Elements Connector

2026-09-23

Contents

Chapter 1: Introduction to the WithSecure Elements solution.....3

1.1 Using WithSecure Elements Security Center.....4

Chapter 2: Elements Connector overview.....37

Chapter 3: Deploying Elements Connector.....39

3.1 System requirements.....40
3.2 Install Elements Connector on Windows.....41
3.3 Install Elements Connector on Linux.....42

Chapter 4: Managing Elements Connector via Elements Security Center.....44

Chapter 5: Configuring Elements Connector as a proxy.....46

5.1 Proxy with commercial certificate.....47
5.2 Proxy with self-generated certificate.....48
5.3 Changing default port values.....50

Chapter 6: Configuring event forwarding.....51

6.1 Configure API access for Elements Connector.....52
6.2 Configure event forwarding settings.....53
6.3 Verify event forwarding.....54

Chapter 7: Troubleshooting.....55

Glossary.....57

Index.....62

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 overview

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

The WithSecure Elements offering

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

To highlight some of the main benefits:

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

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

Supported languages

The Elements Security Center supports the following languages:

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

Endpoint products support the following languages:

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

WithSecure Elements training

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

Accessing the WithSecure Elements Security Center

You can access Elements Security Center as follows: WithSecure Elements Security Center

1.1 Using WithSecure Elements Security Center

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

This chapter describes the following tasks:

- managing access rights
- adding new administrator accounts
- adding customer companies
- using the *scope selector* to broaden or narrow the scope of information displayed in WithSecure Elements Security Center

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

1.1.1 Get started with WithSecure Elements Security Center

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

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

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

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

- If you have a subscription key but no account yet, create the first administrator account with the self-registration link to WithSecure Elements Security Center.

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

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

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

1.1.2 Logging in

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

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

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

Log in to non-federated domains

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

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

1. Open the following link in the web browser: WithSecure Elements Security Center sign-in page.
   *The **Log in** page opens.*
2. Enter your username and password, and select **Log in**.

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

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

Log in to federated domains

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

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

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

1. Open the following link in the web browser: WithSecure Elements Security Center sign-in page.
   You are redirected to the Microsoft login page.
2. Enter your Entra credentials, and select **Log in**.

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

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

Multi-factor authentication

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

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

> **IMPORTANT:** We recommend that you use Multi-Factor Authentication (MFA) to secure access to WithSecure Elements Security Center. Set up MFA immediately in Elements Security Center.

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

When users log in to a system with their username and password, their credentials may already have been compromised, for example, due to a vulnerability in their browser or password manager. These leaked credentials may be on some publicly accessible list, used by attackers to gain entry into systems. With the

addition of MFA, an extra step is needed when logging in. System access is traditionally protected with username and password, something that only you know. MFA introduces additional factors; something that you have (a security key or device) and something that you are (your fingerprint or facial recognition).

MFA methods

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

The methods include the following:

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

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

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

- *Secure USB keys*, such as Yubico YubiKey, Google Titan, and others that support the FIDO2 standard (FIDO2 specification)
- *Smartphones or other devices* that support the FIDO2 standard (FIDO2 specification)
- *Device biometrics*, fingerprint or facial recognition or Windows Hello from your device using WebAuthn (Web Authentication (WebAuthn) specification).

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

Choose multi-factor authentication

Chooses one or more multi-factor authentication methods.

Before you choose a multi-factor authentication method:

- Install an authentication app, for example, Google Authenticator on your mobile device.
- Make sure that your mobile device can read QR codes.

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

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

To choose one or more multi-factor authentication methods:

1. Log in to WithSecure Elements Security Center with your email address and password.
2. Select

   at the top-right corner, then select **My settings**.

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

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

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

Remove a multi-factor authentication

Removes a multi-factor authentication method.

To remove a multi-factor authentication method:

1. Log in with your email address and password.
2. Enter your multi-factor authentication code and select **Continue**.
3. Select

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

Use device biometrics

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

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

To use device biometrics, do the following:

1. In Elements Security Center, select

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

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

1.1.3 User management

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

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

About access rights

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

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

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

Access rights by role

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

Exposure Management – Exposure

Full editing Allows access to the following Exposure Management features:

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

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

Audit logs entry: cspm: admin

Exposure Management – Vulnerabilities

Management

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

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

Audit logs entry: vm: administrator

Team member

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

Audit logs entry: vm: team_member

Read-only

View-only access with no permission for managing users.

Audit logs entry: vm: readonly_team_member

Collaboration Protection

Admin

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

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

Audit logs entry: cpo365:admin

Read-only

Grants view-only access to the Collaboration Protection views.

Audit logs entry: cpo: readonly

Quarantine manager

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

Audit logs entry: cpo365:quarantine_mgr

Collaboration Protection – Management

Admin

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

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

Audit logs entry: fusion_admin

Endpoint Protection

No access

No access to Endpoint protection features including:

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

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

Endpoint Protection - Computers and mobiles

Full editing

Allows the access to the following features:

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

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

Audit logs entry: epp: manage_computers_mobiles_only

or epp: manage_all

Read-only

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

Audit logs entry: epp: manage_servers_only

or epp: readonly

Endpoint Protection - Servers

Full editing

Allows the access to the following features:

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

NOTE: The Security Administrator role, along with the "Computers and mobiles - Full editing" role is required to create additional administrators and assign

> this role to users within the same organization (will be replaced by the IAM role).

Audit logs entry: epp: manage_servers_only

or epp_manage_all

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

Audit logs entry: epp: manage_computers_mobiles_only

epp: readonly

Extended Detection and Response – Toggle off

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

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

Extended Detection and Response – Broad Context Detections

Full editing Permission to manage:

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

Limited access to:

Devices view
Cloud view
Subscription view

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

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

Audit logs entry: elements:xdr-incident-full

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

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-incident-read

Extended Detection and Response – Response

Execute responses

Access to execute:

- response actions
- configure Automated actions

Limited access to Cloud view.

Audit logs entry: elements:xdr-response-full

List responses

Access to review:

executed response actions
respective results available

Limited access to:

Devices view
Cloud view

Download response results requires the Execute Responses permission.

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-response-read

No access

No access to execute or review:

Response actions
Automated actions

Extended Detection and Response – Event Search

Read-only

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-event-search

No access

No access to review event data.

Elements Administration

No access

No rights to create new users or manage other users access rights.

Identity and Access Management	Rights to create, delete and manage all Elements users.

Move between the managed companies

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

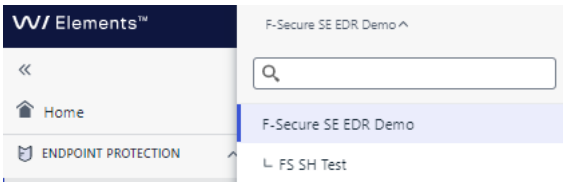
In Elements Security Center, there are different account levels, which determine the access rights:

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

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

1. Select the

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

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

Elements Identity and Access Management (IAM) role

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

Overview

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

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

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

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

Benefits

The IAM role provides several benefits, including the following:

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

Claiming the IAM role

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

Elements IAM role properties

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

IAM administrators can do the following:

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

Acquiring the IAM role

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

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

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

Migration of IAM permissions

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

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

For customer companies	Security administrators with the following identified legacy roles: • Elements Exposure Management: Full editing • Elements Collaboration Protection: Management administrator • Elements Vulnerability Management: Administrator • Elements Endpoint Protection - Computers, servers, and mobiles: Full editing
For Solution Providers and Service Partners	Security administrators with legacy roles for all capabilities and services used by the companies they manage

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

When IAM administrator candidate cannot be identified

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

Frequently asked questions about IAM roles

Answers to frequently asked questions about IAM roles.

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

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

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

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

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

A new administrator account is created.

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

Add a new service partner

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

To create a service partner account:

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

The service partner account is created.

Edit or remove administrators

You can edit or remove administrators accounts.

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

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

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

   The administrator account is deleted.

Create an API client

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

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

To create an API client:

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

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

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

A new API client is created.

Delete an API client

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

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

To delete an API client:

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

Recover your password

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

To recover your password:

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

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

Change your account details

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

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

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

To change your user name:

1. Select

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

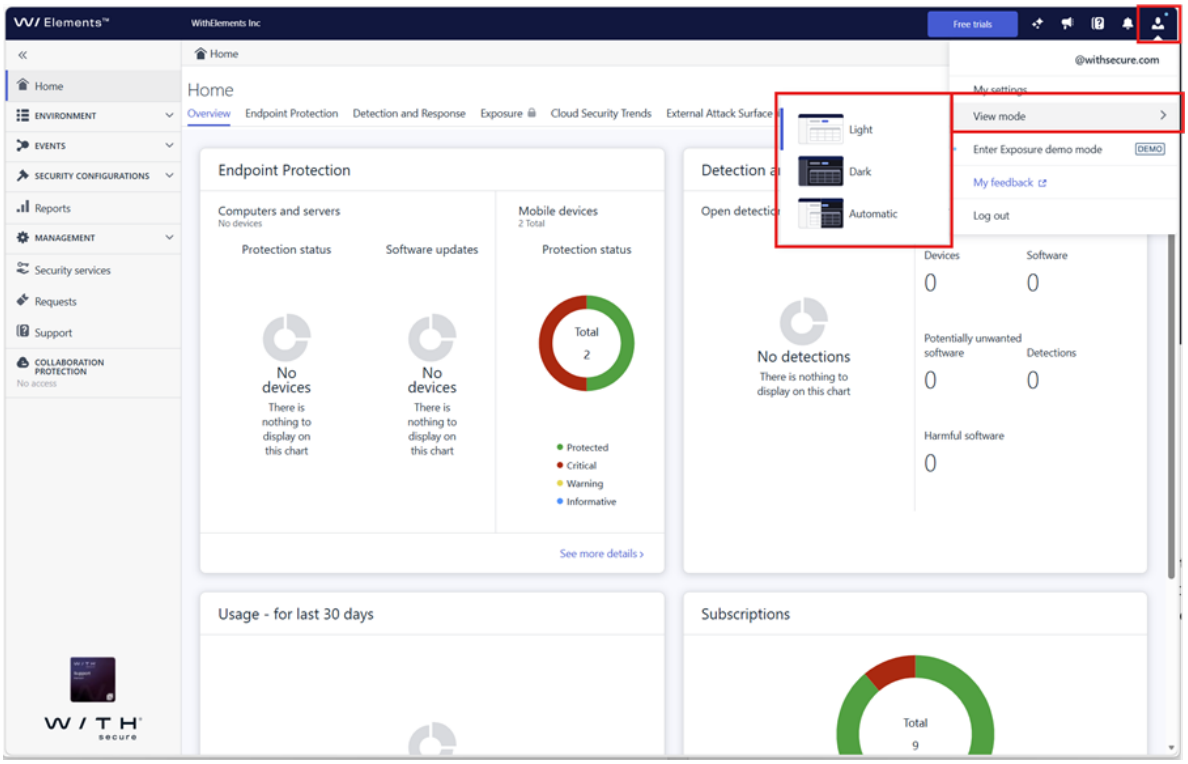
1.1.4 Change the view mode

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

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

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

- **Automatic** – matches the system settings of your device and switches between light and dark automatically.



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

1.1.5 Taking Elements products into use

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

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

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

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

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

Adding a customer company

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

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

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

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

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

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

Assign a subscription key for a customer company

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

You need to consider the following:

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

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

To assign a subscription key:

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

The new subscription key is added to the company account.

Order products for an existing customer company

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

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

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

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

   NOTE: WithSecure Partner Portal requires separate login credentials from WithSecure Elements Security Center. If you do not yet have your login details, complete the **Request Credentials** form on the page and click **Send**. 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, complete the **Request Credentials** form on the page and click **Send**. 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. Enter the customer details and select **Save**.
5. Under **New Order**, enter a reference number for your order.
6. Under **Order Products**, select **Add Products**.
7. Select the required products and follow the ordering instructions.

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

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

View available product subscriptions

To view the available subscriptions:

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

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

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

2. You can use filtering to find the following:

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

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

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

Change the subscription key

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

To change the subscription key:

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

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

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

The new subscription key is applied to the selected devices.

Upgrading your subscriptions

Options for upgrading your WithSecure Elements subscriptions.

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

Upgrading your subscriptions

You can upgrade your subscription in two ways:

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

You have the following options in upgrading your subscriptions:

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

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

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

1.1.6 Federated single sign-on

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

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

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

Prerequisites

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

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

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

Before implementing single sign-on (SSO)

These requirements and considerations apply before you implement single sign-on (SSO).

Why is plus addressing problematic?

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

> **IMPORTANT:**
>
> Do not configure SSO using email aliases or Elements user accounts with plus addressing.

Frequently asked questions

How to avoid users losing access to remove federation?	When implementing federation, make sure that there is a user account without plus addressing or email alias. Otherwise, you may lose access to Elements Security Center.
How does SSO change the login process?	After federation, users authenticate through Microsoft Entra ID, eliminating the need for a separate login flow for Elements Security Center.
How often do users with Elements Entra ID need to authenticate to Elements Security Center?	If users do not have a valid federated authentication session, Elements Security Center requires them to log in and authenticate.

Global impact of SSO

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

Hierarchy-level considerations

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

Handling Microsoft Entra ID account removal

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

Set up federated single sign-on with Microsoft Entra ID

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

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

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

- Entra ID tenant account - an account in the Entra ID tenant that manages the domain that you want to federate. This account is essential for logging in to Elements Security Center and federating the domain.

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

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

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

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

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

Link user identities

Links user identities in Elements Security Center for federated domains.

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

Make sure you have the following:

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

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

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

To link identities:

1. Log in to WithSecure Elements Security Center sign-in page.
2. Enter your email address and select **Continue**.
3. If your email address is already authenticated in the domain, you are redirected to the identity linking flow; if your email address is not yet authenticated in the domain, you are asked to provide your domain password.

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

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

Remove federation from a domain

Removes single sign-on federation from a domain.

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

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

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

To remove federation:

1. Log in to WithSecure Elements Security Center sign-in page.
2. Select **SSO Access Federation**.
   *The **Federated Single sign-on** window opens showing the status of the domain that matches your email address.*
3. Select **Remove Federated Single sign-on**.
   A confirmation window opens.
4. Select **Ok**.
   Single sign-on federation is removed from the domain account.

1.1.7 Adding devices for management

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

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

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

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

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

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

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

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

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

Distributing WithSecure software

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

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

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

  - WithSecure Elements EPP for Computers Premium (Windows only)
  - WithSecure Elements EDR and EPP for Computers Premium (Windows only)
  - WithSecure Elements Exposure Management (Windows only)
- You can install the following software using the same WithSecure Elements Agent for Servers installation package. The subscription key determines which software is installed:
  - WithSecure Elements EPP for Servers (Windows and Linux)
  - WithSecure Elements EDR for Servers (Windows only)
  - WithSecure Elements EPP for Servers Premium (Windows only)
  - WithSecure Elements EDR and EPP for Servers Premium (Windows and Linux)
  - WithSecure Elements Exposure Management (Windows only)
- You can install WithSecure Elements Mobile Protection in two ways:
  - By sending an installation email via the WithSecure Elements EPP portal using the **Add new device**.

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

  - By sending an installation email via a third-party MDM software.
- For installing WithSecure Elements Connector, see instructions at WithSecure Elements Connector documentation.

Send an installation link via email

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

> **NOTE:** The installation link is valid for 30 days.

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

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

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

   next to **Devices**.
   A menu is displayed.
3. From the menu, select **Add new device**.
   *The **Add new device** page opens.*

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

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

   To send multiple invitations, under **Import from CSV file**, select **Choose file** to select a CSV file from which you want to import data. Multiple email addresses must be separated by commas.
7. Select **Send**.
   The listed recipients receive an email that contains a link to the download site and instructions for downloading and installing the product that you selected.

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

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

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

Download software from Elements Security Center

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

To download the software:

1. Log in to Elements Security Center.
2. Select **Downloads** on the sidebar.

*The **Downloads** page opens.*

3. Locate the section for your device type, for example **WithSecure Elements Agent for Computers** or **WithSecure Elements Agent for Servers**.
4. Select the download button for your operating system.

   The available buttons depend on the operating system:

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

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

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

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

After downloading the software, you need to deploy it.

Manage automatic deletion of devices

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

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

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

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

To turn on automatic deletion of devices:

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

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

6. Select **Save**.

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

Manage invitations

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

To manage the invitations:

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

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

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

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

1.1.8 Enhancing device management with custom labels

Create and apply labels to group devices by criteria that you choose.

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

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

Add device labels

You can add device labels in three different ways.

You can add device labels in the following ways.

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

Add device labels in one of the following ways:

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

1.1.9 Managing devices in Elements Security Center

How to manage the selected devices in WithSecure Elements Security Center

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

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

Managing asset groups

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

You can assign devices to asset groups in two ways:

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

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

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

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

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

Create asset groups

Creates an asset group at the company level.

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

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

Next, go to the **Devices** page to add devices to the new asset group.

Add devices to asset groups

Adds devices to one or more asset groups.

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

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

5. Select **Assign**.

Remotely manage a device

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

To remotely manage a device:

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

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

   The instruction is sent to the selected device.

Automatically delete devices

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

NOTE: This feature does not apply to mobile devices.

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

To manage automatic deletion:

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

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

6. Select **Save**.

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

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

View devices based on the Active Directory structure

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

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

To view devices based on the Active Directory structure:

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

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

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

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

Customize the Devices view

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

To customize the Devices view:

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

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

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

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

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

Request diagnostic data

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

If there is an issue with a device in your managed accounts, the WithSecure Elements Security Center administrator can select the device and make a request to the customer, who allows a diagnostics (WSDIAG) file to be collected and uploaded to WithSecure Elements Security Center. The diagnostics file helps determine 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 Connector overview

Elements Connector overview

Elements Connector is an on-premise product that serves three purposes.

- Elements Connector optimizes traffic between the managed endpoints in your environment and WithSecure services by caching Software Updater, updates to malware definitions, and program upgrades. If you download all these updates directly from the internet, your device consumes a huge amount of external traffic. To reduce the costs, you can use WithSecure caching endpoint. This endpoint downloads the requested files only once and then distributes them to the devices within your network.
- The Elements Connector Ultimate proxy acts as a proxy for all traffic between WithSecure endpoints and cloud services. This simplifies firewall configurations and lets you use WithSecure products in semi-closed environments.
- Some companies use security monitoring services such as Splunk. For these companies, Elements Connector forwards security events from WithSecure cloud services to security information and event management (SIEM).

Elements Connector in its proxy role replaces WithSecure Policy Manager Proxy. The most important improvements over the previous product are automatic upgrades and support for centralized manageability from WithSecure Elements Security Center.

Chapter 3

Deploying Elements Connector

Topics:

- System requirements
- Install Elements Connector on Windows
- Install Elements Connector on Linux

Deploying Elements Connector

Deploy Elements Connector by checking the system requirements and then installing the software on a Windows or Linux host.

Deploying Elements Connector consists of two stages. First, confirm that the target host meets the hardware and operating-system requirements. Then install Elements Connector on a Windows or Linux host, depending on your environment.

The installation method differs between Windows and Linux hosts, so use the procedure that matches the host operating system.

3.1 System requirements

The following shows the recommended requirements for installing and using the product.

System requirements for Windows

One of the following Windows operating systems:

- Windows Server 2016; Essentials, Standard or Datacenter editions
- Windows Server 2019; Essentials, Standard or Datacenter editions (Server Core is supported)
- Windows Server 2022; Essentials, Standard or Datacenter editions (Server Core is supported)
- Windows Server 2025; Essentials, Standard or Datacenter editions (Server Core is supported)
- Windows 10
- Windows 11

System requirements for Linux

One of the following 64-bit Linux platforms:

- Alma Linux 8, 9
- Debian 11, 12
- openSUSE Leap 15
- Oracle Linux 8, 9
- Red Hat Enterprise Linux 8, 9
- Rocky Linux 8, 9
- SuSE Linux Enterprise Server 15
- SuSE Linux Enterprise Desktop 12, 15
- Ubuntu 20.04, 22.04, 24.04 LTS

Hardware requirements for both Windows and Linux

- Processor: Dual-core 2GHz CPU or higher
- Memory: 4 GB RAM
- Disk space: minimum of 10 GB of free disk space.

NOTE: If Software Updater update caching is used, the system requires an additional 20 GB of disk space to serve software updates.

NOTE: On Linux platforms, when `/tmp` is mounted as a separate file system, at least 1 GB of free disk space is required.

- Network: 100 Mbit network

3.2 Install Elements Connector on Windows

Installs WithSecure Elements Connector in your managed environment on Windows.

To download and install Elements Connector:

1. In the WithSecure Elements Endpoint Protection portal, go to the **Downloads** page and click **MSI** under **WithSecure Elements Connector** > **Windows**.
2. Save the downloaded `.msi` file to the computer where you want to install Elements Connector.
3. On the command line, locate the installation `.msi` file and run the following command:

```
installer.msi VOUCHER=<subscription key>
```

   Replace `<subscription key>` with a valid subscription key for Elements Connector. You can find your subscription key on the **Subscriptions** page in the WithSecure Elements Endpoint portal.

4. Complete the installation wizard.

After installation, if you want to use event forwarding, you have to configure the API access and assign a profile with the event forwarding settings before using the product.

NOTE: To check whether Elements Connector is correctly installed, open the following URL in your browser: `https://localhost/`. If Elements Connector is installed and working properly, the Elements Connector welcome page opens.

3.2.1 Command-line parameters and MSI properties

When installing WithSecure Elements Connector using an `.msi` package, you can use the command-line parameters and MSI properties listed here.

VOUCHER

Sets the subscription key.

Format: `VOUCHER=<subscription key>`

PROXY_SERVER

Overrides proxy to use for downloads.

Format: `PROXY_SERVER=<url>`

NOTE: If you did not use the PROXY_SERVER parameter during the installation or you need to edit the proxy value after the installation, set it in `c:\ProgramData\WithSecure\NS\ElementsConnector\data\fspms.proxy.config` as follows and restart the Elements Connector service:

```
http_proxy=http://proxy-server-address:80
```

Elements Connector supports the use of multiple HTTP-proxies that you can configure at once. This allows for proxy redundancy, which means that Elements Connector can switch to a next proxy in the list if the current one has connectivity issues. You can configure a list of multiple proxies using the MSI properties

(PROXY_SERVER) or fspms.proxy.config (http_proxy=...). You can also configure multiple proxies via the Elements Connector profile in **General settings** > **Internet connection** > **HTTP proxy**.

> **NOTE:** When adding several proxy addresses in a row, use semicolon to separate them, for example: `http://proxy-server-1:80;http://proxy-server-2:80;http://proxy-server-3:80`

3.3 Install Elements Connector on Linux

Installs WithSecure Elements Connector in your managed environment on Linux.

To download and install Elements Connector:

1. In the WithSecure Elements Endpoint Protection portal, go to the **Downloads** page and click **DEB** or **RPM** under **WithSecure Elements Connector** > **Linux**.
2. Save the downloaded `.deb` or `.rpm` file to the computer where you want to install Elements Connector.
3. On the command line, locate the installation `.deb` or `.rpm` file and run the following command as the root user:
   - Debian, Ubuntu:

     ```
     # dpkg -i elements-connector.deb
     ```

   - Red Hat, CentOS, SuSE, Oracle Linux:

     ```
     # rpm -i elements-connector.rpm
     ```

> **NOTE:** Elements Connector requires Linux capabilities library. Make sure it is installed before installing Elements Connector. SUSE Linux Enterprise Server 11 and SUSE Linux Enterprise Desktop 11 administrators might need to explicitly enable Linux File System Capabilities by adding 'file_caps=1' as a kernel boot option (see SUSE Linux Enterprise Server 11 release notes for more details: SUSE Linux Enterprise Server 11 SP4 release notes).

4. Configure and start Elements Connector by running the following script as the root user:

```
# /opt/f-secure/fspms/bin/fspms-config
```

> **NOTE:** To set the HTTP proxy address, edit `/var/opt/f-secure/fspms/data/fspms.proxy.config` as follows and restart the Elements Connector service: `http_proxy=http://proxy-server-address:80`

> **NOTE:** On the second configuration step, you must enter a valid subscription key for Elements Connector. You can find your subscription key on the Subscriptions page in the WithSecure Elements Endpoint portal.

Elements Connector supports the use of multiple HTTP-proxies that you can configure at once. This allows for proxy redundancy, which means that Elements Connector can switch to a next proxy in the list if the current one has connectivity issues. You can configure a list of multiple proxies using the MSI properties (PROXY_SERVER) or fspms.proxy.config (http_proxy=...). You can also configure multiple proxies via the Elements Connector profile in **General settings** > **Internet connection** > **HTTP proxy**.

> **NOTE:** When adding several proxy addresses in a row, use semicolon to separate them, for example: `http://proxy-server-1:80;http://proxy-server-2:80;http://proxy-server-3:80`

3.3.1 Installation notes

The following lists the Linux dependencies that are required for the installation.

Red Hat, CentOS, and Suse distributions:

- Elements Connector requires both 32-bit and 64-bit versions of the `libstdc++` library. Make sure that the `libstdc++` and `libstdc++.i686` packages are installed before you install Elements Connector.
- On SuSE Linux Enterprise Server/Desktop 15 and OpenSUSE Leap 15, `insserv-compat` need to be installed before installing Elements Connector.

Debian and Ubuntu distributions:

- Install both the 32-bit and 64-bit versions of the `libstdc++` library before you install Elements Connector. Use Multiarch capabilities (Debian Multiarch HOWTO) to install the 32-bit library on 64-bit platforms.
- Install the `libstdc++6` and `libstdc++6:i386` packages before you install Elements Connector. If the installation failed because the compatibility library was not found, install the library. Then run `apt-get install -f` to finish installing the product.

Chapter 4

Managing Elements Connector via Elements Security Center

Managing Elements Connector via Elements Security Center

You can manage Elements Connector via the WithSecure Elements portal.

Via the portal, you can add Connector devices, assign profiles, view their status and details, such as assigned profile and device properties. Device properties also highlight Connector operational issues, for example, low disk space and expired certificates.

For more details on how to configure computer and server profiles and to make sure that they use the Connector, go to the WithSecure Elements help at WithSecure Elements Endpoint Protection | Elements Endpoint Protection | Latest | WithSecure User Guides.

Chapter 5

Configuring Elements Connector as a proxy

Topics:

- Configure Elements Connector as a proxy using commercial certificates
- Configure Elements Connector as a proxy using self-generated certificates
- Changing the default port values on Elements Connector

Configuring Elements Connector as a proxy

For using Elements Connector as a proxy, you need to install it on a computer that has access to the internet and is accessible by your company endpoint computers.

Elements Connector supports two independent modes: caching mode and ultimate mode:

- In the caching mode, Elements Connector implements native support for WithSecure malware definitions and software update distribution protocols that allows an effective optimization of the internet traffic.
- In the ultimate mode, Elements Connector acts as a proxy for all traffic between WithSecure endpoints and cloud services, including the centralized management capabilities, cloud lookups (Karma & Mind), EDR, and other features.

The solution allows you to use WithSecure products in semi-closed environments where endpoints are not allowed to access the internet directly. Elements Connector restricts an outbound connection only to WithSecure cloud services. Therefore, separate firewall configurations are not required.

For the endpoint computers to use Elements Connector as a caching proxy, you must specify its address in the profile settings of the WithSecure Elements Connector endpoint computers.

For the endpoint computers to use Elements Connector as an ultimate proxy, you must specify its address under **Manually defined HTTP proxy address** in the profile settings of the endpoint computers.

Ultimate mode extends the HTTP host interface (default port 80) - use this port value in the endpoint computer profile setting.

NOTE: You can use both the caching and ultimate proxy modes together.

NOTE: An Elements Connector can use another Elements Connector to connect to the internet. In such a case, only the first Elements Connector to which WithSecure endpoints are connecting can act in both the caching and ultimate proxy modes. The other Connectors in the chain function only in the ultimate proxy mode.

If you use Software Updater or cache malware definitions over HTTPS, make sure endpoint devices trust the TLS certificate that is used by the Elements Connector. You can do this using one of two methods:

- You can use proper, commercial certificates (the preferred option).
- You can use self-generated certificates that are automatically created during an Elements Connector installation.

5.1 Configure Elements Connector as a proxy using commercial certificates

Configures Elements Connector as a proxy using a commercial certificate.

To configure Elements Connector:

1. Purchase a commercial certificate or generate a company-issued one for a server running Elements Connector to set up TLS.
2. Create a PKCS#12 archive to bundle a private key with its certificate. For example, with the OpenSSL tool this command may look like the following:

```
openssl pkcs12 -export -in certificate.crt -inkey private.key -out server.p12 -name server -passout
pass:p12password
```

NOTE: In case you have a long list of intermediate certificates, might be useful to include the whole chain to the PKCS#12 archive's source certificate. The command may look like the following: `cat tls.crt ca_intermediate.crt ca_root.crt > certificate.crt`

3. Import the PKCS#12 archive to the Connector keystore to replace the existing certificate by running the following command:
   - On Windows:

```
"<Program Files>\WithSecure\ElementsConnector\jre\bin\keytool.exe" -importkeystore -destkeystore
"<ProgramData>\WithSecure\NS\ElementsConnector\data\fspms.jks" -deststorepass superPASSWORD -destalias
 fspms -destkeypass superPASSWORD -srckeystore server.p12 -srcstoretype PKCS12 -srcstorepass
p12password -srcalias server
```

   - On Linux:

```
/opt/f-secure/fspms/jre/bin/keytool -importkeystore -destkeystore /var/opt/f-secure/fspms/data/
fspms.jks -deststorepass superPASSWORD -destalias fspms -destkeypass superPASSWORD -srckeystore
server.p12 -srcstoretype PKCS12 -srcstorepass p12password -srcalias server
```

4. After importing the certificate, restart the Connector service.

5.2 Configure Elements Connector as a proxy using self-generated certificates

Configures Elements Connector as a proxy using a self-generated certificate.

To configure Elements Connector:

1. Export the certificate from the Connector key store by running the following command:
   - On Windows:

```
"<Program Files>\WithSecure\ElementsConnector\jre\bin\keytool.exe" -keystore
"<ProgramData>\WithSecure\NS\ElementsConnector\data\fspms-ca.jks" -alias fspm-ca -exportcert -file
 connector-ca.crt -rfc -protected
```

   - On Linux:

```
/opt/f-secure/fspms/jre/bin/keytool -keystore /var/opt/f-secure/fspms/data/fspms-ca.jks -alias fspm-
ca -exportcert -file connector-ca.crt -rfc -protected
```

2. Add the exported `connector-ca.crt` certificate as trusted for the endpoint computers.

NOTE: For example, on Windows, the `connetor-ca.crt` certificate must be installed to the following location: `Local Machine > Trusted Root Certificate Authorities`.

5.2.1 Override properties for the self-generated certificates

If Elements Connector cannot properly resolve its own DNS address automatically, that is, if external DNS records differ from the hostnames, you can use Java system properties to explicitly set custom certificate properties.

You can use the following properties:

- `certAdditionalDns` to specify a comma-separated list of additional DNS values for the subject's alternative names
- `certAdditionalIp` to specify a comma-separated list of additional IP addresses for the subject's alternative names
- `certForceSubject` to override the TLS certificate. The subject must contain a comma-separated list of all values that are required to generate the subject.

To start using Java system properties with Elements Connector:

On Windows

1. To specify the Java system properties via the Windows registry, do the following:
   a) Run Regedit as an administrator.
   b) Create the following string registry key: `HKEY_LOCAL_MACHINE\SOFTWARE\WithSecure\ElementsConnector\additional_java_args`
   c) Specify the Java system properties in the following format:

   ```
   -DpropertyName=value
   ```

   If you want to specify multiple properties, use space as the delimiter. Property names and values are case-sensitive. For example:

   ```
   -DcertAdditionalDns="pmserver.mydomain.pro, pmserver.myanotherdomain.com" -DcertAdditionalIp="127.
   0.0.1, 127.0.0.2"
   ```

   d) Restart the WithSecure Elements Connector service (fsconnector) for the new configuration settings to take effect.

On Linux:

2. The above instructions work also for Linux. However, instead of the registry, use the following configuration file: `/etc/opt/f-secure/fspms/fspms.conf`:
   a) Use a line with the following parameter: `additional_java_args`.
   b) Specify the Java system properties with the value in quotes in the following format:

   ```
   -DpropertyName=value
   ```

   If you want to specify multiple properties, use space as the delimiter. Property names and values are case-sensitive. For example:

   ```
   -DcertAdditionalDns="pmserver.mydomain.pro, pmserver.myanotherdomain.com" -DcertAdditionalIp="127.
   0.0.1, 127.0.0.2"
   ```

   c) Restart the WithSecure Elements Connector service (fsconnector) to make the new configuration settings take effect.

3. To force certificate renewal, do the following:
   a) Stop the Elements Connector service.
   b) Depending on which operating system you have, remove one of the following:
      - `c:\ProgramData\WithSecure\NS\ElementsConnector\data\fspms.jks`
      - `/var/opt/f-secure/fspms/data/fspms.jks`
   c) Start the Elements Connector service.

   The certificate is created when the service starts next time.

5.3 Changing the default port values on Elements Connector

By default, Elements Connector uses ports 80 and 443 to proxy the traffic. You can set the **HttpPortNum** and **HttpsPortNum** values in the Windows registry.

Elements Connector proxies client traffic through port 80 for HTTP and port 443 for HTTPS by default. If another service on the host already uses these ports, or if your network policy requires different ports, change the **HttpPortNum** and **HttpsPortNum** values in the **Windows Registry**.

The new port values take effect only after you restart the Elements Connector service.

5.3.1 Change the default port value in Windows

Changes the default port values on Elements Connector in Windows.

You need to have Elements Connector installed before changing the HTTP and HTTPS port values.

To change the default port values:

1. Open **Windows Registry Editor** by entering `regedit` in the search bar.
2. From the results, select **Registry Editor**.
3. Go to `Computer\HKEY_LOCAL_MACHINE\SOFTWARE\WithSecure\ElementsConnector`
4. Select **HttpPortNum** and do the following:
   a) Change **Base** to **Decimal**.
   b) Enter the new HTTP port number
   c) Select **OK**.
5. Select **HttpsPortNum** and do the following:
   a) Change **Base** to **Decimal**.
   b) Enter the new HTTPS port number.
   c) Select **OK**.
6. Open the command prompt as an administrator and run the following commands to start the service:

```
net stop wsconnector
```

```
net start wsconnector
```

After the service restarts, Elements Connector starts using the new ports.

Chapter 6

Configuring event forwarding

Topics:

- Configure API access for Elements Connector
- Configure event forwarding settings
- Verify event forwarding

Configuring event forwarding

WithSecure offers an adaptable solution for the partners who use security information and event management (SIEM) products to monitor managed environments.

You can deploy Elements Connector either on-premise or in the cloud. Use it as a security events forwarder that pulls data from the WithSecure cloud and forwards it to SIEM.

With Elements Connector, you can stream all security events from the WithSecure Elements Endpoint portal to your SIEM. Elements Connector supports Syslog, Common Event Format (CEF), and Log Event Extended Format (LEEF) message formats to stream data. This makes it a generic solution to integrate with almost any SIEM.

You can configure the forwarding feature for the whole partner scope, or limit it to a certain company, depending on the API key used.

To forward the event stream to SIEM, you must first enable access to the Endpoint Protection API and configure Elements Connector to use the API. You must create the API key using a dedicated company-level account so that it only retrieves events that are related to that company. If you use a dedicated partner-level account to create the key, the security events from all the partner-managed companies end up in the desired SIEM. Finally, you need to activate the forwarding feature and configure the destination SIEM in the WithSecure Elements Endpoint Protection portal under Profiles for Connector.

6.1 Configure API access for Elements Connector

When you have installed WithSecure Elements Connector, you have to configure some settings to make sure that the API access works.

After installing WithSecure Elements Connector, configure API access so the Connector can communicate with the Elements API.

1. Create Elements API credentials as follows:
   a) Log in as an EPP administrator to the Elements Security Center.
   b) Under **Management**, open the API client view .
   c) Change your scope to the organization for which you want to create a new pair of credentials.

   NOTE: If you are a partner and you want to create credentials for a company, you must change the scope to the organization for which you want to issue the credentials.

   d) Select **Add new**.
   e) Enter a description for the new client credentials.

   IMPORTANT: You cannot change the description after saving the credentials.

   f) After you have created a new pair of credentials, follow the instructions on the screen.

   NOTE: Remember to save the secret value in a safe place, because you will not be able to read that value again.

   g) Select the **I have copied and stored the secret** option and then select **Done**.
   The new item is shown in the list.
2. Create an `api-access.properties` file in the following folder:

- Windows: `<ProgramData>\WithSecure\NS\ElementsConnector\data`
- Linux: `/var/opt/f-secure/fspms/data`

3. Add the following key-value pairs to the file:

```
apiUrl = https://api.connect.withsecure.com
clientId = <api-client-id>
secret = <api-secret>
```

4. Save the file.
5. Restart WithSecure Elements Connector service as follows:
   - On Windows, restart WithSecure Elements Connector from the Services app.
   - On Linux, run the following command as the root user:

```
systemctl restart wsconnector
```

NOTE: After you turn on event forwarding in the profile settings, the `api-access.properties` file is deleted automatically. The API credentials are stored in an encrypted form in a secure storage.

6.2 Configure event forwarding settings

All the event forwarding settings are grouped under the Event forwarding section of a Elements Connector profile.

To configure event forwarding:

1. In the WithSecure Elements Endpoint Protection portal, go to the **Profiles** page and select **For Connector**.
2. Select the profile for which you want to set up event forwarding.
3. Select **Event forwarding**.
4. Turn **Enable event forwarding** on to allow forwarding security events to a SIEM system.
5. Enter an SIEM system address for the target system.

NOTE: An SIEM system address is a DNS or IP address of the SIEM server to ingest events followed by a port number.

NOTE: If the ports are omitted, the default values for the protocols are: 515 (TCP), 514 (UDP).

6. From the **Message format** drop-down menu, select one of the supported formats for the forwarded messages:
   - Common Event Format (CEF)
   - Log Event Extended Format (LEEF)
   - Syslog
7. From the **Protocol** drop-down menu, select one of the communication protocols that are used to connect to the SIEM:
   - TCP

- UDP
- TCP+TLS

> **IMPORTANT:** After you finish configuring the settings, check the log file to make sure that the Connector trusts the SIEM server certificate.

8. Select **Save and publish**.
   *The new profile now appears on the **For Connector** profile list.*

Once Elements Connector receives the updated profile, it starts polling security events from the WithSecure cloud and forwards those to the destination SIEM.

6.3 Verify event forwarding

Verify that Elements Connector is forwarding security events to your SIEM system after you configure event forwarding settings.

After you configure event forwarding settings, verify that Elements Connector is forwarding events to the SIEM system.

1. Confirm that the profile appears on the **For Connector** profile list.
2. On Windows, check the `fsconnector-forwarding.log` file in `<ProgramData>\WithSecure\NS\ElementsConnector\log` for entries about the events that Elements Connector forwarded.
3. Check the same log file to confirm that Elements Connector trusts the SIEM server certificate.

Once Elements Connector receives the updated profile, it starts polling security events from the WithSecure cloud and forwards those to the destination SIEM.

Chapter 7

Troubleshooting

Troubleshooting

Connector creates several log files that can help you to solve issues that you might have while using it.

On Windows, all Connector logs are stored in the `<ProgramData>\WithSecure\NS\ElementsConnector\log` folder.

- `fsconnector-forwarding.log` contains information about forwarded events,
- `upstream-request.log` collects all Connector requests to WithSecure Cloud.

On Linux, logs are stored in `/var/opt/f-secure/fspms/logs`.

Glossary

Access Control

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

Active Directory (AD)

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

Agent

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

Antivirus

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

Backdoor

An undocumented way of gaining access to a computer system.

Certificate

A certificate is a digital document used to prove the ownership of a public key, issued by a certificate authority (CA) to enable secure communication and authentication.

Certificate Authority (CA)

A Certificate Authority (CA) is a trusted entity that issues and manages digital certificates used for encrypting communications and verifying identities.

Cloud Service

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

Configuration Keys

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

Connector

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

Containment

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

Criticality

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

Custom Labels

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

Customer Company

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

Detection

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

Discovery Scan

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

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a security technology that continuously monitors

endpoints to detect, investigate, and respond to suspicious activity and advanced threats.

Endpoint Protection

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

Endpoint Protection API

API access for managing security policies and configurations within WithSecure Elements.

Entra ID

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

Event Forwarding

A process of transmitting security events from WithSecure Elements to SIEM systems.

Exposure Management

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

False Positive

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

Federated Single Sign-On (FSSO)

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

Group Policy (GPO)

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

IAM Role

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

Identity and Access Management (IAM)

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

Identity Management

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

Identity Provider (IdP)

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

Incident

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

Incident Response

Incident response is the organized process of detecting, containing, investigating, and recovering from a security incident to limit damage and restore normal operations.

Lateral Movement

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

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an open protocol for accessing and

managing directory information, such as users, groups, and devices, over a network.

Linux Authenticated Scanning

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

Malware

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

Malware Definition

A malware definition is a signature or pattern that antivirus software uses to identify known malicious files.

Mobile Device Management (MDM)

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

MSI Properties

Parameters used in command-line installation of software packages via Microsoft Installer (MSI).

Multi-Factor Authentication (MFA)

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

Patch Management

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

Phishing

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

Privacy

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

Profile Assignment

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

Proxy Mode

Proxy mode is an operating mode of the Elements Connector or Policy Manager proxy — such as caching, ultimate, forward, or reverse — that determines how it handles and routes traffic.

Quarantine

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

Remote Monitoring and Management Integration (RMM)

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

Role Assignment

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

Role-Based Access Control (RBAC)

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

Scan

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

Scan Node

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

Scan Templates

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

Scope Selector

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

Security Administrator

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

Security Administrator Role

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

Security Events

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

Security Group

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

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.

Service Partner

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

Severity

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

Software Updater

A feature that scans and reports missing updates for third-party software and deploys security updates.

Solution Provider

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

Subscription Key

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

Tenant

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

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.

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.

Index

A

access management 15–16
access rights 4, 9, 16, 18
account 26
account creation 17
account details 19
account levels 14
account linking 24
Active Directory 34
AD groups 34
adding devices 27, 29, 32
administrator account 4–5, 9, 16–17
Agent for Computers 28
Agent for Servers 28
Agent for Windows 35
API access 52
API client 18
asset groups 32
audit logs entry 9
authenticator app 7
Authenticator applications with Time-Based One-Time Password (TOTP) 7
automatic deletion 30, 33

B

backup 36
biometric authentication 8
Business Account 5

C

change name 19
change subscription 23
command-line parameters 41
commercial certificate 47
company level 32
Company level 33
Connector Ultimate 38
custom labels 31
customer company 9, 20–21

D

dark mode 19
data recovery 36
delete API client 18
deployment 40
device assignment 32
device biometrics 8
Device biometrics 7
device commands 33
device filters 34
device grouping 31–32
device invitations 31
device labels 31
Device list 31
device management 27, 30–34
device view 32, 34
devices 23, 33
Devices page 32
Devices view 34
diagnostic data 35
domain federation 25
downloading software 29
Downloads page 29

E

edit administrator 17
edit profile 19
EDR 23, 29
EDR and EPP for Computers 23
EDR and EPP for Computers Premium 23
EDR and EPP for Servers 23
EDR and EPP for Servers Premium 23
EDR for Computers 23, 29
Elements API 18
Elements Connector 54
email address 24
email aliases 25
email invitation 29, 31
Endpoint 41–42, 52
endpoint computer 47
EPP for Computers 23, 33–34
EPP for Computers Premium 23
EPP for Servers 23, 33–34
EPP for Servers Premium 23
EPP subscription 23
event forwarding 38, 52–54
existing customer company 21

F

federated domain 6, 26–27
federated single sign-on 24–25
fingerprint 8
forgot password 19
FSSO 24

I

IAM administrator 14–16
IAM role 9, 14–16
Identity and Access Management 14
identity provider 24
installation 40–43
installation link 29, 31
installation package 28–29
internet access 47

J

Java system properties 48

L

label assignment 31
light mode 19
Linux 40, 42
Linux dependencies 43
log file 56

logging in 5
login 6, 19
login credentials 5–6
login security 6

M

managed companies 14
MFA 6–8
MFA methods 7
Microsoft Entra Admin Center 24
Microsoft Entra ID 6, 24–26
Mobile Protection 27–28, 33, 35
MSI package 41
MSI properties 41
multi-factor authentication 5–8
My settings 8, 19

N

new customer company 22
non-federated domain 6

O

offline devices 30, 33
on-premise product 38
ordering products 21–22
Organization Settings 16–18, 32

P

partner 16–17, 52
Partner Portal 20–22
password recovery 19
patch management 4
pending invitations 31
permissions 9
Phone number for Short Message Service (SMS) messages with One-Time Passwords (OTP) 7
Policy Manager Proxy 38
port number 50
portal 45, 52
Premium subscription 23
product deployment 20
profile 45, 53
profile assignment 34
profile assignment rules 32
proxy 38, 47–48, 50
Push notifications with Auth0 Guardian authenticator 7

Q

quick start 5

R

remote device management 33
remote request 35
remove administrator 17
removing federation 27
removing MFA 8
reset password 19
role 9
role assignment 9
role permissions 15

S

scope selector 4, 14, 16, 21–22, 29, 32–33
Secure USB keys 7
security administrator 9, 16
Security Administrators 17
Security Center 4–9, 14, 16, 19–22, 24–25, 27, 29–35, 38
security roles 14
self-generated certificate 48
service 36
service partner account 17
SIEM 52
single sign-on 6, 25, 27
Smartphones or other devices 7
software distribution 28
software installation 29
Solution Provider 14, 20–21
subscription 5, 20–22, 27, 30
subscription assignment 21
subscription key 20–23, 28
subscription upgrade 23
subscriptions 20, 22
Subscriptions view 22
support 35
supported platform 40
system requirements 40

T

table columns 34
troubleshooting 56
two-factor authentication 6

U

upgrading options 23
user identity linking 26
user management 9
user name 19

V

view mode 19
Vulnerabilities role 9
vulnerability management 4
Vulnerability Management: 15

W

Windows 40–41, 50
Windows registry 50
WithSecure 4–6, 14–16, 20, 35, 38, 47
WSDIAG file 35