor, or all updates in a particular category.

NOTE: Software updates are categorized into *Critical*, *Important*, *Moderate*, *Low*, *Unclassified*, and *Non-security*.

1. To install updates, select one of the following:

- To install all available updates, on the **Patch Management** page, select the checkbox next to the table header. Updates for the first 50 vendors are shown.
- To install individual software updates, on the **Patch Management** page, select the updates that you want to install.

2. In the menu at the bottom of the page, select **Select devices to update**.

NOTE: You can select **Force close running applications** to close any running application to prevent the installation from failing.

NOTE: From the drop-down menu, you can select either to install updates immediately or pick a time when you want the updates to be installed. This applies only to Windows devices.

*The **Select devices** panel opens.*

3. Select the computer or computers on which you want to install the software updates.
4. Select **Update**.
   A request to install the updates is sent to the selected devices. Each device shows its update status once the installation completes.

8.3 Install software updates automatically

You can configure WithSecure Elements Security Center to automatically install security updates for software to computers in your network.

NOTE: We recommend that you allow automatic installation of software updates.

To turn on automatic installation of security updates:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the profile that you want to edit.

NOTE: You can only edit a profile on the level that it has been created.

3. Select **Automated tasks**.
4. Turn **Automated tasks** on.
5. Under **The list of automated tasks**, select **Add task** and do the following:
   a) Make sure that the switch in the **Active** column is on.
   b) From the drop-down menu in the **Type** column, select one of the following options:
      - Install critical security updates
      - Install critical and important security updates
      - Install all security updates
      - Install all updates
   c) From the drop-down menu in the **Schedule** column, select the interval for installing the updates (for example, hourly, daily, weekdays). Alternatively, you can use a CRON expression to create your own schedule.
   d) In the **Description** column, enter a description for the automated task.

e) When the switch in the **Never skip** column is on, the updates are installed at a scheduled time. If they cannot be installed at a scheduled time, they are installed whenever available. If the switch is turned off, the updates are installed only at a scheduled time.

NOTE: By default, the switch is on.

NOTE: Under **Security Configurations** > **Profiles** > **Software Updater**, you can turn on the **Notify about new missing updates** option to show a notification flyer when a software update is available.

6. Select **Save and Publish** to distribute the policy.

8.3.1 Include or exclude software updates

You can enter the name, bulletin ID, vendor name, severity, and software name for any software that you want or do not want Software Updater to update automatically.

Inclusion and exclusion are based on the update installation status reported by managed hosts. For inclusion, updates are checked based on their severity and depending on what is selected in **Install security updates automatically**. Then, all updates except for the excluded ones are installed.

When a host starts installing missing updates, it checks for any excluded updates and reports that they were not installed due to exclusion by the administrator. This also means that excluded updates do not immediately disappear from the list on the **Software updates** tab, because the hosts only report the installation status once they attempt to install the missing update.

To include or exclude software updates:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the profile that you want to edit.

NOTE: You can only edit a profile on the level that it has been created.

3. Select **Software updater**.
4. To manually enter the details for the software updates that you want to include or exclude:
   a) Do one of the following:
      - Under **Include software for automatic installation**, select **Add rule**.
      - Under **Exclude software from automatic installation**, select **Add rule**.
   b) In the **Rule** column, from the drop-down menu, select one of the conditions and enter the details for the update that you want to include or exclude.

      You can enter the following details:

      - Update name contains - the name of the update or a part of it
      - Software name contains - the name of the software or a part of it

NOTE: For example, if you enter "mozilla", then both "Mozilla Firefox and "Mozilla Thunderbird" are included or excluded.

      - Vendor name contains - the name of the software vendor or a part of it
      - Severity equals to - indicates the level of severity (Critical, Important, Moderate, Low, Not Rated)
      - Bulletin ID equals to - the bulletin ID of the software update

5. Select **Save and Publish** to distribute the policy.

8.3.2 Include updates in scan results

You can specify which software updates you want to be included in scan results.

To include software updates in scan results:

1. Select **Profiles** on the sidebar.
   The Profiles view opens.
2. Select the profile that you want to edit.
3. Under **Software Updater**, go to **Include updates in scan results**.
   The Add rule table is shown.
4. Select **Add rule**.
   The switch in the Active column turns on.
5. In the Rule column, from the drop-down menu, select one of the conditions and enter the details for the update that you want to be included in scan results.

   You can use the following parameters:

   - Update name contains - the name of the update or a part of it
   - Software name contains - the name of the software or a part of it.

   NOTE: For example, if you enter "mozilla", then both "Mozilla Firefox and "Mozilla Thunderbird" are included.

   - Vendor name contains - the name of the software vendor or a part of it
   - Severity equals to - indicates the level of severity (Critical, Important, Moderate, Low, Not Rated)
   - Bulletin ID equals to - the bulletin ID of the software update

   NOTE: Software updates that do not meet the conditions are excluded and not shown in the results.

6. Select **Save and Publish** to save the your changes to the current profile.

8.3.3 Exclude non-security updates from scanning

You can choose to exclude non security-related software updates from scanning.

1. Select **Profiles** on the sidebar.
   The Profiles view opens.
2. Select the profile that you want to edit.
3. Under **Software Updater**, go to **Exclude updates from scanning**.
4. Turn **Non-security updates** on.
   Non security-related updates are excluded from scanning.

8.3.4 Exclude updates from scan results

You can specify which software updates you want to exclude from scan results.

To exclude software updates from scan results:

1. Select **Profiles** on the sidebar.
   The Profiles view opens.
2. Select the profile that you want to edit.

3. Under **Software Updater**, go to **Exclude updates from scanning**.
   The Add rule table is shown.
4. Select **Add rule**.
   The switch in the Active column turns on.
5. In the Rule column, from the drop-down menu, select one of the conditions and enter the details for the update that you want to be excluded from scan results.

   You can use the following parameters:

   - Update name contains - the name of the update or a part of it
   - Software name contains - the name of the software or a part of it

   > **NOTE:** For example, if you enter "mozilla", then both "Mozilla Firefox and "Mozilla Thunderbird" are excluded.

   - Vendor name contains - the name of the software vendor or a part of it
   - Severity equals to - indicates the level of severity (Critical, Important, Moderate, Low, Not Rated)
   - Bulletin ID equals to - the bulletin ID of the software update
6. Select **Save and Publish** to save your changes to the current profile.

8.4 Scan a device for missing software updates

You can use WithSecure Elements Security Center to scan a selected device for missing software updates.

To scan a specific device:

1. Select **Devices** on the sidebar.
   *The **Devices** page is displayed.*

   If the *scope selector* is set to display all customer companies, select the company you wish to manage.
2. Select the checkbox next to the name of the device.
   A menu is displayed at the bottom of the page.
3. In the menu, select **Scan for missing software updates**.
   A command is sent to the installed Elements Endpoint Protection software to scan the device and determine which software updates are missing.

Once the scan is completed, a list of the missing software updates is available in Elements Security Center. You can then view the list and select those you want to install on the device.

8.5 View and install software updates on a specific device

You can view the details of software updates available for a particular device and install them.

> **NOTE:** Missing software updates are also listed on the **Home** page in the Issues table (where they are categorized as *Critical*, *Important* and *Informative*). Click the **View** button to display devices that have updates of the appropriate category awaiting installation.

To view the updates for a specific device:

1. Click **Devices** on the sidebar.
   *The **Devices** page is displayed.*
2. Click on the name of the device.
   A page opens showing the device details.

3. In the Protection status table, click the
   
   icon next to Software updates.
   A drop-down menu listing the number of available updates is displayed.
4. Click the **Select updates and install** button.
   The **Install software updates** page list the latest updates available for specific software, including their Category, CVE ID and Bulletin ID, as well as a link to an external web page containing more information about the update. You can also sort the items in the table for easier viewing by choosing between *All updates*, *All security updates*, *Critical security updates*, *Important security updates*, *Non-security updates* and *Service packs*.
   *The **Install software updates** page is displayed, listing all the updates not yet installed for this device.*
5. To install, select the desired updates and then click the **Install** button.
   The selected updates are installed on the device.

8.6 Configure an HTTP proxy for Software Updater

To reduce Internet traffic, you can set up Software Updater to receive its updates through an HTTP proxy.

You can configure the proxy update settings on the Profile page.

1. Under **Profiles** > **Software updater**, select **Communication**.
2. From the **Use HTTP Proxy** drop-down menu, select one of the options:
   - No - use a direct connection to the Internet
   - From product configuration - use the product proxy settings
   - Remotely managed - specify an alternate proxy URL (user defined)
3. If you selected **Remotely managed** in the previous step, enter an HTTP proxy address in the Remotely-managed proxy address field in the following format: `http://[user[:password]@]host:port`.

8.7 Configure WithSecure Elements Connector for Software Updater

You can set up Software Updater to receive its updates through WithSecure Elements Connector.

You can configure the proxy update settings on the Profile page.

1. Under **Profiles** > **Software updater**, select **Communication**.
2. From the **Use WithSecure Elements Connector** drop-down menu, select one of the options:
   - Always - always use WithSecure Elements Connector
   - If possible - use WithSecure Elements Connector whenever possible
   - Never - use a direct connection to the Internet

8.8 Using Software Updater and Windows Server Update Service to install Microsoft updates

In WithSecure Elements, Software Updater (SWUP) always installs Windows Updates.

There is no possibility to turn off Windows updates installation. The **If WSUS is in use, both Software Updater and WSUS install Microsoft updates** setting exists to prevent the installation of Windows Updates via Software Updater (SWUP) and Windows Server Update Services (WSUS) at the same time.

NOTE: Software Updater does not support Windows optional updates.

If you use WSUS and turn on the setting, while installing Windows updates, SWUP turns off WSUS. Afterwards, SWUP turns WSUS back on, if it was on before the installation started.

IMPORTANT: If this setting is off, SWUP does not turn off WSUS. This may lead to WSUS and SWUP trying to install an update at the same time and result in a serious client-side update error.

NOTE: We recommend that you turn this setting off if you use an actively managed WSUS. If you do not actively manage WSUS, leave the setting on.

Chapter 9

Using WithSecure Luminen

Topics:

- View the weekly security awareness summary
- Analyze a detection with Investigation Assistant
- Luminen executive summary of monthly security reports

Using WithSecure Luminen

WithSecure Luminen makes cybersecurity tasks more manageable and efficient. By using advanced AI technology, it helps you protect your organization more effectively against cyber threats.

Luminen uses AI and Large Language Model (LLM) technologies with preprocessed, structured data, which significantly minimizes the risk of inaccurate recommendations. Its reports are clear and integrated within the WithSecure Elements Cloud.

Luminen analyzes vast amounts of data to provide you with precise, practical recommendations. This means you spend less time sifting through data and more time addressing the most critical issues. For example, it can identify unhandled incidents and suggest specific actions to mitigate them.

Luminen helps you investigate security events, so you can understand and respond to threats. Luminen provides rich contextual insights that help you understand the broader implications of security events. This context allows you to make informed decisions, improving your overall response time and effectiveness.

How it works

WithSecure Luminen is a user-experience layer of Elements. It uses Generative AI and LLMs to provide localized assistance in natural language.

As a leading European cybersecurity company, WithSecure follows strict privacy standards. Luminen uses proven AI models that are continuously improved. Each AI model is dedicated to a single organization, which prevents data exposure between organizations.

Luminen uses LLMs from Amazon AWS Bedrock, and analyzed data stays within AWS. All data is processed in Europe and is not used to train future foundational models. Any training of non-foundational models by WithSecure will only use anonymized data.

To minimize risks like data leakage and AI errors, Luminen uses a technique called Retrieval-Augmented Generation (RAG). This involves providing the AI with specific prompts and context data, such as Security Events, Extended Detection and Response (XDR) and Broad Context Detection (BCD) incidents, and relevant threat intelligence. This data may include usernames, host names, and email addresses. However, Luminen does not have access to any additional data beyond what is already in Security Events or XDR/BCD incidents.

9.1 View the weekly security awareness summary

Security Awareness Assistant is a part of WithSecure Luminen. It offers a summary of findings from an organization during the last 7 days.

Security Awareness Assistant creates a concise summary of the past week's security activities to quickly grasp the overall security posture in the organization. Luminen writes these summaries in plain language, making it easier to understand the types of security events that have been detected and any immediate actions that might be required. The report prioritizes findings based on their criticality, helping you to focus on the most pressing issues first.

Select

at the top right corner.
*The **Security events summary** opens.*

NOTE: The report is generated using generative AI and should be treated with caution. Further investigation and professional consultation may be required to fully address all threats.

9.2 Analyze a detection with Investigation Assistant

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

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

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

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

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

   Luminen analyzes the detection and displays the executive summary.

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

9.3 Luminen executive summary of monthly security reports

A Luminen-generated monthly overview of a company's security posture, available at a company level in Elements Security Center.

The executive summary uses Luminen-generative AI to analyze security-related data and produce a concise, plain-language summary that describes the organization's current security posture. The summary informs executives about current security conditions, highlights vulnerabilities, and supports informed decisions to improve security. It presents important details such as:

- Encryption status
- Password strength
- Update and patch compliance
- Exposure to exploits
- The lifecycle status of the operating system

NOTE: The exact content varies depending on the Elements subscriptions that are in use.

The summary has the following characteristics:

- Bullet-point format for quick reading.
- Automatic localization based on the language that is set in Elements Security Center.
- For executives, IT managers, and security consultants who need rapid situational awareness.
- Support for informed decisions and remediation prioritization.

The summary helps executives and security teams understand the organization's security posture at a glance. It also helps them identify risks and vulnerabilities, prioritize remediation efforts, and make informed security decisions.

9.3.1 Set up an executive summary report

Create a custom widget that generates a monthly executive summary of security reports for your company.

1. Open Elements Security Center.
2. Log in using your credentials.
3. Select **Reports** from the main navigation menu.
4. Select **My Report** from the list of available report options.
5. Select **New View Template** to create a new custom report view.

   This template determines how the executive summary will be displayed.
6. Enter a descriptive name for the template, such as `Executive Report`.
7. Select **Save** to store the new view template.
8. Select **Add Widget** from the newly created report view.

   Widgets allow you to place relevant metrics or summaries directly on the dashboard.
9. Assign a name to the widget, such as `Executive Report`.
10. For **Data source**, select **AI-generated summaries**.
11. Under **Data**, select **Executive Summary Report** > **Create**.
    The widget is added to the report and automatically loads the Luminen monthly security summary for the selected company.

You created a customized summary report that shows the monthly state of your company's security posture.

9.3.2 View a security executive summary report as a partner

Use partner-level credentials to access and generate a monthly executive summary of security reports for companies in your hierarchy.

When you set up a monthly executive summary of security reports at the partner level, the report and widget are reusable across all companies under your partner hierarchy. You only need to set up the report once.

1. Open the report view that contains the Executive Summary Report widget.
2. Use the *scope selector* to choose a customer company.

   Because the executive summary is generated at the company level, the selected company determines which report is shown.
3. Generate the Executive Summary Report for the selected customer.
4. View the Executive Summary Report.
5. To view another company's summary, select a different customer in the *scope selector*.
   The Executive Summary updates instantly without needing to reconfigure the report.

You can review Executive Summary reports for all customer companies through a single, reusable report view.

Appendix A
Elements Agent reinstallation

Topics:

- Reinstallation of Elements Agent without duplicating devices

Elements Agent reinstallation

Reinstalls WithSecure Elements Agent on a device without creating a duplicate entry in WithSecure Elements Security Center.

This chapter describes how to reinstall WithSecure Elements Agent on a device. It explains how to do this without creating a duplicate entry in WithSecure Elements Security Center.

A.1 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
```

Appendix B

Customizing Elements Security Center and software

Topics:

- Adding a customer company
- Assign a subscription key for a customer company
- Order products for a new customer company
- Customize Elements Security Center
- Customize the WithSecure Elements software

Customizing Elements Security Center and software

Using the scope selector to change the displayed information scope, and customizing Elements Security Center and the Elements Endpoint Protection software for partners.

NOTE: Under **Profiles** > **General settings**, you can turn on the Pilot client setting. When this option is on, devices assigned to this profile are able to test new features in advance. The pilot computers receive software updates several days before everyone else. We recommend that you use this to get a preview of the new features and be able to communicate them to your customers.

B.1 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.

B.2 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.

B.3 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.

B.4 Customize Elements Security Center

You can customize WithSecure Elements Security Center with your logo and support link.

To customize Elements Security Center:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
2. Select the **Customization** tab.
3. Select the ••• icon, and then select **Customize portal**.
   *The **Organization logo** page opens.*

4. Upload your logo by dragging and dropping it to the logo box.

NOTE: Your logo must be in the .png format. The required dimensions of the logo are 64 x 64 pixels.

5. In the Support URL field, enter the URL of your support site.
   The link that you provide replaces the default WithSecure support link.
6. Save your changes.

Once customized, Elements Security Center shows your logo at the bottom left corner.

B.5 Customize the WithSecure Elements software

You can customize the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers software with your logo and support link.

NOTE: To have your logo or URL or both visible in the software, you must assign and use a custom profile (not the WithSecure default profile).

To customize the software:

1. Under **Management**, select **Organization Settings** on the sidebar.
   *The **Organization Settings** page opens.*
2. Select the **Client Customization** tab.
   *The **Client Customization logo** page opens.*
3. Upload your logo by dragging and dropping it to the logo box.

NOTE: Your logo must be in the .png format. The required dimensions of the logo are 128x128 pixels. Consider adding a margin for a better look.

4. In the **Partner URL** field, enter a link.
   The link that you provide is an optional link for the logo. It may be, for example, a link to your support site and thus replaces the default WithSecure support link.

The logo that you upload is displayed in the WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers software.

Appendix C

Windows Management Instrumentation

Topics:

- WMI integration
- WMI classes for integration

Windows Management Instrumentation

WithSecure Elements provides Windows Management Instrumentation (WMI) integration, which you can use, for example, to integrate Remote Monitoring and Management (RMM) tools.

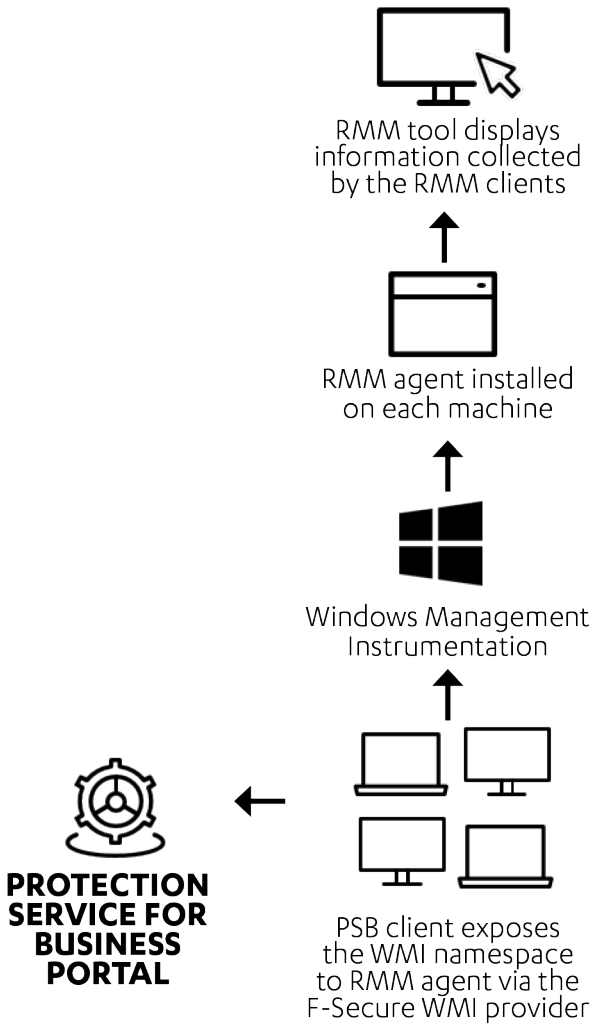
On a service provider level, WMI integration is often used to provide better management of several functions, such as asset discovery and management, configuration, process and service automation, security services, and backups.

C.1 WMI integration

WithSecure Elements uses a Windows Management Instrumentation (WMI) interface to collect read-only status information on WithSecure client applications.

The WMI interface uses a vendor-specific agent installed on the host to forward the collected information to the management console server. No configuration options or general security management functionality are exposed through the WMI interface.

Administrators can also use the WMI interface to remotely start a full scan of the host computers.



The following information can be retrieved from Windows clients and server through the WMI interface:

- Product version
- Real-time scanning status

- Malware definition database information
- Firewall status
- Firewall security level (profile)
- Firewall versions
- Application Control status
- Time of last connection to WithSecure Elements Security Center
- Time of last policy update from WithSecure Elements Security Center
- Name of WithSecure Elements Endpoint Protection profile in use
- DeepGuard status
- Browsing protection status
- Email filtering status
- Software Updater status (status of automatic installation of security updates, counts for missing updates split by type; critical, important, and other)
- Subscription status
- Information on the last manual and scheduled scans that were run

C.1.1 Obtain properties via WMI

Obtains status properties via the WMI interface using PowerShell.

WithSecure exposes read-only status information through a Windows Management Instrumentation (WMI) interface.

1. Turn on the WMI Provider setting as follows:
   a) Log in to WithSecure Elements Security Center.
   b) Under **Security Configurations**, select **Profiles**.
   a) Select **General Settings**.
   b) Under **Integrations**, turn on **WMI Provider**.
   c) Select **Save and Publish**.
   d) Under **Environment**, select **Devices**, and then select your device.
   e) Select **Assign profile**.
   f) From the drop-down menu, select a profile and then select **Assign profile**.
2. Open **Windows PowerShell** with the administrator rights.
3. At the command prompt, enter commands as shown below to retrieve, for example, the following classes and properties.
   - Requesting a listing of all singleton instances

     ```
     Get-WmiObject -Namespace root/fsecure -List | where { $_.Qualifiers["Singleton"].Value }
     ```

   - Retrieving product version

     ```
     $product = Get-WmiObject -Namespace "root/fsecure" -Class Product
     Write-Host Version: $product.Version
     ```

     Result:

     ```
     Version: 18.15
     ```

- Retrieving real-time scanning status

```
$av = Get-WmiObject -Namespace "root/fsecure" -Class AntiVirus2
Write-Host "Is real-time scanning enabled: " $av.RealTimeScanningEnabled
```

Result:

```
Is real-time scanning enabled: True
```

- AvDefinitions

```
$av = Get-WmiObject -Namespace "root/fsecure" -Class AntiVirus2
$status = if ($av.AvDefinitionsAgeInHours -lt 7*24){
"up to date" } else { "outdated" }
Write-Host "AV definitions are" $status
```

Result:

```
Av definitions are up to date
```

- Firewall status

```
$fw = Get-WmiObject -Namespace "root\fsecure" -Class Firewall
Write-Host "Is firewall enabled: " $fw.Enabled
```

Result:

```
Is firewall enabled: True
```

- Time of last policy connection to WithSecure Elements Security Center

```
$cm = Get-WmiObject -Namespace "root\fsecure" -Class CentralManagement2
$status = if ($cm.LastConnectionTimeInHoursAgo -lt 24) { "OK" } else { "Connectivity issues" }
Write-Host "PSB Portal connection status: " $status
```

Result:

```
PSB Portal connection status: OK
```

- Time of last policy update from WithSecure Elements Security Center

```
$cm = Get-WmiObject -Namespace "root\fsecure" -Class CentralManagement
Write-Host "PolicyUpdateTime: " $cm.PolicyUpdateTime
```

Result:

```
PolicyUpdateTime: 20181001144235.000000+000
```

- DeepGuard status:

```
$av = Get-WmiObject -Namespace "root\fsecure" -Class AntiVirus2
Write-Host "Is DeepGuard enabled:" $av.DeepGuardEnabled
```

Result:

```
Is DeepGuard enabled: True
```

- Browsing protection status:

```
$inet = Get-WmiObject -Namespace "root\fsecure" -Class Internet2
Write-Host "Is Browsing Protection enabled:" $inet.BrowsingProtectionEnabled
```

Result:

```
Is Browsing Protection enabled: True
```

- Software Updater status (status of automatic installation of security updates, counts for missing updates split by type; critical, important, and other)

```
$su = Get-WmiObject -Namespace "root\fsecure" -Class SoftwareUpdater
Write-Host "Enabled: " $su.Enabled
Write-Host "InstallSecurityUpdatesAutomatically: " $su.InstallSecurityUpdatesAutomatically
Write-Host "MissingCriticalUpdatesCount: " $su.MissingCriticalUpdatesCount
Write-Host "MissingImportantUpdatesCount: " $su.MissingImportantUpdatesCount
Write-Host "MissingOtherUpdatesCount: " $su.MissingOtherUpdatesCount
```

Result:

```
Enabled: True
```

```
InstallSecurityUpdatesAutomatically : 0
```

```
MissingCriticalUpdatesCount : 2
```

```
MissingImportantUpdatesCount : 1
```

```
MissingOtherUpdatesCount : 1
```

- subscription status:

```
$license = Get-WmiObject -Namespace "root\fsecure" -Class LicenseStatus
Write-Host "License status: " $license.Valid "; End date: " $license.EndDate
```

Result:

```
License status:  True ; End date:  20191231235959.000000+000
```

- Last manual scan report information:

```
$report = Get-WmiObject -Namespace "root\fsecure" -Class LastManualScanReport

Write-Host "HarmfulItemsFound: " $report.HarmfulItemsFound
```

Result:

```
HarmfulItemsFound: False
```

- Last scheduled scan report information:

```
$report = Get-WmiObject -Namespace "root\fsecure" -Class LastScheduledScanReport

Write-Host "HarmfulItemsFound: " $report.HarmfulItemsFound
```

Result:

```
HarmfulItemsFound: True
```

C.2 WMI classes for integration

This appendix provides details on the classes used for Windows Management Instrumentation (WMI) integration in WithSecure Elements.

This appendix describes the Windows Management Instrumentation (WMI) classes that WithSecure Elements exposes for RMM integration, including the WMI namespace and the data available in the Windows registry.

C.2.1 WMI classes

Classes used for WMI integration in WithSecure Elements Security Center.

Introduction to WMI classes

Some classes are available as singleton instances and some are used only as auxiliary types. See examples for details in Obtain properties via WMI on page 252.

AntiVirus

Provides information on anti-virus modules and allows running a full computer scan.

Table 15: AntiVirus properties

Property Name	Description	Type
RealTimeScanning	Status information for real-time scanning	*component*
DeepGuard	Status information for *DeepGuard*	*component*
AvDefinitionsUpdateTime	Time of latest update to anti-virus definitions	*datetime*
AvDefinitions	List of installed anti-virus engines	*AvDefinition*

Table 16: AntiVirus methods

Method Name	Description	Return Type
ScanComputer	Starts a full computer scan and waits for completion	*AvScanResult*

AntiVirus2

Simplified class for providing information on anti-virus modules.

Table 17: AntiVirus2 properties

Property Name	Description	Type
RealTimeScanningEnabled	Status information for real-time scanning	*boolean*
DeepGuardEnabled	Status information for *DeepGuard*	*boolean*

Property Name	Description	Type
AvDefinitionsAgeInHours	Age of anti-virus definitions in hours	*uint32*

API

Provides basic information on the WithSecure WMI namespace API.

Table 18: API properties

Property Name	Description	Type
Version	Actual version of this API	*string*

AvDefinition

Provides information on the Anti-Virus engine.

Table 19: AvDefinition properties

Property Name	Description	Type
EngineId	Unique identifier of the corresponding engine	*uint32*
EngineName	User-friendly name of the corresponding engine	*string*
EngineVersion	Version of the corresponding engine	*string*
UpdateSerialNumber	Unique identifier of the installed update	*string*
UpdateTime	Time when the update was installed	*datetime*

AvScanResult

Result of the scan for viruses.

Table 20: AvScanResult properties

Property Name	Description	Type
StartTime	Time when scan was started	*datetime*
EndTime	Time when scan finished	*datetime*
InfectedFilesCount	Number of infected files found in the scan	*uint32*
InfectedSectorsCount	Number of infected sectors found in the scan	*uint32*
ScanningReportFilePath	File path to the scan report	*string*

CentralManagement

Provides information on interaction with the protection service.

Table 21: CentralManagement properties

Property Name	Description	Type
LastConnectionTime	Time of the last connection to the protection service.	*datetime*
PolicyUpdateTime	Time of latest policy update.	*datetime*
Profile	Currently installed profile.	*Profile*

CentralManagement2

Simplified class for providing information on interaction with the protection service.

Table 22: CentralManagement2 properties

Property Name	Description	Type
LastConnectionTimeInHoursAgo	Time of the last connection to the protection service	*uint32*

CentralManagement3

Provides information on host identity and its type.

Table 23: CentralManagement3 properties

Property Name	Description	Type
HostIdentityType	Host identity type (SMBIOSGUID/RANDOMGUID/WINS/MAC or empty if host identity is not defined).	*string*
HostIdentity	Host identity	*string*

Component

Provides a summary for the product component.

Table 24: Component properties

Property Name	Description	Type
Enabled	State of the component	*boolean*

Firewall : Component

Provides information on WithSecure Firewall.

Table 25: Firewall properties

Property Name	Description	Type
Enabled	Current state of WithSecure Firewall	*boolean*

Property Name	Description	Type
SecurityLevel	Current security level of WithSecure Firewall	*string*
ApplicationControl	Current state of Application Control	*component*
Version	Version of WithSecure Firewall	*string*
Build	Build of WithSecure Firewall	*string*

Internet

Provides information on Internet security components.

Table 26: Internet properties

Property Name	Description	Type
BrowsingProtection	State of browsing protection	*component*
EmailFiltering	State of email filtering	*component*

Internet2

Simplified class for providing information on Internet security components.

Table 27: Internet2 properties

Property Name	Description	Type
BrowsingProtectionEnabled	State of browsing protection	*boolean*

LastManualScanReport

Provides information on the last scan performed manually by a user.

Table 28: LastManualScanReport properties

Property Name	Description	Type
Valid	Indicates whether the report was successfully found and loaded	*boolean*
StartTime	Time when scan was started	*datetime*
EndTime	Time when scan finished	*datetime*
StartTimeInHoursAgo	Time when scan was started (how many hours ago)	*uint32*
EndTimeInHoursAgo	Time when scan finished (how many hours ago)	*uint32*
InfectedFilesCount	Number of infected files found in the scan	*uint32*
TotalScannedFilesCount	Total number of scanned files	*uint32*

Property Name	Description	Type
HarmfulItemsFound	Indicates whether harmful items were found	*boolean*
ScanningReportFilePath	File path to the scan report	*string*

LastScheduledScanReport

Provides information on the last scan performed on schedule.

Table 29: LastScheduledScanReport properties

Property Name	Description	Type
Valid	Indicates whether the report was successfully found and loaded.	*boolean*
StartTime	Time when scan was started	*datetime*
EndTime	Time when scan finished	*datetime*
StartTimeInHoursAgo	Time when scan was started (how many hours ago)	*uint32*
EndTimeInHoursAgo	Time when scan finished (in hours) ago	*uint32*
InfectedFilesCount	Number of infected files found in the scan	*uint32*
TotalScannedFilesCount	Total number of scanned files	*uint32*
HarmfulItemsFound	Indicates whether harmful items were found	*boolean*
ScanningReportFilePath	File path to the scan report	*string*

LicenseStatus

Provides information on the currently used license.

Table 30: LicenseStatus properties

Property Name	Description	Type
Valid	Validity status of the license	*boolean*
EndDate	The end date of the subscription	*datetime*
DaysTillEndDate	The number of days till the end of the subscription	*uint32*
SubscriptionName	Product subscription name	*string*

Product

Provides information on the currently installed security product.

Table 31: Product properties

Property Name	Description	Type
Name	Name of the product	*string*
Version	Version of the product	*string*
Build	Build of the product	*string*

Profile

Provides information on the currently installed profile.

Table 32: Profile properties

Property Name	Description	Type
ProfileName	User-friendly name of the profile	*string*
ProfileVersion	Version of the profile package	*string*
SeriesName	Name of the profile package	*string*
InstallationTime	Time when the profile was installed	*datetime*

RebootStatus

Provides information on the restart status.

Table 33: RebootStatus properties

Property Name	Description	Type
Pending	Indicates whether a restart is pending	*boolean*
Reason	The reason why a restart is pending. Possible values: • *swup* (software updater) • *update* (self-update) • *virus* • *spyware* • *critical* (failed to self-update) • *malfunction*	*string*

SimpleComponent : Component

Default implementation of the base class.

Table 34: SimpleComponent properties

Property Name	Description	Type
Enabled		*boolean*

SoftwareUpdater : Component

Provides information on WithSecure Software Updater.

Table 35: SoftwareUpdater properties

Property Name	Description	Type
Enabled	State of WithSecure Software Updater	*boolean*
InstallSecurityUpdatesAutomatically	Type of updates installed automatically by Software Updater: • 0: None • 1: Critical • 2: Critical and important • 3: All	*uint32*
MissingCriticalUpdatesCount	Number of missing critical updates	*uint32*
MissingImportantUpdatesCount	Number of missing important updates	*uint32*
MissingOtherUpdatesCount	Number of missing updates other than critical and important	*uint32*

C.2.2 WMI classes in the Windows registry

All the WMI classes described in this section are also reflected to the Windows registry.

The classes can be found under the following path:

for 64-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\F-Secure\Monitoring`

for 32-bit systems: `HKEY_LOCAL_MACHINE\SOFTWARE\F-Secure\Monitoring`

NOTE: The WMI Provider setting must be turned on in WithSecure Elements Security Center for this registry key to appear.

Related reference

WMI classes on page 255

Classes used for WMI integration in WithSecure Elements Security Center.

Appendix D

Blocking unsuitable web content

Topics:

- Web content categories
- Select the content to block
- Access a blocked web site

Blocking unsuitable web content

You can block managed hosts' access to web sites and pages that contain unsuitable content with Web content control.

IMPORTANT: The Browsing Protection extension is required for Web Content Control to function properly.

Web content control uses WithSecure's reputation analysis data to categorize web sites and block access to any sites that contain content selected for the policy.

D.1 Web content categories

Use the categories listed here to block access to web sites based on the results of WithSecure's Network Reputation Service (NRS) content analysis.

NOTE: Category names used in the ini file are marked in parentheses.

Abortion	Web sites that provide information about abortion, discuss, promote, or encourage it, describe abortion procedures, or offer help in obtaining or avoiding abortions.
Ad serving	Web sites that offer for downloading files that show advertisements or other promotional content, for example, web sites that install potentially harmful browser plugins browser.
Adult	Web sites that are aimed at an adult (above 18) audience with content that is clearly sexual, or containing sexual innuendo. For example, sex shop sites or sexually-oriented nudity.
Alcohol and tobacco	Web sites that display or promote alcoholic beverages or smoking and tobacco products, including manufacturers such as distilleries, vineyards, and breweries. For example, sites that promote beer festivals and web sites of bars and night clubs.
Anonymizers	Web sites that allow or instruct people how to bypass network filters, including web-based translation sites that allow people to do so. For example, sites that provide lists of public proxies that can be used to bypass possible network filters.
Artificial Intelligence	Websites that use or provide artificial intelligence (AI) or machine learning (ML). This includes sites where you can use AI tools, download AI software, learn about AI, or use services that are powered by AI (like chatbots, image generators, or smart assistants).
Auctions	Web sites of online marketplaces where people can buy and sell their products or services. This includes sites that provide lists of products or services even though the actual transaction may happen somewhere else.
Banking	Web sites that provide online banking functionality, for example, bank deposits, electronic transfers between bank accounts, and currency conversion.
Blogs	Blog sites or forums that provide either free or paid services for creating and maintaining blogs.
Chats	Web sites that provide web-based services or downloadable software for text-based instant messaging or chats allowing people to chat online on the same site in real time.

Dating	Web sites that provide a portal for finding romantic or sexual partners. For example, matchmaking sites or mail-order bride sites.
Disturbing	Web sites that contain any information (for example, images, explanations or video games) that are disgusting and gross in nature.
Drugs	Web sites that promote drug use. For example, sites that provide information on purchasing, growing, or selling any form of these substances.
Entertainment	Web sites that promote or provide information about various movies, music, books, television, or magazines
File sharing	Web sites that provide file sharing applications.
Gambling	Web sites that promote or provide information on gambling and where people can bet online using real money or some form of credit. For example, online gambling and lottery web sites.
Games	Web sites that provide access to online games, for example, to play against other people online.
Hacking	Web sites that instruct on or promote questionable or illegal use of equipment and software to create viruses, hack passwords, or gain access to other computers.
Hate	Web sites that indicate prejudice against a certain religion, race, nationality, gender, age, disability, or sexual orientation. For example, sites that promote damaging humans, animals or institutions, or contain descriptions or images of physical assaults against any of them.
Illegal	Adult sites that contain images and information of children in sexual acts, and web sites that seek to exploit children.
Job search	Web sites of headhunting or recruitment agencies that are dedicated to job searching, job listings, and resume exchanges.
Payment service	Services that specialize in online payments or offer financial services, for example, various online payment methods, for online web stores.
Scam	Illegitimate or fraudulent web sites that contain malicious software that is used to attack a user's computer and obtain their personal information.
Shopping	Web sites where people can purchase any products or services, including sites that contain catalogs of items that help online ordering and purchasing and sites that provide information on ordering and buying items online.
Social networking	Networking portals that connect people in general or with a certain group of people for socialization, business interactions, and so on. For example, sites where you can create a member profile to share your personal and professional interests. This includes social media sites such as Twitter.
Software download	Web sites that provide free, trial, or paid software downloads.
Spam	Web sites with addresses that have been found in spam messages.
Streaming media	Web sites that provide music or video downloads and offer streaming video or audio content.
Unknown	Web sites whose reputation is unknown (typically due to them being not popular and not frequently accessed) or are not categorized even if they have a safety rating.

Violence	Web sites that may incite violence or contain gruesome and violent images or videos. For example, sites that contain information on rape, harassment, snuff, bombs, assault, murder, and suicide.
Warez (illegal downloads)	Web sites that allow users to download without fees or royalties; file sharing between a large number of people, which allows users to download; unauthorized file sharing or software piracy that is distributed by a group of people for free or to make profit.
Weapons	Web sites that promote the use of any material or contain information, images, or videos of weapons or anything that can be used as a weapon to inflict harm to a human or animal, including organizations that promote these weapons, such as hunting and shooting clubs. This category includes toy weapons such as paintball guns, airguns, and BB guns.
Webmail	Web sites that provide users free, web-based email services that can be accessed using any internet browser.

Trusted and disallowed sites configuration

Trusted sites	Contains a list of trusted site patterns.
Disallowed sites	Contains a list of disallowed site patterns.
Suspicious sites	Contains a list of suspicious site patterns.
Prohibited sites	Contains a list of prohibited site patterns.

D.2 Select the content to block

You can select the types of web content to block under the Web content control settings.

IMPORTANT: The Browsing Protection extension is required for Web Content Control to function properly.

Web content control blocks the website categories you select for managed devices once Browsing Protection is enabled.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
   *The **Profiles** page opens.*
2. Select the **Computer profiles** tab, and then select the profile that you want to edit.
3. Select **Browsing protection**.
4. Turn on **Web content control**.
5. Select next to **Web content control**.
   The list of web content categories opens.
6. Under **Disallowed**, turn on the categories that you want to block for managed hosts.
7. Click **Save and Publish**.

D.3 Access a blocked web site

A Browsing Protection block page appears when you try to access a site that has been rated harmful.

When a Browsing Protection block page appears:

1. If you want to enter the web site anyway, click **Allow website on this computer**.

Windows User Access Control asks you to confirm this action.

2. If necessary, enter your administrator account information.
3. Confirm the change.

You can now access the website.

Appendix E

Migration via Policy Manager Console

Topics:

- Migrate computers
- Migrate from Client Security for Mac to Elements Agent for Computers (Mac)

Migration via Policy Manager Console

If you have used Policy Manager, follow these instructions to migrate computers using a `.jar` file for Policy Manager.

If you manage computers with Policy Manager, you can migrate them to WithSecure Elements using a `.jar` file. This section describes how to migrate Windows computers and how to migrate Mac computers.

E.1 Migrate computers

Migrates computers from WithSecure Client Security to WithSecure Elements EPP for Computers and from Server Security to WithSecure Elements EPP for Servers.

To apply the `.jar` file and migrate, you need a Policy Manager console and the `.jar` file that you can download from the following link: https://download.withsecure.com/PSB/bs2cp/bs2elements.jar.

To migrate computers:

1. Open the Policy Manager console and select the group of computers that you want to migrate.
2. Select the **Installation** tab.
   *The **Installation** page opens.*
3. Under Policy-based installation, select **Install...**.
   *The **Choose installation package** window opens.*
4. Select **Import...** to import the installation packages.
   The available `.jar` file is shown.
5. Select the `.jar` file, and then select **Import**.
   Policy Manager imports the `.jar` file, and shows the package details.
6. Select **OK** to apply the `.jar` file.
7. In the **Installation options** window that opens, do the following:
   a) Enter a valid subscription key.
   b) Select the installation language, and then select **Finish**.
8. In the **Installation** window, select the
   
   icon at the top-left corner to distribute the policies to the selected computers.
   The selected computers are migrated and the policies are distributed to them.

If necessary, restart the selected computers to complete the installation.

E.2 Migrate from Client Security for Mac to Elements Agent for Computers (Mac)

Migrates Client Security for Mac to Elements Agent for Computers (Mac).

NOTE: These instructions apply only to Elements Agent for Computers (Mac) version 25.1. and newer.

Before installing the product, complete the following steps:

1. In the WithSecure Elements Security Center, create a custom profile that matches your Client Security for Mac policy. For detailed instructions, see Creating a new computer profile and Managing policies.

2. Rename your Elements Agent for Computers installer package to include your subscription key and the profile ID from the previous step. Use the following format:

```
ElementsAgentInstaller__<subscription-key>__<profile-id>__.pkg
```

NOTE: Remember to use a double underscore (__) as a separator. Profile IDs must always be used together with subscription keys, for example:
`ElementsAgentInstaller__XXXX-XXXX-XXXX-XXXX-XXXX__0000001__.pkg`

3. Review the available deployment methods for Elements Agent for Computers.
4. Select either a manual or an automated deployment.
5. Incorporate the installer name that you created earlier into your automation scripts.

The Elements Agent for Computers installer automatically uninstalls Client Security for Mac, activates the new product, and applies the profile that is specified in the installer name.

Related reference

Installer parameters for macOS on page 90
Use these installer filename patterns and `activator` command-line options to configure WithSecure Elements Agent for Computers (Mac) at install time.

Appendix F

Frequently asked questions

Topics:

- How can I change the language in Elements Security Center?
- Where can I find the WithSecure Email and Server Security email settings in Elements Security Center?
- How to order a new subscription key in Elements Security Center?
- How to renew or expand my current subscription key?
- How to clear the list of removed computers from Elements Security Center?
- Check for unsupported Elements clients
- When do I need to create my own security profile?
- Reinitialize the installed software

Frequently asked questions

Answers to frequently asked questions about WithSecure Elements Endpoint Protection and Elements Security Center.

This section answers frequently asked questions about WithSecure Elements Endpoint Protection and Elements Security Center, covering common portal, subscription, and device-management tasks.

If you do not find the answers to your questions, please contact support.

NOTE: For discussion and product updates, you can also check the WithSecure Community pages.

F.1 How can I change the language in Elements Security Center?

You change the interface language of WithSecure Elements Security Center in your personal settings.

1. Log in to WithSecure Elements Security Center.
2. At the top-right corner, select
   
3. Select **My settings**.
4. From the **Language** drop-down menu, select the language that you want to use.
5. Select **Save**.

F.2 Where can I find the WithSecure Email and Server Security email settings in Elements Security Center?

The WithSecure Email and Server Security email settings are not available in WithSecure Elements Security Center.

You cannot find the WithSecure Email and Server Security email settings in WithSecure Elements Security Center. Instead, view and modify them through the local Elements Endpoint Protection management console.

F.3 How to order a new subscription key in Elements Security Center?

You order WithSecure Elements Security Center subscriptions through the Partner Portal.

WithSecure Elements Security Center subscriptions are ordered through the Partner Portal.

F.4 How to renew or expand my current subscription key?

Partners renew or expand WithSecure Elements Endpoint Protection subscription keys through the Partner Portal.

NOTE: This applies only to partners.

WithSecure Elements Endpoint Protection subscription keys are renewed and expanded through Partner Portal.

F.5 How to clear the list of removed computers from Elements Security Center?

Removing a computer from WithSecure Elements Security Center adds the computer to a blocklist. The blocklist stops the computer from reconnecting to Elements Security Center.

As a result, the WithSecure Email and Server Security (ESS) installation cannot accept the same computer in a new installation with the same subscription key. A new or different subscription key, however, works on this computer. This means the computer is blocked from connecting to Elements Security Center only when it is tied to the specific subscription key.

F.6 Check for unsupported Elements clients

The **Issues** page in WithSecure Elements Security Center lists devices that run an outdated or unsupported Elements client.

Older Elements clients no longer receive engine and definition updates. To keep devices protected, find any unsupported clients and upgrade them to the latest WithSecure Elements version.

1. Log in to WithSecure Elements Security Center.
2. Select **Home** > **Endpoint Protection** > **Issues**.
3. Review the listed devices and upgrade each one to the latest WithSecure Elements client.

The upgraded devices receive the latest engine and definition updates and stay protected. The **Issues** page no longer flags them as outdated.

F.7 When do I need to create my own security profile?

In WithSecure Elements EPP for Computers and WithSecure Elements for Servers, you need to create a new security profile if none of the WithSecure predefined profiles match the needs of your end customers.

For example, you might have a program on your computer that slows down too much because of real time scanning operations. If so, you need to create a profile in which that program is excluded from scanning. Or a network software such as a VPN client might not be able to connect to the Internet with the default firewall rules. If so, you must create a new security profile with specific firewall rules for the software.

F.8 Reinitialize the installed software

The `ws_oneclient_logout` tool allows you to log out from WithSecure Elements EPP for Computers so that you can re-enter the subscription key to connect a device to the correct company in WithSecure Elements Security Center.

Using the tool, you can remove the current subscription from WithSecure Elements EPP for Computers and return it to its initial state, which has not yet had a subscription key entered.

TIP: This is useful, for example, when you want to clone new Citrix instances from a main image.

To reinitialize the product:

1. Open a command prompt with administrator privileges.
2. Navigate to the installation directory of the WithSecure Elements EPP client by executing the following command:

```
c: && cd %ProgramFiles(x86)%\F-Secure\PSB
```

3. To log out from the product and automatically register to Elements Security Center, enter the following command:

```
.\ws_oneclient_logout.exe
      --keycode <subscription-key>
```

The product logs out and starts using the subscription key that you entered.

When reinitializing the product, you can use the following command-line parameters

--psb1, --psb2, --psb3, --psb4, --psbsmieu

Allows you to switch registered clients between the portals.

NOTE: Specify the portal name only when you switch a client to another portal. Do not add these command parameters if you are switching a subscription key within the same portal.

--nokeycode

Removes the current subscription key. The product (WithSecure Elements EPP for Computers) stops working and asks you to manually enter a new subscription key when you open the main view of the application.

--profile-id <profileId>

Allows you to force of the assignment of any profile. When you re-register your device, the default profile is assigned to it. With this parameter, you can assign your device the desired profile. For example: `"%ProgramFiles(x86)%\F-Secure\PSB\ws_oneclient_logout.exe" --keycode <subscription-key> --profile-id profileId`

NOTE: The desired profile is stored on the product. If you use the `ws_oneclient_logout.exe` tool again without adding the --profile-id command line parameter, the same profile will be assigned again.

--proxy

Specifies a proxy to be used during a login process. For example: `--proxy your.proxy:80`

NOTE: The proxy should be in the following format: proxy:port.

--wait-uuid-changed

Can be used on cloned virtual machines if SMBIOS UID does not change immediately after cloning. If you use the `ws_oneclient_logout.exe` tool with this option (`ws_oneclient_logout.exe --wait_uuid_changed`), the system waits until the UUID is changed to make sure that the device registers with the correct, unique ID on Elements Security Center.

This option works only if SMBIOS is used to identify the device. It has no effect if other identification methods are used.

If the tool runs successfully, it returns `0` as the result. In other cases, for example if the network is unavailable or you enter an incorrect subscription key, WithSecure Elements EPP for Computers stays in the "expired" state and asks you enter the new subscription key manually.

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.

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.

App Configuration

App configuration is the set of settings or values used to preconfigure application behavior, permissions, or features during deployment or management.

Application Control

Application Control is a rule-based endpoint security feature that prevents the execution and installation of selected applications and stops them from running scripts.

Automated Tasks

Automated tasks are predefined tasks that run automatically on devices or systems according to configured schedules, triggers, or conditions.

Automation

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

Backdoor

An undocumented way of gaining access to a computer system.

Banking Protection

Protects users against harmful activities when they access online banks or make transactions online.

Behavioral Analysis

Behavioral analysis is a detection approach that identifies threats by observing deviations from normal patterns of activity rather than relying only on known signatures.

Blocklist

A blocklist is a list of entities — such as applications, websites, senders, or file hashes — that are explicitly denied access or execution; the opposite of an allowlist.

Breach

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

Broad Context Detection (BCD)

A Broad Context Detection is a group of related detections that WithSecure Elements EDR correlates into a single incident, ranked by criticality, to show the full context of an attack.

Browsing Protection

A feature that evaluates the safety of visited websites and prevents users from unintentionally accessing harmful websites.

Browsing Protection Extension

The Browsing Protection Extension is a browser component that enables web protection features such as reputation-based site analysis and policy-based web content control.

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 Security

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

Cloud Service

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

Configuration Keys

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

Connection Control

A feature that automatically detects when you access an online banking web site and blocks all other connections while it is active.

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.

DataGuard

A security feature that protects sensitive files from unauthorized access, encryption by ransomware, or exfiltration.

DeepGuard

A feature that protects the computer against unknown threats by monitoring program behavior in real-time and stopping dangerous activities.

Detection

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

Device Control

A security feature that restricts the use of external devices such as USB drives, Bluetooth peripherals, and other removable media to prevent data leaks and malware infections.

Discovery Scan

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

Disinfect

A function of an antivirus program that attempts to remove the virus from an infected file without deleting the whole file.

Encryption

Encryption is the process of converting data into a secure format using cryptographic algorithms, ensuring confidentiality and protection against unauthorized access.

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.

Endpoint Security

Endpoint security is the protection of end-user devices — such as laptops, servers, and mobile devices — from threats through prevention, detection, and response controls.

Entra ID

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

Exclusion Rules

Exclusion rules are rules that omit specific files, paths, processes, or other items from scanning, monitoring, or enforcement.

Exploit

Objects or methods that take advantage of a flaw in a program to make it behave unexpectedly. Doing so creates conditions that an attacker can use to perform other harmful actions.

Exposure Management

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

External Attack Surface (EAS)

The collection of internet-facing assets, services, and vulnerabilities that an attacker can exploit.

False Positive

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

Federated Single Sign-On (FSSO)

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

Firewall Configuration

The process of setting rules and policies to control inbound and outbound network traffic, ensuring network security and compliance.

Firewall Profile

A firewall profile is a defined set of firewall rules and settings that is applied to a device or network context.

Firewall Rules

Firewall rules are individual allow, block, or filtering directives that define how firewall traffic is handled.

Golden Image

A golden image is a preconfigured system image used as the standard source for cloning or deploying identical devices or virtual machines.

Group Policy (GPO)

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

Harmful Content

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

Highest Impact Recommendations

A prioritized list of security findings that require immediate attention to reduce cyber risks.

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.

Infection

An infection is the state in which a file, object, system, or workload contains or has been affected by malicious code or other harmful content.

Lateral Movement

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

License Key

A license key is a unique code that activates a software product or subscription and verifies that its use is authorized.

License Status

The current state of a security product's subscription, determining its validity and expiration date.

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.

Malware Definition

A malware definition is a signature or pattern that antivirus software uses to identify known malicious files.

Malware Protection

Malware Protection is the feature that detects, blocks, and removes viruses and potentially unwanted applications on a device.

Malware Scan

A malware scan is a scan that checks a device, file set, or workload for malicious software or other harmful content.

Manual Scanning

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

Membership

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

Mobile Device Management (MDM)

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

MSI Properties

Parameters used in command-line installation of software packages via Microsoft Installer (MSI).

Multi-Factor Authentication (MFA)

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

Network Gateway

Network Gateway is a mobile protection component that routes and inspects device traffic — for example, through a remote proxy — to block unsafe destinations and content.

Network Isolation

Network isolation is a containment action that restricts or blocks a device's network communication to prevent further malicious activity or spread.

Network Protection

Network Protection is a security capability that monitors or controls network traffic to help protect users and devices from unsafe connections and content.

Patch Management

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

Phishing

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

Potentially Unwanted Application (PUA)

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

Privacy

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

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.

Ransomware

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

Ransomware Protection

A feature that monitors a set of folders for potentially harmful changes made by ransomware or other, similar harmful software.

Real-Time Protection

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

Real-Time Scanning

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

Remote Monitoring and Management Integration (RMM)

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

Reputation Service

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

Riskware

Software that is not designed specifically to harm computers, but that may cause problems if it is misused.

Role Assignment

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

Role-Based Access Control (RBAC)

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

Sample Submission

A sample submission is a request that sends a suspicious file, URL, or email for analysis and follow-up handling.

Sample Validation

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

Scan

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

Scan Node

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

Scan Templates

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

Scheduled Scan

A scheduled scan is a scan configured to run automatically at defined times, intervals, or system conditions without needing a user to start it manually.

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 Cloud

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

Security Events

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

Security Group

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

Security Information and Event Management (SIEM)

Security Information and Event Management (SIEM) is a technology that collects, correlates, and analyzes log and event data from across an environment to detect threats and support incident response.

Security Monitoring

Security monitoring is the continuous collection and analysis of system and network activity to detect, alert on, and investigate potential security threats.

Security Policy

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

Sensor

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

Server Share Protection

Server Share Protection is a capability that monitors access to shared files and helps detect or limit ransomware activity affecting shared data.

Service Account

A service account is a special type of account used by applications, scripts, or automated processes to interact with systems and services, often with predefined permissions.

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.

Spam

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

Spyware

Software that aims to gather information about a person or organization without their knowledge

and that may send such information to another entity without the consumer's consent, or that asserts control over a computer without the consumer's knowledge.

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.

Tamper Protection

A security control that prevents the disabling or modification of security solutions by unauthorized users or malware.

Tenant

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

Threat Detection

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

Threat Intelligence

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

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.

Virus

A virus is usually a program that can attach itself to files and replicate itself repeatedly; they can alter and replace the contents of other files in a way that may damage the computer.

Virus Protection

Prevents viruses, worms and Trojan horses from getting onto a computer as well as removes any malicious software code that has already infected a computer.

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.

Web Content Control

A feature that blocks access to web content based on predefined categories and security policies.

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.

Zero-Day

A zero-day is a vulnerability or exploit that is unknown to the vendor and has no available fix, leaving affected systems exposed until a patch is released.

Index

A

B

C

D

E

F

G

H

I

J

K

L

M

S

T

U

V

W

X

Z