Elements Connector

Getting Started Guide

Contents

Chapter 1

Introduction to the WithSecure Elements solution

Topics:

This page gives you an overview of the WithSecure Elements solution.

WithSecure Elements in a nutshell

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

The WithSecure Elements offering

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

To highlight some of the main benefits:

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

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

Supported languages

Language support has been streamlined across all of the Elements touchpoints. This means that all Elements products and related support and documentation will offer the same set of languages as follows:

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

WithSecure Elements training

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

Accessing the WithSecure Elements Security Center

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

1.1 Using WithSecure Elements Security Center

This chapter provides basic information that is useful in everyday use of WithSecure Elements Security Center.

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 Logging in

This section gives you instructions on how to log into the WithSecure Elements Security Center.

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.

Logging in to non-federated domains

Instructions on how to log in to non-federated domains.

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

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

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

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

Logging in to federated domains

Instructions on how to log in to federated domains.

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

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

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

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

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

Multi-factor authentication

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

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

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

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

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

MFA methods

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

The methods include the following:

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

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

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

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

Choosing multi-factor authentication

Instructions on how to choose one or more multi-factor authentication methods.

Note: Before choosing your 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.

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.

Once you have taken MFA into use, the next time you log in, the system suggests that you simplify your login process by taking device biometrics into use. You can choose to take them into use, not to do so in a given device, or postpone the process by selecting the Remind me later option. If you choose to simplify your login flow with biometrics in a given device, during your login process, the second factor validation can be done by using, for example, your fingerprint.

Removing a multi-factor authentication

Instructions on how to remove multi-factor authentication (MFA),

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.

1.1.2 User management

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

About access rights

You can limit the access rights so that the selected type of information can be shown but not edited.

Elements Security Center has the following access rights:

Role	Description	Visible in Audit logs in Elements Security Center as
Identity and Access Management (IAM) - Full editing	Elements Identity and Access Management (IAM) role on page 10	

Role	Description	Visible in Audit logs in Elements Security Center as
Exposure Management - Exposure - Full editing	Allows access to the following Exposure Management features: • Environment: Devices, Cloud, Network, Exposure, Identities • Security configurations • Reports • Management Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by an IAM role)	cspm:admin
Exposure Management - Vulnerabilities -Management	Allows full access to the Vulnerability Management views, settings, and findings Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)	vm:administrator
Exposure Management - Vulnerabilities - Team memebr	Allows access to the Vulnerability Management views, settings, and findings, with no permission for managing users and the system	vm:team_member
Exposure Management - Vulnerabilities - Read-only	View-only access with no permssion for managing users	vm:readonly_team_member
Collaboration Protection - Administrator	Allows the administrator to access the Collaboration Protection views and edit the following protection features: • Handling detections • Managing Exchange and shared files settings • Managing policies, quarantining files, and generating repots	cpo365:admin
Collaboration Protection - Read-only	Grants view-only access to the Collaboration Protection views	cpo:readonly
Collaboration Protection - Quarantine manager	Allows access to the Collaboration Protection views that are related to detections and quarantining files	cpo365:quarantine_mgr

Role	Description	Visible in Audit logs in Elements Security Center as
Collaboration Protection Management - Administrator	Allows the administrator to access management features, including user creation, role management, subscription details, and organization settings Security Administrators can create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)	fusion_admin
Endpoint Protection computers and mobiles - Full administrator	Allows the administrator to access the following features: • Security settings (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 • Installers The Security Administrator role, along with the "Servers - Full administrator" role is required to create additional administrators and assign this role to users within the same organization (will be replaced by the IAM role)	epp:manage_computers_mobiles_only or epp:manage_all
Endpoint Protection computers and mobiles - Read-only	View-only access with no permission to perform operations or manage other users and profiles	epp:manage_servers_only or epp:readonly

Role	Description	Visible in Audit logs in Elements Security Center as
Endpoint Protection Servers - Full administrator	Allows the administrator to access the following features: • Security settings (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 • Installers The Security Administrator role, along with the "Computers and mobiles - Full administrator" role is required to create additional administrators and assign this role to users within the same organization (will be replaced by Ihe IAM role)	epp:manage_servers_only or epp_manage_all
Endpoint Protection Servers - Read-only	View-only access with no permission to perform operations or manage other users and profiles	epp:manage_computers_mobiles_only epp:readonly

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

Moving between the managed companies

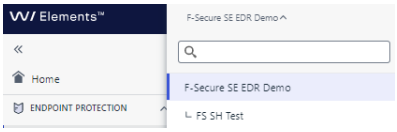
Use the ***scope selector*** to broaden or narrow the scope of information displayed in WithSecure Elements Security Center.

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 functionalities, capabilities, and services. The IAM role simplifies the previously complex process of assigning roles across different capabilities.

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. Consequently, 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, thereby gaining 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 functionalities 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

This topic answers the most frequently asked questions about IAM roles.

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 adinistrator 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 oher Endpoint Protection administrator users?	Yes, for time being, this is still possible. In the future, all user management action rights will be restricted to IAM role holders only.
Can one organization have multiple IAM administrator users?	Yes, there is no limit to the number of IAM administrators that an organization can have.
Why are the Claim and Decline options not displayed for some administrator users?	In the first stage, the IAM Claim button is shown to users who have full administrator rights on all products for which the organization has subscriptions. For example, if a company has subscriptions for Elements Endpoint Protection and Collaboration Protection, the IAM Claim button is shown to users with full administrator roles on both products.

How can I find out who in my organization has claimed an IAM role?	The IAM role is shown, and users with the role can be filtered in a table under **Management** > **Security Administrators**.

Adding 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 admin**.
5. In the **Add administrator** screen, fill in the administrator details as follows:
   - 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.
   - 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.

Adding a new service partner

To create a service partner account:

1. Under **Management**, select **Organization Settings** on the sidebar.
   The **Organization Settings** page is displayed.
2. Select the **Endpoint Protection Accounts** tab.
   The **Accounts** page opens.
3. Select ··· next to **Accounts**, and then select **Create new service partner account**.
   The **Create service partner** page opens.
4. Enter a name for the new service partner account, and select **Create**.
   The service partner account was created.
5. Select **Submit**.

A new service partner administrator account is created.

Editing or removing administrators

You can edit or remove administrators accounts.

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 thatyou 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.

Recovering 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.

1.1.3 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 there is a need for an administrator who would manage the subscriptions and devices in the new customer company, you need to create an administrator account through Elements Security Center.

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

Once the purchase order for the new customer has been successfully added from your Partner Portal account, it will be automatically added as a new customer 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.

Assigning 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. In 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.

Ordering products for a customer company

You can order WithSecure Elements products for a customer company via WithSecure Partner Portal.

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

To order WithSecure Elements products via WithSecure Partner Portal:

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

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

   The **eOrdering** page is displayed.
2. To order products for an existing customer company:
   a) On the main page, select **My Customers**, and then select the name of the customer company for which you are ordering products.
   b) In the **Order** column, select either **New SaaS Order** or **New Yearly Order**.
   The Welcome to Ordering window opens.
   c) Under **New Order**, enter a reference number for your order.
   d) Under **Order Products**, select **Add Products**.
   e) 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.
3. To order products for new customer company:
   a) On the main page, select **New Order**.
   b) Enter the name of the new customer company and select **Add New**.

The **New Customer** window opens.

c) Fill in the customer details and select **Save**.
d) Under **New Order**, enter a reference number for your order.
e) Under **Order Products**, select **Add Products**.
f) 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.

Viewing available product subscriptions

To view the available subscriptions:

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

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

2. You can use filtering to find the following:

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

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

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

Changing the subscription key

Instructions on how to change the subscription key through WithSecure Elements Security Center.

To change the subscription key:

Note: This feature is currently available for partner accounts and for company accounts when you want to change a subscription from the WithSecure Elements EPP for Computers, WithSecure Elements EPP for Computers Premium, WithSecure Elements EPP for Servers or WithSecure Elements EPP for Servers Premium software to the WithSecure Elements EDR and EPP for Computers, WithSecure Elements EDR and EPP for Computers Premium, or WithSecure Elements EDR and EPP for Servers Premium software.

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

This chapter explains how you can upgrade your subscriptions and what the upgrading options are.

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.

1.1.4 Federated single sign-on

This section explains federated single sign-on and provides instructions on how to set it up.

Federated single sign-on (FSSO) is a mechanism that allows users to authenticate and access several applications or services across different domains or organizations without the need to log in separately for each. When users log in, they submit their credentials (such as username and password) to an identity provider who then verifies these credentials. After successful authentication, the identity provider generates a digitally-signed token that serves as proof of the user's identity. When the users accesses other applications or services that are located in different domains or organizations, their browser automatically uses this token. The cloud identity service validates the token and grants access without requiring the user to log in again.

FSSO simplifies access across various systems by allowing users to authenticate once and move seamlessly between different applications or services. It enhances security and user experience by eliminating the need for multiple logins. Furthermore, when a user is removed from an identity provider, they automatically lose the ability to log in to Elements Security Center, which makes managing user access easier and more secure.

Prerequisites

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

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

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

Before implementing single sign-on (SSO)

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

Why is plus addressing problematic?

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

Important:

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

How to avoid users losing access to remove federation?

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

How does SSO change the login process?

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

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

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

Global impact of SSO

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

Hierarchy-level considerations

Make sure to generate SSO from the approrpiate 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.

Setting up federated single sign-on with Microsoft Entra ID

Instructions on how to set up Microsoft Entra ID federated single sign-on.

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.

1. Log in to https://elements.withsecure.com.
2. Under **Management** > **Organization Settings**, select **SSO Access Federation**.
   The **Single sign-on access federation** 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 SSO Federation**.
   After you have federated the domain, its status changes to **The SSO Federation is enabled for [domain name]**.

Linking user identities

Instructions on how to link user identities in Elements Security Center.

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 previously

To link identities:

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

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

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

Removing federation from a domain

Instructions on how to remove single sign-on federation from a domain.

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

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

Note: When federation is removed from a domain, users that have email address in that domain must use their Elements credentials to log in. However, if an Elements account was created after the domain was

federated, users have not received an email with their initial password and do not know their Elements credentials. In that case, they must reset their password.

To remove federation:

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

1.1.5 Enhancing device management with custom labels

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

Adding lables 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.

Related concepts

MSI properties

Related tasks

Adding device labels on page 19
You can add device labels in three different ways.

Adding device labels

You can add device labels in three different ways.

- Manually in the **Device** view:
  - The **Device list** view
    1. On the **Device list** view, select the devices to which you want to assign a label.
    2. On the **Actions** panel at the bottom of the page, select **Manage labels** > **Add labels**, and then select an existing label or add a new one.
    3. Select **Add** to assign the label to the selected devices.
  - The **Devices details** view
    1. In the **Actions** panel, select **Manage labels** > **Add labels**, and then select an existing label or add a new one.
    2. Select **Add** to assign the label to the selected devices.
- Using the rules in the **Profiles** section:
  1. In Elements Security Center, navigate to **Security Configurations** > **Profiles** > **Profile assignment rules**.
  2. In the **Outbreak rules** and **Profile assignment rules** sections, for each rule, you have an option to add labels when the rules match
- During the Elements agent installation process:
  - Review step 2 in the Assigning a default profile and installation tags section for more details.

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

1.1.6 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 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, malware definition updates, 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, which 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 simplifying firewall configurations and allowing the use of WithSecure products in semi-closed environments.
- For companies that use security monitoring services such as Splunk, Elements Connector provides security events forwarding 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:

Instructions on how to deploy the product.

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 2008 R2 with latest SP1; Standard, Enterprise or Web Server editions
- Windows Server 2012; Essentials, Standard or Datacenter editions
- Windows Server 2012 R2; Essentials, Standard or Datacenter editions
- 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 10
- Windows 11

System requirements for Linux:

One of the following 64-bit Linux platforms:

- Alma Linux 8
- CentOS 7, 8
- Debian 9, 10, 11, 12
- openSUSE Leap 15
- Oracle Linux
- Red Hat Enterprise Linux 6, 7, 8
- Rocky Linux 8
- SuSE Linux Enterprise Server 11, 12, 15
- SuSE Linux Enterprise Desktop 11, 12, 15
- Ubuntu 16.04, 18.04, 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: 10 GB of free disk space
- Network: 100 Mbit network

3.2 Installing Elements Connector on Windows

Follow these instructions to install 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.

Related concepts

Configuring event forwarding on page 32

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.

MSI property	Explanation
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 Installing Elements Connector on Linux

Follow these instructions to install 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: https://www.suse.com/releasenotes/x86_64/SUSE-SLES/11-SP4).

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:

- Both 32-bit and 64-bit versions of the `libstdc++` library must be installed prior to installing Elements Connector. Use Multiarch capabilities (https://wiki.debian.org/Multiarch/HOWTO) to install the 32-bit library onto 64-bit platforms.
- Install the `libstdc++6` and `libstdc++6:i386` packages before installing Elements Connector. If installation was not completed because the compatibility library was not found, install the library and then use the `apt-get install -f` command to complete installing the product.

Chapter
4

Managing Elements Connector via the portal

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:

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 are using the Software Updater feature, you need to make endpoint computers trust the TLS server certificate of the Elements Connector by using one of the two options:

- 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 Configuring Elements Connector as a proxy using commercial certificates

Instructions on how to configure 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 Configuring Elements Connector as a proxy using self-generated certificates

Instructions on how to configure 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 Overriding 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.

5.3.1 Changing the default port value in Windows

Instructions on how to change 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:

WithSecure offers an easily-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 and use it to serve as a security events forwarder that pulls data from the WithSecure cloud and forwards it to SIEM. For an Microsoft Sentinel integration, Elements Connector is available in the Azure Marketplace:https://azuremarketplace.microsoft.com/en-us/marketplace/apps/withsecurecorporation.sentinel-solution-withsecure-via-connector.

Note: For more information on how to configure Elements Connector to be used with Microsoft Sentinel, see https://learn.microsoft.com/en-us/azure/sentinel/data-connectors/withsecure-elements-via-connector.

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, which makes it a generic solution to integrate seamlessly with almost any SIEM.

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

To get the event stream forwarded to SIEM, you first have to make sure to 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 Configuring 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.

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>
```

   Note: The user account should be the same as the one that you specified while generating the API credentials.
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:

```
#/etc/init.d/fsconnector restart
```

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 Configuring 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.

Chapter
7

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`.