



WithSecure Elements Identity Security for Entra ID

Contents

Chapter 1: WithSecure Elements XDR Cloud Security for Azure overview.....	4
1.1 Getting started.....	5
1.2 Using WithSecure Elements Detection and Response features.....	6
1.3 Deployed infrastructure overview.....	7
1.4 How Identity Security and Cloud Security work.....	10
1.5 Prerequisites.....	11
Chapter 2: Onboarding configuration.....	12
2.1 Add an Azure tenant.....	13
2.2 Connect Identity Inventory.....	13
2.3 Add a security capability.....	14
2.4 Prepare the Azure environment	14
2.5 Deploy resources.....	16
2.6 Post-deployment verifications.....	16
2.7 Connect Azure to Elements Cloud.....	20
2.8 Check that the detection capability works.....	21
2.9 Finish the onboarding.....	21
2.10 Configure email reports.....	21
2.11 Create a custom view for security events.....	22
Chapter 3: Ongoing management.....	23
3.1 When to rerun the script.....	24
3.2 When a new tenant is created.....	24
3.3 Verify event hub capacity.....	24
3.4 Regular release of the script.....	25
3.5 The Detection module overview.....	25
3.6 Update notification recipients.....	25
Appendix A: Offboard the deployed resources.....	26
Appendix B: Troubleshooting.....	29
B.1 Check the connection status.....	30
Appendix C: Introduction to the WithSecure Elements solution.....	31
C.1 Using WithSecure Elements Security Center.....	32

Glossary.....	65
Index.....	70

Chapter 1

WithSecure Elements XDR Cloud Security for Azure overview

Topics:

- Get started with WithSecure Elements Identity Security
- Using WithSecure Elements Detection and Response features
- Deployed infrastructure overview
- How Identity Security and Cloud Security work
- Prerequisites

WithSecure Elements XDR Cloud Security for Azure overview

Configuration required to provide access for WithSecure to retrieve Entra ID and Azure logs from your Microsoft Tenant.

WithSecure Elements Identity Security for Entra ID is a foundational module that is designed for organizations that use Entra ID for identity and access management of Users, Services, and Resources within the Microsoft Cloud ecosystem.

WithSecure™ Elements XDR Cloud Security for Azure is an additional module for organizations that build, deploy, and manage their own applications and solutions in Microsoft Cloud.

- Time and distance between sign-ins (to detect impossible travel)
- Access to suspicious applications or email clients



NOTE:

-
-
-

1.1 Get started with WithSecure Elements Identity Security

Gets started with WithSecure Elements Identity Security by onboarding your Azure tenant.

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

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

You also need to have Elements Endpoint Detection and Response configured.

This quick start guide walks you through getting started with WithSecure Elements Identity Security by onboarding your Azure tenant.

1. Login to Elements Security Center and start onboarding your Azure Tenant.



TIP: You can watch the onboarding video that covers the Elements and Azure deployment activities.

- a) Log in to the Elements Security Center, using the existing credentials you have for Elements Endpoint Detection and Response.
- b) After confirming you have a subscription to Elements XDR Cloud Security for Azure, navigate to **Environment > Cloud > Microsoft Tenants and Azure Subscriptions** to add a tenant.

2. Review the Deployed infrastructure and prerequisites.

For more information, see Prerequisites.

3. Add a Azure Tenant to Elements Security Center to start the onboarding.

For more information, see Onboarding configuration.

4. Prepare the Azure environment by ensuring you have the required permissions to run the onboarding script.

For more information, see Preparing the Azure environment.

5. Deploy the resources.

For more information, see Deploying resources.

6. Complete the post-deployment verification steps.

For more information, see Post-deployment verifications.

7. Return to the Elements Security Center and add the connection string to connect Elements Security Cloud to the Azure tenant.

Elements Cloud is receiving the data from the Azure tenant now.

8. Test that the detections are working.

For more information, see Checking that the detection capability works.

9. Close the onboarding session.

For more information, see Finishing onboarding.

Refer to Troubleshooting if you experience any issues and raise a ticket to Customer Care if your issue is still not resolved.



NOTE: There are no additional roles required to view Cloud Broad Context Detections (BCDs).

1.2 Using WithSecure Elements Detection and Response features

Using WithSecure Elements Detection and Response features with WithSecure Elements Identity Security requires endpoint sensors deployed on your endpoints.

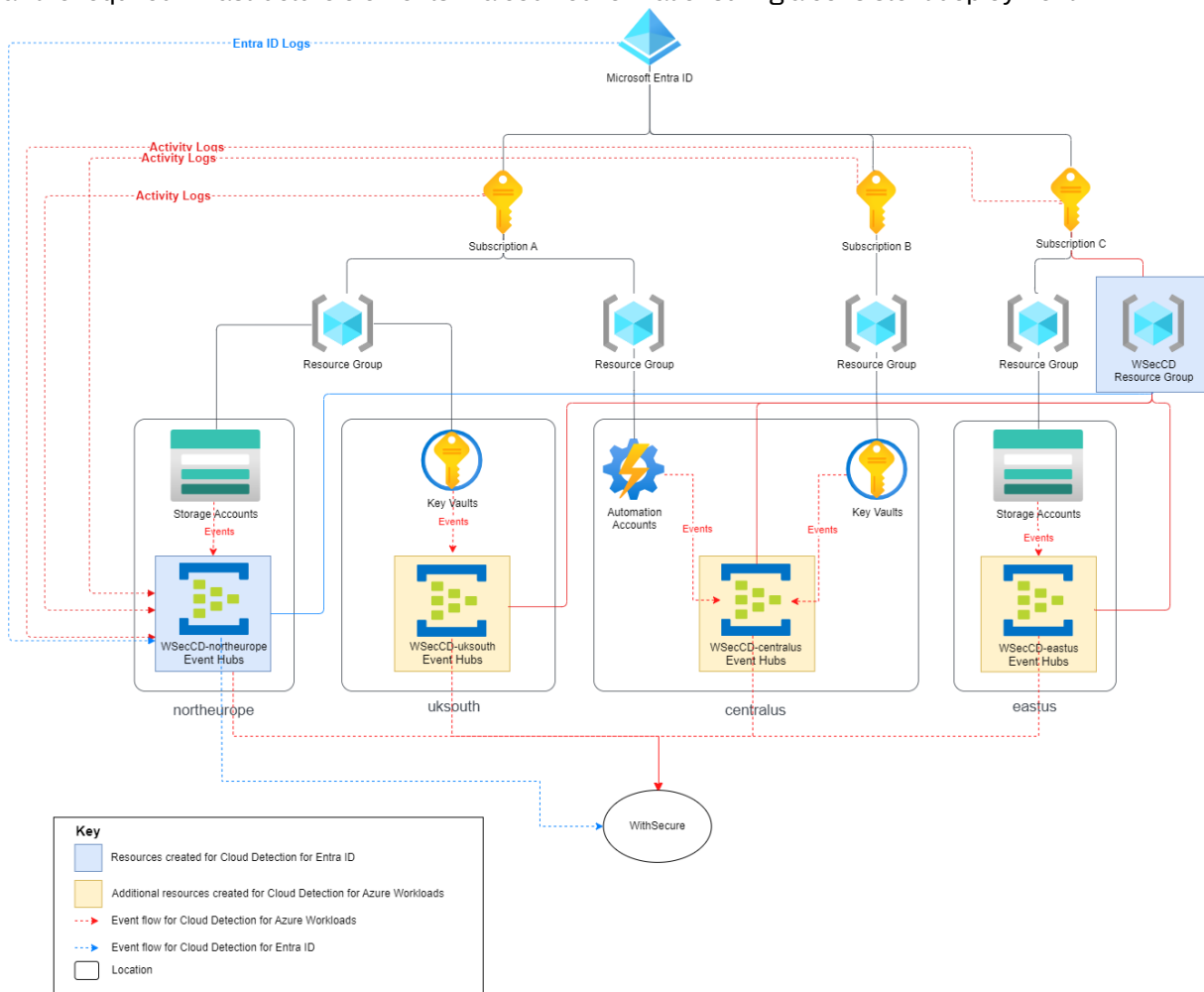
To use Elements Identity Security effectively, you must have Elements Detection and Response deployed on the endpoints.

Endpoint sensors are lightweight, discreet sensors, which are deployed on all relevant computers within your organization. These sensors collect behavioral data from endpoint devices and are specifically designed to withstand attacks from various attacks. When setting up WithSecure Elements Endpoint Detection and Response, you need the endpoint sensor installation package. The installation package consists of a binary installer file, and an WithSecure Elements Endpoint Detection and Response activation code.

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

1.3 Deployed infrastructure overview

You can use the Infrastructure as Code (IaC) template to deploy it in the environment. The template defines all the required infrastructure elements in a codified format ensuring a consistent deployment.



The diagram illustrates the effects of the template used during the onboarding process. In this example, all resources created are deployed into Subscription C.

The process creates, configures, and deploys the following infrastructure:

- A resource group is created in the target tenant that contains all the resources deployed by the WithSecure Entra ID configuration script (Event Hubs, alerts, action group) which are collectively used for WithSecure log data collection.
- A Standard Tier Event Hub is deployed for each region. The Event Hub is configured to retain telemetry events for 24 hours. The number of resources monitored and their activity impact the load on the Event Hub.



NOTE: To handle the load, the Event Hubs are configured with the "Auto-Inflate" feature turned on, with an upper limit of Throughput Units (TU) set to the maximum value (40). In practice, this means that the Event Hubs are deployed with the minimum capacity (1 TU), and additional TUs are deployed according to the load up to the maximum (40 TU).



NOTE: The number of TUs does not decrease automatically when the load decreases. The number of TUs affects the cost of the Event Hubs.

- An email alert to inform you when the Event Hub is not capable of handling the load if event hub reaches its maximum capacity. In this case, some telemetry data may be lost so an alert is deployed to bring visibility on the issue.



NOTE: An increase in the number of TUs will trigger the alert.

- Diagnostic settings that forward all Entra ID logs to an Event Hub are produced. These are:
 - Audit logs
 - Sign in logs
 - Non Interactive Users Sign In Logs
 - Service Principal Sign In Logs
 - Managed Identity Sign In Logs
 - Provisioning Logs
 - ADFS Sign In Logs
 - Risky Users
 - User Risk Events
 - Network Access Traffic Logs
 - Risky Service Principals
 - Service Principal Risk Events
 - Enriched Office365 Audit Logs
 - Microsoft Graph Activity Logs



NOTE: If your organization has a P1/P2 license (which is included in Microsoft 365 E3/E5 plans), the solution collects the risk reports that are generated by Microsoft and combines them with our complementary detection logic. The solution also provides detections for disabling Conditional Access, which is a feature that is exclusive to Azure Active Directory Premium P1 or P2 licenses, which are part of the E3 and E5 plans, respectively.

- The following diagnostic settings that forward the following Azure Activity logs to an Event Hub are produced:
 - Administrative
 - Security
 - Alert
 - Recommendation
 - Policy
 - Autoscale
 - Resource Health
 - Service Health
- Policies that produce diagnostic settings to forward Resource logs to an Event Hub are deployed, including Automation, Key Vault, and Storage.

The following table describes the use of the key log sources that are collected as part of the Entra ID and Azure modules.

Table 1: Log categories

Log Categories	Description
Audit logs	Required to monitor changes to applications, users, and tenant configuration changes. For example, changes in permissions of applications registrations, and new conditional access policy created/modified.
Sign in logs	Contains authentication and authorization events for the tenant. For example, sign-in events and metadata associated with a user log in.
Non Interactive Users Sign In Logs	Contains information relating the system activities where there is no human interaction. Service accounts can be targeted by attackers.
Service Principal Sign In Logs	Contains information relating the service principals activities where attackers can abuse Microsoft principals to achieve their goals.
Managed Identity Sign In Logs	Contains information relating to the interactions of applications, services or systems using managed identities. Monitoring managed identities can detect authorized access made by attackers.
Risky Users	Provides information about "risky users" and associated events deemed risky by M365 Defender. For example, suspicious logons, and malformed or suspicious token provided.
User Risk Events	
Risky ServicePrincipals	Provides information about "risky service principals" and associated events deemed risky by M365 Defender.
Service Principal Risk Events	
Administrative, Security, Alert, Recommendation, Policy, Autoscale, Resource Health, Service Health	By integrating these logs into your security monitoring and analysis processes, you can gain a comprehensive view of your environment's security posture and detect and respond to potential threats.
Automation, Key Vault and Storage	Contains information about automated processes, access and usage of secrets, keys, and certificates, and operations on storage accounts. Monitoring these logs helps ensure the security and proper functioning of automation tasks, sensitive information, and data storage.

Once the configuration has been completed, the data can be collected and analyzed by WithSecure to provide detection coverage.

For multiple tenants, follow the steps outlined in this guide for each tenant. WithSecure requires a connection string for each tenant's event hub. For example, you have to provide 3 unique connection strings for 3 tenants.



NOTE: This document refers to Azure documentation in many places to avoid duplicating content.

Associated Microsoft Costs

The deployed Event Hub configuration uses Standard Tier Event Hubs, optimized by provisioning one Event Hub per region and setting a 24-hour event retention period.

Event Hubs are billed at approximately EUR 22 per month per Throughput Unit (TU). The number of TUs required depends on the volume of incoming events. The system can scale up to 40 TUs, depending on the event load. In addition to TU charges, there is a data ingress fee of EUR 0.026 per million events received.

Example scenarios:

- Mid-sized customers typically generate around 100 million events per month and generally require no more than 1 TU. The estimated monthly cost is approximately EUR 25.
- Larger customers may generate around 300 million events per month, still typically within the capacity of 1 TU. The estimated monthly cost in this case is approximately EUR 30.

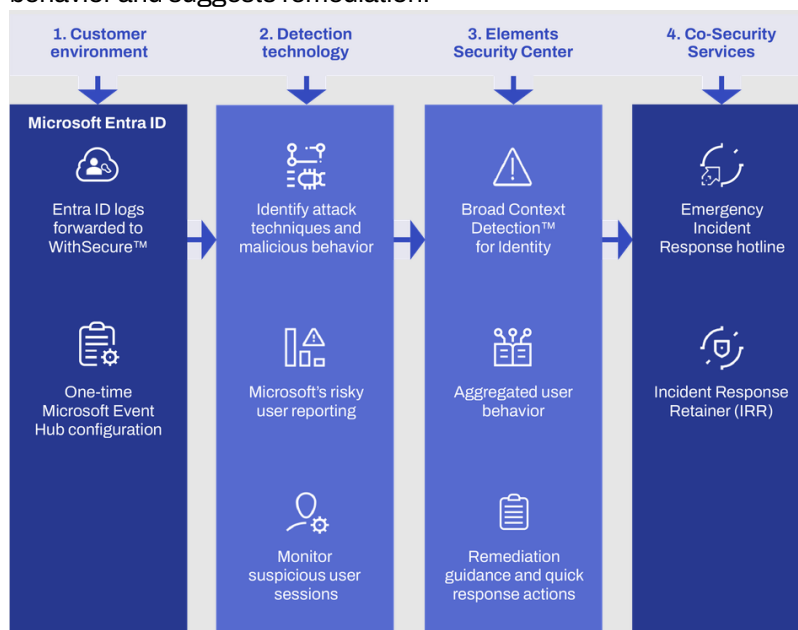


NOTE: During an external Distributed Denial of Service (DDoS) attack, the event volume may increase by 200 million and the events per second may rise tenfold. The monthly cost could then rise to approximately EUR 250.

To reduce unexpected costs, we recommend that you configure Azure cost and billing alerts. These alerts help you scale down TUs promptly after such incidents.

1.4 How Identity Security and Cloud Security work

and WithSecure Elements XDR Cloud Security for Azure send logs to WithSecure. The service detects suspicious behavior and potential threats, while WithSecure Elements Security Center analyzes user behavior and suggests remediation.



A one-time Microsoft Event Hub configuration sends Microsoft Entra ID logs to WithSecure during onboarding. WithSecure uses the logs to identify attack techniques, detect malicious behavior, and flag possibly compromised accounts. It also monitors suspicious user sessions for unusual activity.

WithSecure Elements Identity Security and Cloud Security combines user behavior to assess identity and cloud threats as Broad Context Detections. It also provides remediation guidance and response actions.

Incident Response Retainer helps you prepare for and respond to security incidents. The Emergency Incident Response hotline provides immediate support during an incident.

1.5 Prerequisites

The following prerequisites must be met before configuration starts.

- The organization must have subscriptions to WithSecure Elements Endpoint Protection and WithSecure Elements Endpoint Detection and Response. You must have the WithSecure Elements Endpoint Protection administrator role during onboarding. You must have the WithSecure Elements Identity Security for Entra ID.
- You must be able to sign in as a Global Administrator on the Azure account to run the script in Azure Cloud Shell.
- You must have your tenant ID, subscription ID, and deployment location known and ready before you start the deployment. For instructions, see [Get subscription and tenant IDs in the Azure portal](#).
- The subscription must be assigned to an Azure Management Group. To set up an Azure Management Group, see [Create a management group](#).

Chapter 2

Onboarding configuration

Topics:

- Add an Azure tenant
- Connect Identity Inventory
- Add a security capability to an Azure tenant
- Prepare the Azure environment
- Deploy resources
- Post-deployment verifications
- Connect Azure to Elements Cloud
- Check that the detection capability works
- Finish the onboarding
- Configure email reports
- Create a custom view for security events

Onboarding configuration

Steps to onboard your cloud environment so WithSecure can start collecting Azure log data.

To start collecting Azure log data in Identity Security, you onboard your cloud environment. Onboarding covers adding your cloud subscription, preparing the environment, deploying the required resources, verifying the deployment, connecting to Elements, and configuring email notifications.

For a step-by-step walkthrough of onboarding WithSecure XDR for Entra ID and XDR Cloud for Azure, see the XDR Cloud for Azure onboarding video.

2.1 Add an Azure tenant

Add a new Azure tenant to WithSecure Elements Security Center.

To add a new Azure tenant:

1. In WithSecure Elements Security Center, go to **Environment > Cloud > Microsoft Tenants and Azure Subscriptions**.
2. Select **Add Azure tenant**.
3. On the **Tenant information** page, enter the following details and select **Next**:
 - **Display name**: enter the name of the new Azure tenant as it will appear in WithSecure Elements Security Center.
 - **Tenant ID**: paste the tenant ID from the Azure portal.
 - **Organization**: select the WithSecure Elements Security Center organization for the tenant.
4. On the next page, enter the following and select **Next**:
 - **Importance**: set the importance of the cloud account. The importance is used in risk evaluations.
 - **Business context**: provide the business context for the tenant.

The tenant is added and the Connect Identity Inventory capability page opens.



IMPORTANT: You must configure Identity Inventory before you add any other capabilities. See Connecting Identity Inventory.

2.2 Connect Identity Inventory

Connect Identity Inventory for an Azure tenant.



NOTE: For information on how to create a tenant, see Add an Azure tenant on page 13.



IMPORTANT: You must configure Identity Inventory before you add any other capabilities to the tenant.

To connect Identity Inventory:

1. Under **Security capabilities**, select **Identity Inventory**.
2. Select **Connect now**.
3. Read the introduction and instructions, select the checkbox to confirm, and select **Start**.
4. Grant the required permissions for the Identity Inventory capability.

- If you are the Azure tenant administrator, select **Accept Permissions**, then approve the required permissions.
- If you cannot grant permissions, select **Copy URL** to copy the URL and send it to your Azure administrator.

Identity Inventory is connected and its required permissions are granted.

2.3 Add a security capability to an Azure tenant

Add a security capability to an Azure tenant in WithSecure Elements Security Center.

Before you add a security capability, add the Azure tenant. See [Adding an Azure tenant](#).



IMPORTANT: Identity Inventory is mandatory. You must connect it before you add any other capability. See [Connecting Identity Inventory](#).

After you add the tenant and connect Identity Inventory, add the security capability to the tenant:

1. Under **Security capabilities**, select **Identity and Azure Detection**.
2. Select **Add**.
3. Enter the following information in the **Connection details** page.
 - **Deployment Subscription ID:** Paste the subscription ID from the Azure portal that the new resources will be created within. We recommend that if you do not use subscriptions already, you create a new subscription. For instructions, see [Create an EA subscription to create an Enterprise Agreement subscription](#).
 - **Deployment location:** Select the region where the new resources will be created. We recommend that you choose a location that you already use.
 - **Email address for notification:** Enter the address where Microsoft sends notifications if the Event Hub reaches its capacity.



NOTE: After typing the email address, save it by pressing Enter.

4. Download the onboarding WithSecure Elements XDR Identity Security for Entra ID.zip file.

The security capability is added and the onboarding package is downloaded.

Next, configure the infrastructure in Azure.

2.4 Prepare the Azure environment

Prepares your Azure tenant with the elevated permissions and onboarding files that the configuration script needs.

Before you begin, make sure you are signed in with a role that can use Azure's **Elevate access** feature (typically the Global Administrator role in Microsoft Entra ID), and that you have already downloaded the onboarding package for this integration.

This prepares your Azure tenant with the elevated permissions and onboarding files that the WithSecure Identity Security configuration script needs, before you run it in a later step.

1. In the Azure Portal, temporarily elevate your access to manage the tenant.

Use the instructions provided on the following page to temporarily elevate access to manage all subscriptions: [Elevate access to manage all Azure subscriptions and management groups | Microsoft Learn](#).

2. Sign out.
3. Sign back in to refresh your access with elevated access rights.
4. Switch the **Access Management for Azure resources** option to **Yes**.

The screenshot shows the Microsoft Entra ID Default Directory Overview page, specifically the Properties tab. The left sidebar contains a navigation menu with options like Overview, Preview features, Diagnose and solve problems, and various management options. The main content area displays properties for the Default Directory, including Data location (EU Model Clause compliant datacenters), Notification language (English), Tenant ID, Technical contact, Global privacy contact, and Privacy statement URL. The 'Access management for Azure resources' section is highlighted, showing a toggle switch set to 'Yes'. Below this, a message states that the user (@gmail.com) can manage access to all Azure subscriptions and management groups in this tenant. The 'Security defaults' section is also visible, indicating that security defaults are enabled and the organization is protected by them. At the bottom, there are 'Save' and 'Discard' buttons.



NOTE: This may create a Microsoft Defender for Cloud alert.

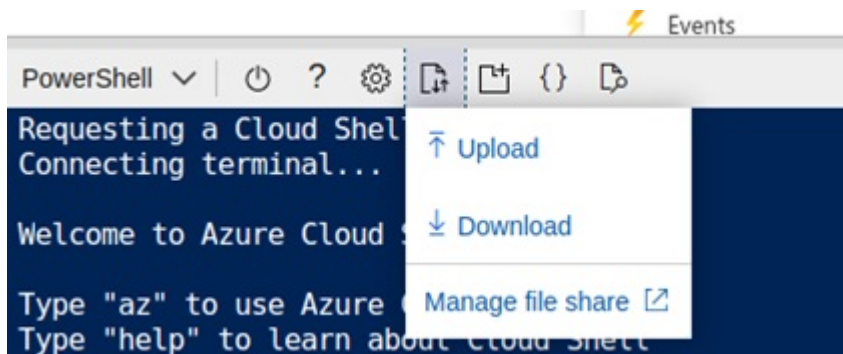
5. Sign out.
6. Sign back in for the change to take effect.
7. Open Azure Cloud Shell with PowerShell.



NOTE: Azure Cloud Shell needs a storage account instance to store local files. You must create an instance, which is typical if Azure Cloud Shell has not been used on the tenant before. The following link explains how to create a storage account instance for cloud shell: [Start Cloud Shell](#)

If Microsoft asks you to register your subscription with the Azure Cloud Shell resource provider, use the instructions in the following link: [Registering your subscription with Azure Cloud Shell](#)

8. Upload the onboarding zip file that you downloaded earlier to Azure Cloud Shell, using the upload feature at the top of the shell screen. It will be uploaded to the current working directory.



9. Decompress the package using unzip command on the package.

```
unzip './WithSecure Elements XDR Identity Security for Entra ID.zip'
```

This decompresses all files into a new withsecure folder.

10. Change the directory to the folder with decompressed files.

```
cd withsecure
```

11. Run the following command in Azure Cloud Shell to assign *Owner* to the principal that needs to deploy the WithSecure Entra ID configuration script, update the *[userId]* with your **User principal name (from Azure)**:

```
New-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```

The Azure environment is prepared for onboarding.

2.5 Deploy resources

The WithSecure configuration script is ready to deploy after you have prepared the environment.

The WithSecure configuration script deploys the resources required to forward relevant Entra ID and Azure logs into an Event Hub so that WithSecure can collect the data to perform detection.

Deploy the resources by running the following command:

```
./deploy.ps1
```

The resources are deployed to your Azure environment.

2.6 Post-deployment verifications

Verification methods to confirm that a deployment works as expected.

After you deploy the required resources, verify that the deployment works as expected. Verification covers confirming that the Event Hub receives events and that the diagnostic settings forward logs to Identity Security.

2.6.1 Validate the Event Hub

Validates that the Event Hub was created and receives events.

To validate Event Hubs:

1. Check the Resource Group called *WSecCD* to validate that the Event Hub has been created.

Home > Resource groups > WSecCD Resource group

Search

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Essentials

Resources Recommendations

Filter for any field...

Type equals all X

Location equals all X

Add filter

Showing 1 to 5 of 5 records. Show hidden types

No grouping

Name	Type	Location
WSecCD-action-group	Action group	Global
WSecCD-clouddr-northeurope	Event Hubs Namespace	North Europe
WSecCD-clouddr-northeurope-alert	Metric alert rule	Global
WSecCD-clouddr-uksouth	Event Hubs Namespace	UK South
WSecCD-clouddr-uksouth-alert	Metric alert rule	Global

There should be an Event Hub present
for each monitored region

2. Check that an alert exists and that the action contains the correct email addresses. The alert notifies you when the event hub reaches capacity.

Home > Resource groups > WSecCD Resource group

Search

Overview

Activity log

Access control (IAM)

Tags

Resource visualizer

Events

Settings

Deployments

Security

Deployment stacks

Policies

Properties

Cost Management

Essentials

Resources Recommendations

Filter for any field...

Type equals all X

Location equals all X

Add filter

Showing 1 to 4 of 4 records. Show hidden types

No grouping

JSON View

Name	Type	Location
WSecCD-action-group	Action group	Global
WSecCD-clouddr-northeurope	Event Hubs Namespace	North Europe
WSecCD-clouddr-northeurope-alert	Metric alert rule	Global
WSecCD-clouddr-uksouth	Event Hubs Namespace	UK South

The Event Hub shows the test alert with the correct recipient emails, confirming that events flow through.

2.6.2 Validate diagnostic settings

Validates the diagnostic settings that stream logs to the Event Hub.

To validate diagnostic settings:

1. Check the Diagnostic settings in Entra ID and Azure module. There should be a diagnostic setting named *WSecCD*.

Home > Secure Oyj MDR

Secure Oyj MDR | Diagnostic settings

Microsoft Entra ID

Preview features

Diagnose and solve problems

Manage

Users

Groups

External Identities

Roles and administrators

Administrative units

Delegated admin partners

Refresh

Feedback

Diagnostic settings are used to configure streaming export of platform logs and metrics for a resource to the destination of your choice. You may create up to five different diagnostic settings to send different logs and metrics to independent destinations. [Learn more about diagnostic settings](#)

Diagnostic settings

Name	Storage account	Event hub	Log Analytics worksp...	Partner solution	Edit setting
WSecCD	-	WSecCD-clouddr-nort...	-	-	Edit setting

+ Add diagnostic setting

2. Click **Edit setting** to open the **Diagnostic settings** view.

[Home](#) > [Secure Oyj MDR | Diagnostic settings](#) >

Diagnostic setting ...

 Save  Discard  Delete  Feedback

A diagnostic setting specifies a list of categories of platform logs and/or metrics that you want to collect from a resource, and one or more destinations that you would stream them to. Normal usage charges for the destination will occur. [Learn more about the different log categories and contents of those logs](#)

Diagnostic setting name WSecCD

Logs

Categories

- ☒ AuditLogs
- ☒ SignInLogs
- ☒ NonInteractiveUserSignInLogs
- ☒ ServicePrincipalSignInLogs
- ☒ ManagedIdentitySignInLogs
- ☒ ProvisioningLogs
- ☒ ADFSSignInLogs
- ☒ RiskyUsers
- ☒ UserRiskEvents
- ☒ NetworkAccessTrafficLogs
- ☒ RiskyServicePrincipals
- ☒ ServicePrincipalRiskEvents
- ☒ EnrichedOffice365AuditLogs
- ☒ MicrosoftGraphActivityLogs

 In order to export Sign-in data, your organization needs Azure AD P1 or P2 license. If you don't have a P1 or P2, [start a free trial](#).

Destination details

- ☐ Send to Log Analytics workspace
- ☐ Archive to a storage account
- ☒ Stream to an event hub

For potential partner integrations, [click to learn more about event hub integration](#).

Subscription

ontosoc_secondary_subscription

Event hub namespace *

WSecCD-northeurope

Event hub name (optional) ⓘ

wseccd

Event hub policy name

WSecCD-rule-send

- ☐ Send to partner solution

3. Validate the policy compliance.

- a) Go to **Subscriptions** and select **Policies**.

Home > Subscriptions >

Subscriptions

F-Secure Oyj MDR (ontosoc.onmicrosoft.com)

+ Add Manage Policies ...

Sear... Subscriptions == global filter

My role == all

Status == all

+ Add filter

Subscription name ↑↓

F-Secure MDR ...

F-Secure MDR

Subscription

Search

- Tags
- Diagnose and solve problems
- Security
- Events

Cost Management

- Cost analysis
- Cost alerts
- Budgets
- Advisor recommendations

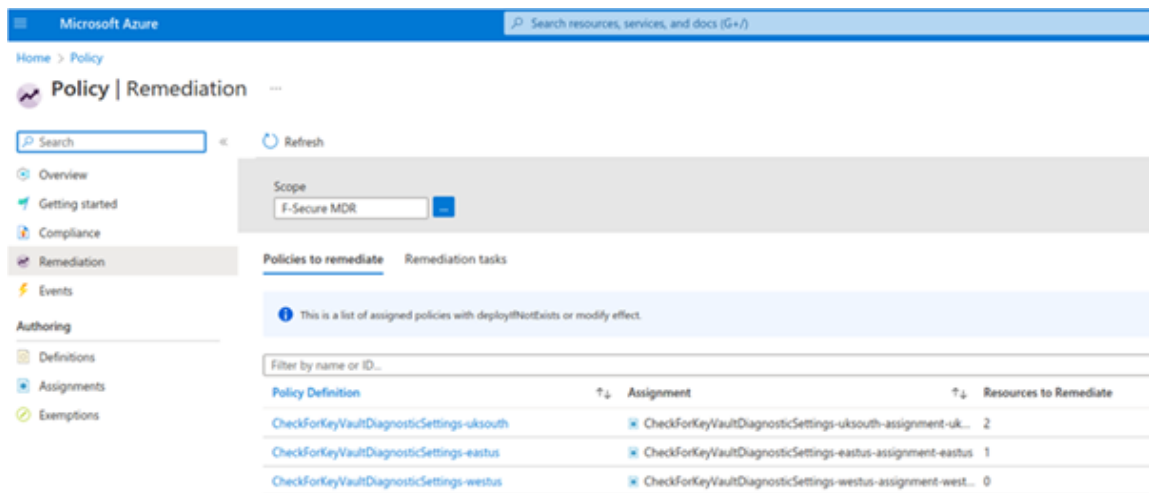
Billing

- Billing profile invoices

Settings

- Programmatic deployment
- Billing properties
- Resource groups
- Resources
- Preview features
- Usage + quotas
- Policies

a) Select **Remediation** where the corresponding remediation will be listed.



The diagnostic settings are validated, and any required remediation is listed.

2.7 Connect Azure to Elements Cloud

Connect Microsoft tenants to Elements Cloud in WithSecure Elements Security Center.

Follow these instructions after the deployment is complete:

1. In WithSecure Elements Security Center, go to **Environment > Cloud > Microsoft Tenants and Azure Subscriptions**.
2. Select the Azure Tenant from the list.
3. On the **Security capabilities** page, select **Add connection string**.
4. Copy and paste the whole connection string, including `Endpoint=sb://`, from the Azure CLI and select **Add**.



NOTE: This process can take up to 5 minutes.

*When the connection is working, the status changes to **The tenant is protected**, with a green tick mark.*

If you have multiple tenants, return to the **Cloud environment** view and go to the **Microsoft Tenants** tab to configure another tenant.

Once the deployment has succeeded, proceed to the post-deployment verification.



NOTE: If the deployment fails, create a ticket for WithSecure Customer Care.



IMPORTANT: Download a new deployment script from WithSecure Elements Security Center in the following cases:

- If you create a new tenant.
- If WithSecure makes any changes to cloud platform or to the script to align to the security best practice.

2.8 Check that the detection capability works

After connecting Elements Cloud to the Entra ID Tenant, you can verify the success of the WithSecure Elements XDR Cloud Security for Azure installation by running a script in the `onboarding.zip` file.

The script creates a new app registration, triggers a broad context detection (BCD) in Elements Security Center, and then deletes the app registration to maintain a clean environment.

To check the identity security detection capability:

1. Within the cloud shell, run the following command:

```
./WithSecureIdentitySecurityTestingTool.ps1
```

2. Wait for the script to run.
3. Make sure that the application registrations have been created and deleted.
4. Navigate to Elements Security Centre, select **Events > Broad Context Detections** to verify that a broad context detection has been created for this activity.

The broad context detection contains a detection called `WithSecure test detection add application`.

5. Close the broad context detection.

A broad context detection appears in Elements, confirming that the detection capability works.

2.9 Finish the onboarding

Finalize the onboarding process by adjusting role assignments and subscription access.

After you validate the deployment and add the connection string to WithSecure Elements Security Center, adjust roles and access rights as follows:

1. Run the following command in the Cloud Shell to revoke the elevated access that was necessary for deploying the WithSecure Entra ID configuration script:

```
Remove-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```

Use your **User principal name** as the `userId`.

2. Follow the Microsoft instructions to disable the **Elevate Access to all subscriptions** option: Elevate access to manage all Azure subscriptions and management groups

The onboarding session is finished.

Now that you have onboarded the detection capability, you can add the identity response capability to minimize the impact of threats during a cyber attack.

2.10 Configure email reports

You can configure automated email reports using the **Email notification and reports** feature available under the **Reports**.

You must have a custom view for security events to use as a template.

After creating a custom view, you can add, configure, and schedule email reports and define their recipients.

1. To add a new email report and configure it, do the following:
 - a) Select **Reports** on the left-hand navigation pane.
 - b) On the **Reports** page, go to the **Email notification and reports** tab.

- c) Select **Add email report**.

*The **Add new email report** pane opens.*

- d) Enter a name for the report (for example, **Azure report**).
- e) From the **Data source** drop-down menu, select **Security Events**.



NOTE: If you select **Security Events** as the data source, the email sent to recipients includes a link to the **Security Events** view in Elements Security Center. If you select **My report** as the data source, the email sent to recipients includes a link to download the report as a PDF file. The content of the report is customized using the selected template.

- f) From the **Template** drop-down menu, select the template that you already created on the **Security Events** page (for example, **Azure events**).
 - g) Choose your preferred language for the report.
2. To configure schedule and recipients, do the following:
- a) By default, **Send only when report has content** under **Schedule** is turned on. Turn it off to receive reports even when there are no events.
Reports for security events are sent every 10 minutes.



NOTE: The first report includes data from the last 24 hours; subsequent reports include data from the last ten minutes.

- b) In **Recipients**, enter email addresses separated by commas.

3. Select **Save**.

The email report settings are saved.

2.11 Create a custom view for security events

You can create a custom view for **Azure** security events to use as a template, for example, when configuring email reports.

1. Under **Events**, select **Security Events**.
2. Open the **View** drop-down menu and select **Azure**.
3. Select **Save as** and enter a name for your custom view, for example, **Azure events**.
4. Select **Save**.

*The custom view appears under **My views** at the top of the list.*

Chapter 3

Ongoing management

Topics:

- When to rerun the script
- When a new tenant is created
- Verify event hub capacity
- Regular release of the script
- The Detection module overview
- Update notification recipients

Ongoing management

Maintenance activities required to keep Identity Security connected and operating at the expected service level.

After onboarding, you perform ongoing maintenance to keep Identity Security connected and operating at the expected service level. Maintenance activities include:

- Rerunning the deployment script when your cloud environment changes
- Onboarding new tenants
- Monitoring Event Hub capacity
- Applying new releases of the deployment script
- Updating notification recipients

3.1 When to rerun the script

The diagnostic settings and policies implemented during the onboarding process will account for some changes to the cloud environment.

After the initial onboarding process, diagnostic settings and policies are designed to automatically detect and handle some changes in the cloud environment. However, if there are significant changes or updates that are not covered by these settings and policies, you have to rerun the script.

3.2 When a new tenant is created

When a new tenant is created, you add it to Elements Security Center and run the deployment script to onboard it.

When a new tenant is created, complete the onboarding configuration to add the new tenant to Elements Security Center and download a new .zip file.

To onboard the new tenant, you then run the deployment script (`deploy.ps1`) again, the same way you ran it during the initial resource deployment.

3.3 Verify event hub capacity

During the onboarding process, the script creates an alert for when the event hub receives more events than it can process.

To verify the event hub capacity, do the following:

1. Go to the Event Hub overview page by entering Event Hubs in the search bar in the Azure portal.
2. Select the name of the Event Hub.
3. On the overview page, check the **Throughput Units** value.

If the number of **Throughput Units** is 40, or if you do not receive an email mentioning that the alert is resolved shortly, contact WithSecure Customer Care.

The Event Hub overview shows the Throughput Units value, confirming its capacity.

3.4 Regular release of the script

The script used to configure event hubs, diagnostic settings, and policies may require changes and improvements over time.

The changes could be required due to extensions in detection coverage, alignment to latest cloud best practice, or underlying cloud platform changes.

You can see the **Onboarding files** status in WithSecure Elements Security Center when the latest version of the files has not been deployed. To redeploy, download the latest version of the script and use the command `deploy.ps1 -update $true`.

3.5 The Detection module overview

Identity Security identifies risky sign-ins and potential privilege escalations. The Detection module builds on top of this to provide deeper insights into attacker activity following the use of stolen credentials.

The Detection module integrates with Elements Endpoint Protection, Elements Endpoint Detection and Response, and Elements Identity Security solutions to enhance visibility into attacker behavior, when stolen credentials have been used.

The Detection module aggregates detections from both Identity Security and Detection and combines the suspicious activity as unified Broad Context Detections (BCD).

The Detection module monitors the following Azure cloud services:

- **Azure Key Vault:** Detects unauthorized access to sensitive keys and secrets, which may be used to advance an attack.
- **Network Security Group:** Identifies changes that open network paths that could be used to steal sensitive information.
- **Azure Virtual Machines (VMs):** Monitors for harmful code being run when a virtual machine starts up, and for signs of cryptojacking - when attackers use the organization's systems to secretly mine cryptocurrency.
- **Azure Storage:** Detects modifications to setup scripts that run when an administrator opens Cloud Shell. These changes can grant attackers administrator-level privileges and allow silent code execution.

3.6 Update notification recipients

You cannot update notification recipients in Elements Security Center. To change the recipient list, edit the action group in the Azure portal.

Notification recipients receive the email alerts that the onboarding script deploys, such as the alert that fires when the Event Hub reaches its capacity.

1. Sign in to the Azure portal and go to **Resource groups**.
2. Open the resource group named *WSecCD*.
3. In the **Overview** section, under **Resources**, select the action group named *WsecCD-action-group*.
4. Edit the action group to add or remove notification recipients.



IMPORTANT: These changes do not appear in Elements Security Center.

The notification recipients are updated in the action group.



Appendix A

Offboard the deployed resources

Offboard the deployed resources

Removes the deployed WithSecure Identity Security for Entra ID resources from your Azure environment.

This should be done in any of the following cases:

- There were some issues in the deployment process and the deployment should be started over, or
- you want to opt out of the service and remove the monitoring resources.

To delete the resources, follow these instructions:

1. Download the latest *onboarding script* that is available in the **Tenant details** view under the **Environment > Cloud > Microsoft Tenants and Azure Subscriptions** tab.

2. In the Azure Portal, temporarily elevate your access to manage the tenant.

Use the instructions provided on the following page to temporarily elevate access to manage all subscriptions:
Elevate access to manage all Azure subscriptions and management groups | Microsoft Learn.

3. Go to the Azure portal, switch the **Access Management for Azure resources** option to **Yes**.

4. Open Azure Cloud Shell with PowerShell.

5. Use **Manage files > Upload** at the top of the shell screen to upload the *onboarding script* zip file that you downloaded in the step 1 to Azure Cloud Shell.

The onboarding zip file is uploaded to the current working directory.

6. Decompress the package using the unzip command on the package.

```
unzip './WithSecure Elements XDR Identity Security for Entra ID.zip'
```

This decompresses all files into a new withsecure folder.

7. Change to the directory that contains decompressed deployment files.

```
cd withsecure
```

8. Run the following command in Azure Cloud Shell to assign **Owner** to the principal that needs to deploy the WithSecure Entra ID configuration script, update the *[userId]* with your **User principal name**:

```
New-AzRoleAssignment -SignInName "[userId]" -Scope "/" -RoleDefinitionName "Owner"
```



NOTE: This may create a Microsoft Defender for Cloud alert.

9. To delete the resources, run the following command from inside the withsecure directory:

```
./cleanup.ps1
```

This removes WithSecure Identity Security for Entra ID related resources in your Azure environment (WSecCD resource group, action group, Event hub namespace, and metric alert rule).

10. Return to the Elements Security Center to delete the Azure Tenant connection that is related to WithSecure.

- a) In WithSecure Elements Security Center, go to **Environment > Cloud > Microsoft Tenants and Azure Subscriptions**.
- b) Select the tenant that you want to remove.
- c) Under **Quick actions**, select **Remove Azure tenant**.
- d) Read the notification and select the **Remove Event Hub connections** check box.

e) Select **Remove**.

You will receive a confirmation that the tenant connection was removed successfully.

The deployed resources are removed from your environment.



Appendix **B**

Troubleshooting

Topics:

- Check the connection status

Troubleshooting

Troubleshooting information helps you resolve product issues.

- If Cloud shell terminal has been closed before the deployment completes: Follow the steps to deploy the resources again.
- If running the `deploy.ps1` script fails with an error about an ongoing deployment, wait 15 minutes before retrying.
- If deployment fails with an error indicating that the subscription is not registered to use namespace `Microsoft.PolicyInsights`, do the following:
 1. Go to this subscription page and click on **Resource Providers**.
 2. Click the Provider **Microsoft.PolicyInsights** and then **Register** or **Re-register**.
 3. Once the registration completed, restart the process by running the `./deploy.ps1` script.

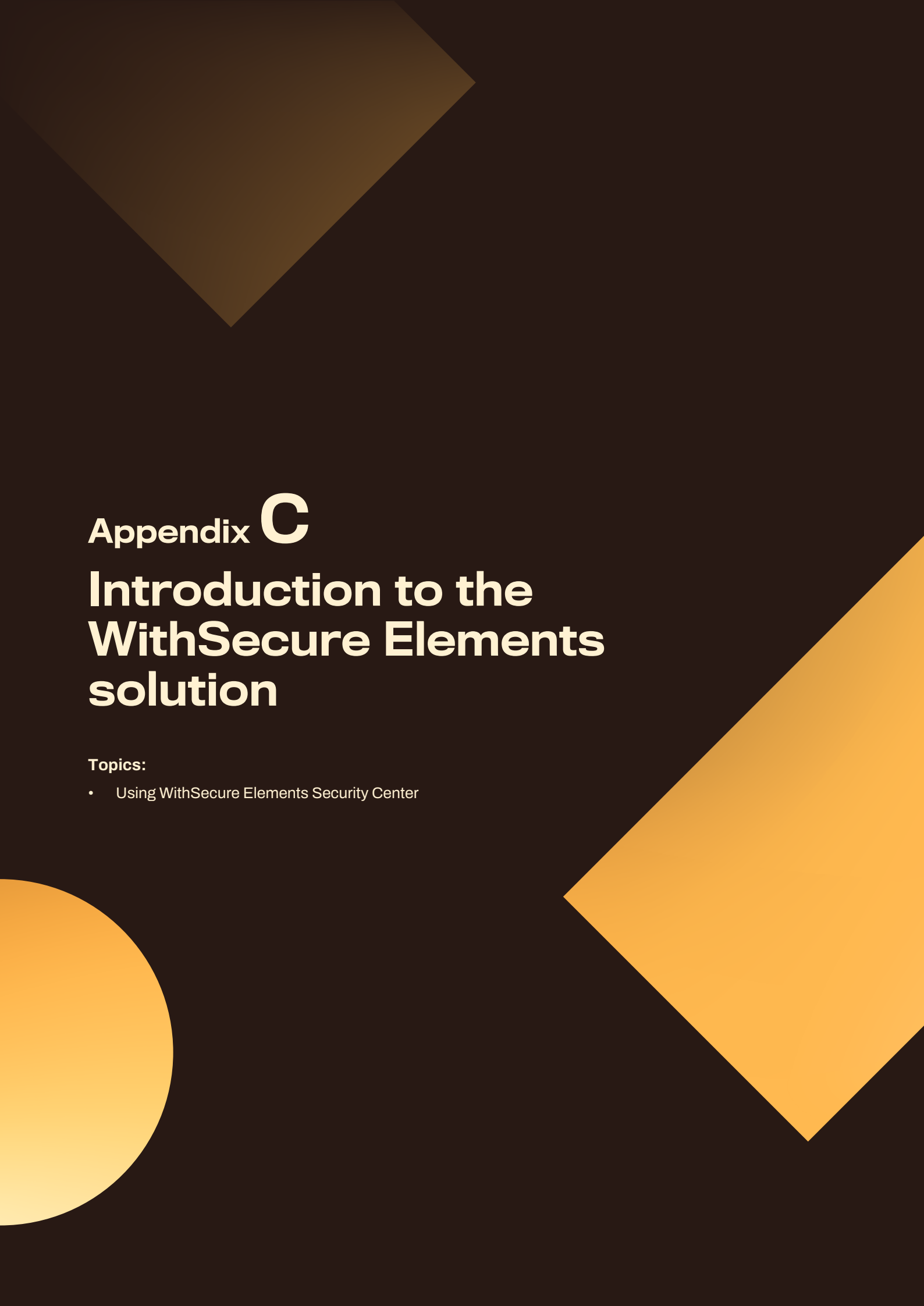
B.1 Check the connection status

You can view the connection status in WithSecure Elements Security Center

If Identity Security protection appears inactive, check the connection status of each tenant in the Elements Security Center.

1. In WithSecure Elements Security Center, go to **Environment > Cloud > Microsoft Tenants and Azure Subscriptions**.
2. Review the **Identity Security** status for each tenant that is displayed in the list.

The Identity Security connection status is shown for each tenant.



Appendix **C**

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

C.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.

C.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.

C.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 known 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.

C.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: |
| | <ul style="list-style-type: none"> • 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.

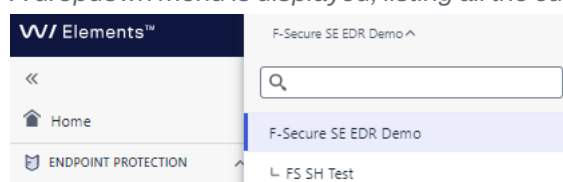
To use the scope selector to focus on a particular company:

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 possess 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**.

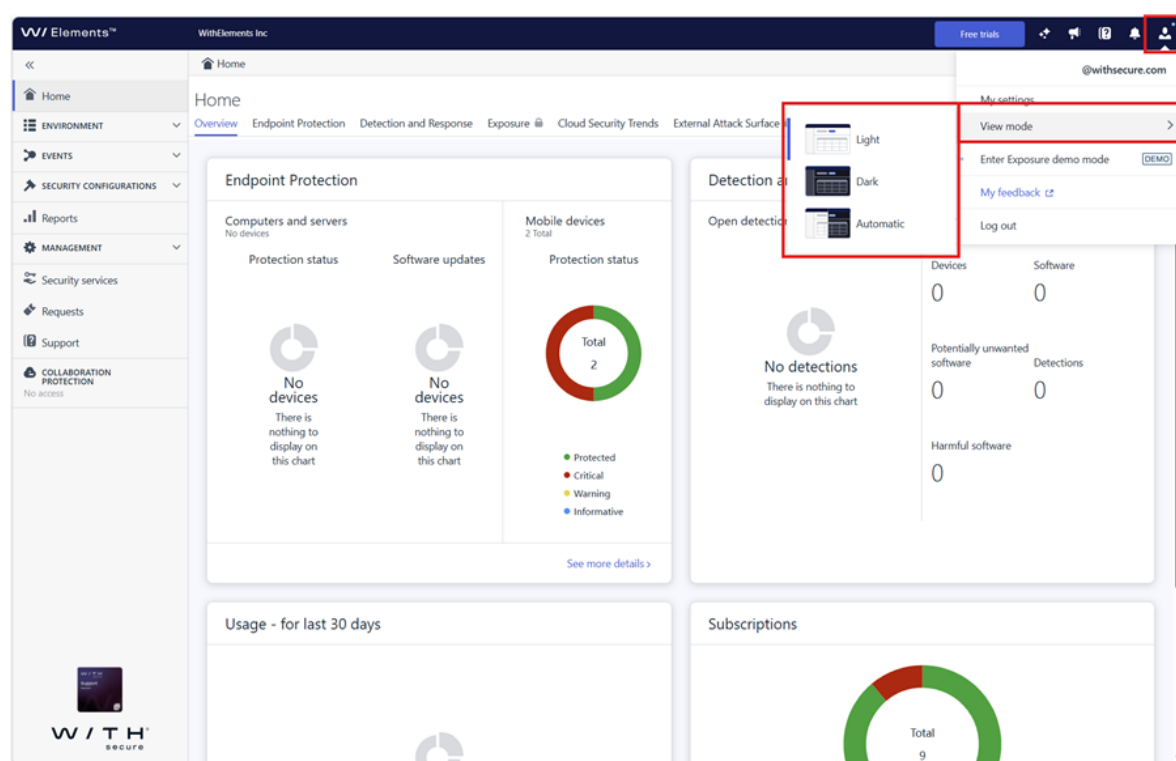
C.1.4 Change the view mode

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.

C.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.

C.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.

C.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**.

C.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.

C.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.

C.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.

Glossary

Access Control

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

Activation Code

An activation code is a code entered during installation to activate a product and apply its configuration.

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.

Anomaly

An unusual deviation from expected system or user behavior, often indicating a potential security threat.

Automation

Automation is the use of technology to perform tasks or processes with minimal human intervention, improving efficiency, accuracy, and scalability.

Broad Context Detection (BCD)

A Broad Context Detection is a group of related detections that WithSecure Elements EDR correlates into a single incident, ranked by criticality, to show the full context of an attack.

Business Context

Additional metadata assigned to an asset to provide insight into its role, importance, and relevance to business operations.

Cloud Account

A cloud account is a user or organizational profile that grants access to cloud computing services and resources, managed by a cloud provider.

Cloud Security

Cloud security is the set of policies, controls, and technologies that protect data, applications, and infrastructure hosted in cloud environments.

Cloud Service

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

Compromised Account

A compromised account is a user account that attackers have accessed, abused, or taken over without authorization.

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.

Entra ID

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

Exposure Management

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

False Positive

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

Federated Single Sign-On (FSSO)

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

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.

Identity Response

A security feature in WithSecure Elements that integrates with Microsoft Entra ID to detect and mitigate identity-based threats.

Identity Security

Identity Security is a security capability that detects risky sign-ins, identity misuse, and privilege-related threats affecting user identities and access systems.

Incident

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

Incident Response

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

Incident Response Retainer

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

Infrastructure-as-Code (IaC)

The management and provisioning of IT infrastructure through machine-readable configuration files rather than manual processes.

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.

Mobile Device Management (MDM)

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

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.

Offboarding

Offboarding is the controlled process of removing a product, integration, service connection, or granted permissions from an environment when it is no longer needed.

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.

Privilege Escalation

The act of gaining higher access levels within a system than originally permitted.

Profile Assignment

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

Quarantine

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

Remote Monitoring and Management Integration (RMM)

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

Reputation Service

A service that puts files in context based on their age, frequency, and location to expose threats that could be otherwise missed.

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 Cloud

Security Cloud is WithSecure's cloud-based threat analysis and reputation service that helps classify files, websites, and other security-relevant observations and deliver up-to-date protection against emerging threats.

Security Events

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

Security Group

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

Security Monitoring

Security monitoring is the continuous collection and analysis of system and network activity to detect, alert on, and investigate potential security threats.

Sensor

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

Service Partner

A service partner is an organization or partner tier that manages services, customer organizations,

or delegated operational responsibilities on behalf of others.

Severity

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

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.

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 43–44
 access rights 32, 37, 44, 46
 account 54
 account creation 45
 account details 47
 account levels 42
 account linking 52
 action group 25
 Active Directory 62
 AD groups 62
 adding devices 55, 57, 60
 administrator account 32–33, 37, 44–45
 Agent for Computers 56
 Agent for Servers 56
 Agent for Windows 63
 alert rule 16
 API client 46
 app registration 21
 asset groups 60
 audit logs entry 37
 authenticator app 35
 Authenticator applications with Time-Based One-Time Password (TOTP) 35
 automatic deletion 58, 61
 Azure 13
 Azure cloud service 25
 Azure Cloud Shell 11, 14, 27
 Azure Key Vault 25
 Azure log collection 13
 Azure Management Group 11
 Azure portal 13–14, 24–25
 Azure Storage 25
 Azure tenant 5, 13–14, 20, 27, 30
 Azure Virtual Machines (VMs) 25

B

backup 64
 biometric authentication 36
 broad context detection 5, 10, 21, 25
 Business Account 5, 33

C

capacity alert 24
 change name 47
 change subscription 51
 cleanup script 27
 Cloud 20
 cloud account 13–14
 cloud environment 24
 Cloud Shell 21, 30
 company level 60
 Company level 61
 compromised account 10
 configuration script 16, 24–25
 connection status 30
 connection string 20
 connectivity 24
 custom labels 59

custom view 21–22
 customer company 37, 48–49

D

dark mode 47
 data recovery 64
 delete API client 46
 deploy.ps1 -update \$true 25
 deployed infrastructure 7
 deployed resources 27
 deployment script 24, 30
 detection 6
 Detection and Response 6
 detection capability 21
 Detection module 25
 device assignment 60
 device biometrics 36
 Device biometrics 35
 device commands 61
 device filters 62
 device grouping 59–60
 device invitations 59
 device labels 59
 Device list 59
 device management 55, 58–62
 device view 60, 62
 devices 51, 61
 Devices page 60
 Devices view 62
 diagnostic data 63
 diagnostic settings 7, 16–17, 24
 domain federation 53
 downloading software 57
 Downloads page 57

E

edit administrator 45
 edit profile 47
 EDR 51, 57
 EDR and EPP for Computers 51
 EDR and EPP for Computers Premium 51
 EDR and EPP for Servers 51
 EDR and EPP for Servers Premium 51
 EDR for Computers 51, 57
 Elements API 46
 elevated access 14, 21
 email address 52
 email alert 25
 email aliases 53
 email invitation 57, 59
 email report 21
 Emergency Incident Response 10
 endpoint sensor 6
 Entra ID 5, 13, 17, 27
 Entra ID configuration script 7, 14, 21
 Entra ID logs 10, 16
 EPP for Computers 51, 61–62
 EPP for Computers Premium 51
 EPP for Servers 51, 61–62
 EPP for Servers Premium 51

- EPP subscription 51
- Event Hub 7, 10, 13, 16, 24
- Event Hub capacity 24
- existing customer company 49

F

- federated domain 34, 54–55
- federated single sign-on 52–53
- fingerprint 36
- finishing onboarding 21
- forgot password 47
- FSSO 52

G

- getting started 5
- Global Administrator 11

I

- IAM administrator 42–44
- IAM role 37, 42–44
- Identity and Access Management 42
- Identity Inventory 13–14
- identity provider 52
- Identity Security 5–6, 10–11, 13, 16, 21, 24–25, 30
- Identity Security and Cloud Security 10
- Incident Response Retainer 10
- Infrastructure as Code 7
- installation link 57, 59
- installation package 6, 56–57

L

- label assignment 59
- light mode 47
- logging in 33
- login 34, 47
- login credentials 33–34
- login security 34

M

- managed companies 42
- MFA 34–36
- MFA methods 35
- Microsoft 14
- Microsoft Defender for Cloud 14
- Microsoft Entra Admin Center 52
- Microsoft Entra ID 34, 52–54
- Microsoft Tenant 5
- Microsoft.PolicyInsights 30
- Mobile Protection 55–56, 61, 63
- multi-factor authentication 33–36
- My settings 36, 47

N

- Network Security Group 25
- new customer company 50
- new tenant 24
- non-federated domain 34
- notification recipients 21, 25

O

- offboarding 27
- offline devices 58, 61
- onboarding 5, 13
- onboarding configuration 13
- onboarding script 14, 24
- ongoing management 24
- ordering products 49–50
- Organization Settings 44–46, 60

P

- partner 44–45
- Partner Portal 48–50
- password recovery 47
- patch management 32
- pending invitations 59
- permissions 13, 37
- Phone number for Short Message Service (SMS) messages with One-Time Passwords (OTP) 35
- policy 24
- policy compliance 17
- post-deployment verification 16
- PowerShell 14
- Premium subscription 51
- preparing environment 14
- prerequisites 11
- product deployment 48
- profile assignment 62
- profile assignment rules 60
- Push notifications with Auth0 Guardian authenticator 35

Q

- quick start 33

R

- redeployment 25
- remote device management 61
- remote request 63
- remove administrator 45
- removing federation 55
- removing MFA 36
- rerun script 24
- reset password 47
- resource deployment 16
- resource group 7, 16, 27
- resource provider 30
- risky sign-in 5, 25
- role 37
- role assignment 14, 21, 37
- role permissions 43

S

- scope selector 32, 42, 44, 49–50, 57, 60–61
- script update 25
- Secure USB keys 35
- security administrator 37, 44
- Security Administrators 45
- security capability 13–14
- Security Center 5–6, 13–14, 20–21, 24–25, 27, 30, 32–37, 42, 44, 47–50, 52–53, 55, 57–63
- Security Centre 21

- security events 21–22
- security roles 42
- service 64
- service partner account 45
- single sign-on 34, 53, 55
- Smartphones or other devices 35
- software distribution 56
- software installation 57
- Solution Provider 42, 48–49
- subscription 11, 33, 48–50, 55, 58
- subscription access 21
- subscription assignment 49
- subscription key 48–51, 56
- subscription upgrade 51
- subscriptions 48, 50
- Subscriptions view 50
- support 63

T

- table columns 62
- testing tool 21
- Throughput Units 24
- troubleshooting 30

- two-factor authentication 34

U

- unzip 14, 27
- upgrading options 51
- user identity linking 54
- user management 37
- user name 47

V

- validation 16–17
- view mode 47
- Vulnerabilities role 37
- vulnerability management 32
- Vulnerability Management: 43

W

- WithSecure 32–34, 42–44, 48, 63
- WSDIAG file 63
- WSecCD 16–17, 25