

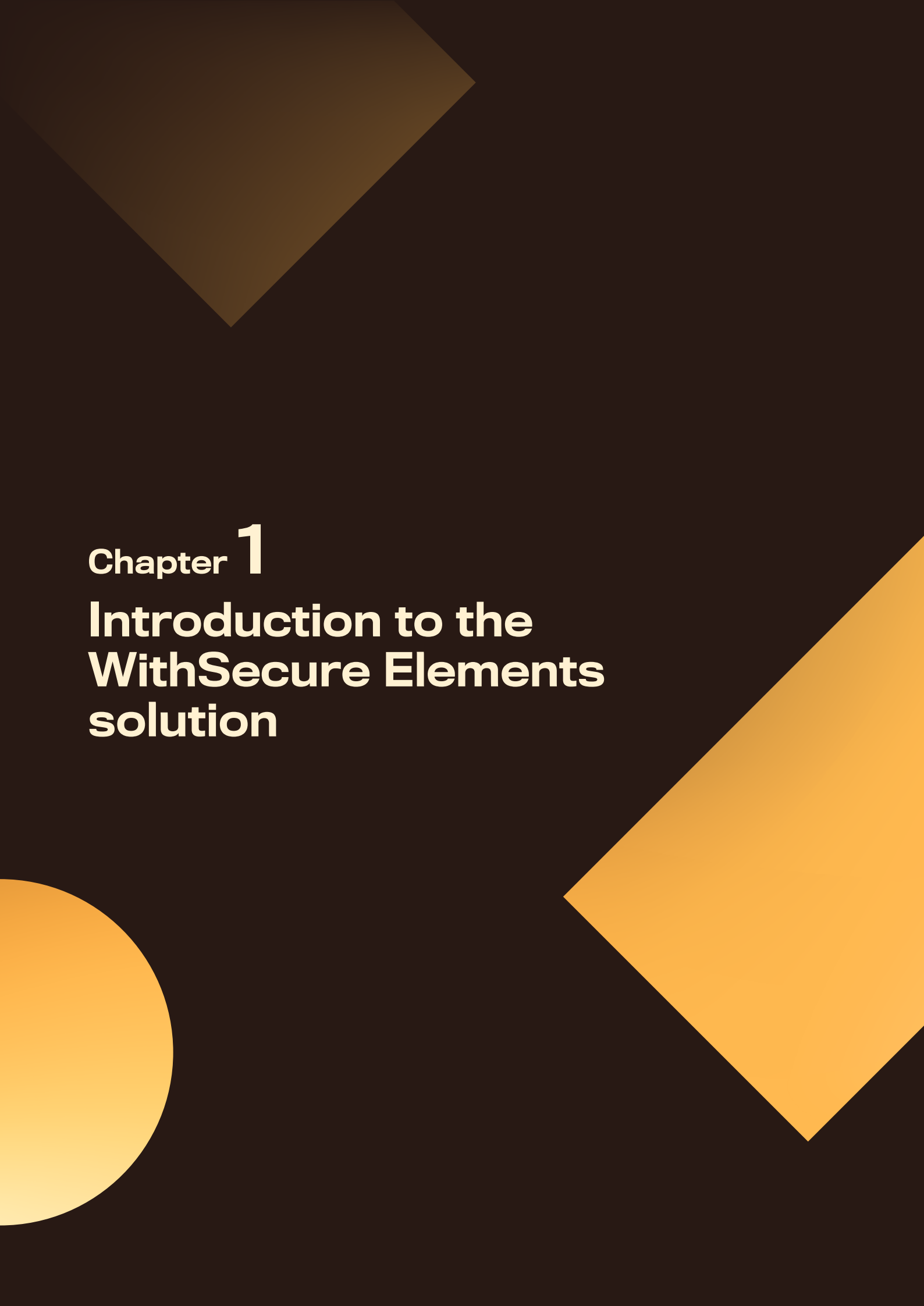


WithSecure Elements

Contents

Chapter 1: Introduction to the WithSecure Elements solution.....	4
Chapter 2: Logging in.....	6
2.1 Log in to non-federated domains.....	7
2.2 Log in to federated domains.....	7
2.3 Multi-factor authentication.....	8
Chapter 3: Federated single sign-on.....	11
3.1 Prerequisites.....	12
3.2 Federated SSO setup.....	13
3.3 Link user identities.....	14
3.4 Remove federation from a domain.....	14
Chapter 4: User management.....	16
4.1 About access rights.....	17
4.2 Scope selector.....	21
4.3 IAM role.....	22
4.4 Add a new administrator.....	23
4.5 Add a new service partner.....	24
4.6 Edit or remove administrators.....	24
4.7 Create an API client.....	25
4.8 Delete an API client.....	25
4.9 Recover your password.....	26
4.10 Change your account details.....	26
Chapter 5: Taking Elements products into use.....	27
5.1 Adding a customer company.....	28
5.2 Assign subscription key.....	28
5.3 Order products for a new customer company.....	29
5.4 View available product subscriptions.....	29
5.5 Change the subscription key.....	30
5.6 Upgrading your subscriptions.....	30
Chapter 6: Security services overview.....	32

Chapter 7: Adding devices for management.....	34
7.1 Distributing WithSecure software.....	35
7.2 Manage invitations.....	37
7.3 Custom labels.....	38
7.4 Managing devices in Elements Security Center.....	38
7.5 Elements data recovery.....	43
Chapter 8: Interacting with WithSecure Services.....	44
8.1 Sample Validation overview.....	45
Chapter 9: AI Security.....	67
9.1 View the AI Security dashboard.....	68
9.2 AI software in the software inventory.....	69
9.3 AI and agentic identities.....	70
Chapter 10: Elevate Requests.....	71
10.1 Create a request.....	72
10.2 View and manage request details.....	72
Chapter 11: Third-party integrations.....	74
11.1 Autotask PSA.....	75
11.2 ConnectWise PSA.....	76
11.3 HaloPSA.....	77
Appendix A: Access control.....	79
A.1 Core concepts.....	80
A.2 Planning your deployment.....	92
A.3 Managing security administrators.....	106
A.4 Setting up Microsoft Entra ID integration.....	138
A.5 Migrating to Elements RBAC.....	149
A.6 RBAC reference.....	162
Glossary.....	168
Index.....	175



Chapter 1

Introduction to the WithSecure Elements solution

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



Chapter 2

Logging in

Topics:

- Log in to non-federated domains
- Log in to federated domains
- Multi-factor authentication

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 the managed 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 the managed organization. To do that, use the company self-registration link for your specific region.

2.1 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.

2.2 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.

2.3 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).

2.3.1 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.

2.3.2 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.

2.3.3 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.

2.3.4 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.

Chapter 3

Federated single sign-on

Topics:

- Prerequisites
- Set up federated single sign-on with Microsoft Entra ID
- Link user identities
- Remove federation from a domain

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.

3.1 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.

3.1.1 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.

3.2 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]**.*

3.3 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.

3.4 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.

Chapter 4

User management

Topics:

- About access rights
- Move between the managed companies
- Elements Identity and Access Management (IAM) role
- Add a new administrator
- Add a new service partner
- Edit or remove administrators
- Create an API client
- Delete an API client
- Recover your password
- Change your account details

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.

4.1 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.

4.1.1 Access rights by role

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

Exposure Management – Exposure

Full editing Allows access to the following Exposure Management features:

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



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

Audit logs entry: cspm: admin

Exposure Management – Vulnerabilities

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



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

Audit logs entry: vm: administrator

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

Audit logs entry: vm: team_member

Read-only	View-only access with no permission for managing users. Audit logs entry: vm: readonly_team_member
------------------	---

Collaboration Protection

Admin	Allows the access to the Collaboration Protection views and edit the following protection features: • Handling detections • Managing Exchange and shared files settings • Managing policies, quarantining files, and generating reports Audit logs entry: cpo365:admin
Read-only	Grants view-only access to the Collaboration Protection views. Audit logs entry: cpo: readonly
Quarantine manager	Allows access to the Collaboration Protection views that are related to detections and quarantining files. Audit logs entry: cpo365:quarantine_mgr

Collaboration Protection – Management

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



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

Audit logs entry: fusion_admin

Endpoint Protection

No access	No access to Endpoint protection features including: - Device management - Patch management - Device security posture - Software reputation - Security Events - Profiles - Home/Endpoint protection - Reports
------------------	--



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

Endpoint Protection – Computers and mobiles

Full editing	Allows the access to the following features: • Security configuration/profiles • Security information, including device status, dashboard, security events and patch management
---------------------	--

- Security operations, such as removing or isolating devices, updating profiles
- Handling subscriptions
- Managing user accounts
- Do cloud onboarding



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

Audit logs entry: epp: manage_computers_mobiles_only

or epp: manage_all

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

Audit logs entry: epp: manage_servers_only

or epp: readonly

Endpoint Protection - Servers

Full editing Allows the access to the following features:

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



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

Audit logs entry: epp: manage_servers_only

or epp_manage_all

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

Audit logs entry: epp: manage_computers_mobiles_only

epp: readonly

Extended Detection and Response - Toggle off

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

- Broad Context Detections
- Response actions
- Automated actions
- Dashboard content related to Detection and Response
- Software Reputation

- Organization Settings related to Detection and Response
- Event Search pages
- Elevate to WithSecure
- Subscription view

Extended Detection and Response – Broad Context Detections

Full editing Permission to manage:

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

Limited access to:

Devices view
Cloud view
Subscription view

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



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

Audit logs entry: elements:xdr-incident-full

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

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-incident-read

Extended Detection and Response – Response

Execute responses Access to execute:

- response actions
- configure Automated actions

Limited access to Cloud view.

Audit logs entry: elements:xdr-response-full

List responses	Access to review: - executed response actions - respective results available Limited access to: - Devices view - Cloud view Download response results requires the Execute Responses permission. Access to the Subscription view is limited. Audit logs entry: elements:xdr-response-read
No access	No access to execute or review: - Response actions - Automated actions

Extended Detection and Response - Event Search

Read-only	Access to review, execute filtered searches and create customized views to event data. Access to the Subscription view is limited. Audit logs entry: elements:xdr-event-search
No access	No access to review event data.

Elements Administration

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

4.2 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.

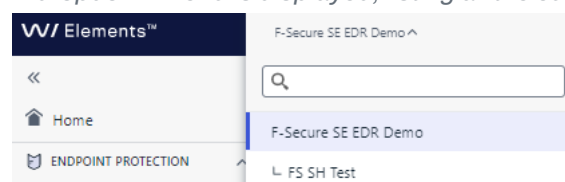
To use the scope selector to focus on a particular company:

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.

4.3 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.

4.3.1 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.

4.4 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.

4.5 Add a new service partner

Add a service partner account to the managed 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.

4.6 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.

4.7 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.

4.8 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.

4.9 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.

4.10 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 the managed 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**.

Chapter 5

Taking Elements products into use

Topics:

- Adding a customer company
- Assign a subscription key for a customer company
- Order products for a new customer company
- View available product subscriptions
- Change the subscription key
- Upgrading your subscriptions

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.

5.1 Adding a customer company

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



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

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



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

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

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

5.2 Assign a subscription key for a customer company

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

You need to consider the following:

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



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

To assign a subscription key:

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

The new subscription key is added to the company account.

5.3 Order products for a new customer company

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



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

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

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



NOTE: WithSecure Partner Portal requires separate login credentials from WithSecure Elements Security Center. If you do not yet have your login details, 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.

5.4 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 managed 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.

5.5 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.

5.6 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.

5.6.1 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.

Chapter 6
**Security services
overview**

Security services overview

The **Security services** page shows which WithSecure services the managed organization already uses and which ones you can still add.

The **Security services** page is available under **Management > Security services**. It brings together the WithSecure services connected to the managed organization and the WithSecure services that the managed organization has not yet added.

My WithSecure services	Lists the WithSecure services that the managed organization already uses.
Available WithSecure services	Lists the WithSecure services that the managed organization can still add.

The **Available WithSecure services** section groups services by category, including **Co-Security** and **Attack Surface Management**. The **Co-Security** category includes:

Infinite	Infinite bundles the full range of WithSecure solutions and services: continuous threat exposure management (CTEM), endpoint protection, detection and response (XDR), managed detection and response (MDR), full WithSecure Elements platform access, customer success management (CSM), and an incident response retainer.
MDR for Endpoints	WithSecure Elements Managed Detection and Response is a continuous, 24/7 managed detection and response service. WithSecure security experts investigate and remediate attacks using data collected by WithSecure Elements Endpoint Detection and Response. MDR customers get priority access to the Incident Response service.
MDR for Identities (Entra ID)	WithSecure Elements Identity Security is an identity threat detection and response (ITDR) solution. It protects against identity-based attacks, including attacks on Microsoft Entra ID single sign-on (SSO), by detecting potentially compromised Entra ID identities and enabling a quick response.
Elevate	Elevate is a threat analysis service available to WithSecure Elements Endpoint Detection and Response users. WithSecure experts validate and investigate difficult detections and provide remediation guidance when needed.
Incident Readiness and Response	Incident readiness helps you prepare for a cyber attack by assessing your current level of readiness and setting goals for improvement. Incident response investigates an incident, determines its root cause, and executes a containment strategy that limits the attacker's ability to retaliate or cause further damage.
Digital Forensics and Incident Response	WithSecure Elements DFIR Retainer provides 24/7, SLA-backed access to Digital Forensics and Incident Response specialists for the duration of the contract. When an incident occurs, the DFIR team ensures business continuity through rapid triage, evidence preservation, containment, and remediation guidance. The service is accredited by the UK National Cyber Security Centre (NCSC) and the German Federal Office for Information Security (BSI), and supports compliance with NIS2, GDPR, and DORA.

Chapter 7

Adding devices for management

Topics:

- Distributing WithSecure software
- Manage invitations
- Enhancing device management with custom labels
- Managing devices in Elements Security Center
- Elements data recovery

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.

7.1 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.

7.1.1 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.

7.1.2 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.

7.2 Manage invitations

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

To manage the invitations:

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

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

*The **Devices** page is displayed.*

2. Select



Manage device invitations.

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

The **Pending** tab lists those email invitations that include an installation link that has not been used yet.

The **Expired** tab lists the expired email invitations.

3. For the pending invitations, you can send a reminder by selecting **Send reminder** as long as the installation link is valid (for 30 days). After that the invitations are shown under the Expired tab.
4. For the expired invitations, you can send another invitation link by selecting **Send new invitation**.



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

7.3 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.

7.3.1 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.

7.4 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

7.4.1 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**.

7.4.2 Remotely manage a device

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

To remotely manage a device:

1. Under **Environment**, select **Devices** on the sidebar.
The **Add new device** option next to **Devices** is visible only at a company level. If the *scope selector* is set to show all customer companies, select the company you wish to manage.
*The **Devices** page is displayed.*
2. Select one of the following tabs:
 - **Computers** - shows devices with WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers
 - **Mobile devices** - shows devices with WithSecure Elements Mobile Protection
 - **Connectors** - shows devices with WithSecure Elements Connector
 - **Unmanaged devices** - shows devices in a customer Active Directory (not in EPP)
3. Select the checkbox next to the name of the device.
A menu is displayed at the bottom of the page.

4. Select the desired operation from the menu.



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

The instruction is sent to the selected device.

7.4.3 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.

7.4.4 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.

7.4.5 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**.

7.4.6 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.

7.5 Elements data recovery

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

No actions are required from you.



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



Chapter 8

Interacting with WithSecure Services

Topics:

- WithSecure Sample Validation

Interacting with WithSecure Services

WithSecure services for validating suspicious samples and reporting ransomware or other active threats.

Use these services to submit files, URLs, and email samples to WithSecure for validation, and to report ransomware or active threats where no detection was observed.

8.1 WithSecure Sample Validation

WithSecure™ Sample Validation improves threat detection by reviewing samples, correcting false results, and finding gaps.

WithSecure™ Sample Validation was formerly called Submit a Sample. This topic describes the service, its features, and planned updates.

WithSecure Sample Validation is a cybersecurity service in the Elements Security Center. WithSecure malware experts use proprietary cloud technology to deliver the service. The service provides accurate and consistent detection across all vectors and improves continuously.

Sample Validation improves detection performance by:

- Correcting false positives and false negatives.
- Finding detection gaps.
- Improving security posture.
- Combining expert human review with malware analysis and threat research.

Automation, cloud intelligence, and analyst expertise help organizations understand emerging threats. They make detection, containment, and remediation more precise. These processes also become faster and more reliable.

8.1.1 Service Offering

The WithSecure™ Sample Validation service is available to all customers using our solutions, official engines, or APIs. It covers any situation where a file, URL, email, or behavior is incorrectly flagged - or not flagged - by WithSecure components.

You can submit requests related to:

- Incorrect detections (false positives)
- Missing detections (false negatives)
- URL categorization
- Phishing and spam classification issues
- Allowlisting of safe applications or processes

This capability is included as part of WithSecure Support, ensuring all customers have access to detection-quality improvements at no additional cost.

False Detections (Incorrectly Detected)

These issues occur when legitimate content is incorrectly identified as malicious or unwanted.

Table 1: False detection issue types

Issue Type	Reason	Descriptions	Plan Type
File-based False Positives	FP - Clean file was blocked	A safe file that's mistakenly flagged as harmful or infected by WithSecure solutions.	Included in Support
PUAs	PUA - Potentially unwanted application detected	A program that isn't exactly malware but may perform actions you didn't expect - like showing ads, changing settings, or slowing your system down.	Included in Support
URL-based False Positives	FP - Trusted URL blocked	A safe website or web link that's incorrectly marked as dangerous or blocked by WithSecure solutions.	Included in Support
URL Categorization	CAT - URL has incorrect content category	Included in Support	Included in Support
Unknown URLs	CAT-M - URL missing content category	Web addresses that haven't yet been analyzed or categorized - their safety status is still unknown.	Included in Support
Phishing False Positives	Legitimate site flagged as phishing	A legitimate website or email that's mistakenly flagged as a phishing attempt.	Included in Support
Spam False Positives	Legitimate email flagged as spam	A genuine email incorrectly identified and filtered as spam or junk.	Included in Support
Request Whitelisting	Allow safe apps blocked by security filters	A trusted app, site, or process is blocked by security rules.	Included in Support

Missed Detections (Not Detected)

These issues occur when malicious content is not correctly identified or blocked.

Table 2: Missed detection issue types

Issue Type	Reason	Description	Plan Type
File-based False Negatives	FN - Malicious file not detected	A malicious file that goes undetected and is incorrectly marked as safe.	Included in Support

Issue Type	Reason	Description	Plan Type
URL-based False Negatives	FN - Malicious URL not blocked	A harmful or malicious website that isn't detected and is mistakenly considered safe.	Included in Support
Phishing False Negatives	FN - Phishing not detected	A real phishing website or email that's not detected and is wrongly treated as safe.	Included in Support
Spam False Negatives	FN - Spam not detected	A spam email that slips through filters and appears in your inbox as if it were normal mail.	Included in Support
Email based false negatives	FN- suspicious email attachment	A <i>false negative</i> occurred when an email containing a malicious or suspicious attachment was not detected or blocked by the email security system.	Included in Support

8.1.2 Scope clarification

WithSecure™ Sample Validation focuses exclusively on detection accuracy issues and is included within your support entitlement.

Included in Support

- False positives (any vector)
- False negatives (any vector)
- URL categorization issues
- Allowlisting of safe items
- Detection-quality improvements

Not Included in Support

Compromised systems
Breaches or intrusions
Active or ongoing security incidents

For incident response support, see:

- WithSecure Incident response
- WithSecure™ Elements Infinite
- WithSecure™ Elevate
- WithSecure™ Co-Monitoring Service

8.1.3 Getting started with WithSecure Sample Validation: What you need and Why it helps

Explains the requirements for submitting samples through WithSecure Sample Validation and the benefits of the service.

Requirements

To benefit from the WithSecure Sample Validation service, make sure the following requirements are met:

- | | |
|--|--|
| Valid Elements subscription | <ul style="list-style-type: none">• A current Elements subscription is required to access the service.• If you are using another WithSecure solution - such as On-Premises solutions Business Suite, Atlant, Email and Server Security) - and need access to the service, you can request access through WithSecure email support. |
| Elements administrator user account | <ul style="list-style-type: none">• You must have an active Elements administrator account.• If you do not have one, contact your system administrator, solution provider, or service provider to request access.• If you need to add or assign administrator permissions, refer to the detailed guide: Adding a new administrator |
| Valid sample submission | <ul style="list-style-type: none">• You must submit a valid sample (e.g., a file, URL, or email) for analysis. |
| One sample per request | <ul style="list-style-type: none">• Each request may contain only one sample. Multiple submissions within the same request are not supported. |



IMPORTANT: Sample requests must not be submitted to the Technical Support team.

Main benefits of the WithSecure Sample Validation service

- | | |
|---|---|
| Stronger Security & Authentication | <ul style="list-style-type: none">• Access to the service now requires verified WithSecure Elements accounts• Enhances security, accountability, and data integrity |
| Improved Tracking & Visibility | <ul style="list-style-type: none">• Each submission includes status updates, reference IDs, and full history• Enables auditing, case management, and transparent communication |
| Greater Control & Efficiency | <ul style="list-style-type: none">• Verified access safeguards customer environments• Every request is traceable for full accountability• Streamlined processes deliver faster, more reliable resolutions |

Service Availability

The WithSecure Sample Validation service has defined availability hours for handling submitted requests.

Service Hours Business hours

Standard support only from Monday to Friday, 08:00–17:00 CEST.

Support is not available outside these times, on weekends, or on public holidays unless explicitly agreed otherwise.

Time Zone	Applicable time zone for service hours All stated service hours operate under the <i>Central European Summer Time (CEST)</i> time zone.
Support Channels	Where requests can be submitted All service requests must be created through the WithSecure Elements Security Center Portal. You can open a new request directly from the Requests page within the Elements portal.
Response Times	Target timeframe for initial acknowledgment WithSecure aims to acknowledge incoming requests within 24 hours during standard service hours. Actual resolution times may vary depending on the complexity and nature of the request.
Coverage Scope	Environments or regions included in the service The service is available globally and applies to all supported WithSecure Products. Support is limited to environments explicitly supported by WithSecure's product documentation.
Service Exceptions	Conditions where service may be limited or unavailable Conditions where service may be limited or unavailable. The request service does not include: • Investigation of security incidents or potential compromises • Forensic analysis or system recovery • Activities outside the scope of the submitted sample Requests involving configuration guidance or product-specific operational questions are handled by WithSecure Technical Support, not by the Sample Validation service. Additional limitations include: • Support is provided in English only • No phone calls, remote sessions, or direct system access • Assistance is delivered exclusively via comments in the request • Samples over 100 MB must be submitted via the Dropzone • A <i>valid vendor certificate</i> is required for allowlisting requests (see How to Request Whitelisting for details)
Escalation Process	Path for urgent or unresolved cases There is currently no formal escalation process. For updates, clarifications, or follow-ups, use the comment section in your existing request. The comments show the reference ID for your request. Include this ID in any related communication.

Service Delivery

The WithSecure Sample Validation service follows a defined delivery process for handling submitted requests.

Delivery Process	Steps or workflow for delivering the service Requests are submitted through the WithSecure Elements Security Center, where they are reviewed, validated, and analyzed by WithSecure experts. Throughout the investigation, all findings, updates, and final results are communicated within the same request, ensuring a clear and trackable audit trail. For more information, see Resolution.				
Roles and Responsibilities	Who is responsible for each part of the service <table border="0"> <tr> <td data-bbox="478 627 638 660">Customer</td><td data-bbox="638 627 1437 784"> - Submits samples or requests via the Elements Security Center. - Provides the necessary files, context, or supporting information to enable efficient analysis. </td></tr> <tr> <td data-bbox="478 806 638 840">WithSecure</td><td data-bbox="638 806 1437 929"> - Reviews and analyzes submitted materials. - Provides verdicts, detection updates, or guidance based on the findings. </td></tr> </table>	Customer	- Submits samples or requests via the Elements Security Center. - Provides the necessary files, context, or supporting information to enable efficient analysis.	WithSecure	- Reviews and analyzes submitted materials. - Provides verdicts, detection updates, or guidance based on the findings.
Customer	- Submits samples or requests via the Elements Security Center. - Provides the necessary files, context, or supporting information to enable efficient analysis.				
WithSecure	- Reviews and analyzes submitted materials. - Provides verdicts, detection updates, or guidance based on the findings.				
Service Channels	Where and how delivery takes place All requests and sample submissions are processed through the WithSecure Elements Security Center. For large files (over 100 MB) or extensive log collections, customers should use the secure Dropzone				
Tools and Systems Used	Platforms and systems supporting the service WithSecure uses internal analysis platforms, automated threat intelligence systems, and advanced detection technologies to review submissions. Final verdicts, detections, and updates are delivered through the WithSecure Security Cloud, including any relevant rules or virus definition updates. For more information, see Resolution.				
Communication and Updates	How and when customers receive updates You can track progress and view all communication directly within the Request details page in the Elements Security Center. All communication - status updates, clarifications, findings, and final outcomes - occurs within the request itself to maintain clarity and ensure complete record-keeping.				
Targeted Delivery Time	Expected timelines for investigation or resolution Typical analysis is completed within 2 hours to 5 business days, depending on the complexity, type, and size of the request or sample. All results and feedback are provided directly within the same request. For details, see Resolution.				
Dependencies	Requirements for effective service delivery				

To maintain efficient analysis and timely delivery, you must provide sufficient information, samples, or evidence with their initial submission.

If additional data is required - for example, when investigating a possible false negative - WithSecure will request the needed details through the same request thread.

Creating and viewing sample validation requests in the request views

Create sample validation requests for suspicious files, URLs, and email, and track their status in the request views.

From the request views you can submit new samples for validation, add comments to open requests, and follow each request through to resolution.

Choosing the correct Sample Type

Selecting the correct sample type when submitting a request ensures accurate analysis and faster resolution.

File Sample Type	Choose this category when the issue involves a file from a device.
File-Based False Positive	A clean file incorrectly detected as malware. For example: A company's internal tool flagged as a trojan.
Potentially Unwanted Application (PUA)	Legitimate software detected as unwanted. For example: A remote admin or adware-style installer used for business purposes.
File-Based False Negative	A malicious file not detected by the product. For example: A ransomware executable encrypts data without being blocked.
URL Sample Type	Choose this category when the issue involves a URL, website, or IP address.
URL-Based False Positive	A safe website is blocked by mistake. For example: <code>https://partnerportal.company.com</code> blocked as phishing.
URL Categorization	Request to update or correct the URL category. For example: Reclassifying a corporate blog from "Unknown" to "Business."
Unknown URL	A new or uncategorized domain requiring classification. For example: Submitting <code>https://newvendor.io</code> for review.
URL-Based False Negative	A harmful website is not blocked by the product. For example: <code>http://malicious-site.ru</code> remains accessible and serves malware.
Email Sample Type	Choose this category when the issue involves an email sample.
Phishing False Positive	A legitimate email incorrectly marked as phishing. For example: Vendor invoice emails flagged incorrectly.
Phishing False Negative	A phishing email not detected. For example: A spoofed Microsoft 365 login email reaches the inbox.
Email Attachment Not Detected	A malicious attachment is not detected by security products. For example: Unexpected ZIP/Invoice file requiring a password mentioned in the email.
Spam False Negative	Junk or promotional emails delivered to inbox.

Email Sample Type**Choose this category when the issue involves an email sample.**

For example: Promotional spam not filtered out.

Allowlisting Requests**Request Whitelisting****Choose this category for allowlisting tools, apps, or scripts.**

Request to whitelist legitimate tools, scripts, or applications - often during development. May require temporary security exceptions.

For example: WithSecure products block unsigned binaries, packers, automation scripts, or local dev servers, and adjustments are not feasible during early development stages.

Submit a file sample

Submit a file sample for validation in the Elements Security Center.

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, first select the appropriate **Customer company** using the *scope selector* located at the top of the Elements portal.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication



IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. Once the correct customer company has been selected, you can proceed to the **Requests** page to create or view **Sample Validation requests**.

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **File**

Make sure you selected the correct sample type for the file.

- File-Based False Positive: A clean file incorrectly detected as malware. For example, a company's internal tool flagged as a trojan.
- Potentially Unwanted Application (PUA): Legitimate software detected as unwanted. For example, a remote admin or adware-style installer used for business purposes.
- File-Based False Negative: A malicious file not detected by the product. For example, a ransomware executable encrypts data without being blocked.

6. Drag and drop the file or click **Browse** to upload the file
7. Open the **Request reason** drop-down menu and select one option:
 - a. False Positive - Clean file was blocked
 - b. False Negative - Malicious file not detected

- c. Potentially unwanted application detected
- d. Request whitelisting

8. Open the **Product name** drop down menu and select the product.
9. Add a short title for the request in the **Title** field.
10. Write down a description of the file or summary of concern.
11. Click **Create Request**.

The sample request is submitted to WithSecure.

Submit a URL sample

Submit a URL sample for validation in the Elements Security Center.

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, first select the appropriate customer company using the scope selector located at the top of the Elements portal.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication



IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. Once the correct customer company has been selected, you can proceed to the Requests page to create or view Sample Validation requests .

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **URL**.

Make sure you selected the correct sample type.

- URL-Based False Positive: A safe website is blocked by mistake. For example, `https://partnerportal.company.com` blocked as phishing.
- URL Categorization: Request to update or correct the URL category. For example, reclassifying a corporate blog from "Unknown" to "Business."
- Unknown URL: A new or uncategorized domain requiring classification. For example, submitting `https://newvendor.io` for review.
- URL-Based False Negative: A harmful website is not blocked by the product. For example, `http://malicious-site.ru` remains accessible and serves malware.

6. Enter URL or IP address.
7. Open the **Request reason** drop-down menu and select one option:
 - a. False Negative - Malicious URL not blocked
 - b. False Positive - Trusted URL blocked

- c. CAT - URL has incorrect content category
- d. CAT - M - URL missing content category

8. Open the **Product name** drop-down menu and select the product
9. Add a short title for the request in the **Title** field
10. Write down a description of the file or summary of concern.
11. Select **Create Request**.

The sample request is submitted to WithSecure.

Submit an email sample

Submit an email sample for validation in the Elements Security Center.

Make sure that you are using one of the supported browsers:

- Chrome
- Edge
- Firefox

Access from mobile devices is not supported.

If you are an administrator with Solution Provider (SOP) or Service Provider (SEP) level access, first select the appropriate customer company using the scope selector located at the top of the Elements portal.

The WithSecure Sample Validation service is located in the Elements Security Center portal:

- Logging in to non-federated domains
- Logging in to federated domains
- Multi-factor authentication



IMPORTANT: Sample Validation requests in the Elements portal are always created at the company level. Once the correct customer company has been selected, you can proceed to the **Requests** page to create or view **Sample Validation requests**.

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. Select **Create Request**.
4. Open the **Request type** drop-down menu and select **Submit sample for validation**
5. Open the **Sample type** drop-down menu and select **Email**.

Make sure you selected the correct sample type.

- Phishing False Positive: A legitimate email incorrectly marked as phishing. For example, vendor invoice emails flagged incorrectly.
- Phishing False Negative: A phishing email not detected. For example, a spoofed Microsoft 365 login email reaches the inbox.
- Email Attachment Not Detected: A malicious attachment is not detected by security products. For example, unexpected ZIP/Invoice file requiring a password mentioned in the email.
- Spam False Negative: Junk or promotional emails delivered to inbox. For example, promotional spam not filtered out.

6. Drag and drop the email file or click **Browse** to upload the email file
7. Open the **Request reason** drop-down menu and select one option:
 - a. False Positive - Legitimate email was blocked
 - b. False Negative - Phishing not detected

- c. False Negative - Spam not detected
- d. False Negative - Malicious email not detected

8. Open the **Product name** drop-down menu and select the product.
9. Add a short title for the request in the **Title** field.
10. Write down a description of the file or summary of concern.
11. Click **Create Request**.

The sample request is submitted to WithSecure.

Managing and viewing Open Requests

The Request view shows the dashboard fields, the request statuses, and the auto-reminder and automatic-closure rules for sample validation requests in Elements Security Center.

Request View / Dashboard Overview

In the Request view, you will find key information related to each submitted request such as:

Table 3: Request view fields

Field	Description
Title	A short, descriptive name that identifies the request.
Request Type	Indicates the type of request submitted, such as Sample Validation or Whitelisting.
Created At	The date and time when the request was originally submitted.
Updated At	The most recent date and time when the request was modified or a comment was added.
Status	Shows the current progress of the request (New, Acknowledged, In Progress, Waiting for Customer, or Closed).
Comments	Displays the number of comments exchanged during the handling of the request; opening the request reveals the full conversation.

Request Statuses and Descriptions

Each request includes a status that appears both in the **Status** column on the Requests page and within the request details.

The table below explains what each status means and how you should respond.

Table 4: Request status meanings

Status	What It Means	What You Should Do
New	We've received your request, and it is waiting to be acknowledged by the team.	No action needed - the request is now in the queue.

Status	What It Means	What You Should Do
Acknowledged	The team has seen your request and accepted it for handling. The scope of the request has been reviewed and confirmed to fall within the service scope, and a Malware Analyst has accepted it for processing.	No action needed - analysis will begin shortly.
In Progress	Our experts are actively analyzing your request.	No action required unless we contact you for additional information.
Waiting for Customer	We need more information to continue with the analysis.	Provide the requested details by replying within the request.
Closed	The request has been processed and completed.	No further action required - the request remains available for reference.

Auto-reminders and automatic Closure of Request

Reminder After 5 Days of Inactivity	If a sample submission request remains in Waiting for Customer status with no response for 5 days, an automatic reminder will be sent to the customer requesting the required information or samples.
Automatic Closure After 7 Days of Inactivity	If no customer response is received within 7 days while the request is in Waiting for Customer status, the ticket will be automatically closed.



IMPORTANT:

Closed requests cannot be reopened. If you need more help after a case closes, create a new support request.

Add and View Comments

Check your open requests and send comments to WithSecure from the Elements Security Center.

On the Requests page in the Elements Security Center, you can review your open requests and exchange comments with WithSecure.

1. Log in to the Elements Security Center Portal
2. Go the **Requests** page on the menu on the left
3. On the Requests page you can:
 - check when the request was last updated from the **Updated at** column
 - check if the request has any comments from the **Comments** column . If a request has comments, the **Comments** column will show how many comments the request has.



NOTE: To see the comments, either select the number in the **Comments** column or select the title of the request to open it and see all the comments. To send a new comment, go to the field at the bottom of the **Comments** tab and select **Send Comment**.



IMPORTANT: Screenshots or any other files cannot be added to comments, and comments added to closed requests are not reviewed by WithSecure.

Resolution

While the selected **reason for submission** helps guide the investigation, verdicts are not assigned automatically. The final verdict always reflects the outcome of the analysis.

Example:

If a request is submitted as "clean app was blocked" but the analysis confirms the file is not clean, the verdict will not be changed to "clean."

How Endpoints Receive Updated Verdicts

Security Cloud Engine

All submissions receive a verdict through the WithSecure Security Cloud. If an incorrect verdict has been cached on an endpoint, the device will automatically refresh the verdict once the *cache TTL (time-to-live)* expires.

- If Security Cloud initially returned an incorrect verdict, the endpoint may continue blocking the file until the cached verdict expires.
- To speed up correction, we recommend clearing the WithSecure reputation cache on the affected device.

Local Virus Definitions

Detection updates are also delivered through local virus definition updates.

These updates are distributed automatically to endpoints as soon as new versions are available.

There is no SLA for engine or definition release timing, as updates are published continuously based on threat intelligence findings.

Support and escalations

When you encounter issues with the WithSecure Sample Validation service, choose the correct channel for reporting them or obtaining assistance.

Table 5: Support escalation channels

Issue	Channel to report
Login issues	Contact WithSecure support.
User interface front-end issues	Contact WithSecure support.
Request investigation	Use the comments under your requests in Elements.
Suspected major false positive	Contact WithSecure support.

Other submissions

Some WithSecure products let you report false positives and false negatives directly from the product user interface.

Examples of products and interfaces that support in-product reporting include:

- WithSecure Cloud Protection for Salesforce Analytics
Provides reporting capabilities for false positives and false negatives directly within the analytics dashboard.
- Report False Positive from Elements Security Events
Allows administrators to submit false positive reports directly from the **Security Events** view in the Elements Portal.
- In-Product False Positive Reporting

Some WithSecure products include dedicated **Report False Positive** options within their user interfaces—for example:

- Browsing Protection
- Quarantine views or dialogs

These options enable quick submission of incorrectly detected files, URLs, or events without leaving the product.



NOTE:

The built-in reporting samples are processed by the same Sample Validation service. However, users will not receive feedback, status updates, or tracking details for these submissions. Despite the lack of visibility, all reported samples are handled with the same priority and care as requests submitted through the Elements portal.

8.1.4 Best practices for gathering samples and reporting ransomware

In this section you will find the instructions for a safe file sample gathering for WithSecure Sample Validation Request Service.

This section explains how to gather file, URL, and email samples safely on each platform, and how to report ransomware or active threats that were not detected.

Gathering file samples

Collect file samples for submission to the WithSecure Sample Validation service on Windows, Linux, macOS, and Android.

Choose the procedure for your platform to safely collect and package a file sample for submission.

Gather a File Sample for Windows

Collect a file sample on Windows and submit it for validation in the Elements Security Center.

Before you submit a suspicious file to WithSecure, package it in a password-protected archive so security analysts can handle it safely.

1. Find the file you want to submit
2. Right-click the file **Send to > Compressed (zipped) folder**.
3. Open the ZIP file and **add a password: infected**

You can do this using tools like 7-Zip or WinRAR)

4. When creating a **new Request** in Elements Security Center, attach the ZIP file
5. If the file is larger than the upload limit, upload it via the Dropzone

Remember to still create a request in Elements and include in a comment that the sample was sent via Dropzone.

- Always use the password **infected** — this ensures safe handling by security analysts.
- Never email the file directly. Always upload it through Elements Security Center or the Dropzone in case of sample being larger than 100MB
- Include as much context as possible (where the file came from, what it does, and why you're submitting it).

Gather a File Sample for macOS

Collect a file sample on macOS and submit it for validation in the Elements Security Center.

Before you submit a suspicious file to WithSecure, package it in a password-protected archive so security analysts can handle it safely.

1. Locate the file in Finder
2. Right-click **Compress "[filename]"** to create a ZIP archive.
3. Use terminal or a tool like Keka to add a password: `infected`

Example Terminal Command:

```
zip -e sample.zip /path/to/file
```

4. When creating a **new Request** in Elements Security Center, attach the ZIP file
5. If the file is larger than the upload limit, upload it via the Dropzone

Remember to still create a request in Elements and include in a comment that the sample was sent via Dropzone.

- Always use the password `infected` - this ensures safe handling by security analysts.
- Never email the file directly. Always upload it through Elements Security Center or the Dropzone in case of sample being larger than 100MB
- Include as much context as possible (where the file came from, what it does, and why you're submitting it).

Gather a File Sample for Linux

Collect a file sample on Linux and submit it for validation in the Elements Security Center.

Before you submit a suspicious file to WithSecure, package it in a password-protected archive so security analysts can handle it safely.

1. Locate the file you want to submit
2. Open **Terminal** and run:

```
zip -e sample.zip /path/to/file
```

When prompted, enter the password: `infected`

3. When creating a **new Request** in Elements Security Center, attach the ZIP file
4. If the file is larger than the upload limit, upload it via the Dropzone

Remember to still create a request in Elements and include in a comment that the sample was sent via Dropzone.

- Always use the password `infected` - this ensures safe handling by security analysts.
- Never email the file directly. Always upload it through Elements Security Center or the Dropzone in case of sample being larger than 100MB
- Include as much context as possible (where the file came from, what it does, and why you're submitting it).

Collect quarantined files using Quarantine Dumper Tool

Collect quarantined files with the WithSecure Quarantine Dumper tool so you can submit them for validation.

The WithSecure Quarantine Dumper is a command-line tool that gathers quarantined files into a password-protected archive for submission.

1. Download the tool and save it to a location of your choice, for example `c:\temp`:

- 32bit version
- 64bit version:

2. Launch Command Prompt (CMD)

3. Navigate the directory to the location you selected in step 1.

For example, type `cd c:\temp\` and press Enter on your keyboard to go to `c:\temp\` folder.

4. Type `wsdumpqrt.exe -d c:\temp\` to run the tool.

5. Enter your administrator credentials when prompted. WithSecure license terms are now shown.

6. Scroll all the way to the end of the license terms before you can accept them.

7. Press E on your keyboard to accept the license terms.

8. Press any key to complete the run.

The quarantined files will be collected in a file named `malware_samples.zip` with the default password infected in the location you specified in step 1. These are the parameters that can be used in the tool:

- `-d, --destination`: Destination directory for output (default: current admin desktop)
- `-p, --password`: Password for output (default: "infected")
- `-v, --verbose`: Verbose output
- `-a, --accept-eula`: Accept EULA
- `-s, --silent`: Silent mode
- `-l, --list`: Only list contents, nothing is written to disk



TIP: Running the `wsdumpqrt.exe` tool in command prompt without additional command line parameters will print out a short tool description and the extra parameters for using the tool.

Gathering URL samples

Collect URL samples for submission to the WithSecure Sample Validation service on Windows, Linux, and macOS.

Choose the procedure for your platform to capture and package a URL sample for submission.

Gather a URL sample for Windows

Collect a URL sample on Windows and submit it for validation in the Elements Security Center.

Copy or paste the exact URL rather than clicking it, so analysts can assess the link without exposing your device to risk.

1. Copy the exact URL from your browser's address bar or from the email/message where it appeared.
2. If available, also collect the full email header that contained the URL (for phishing cases).
3. Paste the URL and a short description of its behavior (e.g., "Phishing site not blocked" or "Suspicious download link") into your **new Request** in Elements Security Center.
4. If the URL is inside an email, save that email as a `.msg` or `.eml` file and attach it to your request.
 - Always include the complete URL, even if it's long.



WARNING: Do not click suspicious links before or after collecting them.

- Provide context (where you saw it, what happened, and which product didn't block it).
- If the URL was part of a large email sample or multiple links, you can upload related files (like `.eml`) through the Customer Protection Dropzone: Dropzone.

Example:

1. `https://maliciousdomain.net/login.php`
2. Behavior: Phishing page not blocked by Elements Agent

Gather a URL sample for macOS

Collect a URL sample on macOS and submit it for validation in the Elements Security Center.

Copy or paste the exact URL rather than clicking it, so analysts can assess the link without exposing your device to risk.

1. Right-click or copy the link directly from Safari, mail or another app.
 2. Paste the exact URL into your **new Request** in Elements Security Center.
 3. Add a short note describing what you observed (for example, Leads to fake login page).
 4. If it came from an email, save the message as an .eml file:
 - a) In Mail: select the email **File > Save As... > Format: Raw Message Source (.eml)**.
 - b) Then attach that file to your request.
- Always include the complete URL, even if it's long.



WARNING: Do not click suspicious links before or after collecting them.

- Provide context (where you saw it, what happened, and which product didn't block it).
- If the URL was part of a large email sample or multiple links, you can upload related files (like .eml) through the Customer Protection Dropzone: Dropzone

Example:

1. `https://maliciousdomain.net/login.php`
2. Behavior: Phishing page not blocked by Elements Agent

Gather a URL sample for Linux

Collect a URL sample on Linux and submit it for validation in the Elements Security Center.

Copy or paste the exact URL rather than clicking it, so analysts can assess the link without exposing your device to risk.

1. Right-click or copy the link directly from Safari, mail or another app.
2. Paste the exact URL into your **new Request** in Elements Security Center.
3. Add a short note describing what you observed (for example, Leads to fake login page).
4. If it came from an email, save the message as an .eml file and attach it to your request.

Example:

(Thunderbird): **File > Save > As > File (eml)**.

- Always include the complete URL, even if it's long.



WARNING: Do not click suspicious links before or after collecting them.

- Provide context (where you saw it, what happened, and which product didn't block it).
- If the URL was part of a large email sample or multiple links, you can upload related files (like .eml) through the Customer Protection Dropzone: Dropzone

Example:

1. `https://maliciousdomain.net/login.php`
2. Behavior: Phishing page not blocked by Elements Agent

Gathering email samples

Collect email samples for submission to the WithSecure Sample Validation service on Windows, Linux, and macOS.

Choose the procedure for your platform to export and package an email sample for submission.

Gather an Email Sample for Windows

Collect an email sample on Windows and submit it for validation in the Elements Security Center.

Save the suspicious email as a file rather than forwarding it, so its technical headers are preserved for analysis.

1. Open the suspicious email in **Outlook** or your mail client.
2. Save the message as .msg or .eml file.
 - In **Outlook desktop**: open the email **File > Save As > Outlook Message Format (.msg)**.
 - In **Outlook Web**: open the message and select **View message details** and copy or download the **full headers**, if available.
3. When creating a **new Request** in Elements Security Center, attach your email file
4. Include any relevant details, such as the **subject line**, **sender address** and a short note about what you observed (e.g. Phishing email not detected by Elements Agent).
 - Always save and attach the email as a file (.eml or .msg) — do not forward it. Forwarding can remove important technical headers that are needed for analysis.
 - Include any context: how you received it, if you clicked any links, and whether any alerts appeared.
 - For large attachments or multiple samples, use the Customer Protection Dropzone and mention it in your request: Dropzone

Example submission

```
Subject: Invoice due today
From: billing@fakevendor.com
Attachment: invoice_8845.zip
Behavior: Suspicious attachment not detected by Elements Agent
```

Gather an Email Sample for macOS

Collect an email sample on macOS and submit it for validation in the Elements Security Center.

Save the suspicious email as a file rather than forwarding it, so its technical headers are preserved for analysis.

1. Open the suspicious email in the Mail app.
2. Select the email, then click **File > Save As...**
3. When creating a **new Request** in Elements Security Center, attach your saved .eml file.
4. Include any relevant details, such as the **subject line**, **sender address** and a short note about what you observed (e.g. Fake invoice email with suspicious link).
 - Always save and attach the email as a file (.eml or .msg) — do not forward it. Forwarding can remove important technical headers that are needed for analysis.
 - Include any context: how you received it, if you clicked any links, and whether any alerts appeared.
 - For large attachments or multiple samples, use the Customer Protection Dropzone and mention it in your request: Dropzone.

Example submission

Subject: Invoice due today
 From: billing@fakevendor.com
 Attachment: invoice_8845.zip
 Behavior: Suspicious attachment not detected by Elements Agent

Gather an Email Sample for Linux

Collect an email sample on Linux and submit it for validation in the Elements Security Center.

Save the suspicious email as a file rather than forwarding it, so its technical headers are preserved for analysis.

1. Open the suspicious email in the Mail app (for example: **Thunderbird** or **Evolution**).
2. Save the message as an .eml file.
 - In **Thunderbird**:: Select the email, then click **File > Save As... > File..**
3. When creating a **new Request** in Elements Security Center, attach your saved .eml file.
4. Include any relevant details, such as the **subject line**, **sender address** and a short note about what you observed (e.g. Attachment attempts to download a file).
 - Always save and attach the email as a file (.eml or .msg) — do not forward it. Forwarding can remove important technical headers that are needed for analysis.
 - Include any context: how you received it, if you clicked any links, and whether any alerts appeared.
 - For large attachments or multiple samples, use the Customer Protection Dropzone and mention it in your request: Dropzone.

Example submission

Subject: Invoice due today
 From: billing@fakevendor.com
 Attachment: invoice_8845.zip
 Behavior: Suspicious attachment not detected by Elements Agent

Report application recognized as malicious (Android)

If WithSecure Mobile Protection flags an application as malicious and you suspect a false positive, take a screenshot of the **Infection details** page and submit it as a file sample for review.

View the infection details page in the WithSecure Mobile Protection app.

1. Open the **WithSecure Mobile Protection** application.
2. Open the **Malware Protection** section.
3. Click **See full scan history**.
4. Click on the detection that has the malicious application.
5. In the Infections section, click on the name of the application.

A window will open with the following details:

- App name
- Package name
- Problems detected

- Size

6. Take a screenshot of the window and submit it as a file sample using Submit a file sample on page 52. In the description field of the submission, note that the attached screenshot shows the details of the Android application.

Reporting ransomware or active threats (no detection observed)

In this section you will find guidance how to report ransomware or another active threat where no detection has been observed.

Follow this guidance to report ransomware or another active threat on Windows, macOS, or Linux when your WithSecure product did not raise a detection, including the information to include in your report.

Report Ransomware or Active Threats (No Detection Observed) Windows

Gather diagnostic information when WithSecure has not detected or blocked suspected ransomware or another active threat on a Windows system.

If you suspect ransomware or another active threat on a Windows device that WithSecure has not detected, act immediately to contain it and report it.

1. Immediately isolate the affected system from the network to prevent the threat from spreading.
2. Locate and collect a sample of the suspicious file, script, or process if possible (e.g. the ransomware executable, encrypted file, or note).
3. Do not attempt to run or analyze the file yourself.
4. Compress the file into a ZIP archive and password-protect it using the password: `infected`.
5. Submit the sample through a **new Request** in Elements Security Center.
6. Include clear details, such as:
 - When and how the threat appeared.
 - What actions were taken by Elements (if any).
7. If the sample size exceeds upload limits, submit it via the Dropzone and include the link in your request.

Report Ransomware or Active Threats (No Detection Observed) macOS/Linux

Gather diagnostic information when WithSecure has not detected or blocked suspected ransomware or another active threat on a macOS or Linux system.

If you suspect ransomware or another active threat on a macOS or Linux device that WithSecure has not detected, act immediately to contain it and report it.

1. Immediately isolate the affected device from the network (unplug Ethernet, turn off Wi-Fi).
2. Identify the suspicious file or process (for example, ransomware binary, dropped file, or ransom note).
3. Compress it into a ZIP archive and password-protect it using the password: `infected`.

Example command

```
zip -e sample.zip /path/to/suspicious/file
```

4. Submit the sample through a **new Request** in Elements Security Center.
5. If the sample size exceeds upload limits, submit it via the Dropzone and include the link in your request.

Provide information for ransomware reporting

Provide the information and files WithSecure needs to investigate your ransomware case thoroughly.

Providing complete data will speed up our analysis and response.

1. Describe the Incident.

In your **Request description** in Elements Security Center, include:

What happened	Describe the situation in detail (e.g., files encrypted, ransom note shown, system slowdowns, alerts triggered, etc.).
When it happened	Provide the exact date and time you first noticed the issue.
Where it happened	Mention the affected device(s) or system(s).

Example: Files in the shared drive were encrypted around 10:45 on 2 November.

A ransom note named "README.txt" appeared on all desktops.

2. Collect the suspicious sample.

We need a sample of the suspicious file (ransomware executable, script or note). Without this, we cannot proceed with the analysis.

- Locate the suspicious file.
- Compress it into a ZIP file.
- Password-protect it using the password: `infected`
- Keep the ZIP file ready. You'll upload it together with your other diagnostic files via Dropzone.

3. Generate WSDIAG (Diagnostic) Logs

Follow the instructions for your operating system:

- Windows: How to create or generate a WSDIAG diagnostics file on a Windows computer?
- macOS: How do I generate WSDiag diagnostic logs on WithSecure Mac products?
- Linux: How do I create an FSDIAG file on Linux systems?

4. Create additional Diagnostic Files

a) Autoruns Log:

- Download: Autoruns
- Run the tool and enable **Hide Signed Microsoft Entries**
- Save the results as `autoruns.arn` on your Desktop.

b) Process Explorer Log

- Download Process Explorer
- Extract the ZIP and run `procexp.exe` as **Administrator**.
- Go to **File > Save** and save the file as `procexp.txt` on your Desktop.

5. Upload All Files via Dropzone

- Rename your diagnostic ZIP file (e.g. `wsdiag_customername.zip`) for easier identification.
- Place the sample file in a password-protected ZIP (`infected`).
- Upload all required files (WSDIAG, sample, `autoruns.arn`, `procexp.txt`) to Dropzone and include the link in your request.

What happens next:

- The WithSecure team will analyze the sample and determine, if it represents a new or undetected threat.
- If detection is missing, a new detection signature or rule will be created and published via Security Cloud updates.
- You'll receive feedback and results directly within your Elements Request.

**IMPORTANT:**

- Do not forward suspicious files or ransomware notes by email. Always use Elements Security Center or the Dropzone for safe submission.
- For widespread or critical infections, immediately contact your security team or incident response lead before submitting the request.
- This service does not include full forensic or incident response, but your report helps improve detection coverage.

**NOTE:**

- Each submission generates a **Reference ID** and status updates.
- Use the **Request History** to monitor progress and respond to analyst feedback.
- Analysts may request additional samples or logs for validation.
- Always use the correct issue type for faster handling.
- Provide full context (file path, environment, observed behavior).
- Keep portal communication active - replies and updates speed up analysis.



WARNING: Never send live malware unprotected. Always use ZIP + password infected

Chapter 9

AI Security

Topics:

- View the AI Security dashboard
- AI software in the software inventory
- AI and agentic identities

AI Security

WithSecure Elements AI Security identifies AI use in the managed organization and lets you control which AI software is approved for use.

Users can introduce AI tools without security administrators' knowledge. This is known as shadow AI. Shadow AI creates a blind spot because security administrators cannot protect access or data that they do not know exists. AI agents also use non-human identities, such as service accounts, to access systems. These are called agentic identities. AI Security helps you discover this software and these identities in the managed organization.

The **AI Security** page shows a summary of the AI software and agentic identities detected in the managed organization.



IMPORTANT: AI Security is available as an Early Access feature for a limited time, for eligible WithSecure Elements subscribers. It is enabled automatically; no installation is required.

Eligible subscriptions

AI Security is available with the following subscriptions:

AI tool visibility	Elements Protect and Proactive bundles, Elements EDR, or Elements XM for Business, Users, and Devices.
Agentic identity visibility	Elements Protect and Proactive bundles, Elements XM for Business, Users, and Identities, or Elements Identity Security (XDR).

9.1 View the AI Security dashboard

You can view a summary of the AI software and AI agent identities detected in the managed organization on the **AI Security** page.

To view the AI Security dashboard:

Under **Environment**, select **AI Security** on the sidebar.

*The **AI Security** page opens.*

The dashboard is composed of multiple sections, each presenting a different aspect of AI asset and AI agent identity data.

Summary	States how many AI items are banned in the managed organization, and on how many devices AI software is present.
AI asset counts	Figures show the total number of different AI assets detected, how many are banned, and how many devices run banned AI software.
Devices with the most blocked AI items	Lists the devices with the highest number of banned AI assets, sorted by banned asset count. Devices with no banned assets are not shown.
Most common AI software	Lists AI software ranked by device count, together with its delivery type, review status, and the number of devices where it is present. Delivery type is one of the following: • AI-native software – a standalone AI application. • Embedded AI – AI functionality embedded in other software.
AI agent identities in your environment	Lists the AI agent identities that are registered in Microsoft Entra ID for the managed organization, together with their permission scope, creation date, and review status.

AI assets by type	Shows the AI software detected for the managed organization, broken down by delivery type and by category, such as AI chat assistant , AI agent , and AI coding assistant .
Approval status breakdown	Shows how the managed organization's AI items are distributed across each review status.



NOTE: Alternatively, go to **My report** under **Reports**, open **View template**, and select **AI Dashboard** to view the summary as a report.

9.2 AI software in the software inventory

You can filter the **Software** page to list all AI software used in the managed organization and control which is approved or banned.

By default, the **Software** page lists all software installed across the managed organization. The **Show AI assets** filter narrows the list to AI tools only, including ones that do not need a full installation, such as browser extensions.



NOTE: AI assets are different from the *Artificial Intelligence* category in Web content control (under **Profile Manager**), which blocks access to AI-related websites. AI asset visibility covers installed AI software and browser extensions.

9.2.1 View AI assets in the software inventory

You can view and filter the AI software used across the managed organization in the software inventory.

By default, the **Software** page lists all software installed across the managed organization.

To view the AI assets in the managed organization:

1. Under **Environment**, select **Software** on the sidebar.
*The **Software** page opens.*
2. Select the **Device software** tab.
3. Select **Show AI assets**.
*The table is filtered to AI software only, using the **Category** filter.*
4. To narrow the list further, select specific categories in the **Category** filter.
5. To view the devices where a specific AI asset is used, select its name in the **Software Name** column.
A details page opens, showing the devices where the software is present and their software versions.

The table lists each AI asset with its version, vendor, platform, known CVEs, review status, and the number of devices where it is present.

Each AI asset is placed in one of the following categories:

AI Chat Assistant	A general-purpose conversational AI tool, such as ChatGPT or Claude.
AI Coding Assistant	An AI tool built specifically to help write, review, or debug code, such as Claude Code.
Generative AI Tool	A tool that generates text, images, or other content from a prompt, without a dedicated chat or coding interface.
AI Agent	Software that carries out tasks on the user's behalf within a defined scope, such as an AI feature embedded in productivity software.
AI Autonomous Agent	An AI agent that plans and takes multiple actions toward a goal, with limited human confirmation at each step.

Unspecified AI Application An application confirmed to use AI capabilities, but not yet classified into one of the other categories.

9.2.2 Approve or ban an AI asset

You can approve or ban the AI software found in the managed organization's software inventory.

You are on the **Software** page, viewing the AI assets you want to approve or ban.

Each AI asset has a review status:

Not reviewed	The default status for a newly discovered AI asset.
Approved	You have reviewed the AI asset and allow its use.
Banned	You have reviewed the AI asset and do not allow its use.



NOTE: Review status is set separately for each organization. The same software can be approved in one organization and banned in another.

To approve or ban an AI asset:

1. On the **Software** page, select the checkbox of the AI asset (or assets) whose status you want to change.
A bar showing the number of selected AI assets appears at the bottom of the page.
2. Select one of the following actions.
 - Select **Set to approved...** to allow the AI asset.
 - Select **Set to banned...** to block the AI asset.
 - Select **Clear status...** to return the AI asset to **Not reviewed**.

The status of the selected AI assets changes immediately.

The **Status** column shows the new status for the selected AI assets.

9.3 AI and agentic identities

WithSecure Elements identifies AI agents, assistants, and other AI-driven identities in the managed organization.

AI tools, agents, and integrations often create their own identities, such as service accounts or access tokens, when they connect to your systems.

WithSecure Elements identifies AI and agentic identities through Microsoft Entra ID service principals. The following identity types are covered:

AI agents	A service principal created for software that performs tasks in the managed organization's systems on its own.
AI chat assistants	A service principal created when a conversational AI tool connects to organizational data or services.
AI coding assistants	A service principal created when an AI tool built for writing or reviewing code connects to development systems.
Generative AI tools	A service principal created when a content-generation tool connects to organizational data.

These identities are listed in the **AI agent identities in your environment** table on the **AI Security** page. The table also shows each identity's permission scope, creation date, and review status.



Chapter 10

Elevate Requests

Topics:

- Create a request
- View and manage request details

Elevate Requests

With Elevate Requests, WithSecure™ Elements Infinite customers can raise security concerns directly to WithSecure experts for investigation and track each request in the Elements Security Center.

WithSecure™ Elements Infinite includes Elevate Requests, a service that lets you raise a security concern or a question about your service directly to WithSecure experts. WithSecure security experts, including the Detection and Response Team (DRT), investigate each request and keep you updated in the Elements Security Center.

Use Elevate Requests for security concerns and service questions, including issues that have not triggered a detection. Elevate Requests are not a channel for technical support with installing or troubleshooting WithSecure products.

When you create a request, you select a request type and describe your concern. After you submit the request, you can track its status and exchange comments with WithSecure in the Requests view of the Elements Security Center.

10.1 Create a request

Create a request in the Elements Security Center to ask WithSecure experts to investigate a security concern.

The **Requests** feature is available only for the Company scope. Before you start, select the correct company scope in the top bar.

1. Go to **Requests** on the left-side menu.
2. Select **Create Request** at the top of the main page.
A flyout panel opens.
3. Select the **Request Type** from the drop-down list.
4. Enter the required details:
 - **Organization ID**
 - **Device UUID/name**
 - **Title**
 - **Description/Summary of concern**
5. Select **Create Request** to submit the request.

10.2 View and manage request details

Open a request in the Elements Security Center to check its status and exchange comments with WithSecure.

1. Go to **Requests**.
The main page shows all requests for the managed organization in a table. Each row shows key details such as:
 - **Title**
 - **Request Type**
 - **Created/Updated dates**
 - **Status**
2. Use the filters to find a specific request.
3. Select the value in the **Title** field to open the details of a request.

The details page shows the **Status**, **Request Type**, created and updated timestamps, title, description, and other metadata.

4. Open the **Comments** tab on the details page to view the full comment thread for the request.
Comments from the WithSecure team appear on the right side with a **WithSecure** label.
5. To add a comment, type your message in the field at the bottom of the **Comments** tab and select **Send Comment**.

Chapter 11

Third-party integrations

Topics:

- Integrating WithSecure Elements with Autotask PSA
- Integrating WithSecure Elements with ConnectWise PSA
- Integrating WithSecure Elements with HaloPSA

Third-party integrations

WithSecure Elements integrates with Autotask, ConnectWise, and Halo professional services automation (PSA) platforms.

Each of these PSA systems includes its own ticketing functionality. The integration allows Elements to exchange ticket information with them.

High-level company-mapping process works as follows:

1. Enabling the integration and opening the mapping view - After entering your PSA API credentials and activating the integration, go to **Management > Integrations** in Elements Security Center. On the enabled integrations card, select **Company mappings**.
2. Matching PSA companies to Elements organizations - A table shows all companies retrieved from your PSA system. For each PSA company, select the corresponding Elements organization from the dropdown list.
3. Saving the mapping to activate the ticket flow - When all required mappings are complete, select **Save**. This enables ticket synchronization for every mapped organization.

11.1 Integrating WithSecure Elements with Autotask PSA

Overview of the Autotask PSA integration with WithSecure Elements for managed service providers (MSPs).

WithSecure Elements provides a built-in integration with Autotask PSA to help MSPs automate cybersecurity workflows. The integration supports Advanced Endpoint Protection, Exposure Management, Extended Detection and Response (XDR), and Managed Detection and Response (MDR) services through the WithSecure Elements Cloud platform.

The integration enables a comprehensive, multi-tenant, and single-agent solution. where security events in Elements automatically generate tickets in Autotask PSA. These tickets include deep links back to detailed information in Elements Security Center.

Configuration is performed centrally in Elements Security Center. It uses Autotask API credentials to establish a secure connection and to map customer accounts for automated ticket creation.

11.1.1 Get integration credentials from Autotask

To integrate Autotask PSA with WithSecure Elements, you must create an API user in Autotask PSA and collect the required credentials.

Make sure that you have administrator access to the Autotask PSA management console.

1. Log in to the Autotask PSA management console at the Autotask website.
2. In the navigation panel, select **Admin**.
3. Under **Admin categories**, select **Organization settings and users**.
4. Open **Resources/Users (HR)** and select **Resources/Users**.
5. From the **New** dropdown list, select **New API User**.
6. In new **Add API user** popup window, fill the required general settings, such as names and email address.



NOTE: Selecting **API user (system) Can't Read Costs** from the Security Level options is sufficient.

7. Under **Credentials**, select **Generate key** and **Generate secret**.
8. Copy the key and secret that you want to use in Elements Security Center.

9. Under **API Tracking Identifier**, select **Integration vendor**, then select **WithSecure**.

10. Select **Save & Close**.

The following credentials are required when configuring the integration in Elements Security Center:

- API username/key
- API password/secret

11.1.2 Configure Autotask PSA integration in Elements Security Center

You can connect WithSecure Elements to Autotask PSA using API credentials and by selecting the ticket queue for automated tickets.

Make sure that you have valid Autotask API credentials and access to Elements Security Center.

To configure the Autotask integration:

1. Log in to Elements Security Center.
2. Go to **Managements > Integrations**.
3. Under **Available PSA/RMM Integrations**, select **Configure** next to Autotask.
The Autotask integration pane opens.
4. In the **Connect** view, enter the API username and API password that you copied from Autotask management console.
5. Select **Connect** to validate the connection and load Autotask queue definitions.
6. Select the queue where you want WithSecure Elements to create tickets and select **Save**.

The integration is now active. After completing these steps and finishing the company mapping, events generated in Elements automatically create tickets in Autotask PSA. The tickets appear in Autotask PSA with the essential details about the related Elements activity and include deep links to Elements Security Center.

11.2 Integrating WithSecure Elements with ConnectWise PSA

Overview of the integration between WithSecure Elements and ConnectWise PSA for managed service providers (MSPs).

WithSecure Elements provides a built-in integration with ConnectWise PSA to help MSPs automate cybersecurity workflows. The integration supports multi-tenant environments and enables automated ticket creation for events that are originating from Elements Security Center.

This integration helps MSPs streamline delivery of services such as Advanced Endpoint Protection, Exposure Management, Extended Detection and Response (XDR), and Managed Detection and Response (MDR). It uses API keys that are generated in the ConnectWise PSA management console and configuration settings that are applied in Elements Security Center.

You can use the integration to accomplish the following:

- Automated ticket creation in ConnectWise PSA based on Elements activity
- Support for multi-tenant MSP environments
- Centralized configuration within Elements Security Center
- Linking customer accounts using ConnectWise company identifiers

11.2.1 Configure ConnectWise PSA integration in Elements Security Center

You can connect WithSecure Elements to ConnectWise PSA by generating API keys in ConnectWise and applying the configuration in Elements Security Center to enable automated ticket creation and customer mapping across multi-tenant environments.

Administrator access to the ConnectWise PSA management console is required to configure the integration.

To configure the ConnectWise PSA integration:

1. In the ConnectWise PSA management console, generate API keys as follows:
 - a) Open the user menu and select **My Account**.
 - b) Select the **API Keys** tab and select the + icon to create a new API key.
 - c) Enter a description, for example, WithSecure Elements.
 - d) Save the entry to generate the public and private keys.
 - e) Copy both keys for later use.
2. Collect the following required information for Elements Security Center:
 - Company ID used to log in to ConnectWise PSA
 - Public API key
3. In Elements Security Center, go to **Management > Integrations**.
4. Under **My Configured Services**, next to **ConnectWise PSA**, select **Configure integration**.
The **ConnectWise Integration** pane opens.
5. Configure the settings as follows:
 - a) From the drop-down menu, select the correct tenant.



NOTE: It is the same as your ConnectWise PSA management console URL

- b) Enter the company ID.



NOTE: It is the same as your ConnectWise PSA management console company ID.

- c) Enter the public and private API keys.
- d) Select **Connect** to validate connectivity.
- e) Save the configuration.

The integration is now active. After completing these steps and finishing the company mapping, events generated in Elements automatically create tickets in ConnectWise PSA. The tickets appear in ConnectWise PSA with the essential details about the related Elements activity and include deep links to Elements Security Center.

11.3 Integrating WithSecure Elements with HaloPSA

Overview of the HaloPSA integration with WithSecure Elements for managed service providers (MSPs).

WithSecure Elements provides a built-in integration with HaloPSA, enabling automated ticket creation and streamlined service workflows for MSPs. This integration helps unify cybersecurity operations across multiple customer environments.

This integration helps MSPs streamline delivery of services such as Advanced Endpoint Protection, Exposure Management, Extended Detection and Response (XDR), and Managed Detection and Response (MDR). The integration uses API credentials that are created in HaloPSA and configuration settings that are applied in Elements Security Center.

You can use the integration to accomplish the following:

- Automated ticket creation in HaloPSA based on Elements activity
- Support for multi-tenant MSP environments
- Centralized configuration within Elements Security Center
- Linking customer accounts using HaloPSA reference IDs

11.3.1 Configure HaloPSA integration in Elements Security Center

You can connect WithSecure Elements to HaloPSA creating API credentials and configuring the integration.

To configure the HaloPSA integration:

1. Create API credentials in HaloPSA as follows:
 - a) Log in to your HaloPSA account.
 - b) Go to **Configurations > Integrations**.
 - c) Select **HaloPSA API**.
 - d) Under **Applications**, select **View applications**.
 - e) At the top-right corner, select **+New** and enter a name, for example, WithSecure Elements.
 - f) Make sure that the application is marked as active.
 - g) Select **Client ID and secret** as the authentication method.
 - h) Copy the generated Client ID and Client Secret.
 - i) Set login type to **Agent** and select the agent identity used for ticket creation.
2. In Elements Security Center, go to **Management > Integrations**
3. Under **My Configured Services**, next to **HaloPSA**, select **Configure integration**.
The HaloPSA Integration pane opens.
4. Configure the settings as follows:
 - a) Enter the HaloPSA tenant URL.
 - b) Enter the client ID and client secret from HaloPSA.
 - c) Select **Connect** to validate connectivity.
 - d) Save the configuration.

The integration is now active. After completing these steps and finishing the company mapping, events generated in Elements automatically create tickets in HaloPSA. The tickets appear in HaloPSA with the essential details about the related Elements activity and include deep links to Elements Security Center.

Appendix **A**

Access control

Topics:

- Core concepts
- Planning your deployment
- Managing security administrators
- Setting up Microsoft Entra ID integration
- Migrating to Elements RBAC
- RBAC reference

Access control

Elements Role-Based Access Control (RBAC) is the access management system for WithSecure Elements Security Center, controlling who can access the portal, what actions they can perform, and which organizational resources they can manage.

Elements RBAC is a new access control approach under **Management > Access Control**. For standard user and access control configuration, see the User management chapter.

Elements RBAC implements an industry-standard role-based access control model that links three components:

Subject	Who gets access (a security administrator or a security group).
Role	What permissions are granted (a set of allowed actions, such as can manage users or can view vulnerability reports).
Resource	Where the permissions apply (always an organization in Elements).

Elements RBAC supports a multi-tenant architecture in which three parties interact:

- WithSecure develops and maintains the Elements Security Center platform.
- Partners, typically Managed Service Providers (MSPs), resell WithSecure Elements and provide security services to multiple customers.
- Companies are end customers that use Elements to protect their IT infrastructure.

Elements RBAC addresses the unique challenges of the partner-customer model by allowing partners to manage hundreds of customer environments efficiently while maintaining strict security boundaries between them.

A.1 Core concepts

Elements RBAC builds on a small set of core concepts: organizations, security administrators, security groups, roles, and role assignments.

These topics define the building blocks of Elements RBAC. Read them in order the first time, then return to them as a reference when you set up your environment or troubleshoot access.

A.1.1 The partner-company business model

Elements RBAC is designed around a three-party business model that allows partners to manage many customer Companies while keeping each customer isolated from the others.

Elements RBAC reflects the structure of WithSecure's business: a security platform delivered by a vendor, offered to customers through partners that provide managed services. This shapes the way access is granted, restricted, and inherited across organizations.

The three parties

WithSecure	Develops and maintains the Elements Security Center platform.
Partners	Typically Managed Service Providers (MSPs). Partners resell WithSecure Elements subscriptions to end customers and provide managed security services. They monitor and respond to security events, and manage multiple customer environments from a single interface.
Companies	The end customers. Companies purchase Elements either through a partner or directly from WithSecure and use the platform to protect their IT infrastructure. Companies operate in isolation from other customers.

Architectural principles

Three principles shape how Elements RBAC supports this business model:

Multi-tenancy	A single Elements deployment serves thousands of isolated customer Companies. Each Company operates as if it were the only tenant on the platform.
Partner visibility	Partners see and manage all their customer Companies from a single interface, switching between organizations through the Scope Selector. This makes it practical to manage hundreds of customer environments from one console.
Customer isolation	Each Company is invisible to every other Company. A Company also cannot see the partner's internal structure, the partner's other customers, or the partner's internal users.

What this architecture delivers

Scalability	Partners manage hundreds of customers from one platform.
Security	Organizational boundaries prevent cross-tenant data access.
Simplicity	Each Company experiences a single-tenant view.

A.1.2 The subject-role-resource model

Elements RBAC follows the industry-standard subject-role-resource model: every grant of access combines a subject (who), a role (what), and a resource (where).

Access in Elements is never expressed as a property of a single security administrator or a single organization on its own. Instead, every grant of access links three components together:

Subject: who gets access	The entity that receives permissions. A subject is either: <table> <tr> <td>A security administrator</td><td>An individual person with an account in the Elements portal.</td></tr> <tr> <td>A security group</td><td>A collection of security administrators that share the same permissions.</td></tr> </table>	A security administrator	An individual person with an account in the Elements portal.	A security group	A collection of security administrators that share the same permissions.
A security administrator	An individual person with an account in the Elements portal.				
A security group	A collection of security administrators that share the same permissions.				
Role: what permissions are granted	A defined set of low-level permissions describing which actions are allowed. Roles are not job titles. They are specific capability sets such as Identity and Access Management (IAM) Administrator , Vulnerability Management: Reading , or Elements Editing All . A role only grants permissions; it never denies them.				
Resource: where the permissions apply	An organization in Elements RBAC. The resource defines the scope of the access (for example, the entire partner hierarchy, a single Service Partner, or a specific Company).				

The three components combine in a role assignment

A role assignment is the operation that links subject, role, and resource, and is the only way to grant access in Elements RBAC. For example:

[Subject: alice@partner.com] + [Role: IAM Administrator] + [Resource: Acme Corp]
= Alice can manage security administrators in the Acme Corp organization

Every permission a security administrator has in Elements comes from a role assignment.

A.1.3 What is an organization

An organization is the fundamental container in Elements RBAC, holding security administrators, security groups, and role assignments.

An organization is the foundational building block of Elements RBAC. Every security administrator, security group, and role assignment belongs to an organization. Organizations also define the scope of access. A role assignment specifies which organization the permissions apply to.

In the subject-role-resource model, an organization is the resource that defines where access applies.

Why organizations matter

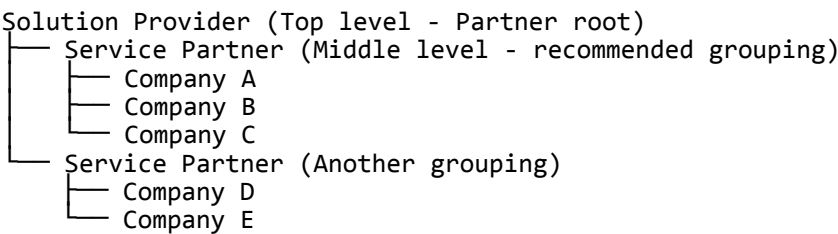
Organizations are the foundation that allows Elements to serve many customers from one system:

Security	Organizational boundaries prevent unauthorized cross-tenant access.
Multi-tenancy	One Elements deployment can serve many isolated customer organizations.
Scalability	Partners can manage hundreds of companies efficiently because each is its own organization.
Delegation	Company-level Identity and Access Management (IAM) administrators can manage access within their organization without seeing other organizations.
Compliance	Data and user management are segregated by organization, supporting regulatory requirements.

Organizational hierarchy and inheritance

Elements RBAC organizations form a three-level hierarchy in which role assignments at a higher level automatically apply to all organizations below.

The organizational hierarchy has three levels: Solution Provider at the top, Service Partner as a recommended middle level, and Company at the bottom. Every partner should create at least one Service Partner, even a single one grouping all Companies, because it is the only level from which roles such as IAM Administrator, API Key Management, and Audit Log access can be scoped to Companies without also granting them across the partner's own internal organization. A Solution Provider can contain Service Partners and Companies directly. A Service Partner can contain Companies. A Company cannot contain any other organization.



This hierarchy is the structure that allows partners to manage many customers efficiently while keeping permissions and visibility correctly scoped.

How inheritance works

Role assignments made at a parent organization automatically apply to all descendant organizations through inheritance. Inheritance flows downward only. A role assigned at one organization never grants access at higher levels.

- A role assigned at the Solution Provider level applies to all Service Partners and Companies below it.
- A role assigned at a Service Partner level applies to all Companies grouped under that Service Partner.

- A role assigned at a Company level applies only to that Company.

For example, granting three roles to a partner team at the Solution Provider level creates three role assignments that apply across all 100 managed companies, rather than the 300 assignments that would be needed without inheritance. When a new Company is added under the partner, it automatically inherits these role assignments. No additional configuration is needed for the partner team to have access to the new Company.

Inheritance flows downward only

A Company never has access to its parent Service Partner or to the Solution Provider, even when it inherits role assignments from above. The inheritance relationship grants access to the receiving organization and its descendants, never to its ancestors. This is what keeps each Company isolated from the partner's internal structure.

A Company can also opt out of inherited partner access for specific Elements features.

Organization types: solution provider, service partner, and company

Elements RBAC has three organization types: Solution Provider, Service Partner, and Company. They represent the partner's root organization, recommended groupings of customer companies, and the end customer organizations themselves.

Each organization in Elements RBAC is one of three types. The type determines the organization's position in the hierarchy and the operations available within it.

Solution Provider

The Solution Provider is the top level of the organizational hierarchy and the root of a partner organization. It is the recommended location for all partner security administrators and security groups. They reach managed companies through role assignments rather than through membership in those companies.

Role assignments made at the Solution Provider level automatically inherit to all Service Partners and Companies below it.

Service Partner

A Service Partner is a recommended middle-level organization that groups related companies under a Solution Provider. Even partners with no need for multiple segments should create at least one Service Partner and place all companies under it, since this is the only way to restrict roles such as IAM Administrator, API Key Management, and Audit Log access to companies rather than the entire partner organization. Partner administrators are typically different individuals from the staff who provide administrative support within customer companies, so this separation matters even for small, single-team partners. Where useful, Service Partners can also segregate access and organize companies into logical clusters, for example:

- By industry (for example, a Healthcare Service Partner and a Legal Service Partner).
- By team (for example, Team A Service Partner and Team B Service Partner).
- By service tier (for example, Premium Service Partner and Standard Service Partner).
- By geography (for example, an East Service Partner and a West Service Partner).

Role assignments made at the Service Partner level inherit to all Companies grouped under it. This allows a team to be granted access to a defined subset of companies through one role assignment rather than many.

**NOTE:**

It is technically possible to add Identity and Access Management (IAM) administrators at the Service Partner level. Their visibility is then limited to that Service Partner and the Companies below it. This delegation is complex and is not recommended for most partners. The simpler pattern is to keep partner IAM administrators at the Solution Provider level and use security groups to segregate access.

Company

A Company is a customer organization and the bottom level of the hierarchy. A Company is a leaf node. It cannot have child organizations beneath it.

Companies operate in isolation from one another. A Company cannot see other Companies managed by the same partner, and Company security administrators can only manage access within their own Company.

The RBAC experience within a Company is simpler than at the partner level:

- The Scope Selector is locked to the Company. There is no other organization to switch to.
- Role assignments do not require explicit scope selection; the Company is the implicit scope.
- Security administrators and security groups all belong to the Company.

A.1.4 What is a security administrator

Security administrator and *portal user* mean the same thing in Elements RBAC: a person who can access Elements Security Center.

In the *subject-role-resource model*, a *security administrator* is the subject that receives permissions. An email address identifies each *security administrator* and is their username. The same identity can be used throughout Elements, so one person can belong to several organizations.



NOTE: In Elements RBAC, *security administrators* and *portal users* differ from *endpoint users* and *identities protected by Elements*.

Partner and company users

Elements distinguishes between users who belong to a partner organization and users who belong to a customer company, and each type has a different scope of visibility and access.

Every security administrator in Elements belongs to a single organization. That organization determines what the user sees in the portal and what the user can manage. A security administrator works in one of two contexts: as a partner user or as a company user.

Partner users

Partner users belong to the Solution Provider organization at the top of the partner hierarchy. From there, they can see and manage the customer companies that the partner is responsible for.

A partner user typically has access to multiple companies and switches between them in the **Scope Selector**. The access itself comes from role assignments. These assignments can target individual companies or Service Partners, or they can be made at the Solution Provider and inherited down the hierarchy to all managed companies.

**IMPORTANT:**

Partner users must not be added to customer companies as members. Access to a company should be granted through role assignments instead. This keeps partner users invisible to company administrators and preserves the boundary between the partner and its customers.

Company users

Company users belong to a specific customer company. They see only that company in the **Scope Selector** and cannot switch to any other organization.

The experience for a company user is simpler than for a partner user. The user works within one organization, one set of security groups, and one place where roles are assigned. Company Identity and Access Management (IAM) administrators manage other company users inside the same company organization.

Partner users can operate inside the company organization through role assignments, but they remain invisible to company administrators because they are not company members.

Comparison**Table 6: Partner users compared to company users**

Attribute	Partner user	Company user
Home organization	Solution Provider	The specific customer company
Organizations visible in the Scope Selector	The Solution Provider, any Service Partners, and the managed companies the user has access to	The home company only
Managed by	Partner IAM administrators at the Solution Provider	Company IAM administrators, with partner IAM administrators assisting at setup
Visible to company administrators	No, when the recommended access model is followed	Yes

A.1.5 What is a security group

A security group is a container for security administrators who share the same permissions, and the recommended way to manage access at scale.

A security group has two key characteristics:

- It is a subject in the RBAC model and receives role assignments as does a security administrator.
- All members of a security group automatically inherit all of the group's role assignments.

Elements has two types of security groups:

- Locally created groups** Created manually in Elements. Can be edited, renamed, or deleted. Membership is managed in Elements.
- Entra-provisioned groups** Synced automatically from Microsoft Entra ID through System for Cross-domain Identity Management (SCIM). Immutable in Elements. They

cannot be edited or deleted. Membership is managed exclusively in Entra ID. Role assignments are defined in Elements.



IMPORTANT:

A security group and a security administrator must belong to the same organization to be linked.

We recommend using security groups to manage permissions instead of assigning roles directly to individual security administrators, for three reasons:

- Scalability** Changing the group's permissions updates all members automatically.
- Consistency** All team members have identical permissions.
- Auditability** You can see who has what by looking at group membership.

Locally created and provisioned security groups

Security groups can be either locally created in Elements or provisioned from Microsoft Entra ID. The two types differ in how they are managed and in who can be a member.

A locally created security group is created and managed entirely within Elements. A provisioned security group is created in Microsoft Entra ID and synced to Elements through System for Cross-domain Identity Management (SCIM). In Elements, it appears as an immutable copy of the Entra group.

How the two types differ

Table 7: Comparison of locally created and provisioned security groups

Aspect	Locally created group	Provisioned group
Creation	Manually, in Elements	Automatically, by sync from Entra ID through SCIM
Group name and description	Managed in Elements	Managed in Entra ID
Membership	Managed in Elements	Managed in Entra ID
Role assignments	Managed in Elements	Managed in Elements
Editing and deletion in Elements	Allowed	Not allowed; the group is immutable

Changes to a provisioned group in Entra ID sync to Elements continuously, typically within minutes. These changes include adding or removing a user, renaming the group, and deleting the group.

Membership rules

Two factors determine who can be added to a security group: organization membership, and whether the security group is locally created or provisioned.

A security administrator and a security group must belong to the same organization to be linked. A Solution Provider security administrator cannot be added to a company security group. Likewise, a security administrator of one company cannot be added to a security group of another company. The combinations of security administrator type and security group type are summarized below.

Table 8: Which security administrators can be added to which groups

Security administrator type	Locally created group	Provisioned group
Local security administrator (invited through Elements)	Can be added or removed through Elements	Cannot be added
Provisioned security administrator (synced from Entra ID)	Can be added or removed through Elements	Membership managed in Entra ID

A.1.6 What is a role

A role is the set of permissions that defines what actions a security administrator can perform in Elements.

In the subject-role-resource model, the role is the "what": the actions that the security administrator (the subject) is allowed to perform in the organization (the resource).

A role is a set of low-level permissions, not a job title or persona. "Identity and Access Management (IAM) Administrator" and "Exposure Management: Vulnerabilities: Management" are roles; job titles such as "Security Analyst" or "IT Manager" are not modeled as roles in Elements.



IMPORTANT:

A role is meaningless without an organizational scope. For example, if a user has the IAM Administrator role but no assigned organization, the role assignment is incomplete. If the user has the IAM Administrator role in organization ABC, the role assignment is complete. The scope is specified at the moment the role is assigned, not when the role is defined.

Granularity

Elements offers dozens of roles, each granting access to a specific subset of functionality. Granularity allows precise access control, at the cost of more configuration effort. We recommend using security groups to compose granular roles into permission sets that can be reused across security administrators.

Roles fall into three categories:

Standard roles	Cover functional areas. Examples: "IAM Administrator", "Exposure Management: Vulnerabilities: Management".
Detailed roles	Cover specific actions within a functional area. Example: "Exposure Management: Vulnerabilities: Vulnerability scans reading".
Large-scope roles	Provide broad read or write access across all Elements functionality. The two large-scope roles are "Elements Editing All" and "Elements Reading All".

Additivity

Roles are additive: they only grant permissions, they never deny. A security administrator's effective permissions are the union of all permissions from all of the administrator's roles.

- Multiple roles produce the sum of all their permissions.
- No role can revoke permissions granted by another role.

- There is no concept of a "deny" role in Elements RBAC.
- Having the same role twice has no additional effect.
- Permissions from direct, indirect, and inherited role assignments all add together.

Combined roles

A security administrator has three role assignments:

- A direct assignment of **Exposure Management: Vulnerabilities: Editing**.
- An indirect assignment of **Exposure Management: Reading** through a security group.
- An inherited assignment of **Response: Execute** from a parent organization.

The administrator can edit vulnerabilities, read exposure data, and execute responses. The three sets of permissions add together.

Large-scope roles: Elements Editing All and Elements Reading All

Elements Editing All and Elements Reading All are two special roles that grant broad access across all Elements functionality. They are continuously maintained as new features are released.

Two special roles provide broad access across all Elements functionality:

Elements Editing All	Provides full read and write access to all Elements functionality. Recommended for root user accounts.
Elements Reading All	Provides read-only access to all Elements functionality. Recommended for auditors and report viewers.

Both large-scope roles are continuously maintained by WithSecure, which means they automatically include access to new features as those features are released.



IMPORTANT:

Granular roles do not have this property. A security group that has been assigned every existing granular role does not automatically gain access to new features. Only the two large-scope roles are continuously maintained. To grant access to a new feature through granular roles, an Identity and Access Management (IAM) administrator must explicitly assign the new role.

A.1.7 What is a role assignment

A role assignment is the fundamental operation in Elements RBAC that links a subject, a role, and a resource to grant access.

A role assignment links a subject (who), a role (what), and a resource (where) into a single grant of access.

Every permission in Elements comes from a role assignment connecting these three components. Access is granted by creating a role assignment and revoked by deleting one.

A role assignment in practice

Consider a role assignment with these three components:

Subject	The SOC Team security group.
----------------	------------------------------

Role	Vulnerability Management: Editing.
Resource	The Healthcare Service Partner organization.
The assignment grants the members of the SOC Team security group the ability to edit vulnerabilities in the Healthcare Service Partner organization.	

Types of role assignments

There are three types of role assignments:

Direct role assignment The role is assigned directly to a security administrator, not through a security group. This type is not recommended except for special cases such as root user accounts, because it is hard to manage at scale.

Indirect role assignment The role is assigned to a security group, and security administrators inherit the role through their group membership. This is the recommended type because it is scalable and maintainable.

Inherited role assignment The role is assigned at a parent organization and automatically applies to all child organizations. This type cannot be removed at the child level; the removal must happen at the parent organization where the assignment was created.

Two perspectives for managing role assignments

Elements presents role assignments from two perspectives:

For a selected subject The member-first approach.

For a selected resource The organization-first approach.

The same assignments are managed from both views.

Direct, indirect, and inherited role assignments

A security administrator can receive permissions through three types of role assignments: direct, indirect, and inherited. The types differ in where the assignment is anchored and how it reaches the administrator.

Every role assignment links a subject, a role, and a resource. What distinguishes the three types is where the assignment is anchored and how the permissions reach a security administrator's effective access.

Direct role assignments

A direct role assignment is anchored to an individual security administrator. The administrator's email address appears as the subject of the assignment, and the assignment is not shared with any other administrator.

In the role assignments table, a direct assignment is shown with the administrator's email as the assignee and a member type of **Security Administrator**. The assignment can be removed directly from the administrator's view.



NOTE:

Direct role assignments are not recommended except for special cases such as root user accounts. They are hard to manage at scale.

Indirect role assignments

An indirect role assignment is anchored to a security group. Security administrators receive the assignment through their membership in the group. All members of the group share the same set of indirect assignments.

In the role assignments table, an indirect assignment is shown with the security group's name as the assignee and a member type of **Security Group**. An indirect assignment cannot be removed from the security administrator's own view. The administrator can lose the assignment in two ways: by being removed from the group, or by the assignment being removed from the group. Removing the assignment from the group affects all members.

Indirect role assignments are the recommended type, because they scale to many security administrators and keep permissions consistent across team members.

Inherited role assignments

An inherited role assignment is anchored at a parent organization and automatically applies to all child organizations. Inheritance flows downward through the organizational hierarchy.

When viewing role assignments at a child organization, inherited assignments are shown with an **inherited** indicator and the parent organization where the assignment was created. Inherited assignments cannot be removed at the child level. To remove an inherited assignment, navigate to the parent organization where it was created.

Inheritance applies only to partner hierarchies, because only partner organizations have child organizations. Company organizations have no children, so inheritance does not apply to them.

How the three types combine

A security administrator can receive permissions through all three types simultaneously. The administrator's effective permissions are the sum of all permissions from direct, indirect, and inherited assignments.

A security administrator with assignments of all three types

A partner security administrator has the following role assignments:

- A direct assignment of **Identity and Access Management (IAM) Administrator** for the Solution Provider organization.
- Membership in the Healthcare Team security group, which has indirect assignments of **Exposure Management: Editing** and **Vulnerability Management: Editing** for the Healthcare Service Partner organization. These reach companies in the healthcare segment through inheritance.
- Membership in the Executives security group, which has an indirect assignment of **Elements Reading All** at the Solution Provider level. This assignment is inherited downward into all Service Partners and companies.

The administrator's effective permissions combine all three sources. These are IAM administration at the Solution Provider, full editing in the healthcare segment, and read-only access across the entire estate.

Effective permissions

A security administrator's effective permissions in an organization are the combined set of permissions granted to that administrator. They include every role assignment that reaches the administrator and applies to that organization.

Permissions in Elements RBAC are additive: every role assignment only grants permissions, never denies them. There are no exclusion rules, and no role can revoke permissions granted by another role. A security administrator's effective permissions are the union of all permissions reaching the administrator through any role assignment.

Three sources contribute to the effective permissions:

- Direct role assignments made to the security administrator.
- Indirect role assignments made to security groups the administrator is a member of.
- Inherited role assignments created at a parent organization that apply to the organization being checked through downward inheritance.

Each source contributes independently, and the contributions accumulate. Having the same role through more than one source has no additional effect.

Effective permissions are organization-specific. A security administrator can have one set of effective permissions in one organization and a different set in another. The difference depends on which assignments apply to each organization.

To inspect the effective permissions of a specific security administrator in a specific organization, use the Check Access feature in the role assignments view.

Access without membership

Partner security administrators can have access to a customer company through role assignments alone, without being members of the company organization.

A security administrator gains access to an organization by having one or more role assignments that apply to that organization. The administrator does not need to be a member of the organization to receive the access.

This pattern is used for partner staff who manage customer companies. The partner security administrator belongs only to the Solution Provider organization. An Identity and Access Management (IAM) administrator assigns roles to the partner staff, with the customer company or a Service Partner as the resource. The mechanics are:

- The partner security administrator is a member only of the Solution Provider organization.
- An IAM administrator assigns roles to the partner staff, with a customer company or Service Partner as the resource.
- The partner staff can manage resources in the company through those role assignments.
- The partner staff does not appear in the company's directory of security administrators.
- The company's IAM administrator cannot see or manage the partner staff.

The benefits of this pattern are:

Privacy	The partner's internal structure stays hidden from customers.
Security	A company cannot accidentally remove a partner's access.
Scalability	The partner manages staff and their access centrally at the Solution Provider.



NOTE:

Inherited access works the same way. When a role is assigned at the Solution Provider level, partner staff gain access to all managed companies through inheritance. They do not need to be members of any of them. Access without membership at the level of a single company is the more specific pattern. Use it when partner staff should have access to only some companies rather than all.

**IMPORTANT:**

This is the recommended approach. Partner security administrators should not be members of customer company organizations. Access should be granted through role assignments alone.

A.2 Planning your deployment

Before you turn on RBAC, plan your organizational structure, security groups, and role assignments based on how your security operations are organized.

Plan your deployment with the guidance for partners and for companies and the best practices for organizations, security groups, and role assignments. The decisions you make while planning shape the structure you create when you set up your environment.

Related reference

System limits on page 166

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

A.2.1 Planning your deployment as a partner

Before turning on RBAC as a partner, plan the organizational hierarchy, identify the security groups you need, and decide whether to integrate with Microsoft Entra ID.

Partner deployments scale to hundreds of customer Companies, so planning before turning on RBAC saves significant effort later. Four decisions shape the deployment.

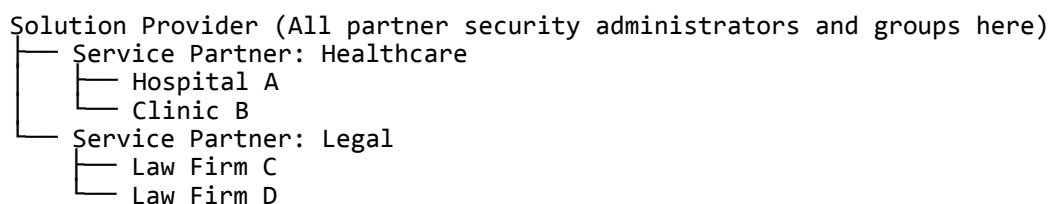
Decide how to group customer Companies

Consider whether your customer Companies fall into natural groupings:

- Do different teams manage different customer segments?
- Are there industry-specific requirements that call for separation (for example, Healthcare, Legal, or Finance)?
- Do you offer different service tiers that need segregated access?

Even if a single team manages all Companies with a consistent access model, or if you have fewer than 10-20 customer Companies, create at least one Service Partner and place all Companies under it rather than skipping the layer entirely. This preserves the ability to scope sensitive roles, such as IAM Administrator, API Key Management, and Audit Log access, to Companies only, without granting them across the whole partner organization.

If distinct groupings are also useful (by team, industry, service tier, or geography), plan to use multiple Service Partners instead of a single Service Partner. For example:



Plan the security groups you will need

Identify the job functions in the managed organization (for example, SOC analysts, security engineers, managers, and executives). Map the required permissions to each function and plan a naming convention for the security groups, such as Elements-SOC-Team or Elements-Admins.

Security groups are the recommended way to manage access at scale and let permission changes apply to all members instantly.

Decide whether to integrate with Microsoft Entra ID

Entra ID integration is strongly recommended for partners that have:

- An existing Microsoft Entra ID infrastructure.
- A portfolio of integrated IT management systems.
- A requirement for automated user lifecycle management.
- Compliance requirements that benefit from centralized identity governance.

Full Entra integration uses both SSO Federation (authentication) and System for Cross-domain Identity Management (SCIM) provisioning (user and group synchronization). Together, they remove the need for day-to-day access management in the Elements portal. Security administrators and group memberships are managed entirely in Entra ID.

Prepare a deployment checklist

Before turning on RBAC, work through the following items:

- Document the organizational hierarchy: which Companies belong under which Service Partners.
- Identify all security administrator roles and the permissions they need.
- Plan the security groups and their role assignments.
- If you plan to integrate with Entra ID, prepare the Entra tenant and create the Entra security groups with the chosen naming convention.
- Configure the filters that determine which Entra users and groups will be provisioned.

Next steps

When the planning decisions are complete, follow the quick start to carry them out.

A.2.2 Planning your deployment as a company

Before turning on RBAC for a Company, identify the size and structure of the security team, decide whether to integrate with Microsoft Entra ID, and plan the security groups you will need.

Company deployments are simpler than partner deployments. A Company has no hierarchy, no Scope Selector switching, and no inheritance to plan for. Three decisions shape the deployment.

Identify the security team and the required access

Consider the structure of the team that will use Elements:

- How many security administrators need access to Elements?
- What are their job functions, and what permissions does each function need?
- Do you want to manage identities in Microsoft Entra ID, or directly in Elements?

Choose an access management approach

Elements supports two ways for a Company to manage security administrators and security groups:

Entra ID integration	Security administrators and security groups are managed in Microsoft Entra ID and synchronized automatically to Elements. SSO Federation handles authentication, and System for Cross-domain Identity Management (SCIM) provisioning handles user and group synchronization. Recommended for organizations with more than five users, or when compliance requirements call for centralized identity governance. Requires an Entra ID tenant.
Local management	Security administrators and security groups are created and maintained directly in Elements. Invitations are issued manually, and security administrators authenticate with Elements credentials and multi-factor authentication. Suitable for small teams without Microsoft 365, for guest or contractor accounts, or as a starting point for organizations that intend to add Entra ID integration later.

Plan the security groups you will need

A common starting point for a Company is three security groups:

Administrators	Full access, typically with the Elements Editing All role.
Security team	Monitoring and response, with feature-specific roles such as Endpoint Protection, Exposure Management, and Response.
Read-only users	Dashboards and reports, typically with the Elements Reading All role.

Adjust the set to match the team's structure.

Prepare a deployment checklist

Before turning on RBAC, work through the following items:

- Decide whether to integrate with Entra ID or to manage access locally.
- If you plan to integrate with Entra ID, prepare the Entra security groups in advance.
- Identify the first administrator who will be assigned the Elements Editing All role.
- Define the security groups based on job functions.
- List all security administrators who will need access.
- Map the role assignments each security group will need.

Next steps

When the planning decisions are complete, follow the quick start to carry them out.

A.2.3 Best practices for Elements RBAC

Apply these recommendations to keep your RBAC deployment maintainable as your environment grows. These best practices cover organizations, security groups, and role assignments. Review them as part of your initial planning, and again whenever your security team or customer portfolio changes.

Best practices for organizations

Plan the organizational hierarchy thoughtfully, use at least one Service Partner in every deployment (grouping all Companies under it if no further segmentation is needed), and keep partner security administrators at the Solution Provider level.

The organizational hierarchy is the backbone of Elements RBAC. Decisions about hierarchy structure affect daily operations, role assignment efficiency, and the security of customer Companies. The following practices help partners and Companies set up an organizational structure that scales:

Plan the hierarchy before enabling RBAC

Decide before deployment whether to use Service Partners and, if so, how Companies will be grouped. Common groupings are by managing team, by industry, by service tier, or by geography. Document the planned structure so team members understand where each Company belongs and why.

Use at least one Service Partner in every deployment

Service Partners are the only level at which sensitive roles, such as IAM Administrator, API Key Management, and Audit Log access, can be scoped to Companies rather than the entire partner organization, so every partner should create at least one, regardless of size. Use multiple Service Partners when:

- Different teams manage different Companies and require segregated access.
- Industry-specific or compliance requirements (for example, Healthcare or Legal) call for separation.
- Different service tiers require different access patterns.

If a single team manages all Companies with a consistent access model, group all Companies under one Service Partner rather than placing them directly under the Solution Provider.

Keep partner security administrators at the Solution Provider level

Partner security administrators should belong only to the Solution Provider organization. Grant them access to managed Companies through role assignments rather than through membership in those Companies. This keeps the partner's internal structure invisible to Company Identity and Access Management (IAM) administrators and simplifies administration on the partner side.

Avoid Service Partner delegation unless necessary

Adding IAM administrators at the Service Partner level is technically possible but is not recommended for most partners. It creates additional administrative complexity and gives the delegated administrators visibility only to that Service Partner and the Companies under it. The simpler pattern is to keep partner IAM administrators at the Solution Provider level and use security groups to segregate access across Service Partners.

Assign roles at the highest level that matches the desired scope

Inheritance flows downward through the hierarchy, so a role assigned at a parent organization applies to all organizations below it. Use this property to keep the number of role assignments small: assign at the Solution Provider for partner-wide access, at a Service Partner for segment-wide access, and at a Company only for Company-specific exceptions.

Enable RBAC one organization at a time when migrating

RBAC enablement is per-organization. Use this property to migrate gradually: enable RBAC in the Solution Provider first, then in selected Companies, while leaving other Companies on the previous access model until you are ready. A phased migration reduces operational risk during transition.

Best practices for security groups

These recommendations cover how to organize security groups, how to use them for permission management, and how to maintain them over time.

For partners

- Create security groups at the Solution Provider level, which is the top-level partner organization.
- Use groups to segregate teams by function, for example "SOC Team", "Engineers", or "Executives".
- Use groups, and assign their roles to Service Partner suborganizations to segregate access by customer segment, for example "Healthcare Team" or "Legal Team".
- Assign roles at the appropriate organizational level: the Solution Provider for broad access, a Service Partner for segment-specific access, and a company for exceptions.

For companies

- Create security groups within the company organization.
- Organize groups by department or role, for example "IT Security", "Administrators", or "Read-Only Users".
- Assign roles to the groups.

Permission management

- Prefer indirect role assignments through security groups over direct role assignments to individual security administrators.
- Use security groups as permission templates.
- One security group can have role assignments to multiple organizations.
- Security administrators inherit all role assignments from all groups they belong to.

Maintenance

- Regularly review security group membership.
- Audit role assignments for each group.
- Remove obsolete groups.
- Document the purpose of each security group.

Best practices for role assignments

These recommendations keep role assignments scalable, maintainable, and auditable as the number of organizations and security administrators grows.

Recommended practices

Prefer security groups over direct user assignments

Create security groups that represent permission profiles, assign roles to the groups rather than to individual security administrators, and add administrators to the appropriate groups. The root user account is the exception. It keeps a direct Elements Editing All assignment as a fallback for recovery.

Group-based assignments also help stay within the per-tenant role assignment limit, because a single assignment on a group serves all of its members. Avoid

creating redundant assignments. Granting the same role to the same subject for the same organization more than once has no additional effect.

Use inheritance for efficiency

When access should apply to multiple child organizations, assign the role at the parent organization and let inheritance carry it downward. This reduces the total number of role assignments, simplifies management, and means that new child organizations automatically inherit access without further configuration.

Use the narrowest appropriate scope

Do not assign a broader scope than the access requires. A team that should only access healthcare companies should have its role assigned at the Healthcare Service Partner organization, not at the Solution Provider. Access intended for a single company should be assigned at that company, not at a parent.

Document the purpose of each security group

Use clear, descriptive names for security groups and keep an inventory of what each group is intended for. Documentation makes audits easier, prevents accidental misuse of broad groups, and helps onboard new Identity and Access Management (IAM) administrators.

Permission design patterns

Four common patterns combine the practices above into a coherent design:

- Role-based groups** Create security groups by job function (for example, Administrators, SOC Team, or Read-only users). Assign roles appropriate to each function and add administrators based on their role.
- Team-based groups** Create security groups by customer segment (for example, Healthcare Team, Legal Team, or Financial Team). Assign roles scoped to the appropriate Service Partner and add administrators based on their team assignment.
- Hybrid groups** Combine function-based and team-based groups. Use function groups at the Solution Provider for broad cross-segment access, and use team groups at the Service Partner level for segment-specific access.
- Entra-driven** Provision security groups from Microsoft Entra ID, assign roles to the provisioned groups in Elements, and manage all membership in Entra ID. This pattern is recommended for organizations already using Microsoft 365 and requires no day-to-day operations in the Elements portal.

A.2.4 Getting started

Turn on RBAC for the managed organization, then follow the quick start that matches your deployment.

Two quick starts are available: one for partner deployments and one for Company deployments. Each lists the tasks in order with links to the detailed procedures. Complete the deployment planning before you start, then follow the quick start that matches your environment.

Turn on RBAC for an organization

Turn on RBAC for the managed organization to start managing access through security groups and role assignments.

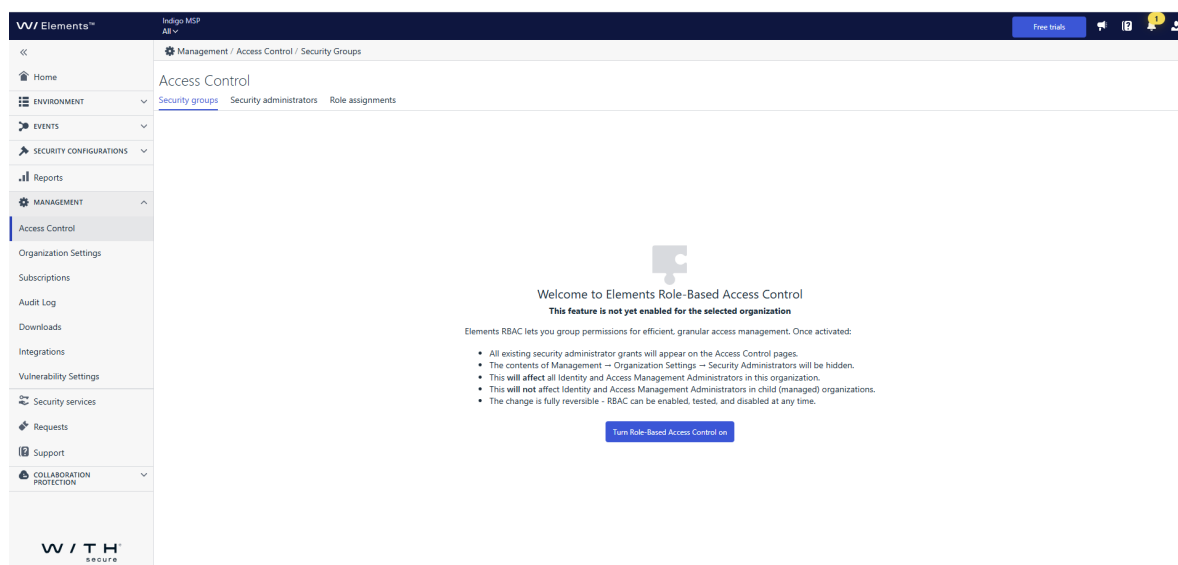
Before you start, make sure you have the Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization.

RBAC must be turned on separately for each organization. Turning on RBAC in a parent organization does not automatically turn it on in managed organizations.

**IMPORTANT:**

If you are a partner and you turn on RBAC in a managed Company, this also affects the IAM administrators of that Company.

1. Select the organization in the Scope Selector.
2. Go to **Management > Access Control**.



The RBAC welcome screen appears.

3. Review the information about what turning on RBAC means.
4. Click **Turn Role-Based Access Control on**.

RBAC is now turned on for this organization:

- The Access Control pages become available for managing security groups, role assignments, and security administrators.
- The previous direct access model converts to the new RBAC model.
- Existing security administrators become explicit members of their organizations.
- Existing permissions convert to direct role assignments.
- All existing access is preserved.

**NOTE:**

After you turn on RBAC, the **Organization Settings > Security Administrators** page changes to show Entra ID configuration only (SSO Federation and System for Cross-domain Identity Management (SCIM) provisioning). Security administrator management moves to **Access Control > Security Administrators**.

**NOTE:**

To revert to the previous access model, use the link on the **Organization Settings > Security Administrators** page. You can revert only after removing all security groups and removing all

access that does not depend on organization membership. Features specific to RBAC are not available in the previous access model.

Set up Elements RBAC for partners

Set up Elements RBAC for a partner organization that manages multiple Companies and is planning Microsoft Entra ID integration.

This quick start is intended for a partner that manages 20 or more Companies and plans to integrate with Microsoft Entra ID. Complete the planning before you start.

1. Turn on RBAC in the Solution Provider organization.
2. If you decided to use Service Partners, create them and move Companies under them.
3. Set up SSO Federation for Microsoft Entra ID integration.
4. Configure System for Cross-domain Identity Management (SCIM) provisioning.
5. Apply filters so that only the Entra security groups you intend to use are synchronized.
6. Define the security groups in Entra ID using the naming convention you chose during planning.

Example groups:

- Elements-Admins for full access to all Companies.
- Elements-SOC for monitoring access to all Companies.
- Elements-Healthcare for full access to a Healthcare Service Partner.
- Elements-Legal for full access to a Legal Service Partner.

7. Assign roles to each Entra-provisioned security group at the appropriate organizational level.

Assign at the Solution Provider for partner-wide access, and at a Service Partner for segment-specific access.

8. Add partner security administrators to the Entra ID security groups.

Membership changes synchronize to Elements automatically.

9. Create the first administrator for each Company.

Assign the Elements Editing All role to the first administrator. The administrator receives an invitation email.

The partner organization now has automated access management, segregated team access through Entra-provisioned groups, and an established administrator in each Company. As ongoing activities, monitor the provisioning sync, train the Company administrators, and review access periodically.

Set up Elements RBAC for companies

Set up Elements RBAC for a Company organization of five to ten security administrators that does not integrate with Microsoft Entra ID.

This quick start is intended for a Company with five to ten security administrators that does not yet integrate with Microsoft Entra ID. Complete the planning before you start.

1. Turn on RBAC for the Company organization.
2. Verify that the first administrator has the Elements Editing All role.

Confirm access by checking that all menu items are available in Elements Security Center.

3. Create the security groups identified during planning.

Example groups:

- Administrators with the Elements Editing All role.
- Security Team with Endpoint Protection, Exposure Management, Vulnerability Management, and Response roles.
- View-Only with the Elements Reading All role.

4. Invite security administrators and add them to the appropriate security groups.

Go to **Access Control > Security Administrators**, click **Invite Security Administrator**, enter the email, and select the security groups. Repeat for each security administrator.

5. Verify access for each security administrator.

Have each security administrator sign in and confirm they can use the functionality they need. Use the Check Access feature to verify their effective permissions.

Company security administrators can sign in to Elements Security Center with permissions managed through security groups. As ongoing activities, consider integrating with Microsoft Entra ID for automated user management, refine the security groups as the team grows, and review permissions periodically.

A.2.5 Organizing your environment

Shape your Elements environment to match how you organize your security operations: create Service Partners, move companies between them, and control what partners can access.

Visibility and isolation between organizations determine what each partner can see. If you move an organization in the hierarchy, this changes that access. The related tasks explain how to create Service Partners, move companies, and restrict partner access.

Visibility and isolation between organizations

Each organization is isolated from other organizations except through the parent-child relationships in the hierarchy, which protects both customer data and the partner's internal structure.

Organizations create visibility boundaries that are enforced by Elements RBAC regardless of role assignments. A security administrator cannot see organizations outside their visibility, even if granted broad permissions.

What each security administrator sees

The set of organizations visible to a security administrator depends on which organization they belong to:

Partner security administrators	See the Solution Provider, any Service Partners, and all Companies managed by the partner. They can switch between these organizations through the Scope Selector to perform management operations on behalf of customers.
Company security administrators	See only their own Company. They cannot see other Companies managed by the same partner, and they cannot see the partner organization above them.

What companies do not see

Company security administrators do not see the partner organization or other Companies managed by the same partner. Specifically, a Company security administrator cannot see:

- How many other Companies the partner manages, or which Companies they are.
- The partner's internal security groups or permission structure.
- Which partner security administrators have access to the Company, unless those security administrators are explicitly members of the Company.

This isolation protects the partner's business structure and prevents customers from gaining competitive intelligence about the partner's other relationships.

The Scope Selector

The Scope Selector is the user interface control that switches the current organizational context. The selected organization determines which security administrators, security groups, and role assignments appear in management screens, and it defines the scope for operations such as inviting security administrators or assigning roles.

Its behavior depends on the security administrator's organization:

- For partner security administrators, the Scope Selector lists the Solution Provider, all Service Partners, and all managed Companies. Switching to a Company shows that Company's security administrators, security groups, and settings.
- For Company security administrators, the Scope Selector is locked to the single Company. There is no other organization to switch to.

Restricting partner access to a company

By default, a partner has inherited access to all Companies it manages. A Company can opt out of this inherited access for specific Elements features, blocking the partner's automatic access to those features while keeping the partner relationship intact for the rest of the product.

If the partner still needs to assist with a feature the Company has restricted, the Company can explicitly invite a partner security administrator as a member of the Company. This makes the partner security administrator visible to the Company's security administrators and brings the relationship under the Company's control.

What happens when an organization moves in the hierarchy

When an organization moves within the hierarchy, Elements automatically revalidates the affected role assignments to maintain security boundaries, but does not revalidate existing memberships.

An organizational move changes the parent of the moved organization. Because role assignments and inheritance depend on the hierarchy, Elements automatically revalidates the resulting configuration and updates it where needed. Memberships are not changed automatically and may need a manual review.

Automatic revalidation of role assignments

Elements automatically revalidates every role assignment that crosses organization boundaries to or from the moved organization. Elements also enforces the cross-organization assignment rules in the new location.

Table 9: Effects on role assignments

Assignment type	What happens
Assignments that remain valid	Role assignments stay in effect when the subject's organization is still compatible with the moved organization's new location in the hierarchy.

Assignment type	What happens
Inherited assignments	Elements recalculates inherited role assignments. The moved organization now inherits from its new parent organizations and no longer inherits from the previous parents.
Assignments that become invalid	Elements removes role assignments where the subject belongs to an organization that is unrelated to the new parent. Elements enforces the cross-organization rule in the new hierarchy.

Memberships are not revalidated automatically

Elements preserves existing memberships in the moved organization after the move and does not re-evaluate whether current members should remain. After the move, review the membership list and remove any security administrators or security groups whose membership is no longer appropriate.

Create a service partner

Create a Service Partner sub-organization to group related Companies under your Solution Provider.

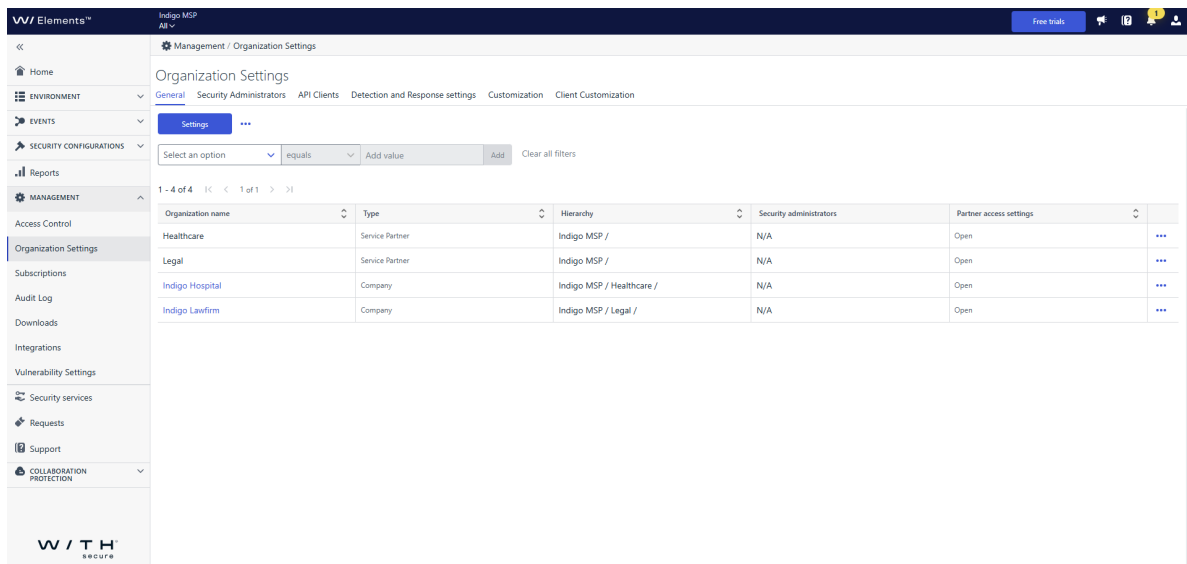
Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role at the Solution Provider level.
- RBAC turned on in the Solution Provider organization.

Service Partners are recommended sub-organizations used to segregate access and to group related Companies under the Solution Provider. Create at least one Service Partner in every deployment, even if it will hold all your Companies, since this is the only way to scope roles such as IAM Administrator, API Key Management, and Audit Log access to Companies rather than to the whole partner organization. Create additional Service Partners when:

- Different teams manage different customer segments.
- You want to organize Companies by industry (for example, Healthcare, Legal, or Finance).
- You offer different service tiers that require segregated access.

1. Go to Management > Organization Settings.



The organization list appears.

2. Click the three-dot menu next to the **Settings** button.

3. Select **Create service partner**.

4. Enter a name for the service partner.

For example: Healthcare, Legal, or Enterprise Tier.

5. Click **Save**.

A new Service Partner sub-organization is created under the Solution Provider. It appears in the organization hierarchy and can be used as a scope for role assignments.



NOTE:

You need to log out and log in again to see the new Service Partner in the Scope Selector.

Move a company to another service partner

Move a Company under a Service Partner to organize the partner hierarchy into logical groupings.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role at the Solution Provider level.
- RBAC turned on in the Solution Provider organization.
- At least one Service Partner created as the move target.

Use Service Partners to group related Companies (for example, by managing team, industry, or service tier). Moving Companies under Service Partners establishes the three-level hierarchy and allows you to scope role assignments to a specific Service Partner rather than to each Company individually.

1. Go to Management > Organization Settings.

The organization list appears.

2. Locate the Company you want to move.

3. Click the three-dot menu next to the Company.

4. Select **Move company to another partner**.
5. Choose the target Service Partner from the dropdown.
6. Click **Save**.

The Company is now organized under the selected Service Partner. The hierarchy reflects the new structure, for example:

```

Solution Provider
├── Service Partner (Healthcare)
│   ├── Hospital A
│   └── Clinic B

```



IMPORTANT:

Existing role assignments that cross organization boundaries to the moved Company are automatically revalidated against the new hierarchy, and any that are no longer valid in the new location are removed.



NOTE:

You need to log out and log in again to see the changes in the Scope Selector.

What restricting partner access means

A company can block its managing partner from inheriting access to specific Elements features, while keeping the partner relationship intact for everything else.

By default, a company inherits the role assignments that its managing partner creates at parent levels of the hierarchy. This inheritance is how partner security administrators gain access to the company. A company can override this default and block the partner from inheriting access to a defined set of features.

The restriction applies only to the following areas:

- Exposure Management,
- Collaboration Protection, and
- access control itself.

When the restriction is active, partner security administrators who would have received the blocked roles through inheritance no longer have the corresponding access in this company. Other inherited partner roles continue to apply as normal, and role assignments made directly at the company level are not affected.

The restriction changes inheritance only. It does not remove the partner relationship, and it does not change which features the company itself can use.



NOTE: If the partner still needs to assist with a restricted feature, the company can explicitly invite a partner security administrator as a member of the company. The partner security administrator then becomes visible to the company security administrators, and the company controls that access.

Restrict partner access to a company

Block a subset of inherited partner role assignments for a company, so that partner security administrators do not have those roles in this company.

Before you start, make sure you have the Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the company organization.

By default, a company inherits the role assignments that its managing partner creates at parent levels of the hierarchy. You can block the partner from inheriting access to specific features. The restriction applies only to Exposure Management, Collaboration Protection, and access control itself. Other inherited partner roles, and role assignments made directly at the company level, are not affected.

1. Select the company organization in the Scope Selector.
2. Go to **Organization Settings > General > Access Policies**.
3. Turn on **Restrict Partner access**.
4. Select the partner roles that should not be inherited in this company.

You can restrict roles in Exposure Management, Collaboration Protection, and access control.

Partner security administrators who would have received the selected roles through inheritance no longer have the corresponding access in this company. Other inherited partner roles, and role assignments made directly at the company level, continue to apply.

Organization limitations

Several constraints affect how organizations, their members, and their role assignments can be configured in Elements RBAC.

Plan organizational deployments with the following constraints in mind:

Organization membership is distinct from access

Being a member of an organization is not the same as having access to it:

- | | |
|-------------------|---|
| Membership | A security administrator explicitly belongs to the organization's directory and is visible to Identity and Access Management (IAM) administrators in that organization. |
| Access | A security administrator has role assignments that allow them to work with the organization's resources. |

Partner security administrators typically have access to managed Companies without being members of those Companies, which keeps them invisible to Company IAM administrators.

Security groups and members must share an organization

A security administrator and a security group must belong to the same organization to be linked through membership. You cannot, for example, add a security administrator from one Company to a security group in another Company.

Multiple organization membership is discouraged

A security administrator can belong to multiple organizations, but this is discouraged because it creates ambiguity:

- It is unclear which organization manages the security administrator.
- Permissions become harder to track.
- The security administrator can appear in multiple contexts simultaneously.

Partner security administrators should belong only to the Solution Provider. Company security administrators should belong only to their own Company.

Role assignments require explicit scope

When assigning roles from a partner organization, you must specify the target organization as the scope. There is no default scope. The level you choose determines the reach of the assignment:

- Granting at the Solution Provider level applies to the entire hierarchy below.

- Granting at a Service Partner level applies to that Service Partner and the Companies under it.
- Granting at a Company level applies only to that Company.

RBAC must be enabled per organization

RBAC enablement is per-organization. Turning on RBAC in a Solution Provider does not automatically enable it in the managed Companies. Each organization opts in independently, which allows partners to migrate gradually.

A.3 Managing security administrators

Security administrators sign in to Elements Security Center to monitor and manage the managed organization's security.

Each security administrator account has an owner. You can invite and manage accounts manually or let Microsoft Entra ID manage their lifecycle. Choose the approach that fits your environment. Microsoft Entra ID integration is recommended for organizations that already use Microsoft 365. Manual management suits smaller teams.

A.3.1 Account types and ownership

Security administrator accounts differ by ownership model, role within the organization, and how they relate to the wider Elements directory.

Security administrator accounts differ in four ways:

- the distinction between federated and local accounts
- the special role of the root user
- how membership and access work together
- the cross-tenant policies that govern who can invite whom

Understand these differences before you start inviting security administrators, so that the lifecycle decisions you make are intentional.

Account Ownership: federated and local accounts

Elements supports two account ownership models (federated and local) which determine who controls a user account and what management capabilities Identity and Access Management (IAM) administrators have over it.

Federated accounts

A federated account is a user account where SSO Federation is enabled for the user's email domain. The account is owned by the federated organization, not by the user. Authentication is handled by Microsoft Entra ID, so the user does not have an Elements password. The IAM administrator has full control over the account.

An IAM administrator can:

- Remove the user from an organization they manage (standard removal).
- Remove the user from all organizations in the Elements system (hard delete).
- Delete the user even if the user is invited to organizations outside the IAM administrator's scope.

The user cannot:

- Change their own account details in Elements.

- Control the account lifecycle.
- Remain in the system after the organization removes them.

The security benefits of a federated account include centralized identity governance, immediate revocation, MFA enforced by Entra ID, password policies managed centrally, and an audit trail in Entra ID.

A federated account is created when SSO Federation is configured for the user's email domain and the organization proves domain ownership through Entra integration.

We recommend federated accounts for organizational users, to enable full IAM administrator control and centralized identity management.

Local accounts

A local account is a user account created without SSO Federation, by manual invitation. The account is owned by the user and WithSecure. Authentication uses an Elements password and MFA. The IAM administrator has limited control over the account.

An IAM administrator can:

- Remove the user from organizations they manage.
- Remove role assignments granted through their organizations.
- Remove the user from security groups in their organizations.

An IAM administrator cannot:

- See the user's membership in organizations they do not manage.
- Remove the user from organizations outside their scope.
- Perform hard deletion of the user account.
- Fully control the account lifecycle.

The user can:

- Accept invitations to multiple organizations independently.
- Exist in organizations unknown to a specific IAM administrator.
- Retain the account even after removal from one organization.

Local accounts are useful for small organizations without Microsoft 365, guest accounts, contractors who need temporary access, and organizations not ready for Entra integration.



NOTE:

A local account can become federated if SSO is later configured for its email domain. The first time the user signs in after federation is enabled, the user is prompted for their existing Elements password once. This links the local account to the federated identity. From the next sign-in onwards, authentication uses Entra ID and no Elements password is required.

Root User

The root user is the first administrator in an organization and receives the Elements Editing All role assigned directly to the user account, to make sure that at least one account always has full administrative access.

When a new organization first uses RBAC, no security groups exist yet and no other users have been invited. The first user in that organization is the root user. The root user receives the **Elements Editing All** role assigned directly to the user account, not through a security group.

The root user account serves two purposes:

- It guarantees that at least one account in the organization has full administrative access. If other access is revoked or misconfigured, the root user can recover the organization.
- It allows the first administrator to set up the rest of the organization, including creating security groups, inviting other users, and configuring role assignments.

The root user is the recommended exception to the general guidance that roles should be assigned to security groups rather than to individual users. Other direct role assignments can be removed once security groups are in place. The root user's direct assignment is kept indefinitely as a fallback for recovery.

Each organization has its own root user:

- In a partner organization, the first user invited to the Solution Provider is the partner's root user.
- In a company organization, the first administrator (usually invited by the partner on behalf of the customer) is that company's root user.



IMPORTANT:

Do not remove the **Elements Editing All** role from the root user even after security groups are configured. Doing so risks locking the organization out of full administrative access if security group memberships fail or are misconfigured.

Organization membership and access

Membership (belonging to an organization) and access (having permissions in that organization) are separate in Elements, and a user can have one without the other.

A user joins an organization by being explicitly invited to it. Membership determines what the user can see and manage, subject to further restriction through role assignments. A user can belong to multiple organizations, although we do not recommend this.

Membership and access are two distinct concepts:

Member of an organization The user exists in that organization's directory, is visible to Identity and Access Management (IAM) administrators of the organization, and may later be granted access to the organization or its child organizations.

Access to an organization The user has role assignments for that organization. The user can have access even if they are only a member of a parent organization.

A user can exist in security groups without any role assignments, in which case the user has no access yet.

Partner users typically have access to companies without being members of those companies. This keeps partner users invisible to company administrators.

Cross-tenant access policies

Elements enforces cross-tenant access policies that restrict which users an organization can invite, to prevent phishing and unauthorized access between unrelated tenants.

Cross-tenant access policies prevent malicious organizations from phishing users, protect against unauthorized cross-tenant access, and maintain organizational boundaries between tenants.

Policy rules

An organization cannot invite a user if:

- The user belongs to an unrelated organization.
- The invitation would create a security risk.

An organization can invite a user if:

- The user does not yet exist in Elements.
- The user belongs to the managing partner organization.
- The user is already associated with the inviting organization or with its managing partner organization in other WithSecure portals, such as the Partner Portal.

Examples

Allowed invitations:

- A partner invites a new user to a company the partner manages.
- A company invites its own employees.
- A company invites an employee of its managing partner.

Blocked invitations:

- A competitor tries to invite users from another organization.
- A partner organization attempts to add users of a company it does not manage.
- A user from organization A is invited to a trial organization T.

A.3.2 Inviting and managing manually

Manage security administrators directly in Elements Security Center, without Microsoft Entra ID provisioning.

Manual management covers the day-to-day work for organizations that manage security administrators locally. Administrators:

- Send invitations to partner and company organizations
- Create the first company administrator
- Adjust security group membership
- Remove security administrators when access is no longer needed

Manual management is the right choice when an Entra ID tenant is not available. It also suits teams that are too small for automation to be worthwhile.

Managing Security Administrators manually

Without Entra ID provisioning, all security administrators are managed manually in the Elements Security Center portal.

In manual mode, the Identity and Access Management (IAM) administrator uses the invitation wizard in the portal to invite security administrators. Each invited administrator receives an email and creates an account with an Elements password and multifactor authentication (MFA). They then become a member of the inviting organization.

Daily tasks include adding and removing security administrators from security groups and removing them from organizations.

Inviting Users (no Entra ID Provisioning)

User invitation adds new security administrators to an organization, issued by partners for the companies they manage or by company administrators for their own company.

Invitations are the manual alternative to Entra ID provisioning. They are used when an organization does not use System for Cross-domain Identity Management (SCIM) provisioning, or when adding an individual user outside the provisioned scope, such as a guest or contractor.

An invitation creates organization membership: the invited user appears in the organization's security administrators list. Whether the user gains access to the organization depends on the role assignments configured during, or after, the invitation.

Three invitation scenarios are common:

- A partner administrator invites a partner employee to the Solution Provider organization.
- A partner administrator invites the first company administrator to a customer's company organization.
- A company administrator invites a colleague to the company organization.

What happens to the invitee depends on whether they already have an Elements account:

New user	Elements creates a new account, sends an invitation e-mail with a temporary password, and requires multi-factor authentication setup on first sign-in.
Existing user	Elements adds the existing user as a member of the organization. No new account is created and no password is issued. The user sees the additional organization in the Scope Selector after the next sign-in.



IMPORTANT:

A user can have access in more than one organization. If the email address already has rights in another company or partner account, an administrator of that account must remove the user there before you can manage them in this organization.



IMPORTANT:

An invited user always becomes a member of the organization selected in the Scope Selector. Partners must select the Solution Provider organization when inviting partner employees, and the customer's company organization when inviting a customer administrator. Inviting a partner employee directly to a customer company breaks the recommended access model, and exposes the partner employee to the customer's Identity and Access Management (IAM) administrators.

Invite Security Administrator to Partner Organizations

Invite a partner employee to the Solution Provider organization, where the new user can be granted access through security groups.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role at the Solution Provider level.
- The Solution Provider organization selected in the Scope Selector.
- The user's email address.

Invited users always belong to the organization selected in the Scope Selector. Partner employees should be invited to the Solution Provider, not to customer companies.

1. Go to **Access Control > Security Administrators**.
2. Click **Invite Security Administrator**.

W/ Elements™

Indigo MSP

AM

Free trials

Home

ENVIRONMENT

EVENTS

SECURITY CONFIGURATIONS

Reports

MANAGEMENT

Access Control

Organization Settings

Subscriptions

Audit Log

Downloads

Integrations

Vulnerability Settings

Security services

Requests

Support

COLLABORATION PROTECTION

Management / Access Control / Security Administrators

Access Control

Security groups Security administrators Role assignments

Invite security administrator

Select an option

contains

Add value

Add

Clear all filters

Email	Type	Status	Created at
indigo-root@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-1@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-2@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-3@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-4@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-5@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-6@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-7@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-8@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-9@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-10@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-11@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-12@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-13@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-14@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-15@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-16@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-17@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-18@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-19@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48
indigo-user-20@elementstratest06.onmicrosoft.com	Provisioned	Active	Mar 20, 2026, 12:48

3. Enter the user's email address, and click **Next**.

If the email address already exists in Elements, the invitation adds the user to this organization, unless the user already has rights in another company or partner account. In that case, an administrator of that account must remove the user there first. If the email address is new, Elements creates a new account and sends an invitation email with a temporary password.

If you are inviting a partner employee, confirm that the Solution Provider is selected in the Scope Selector. A warning appears to prevent accidentally inviting a company user to the partner organization.

4. Optionally select one or more security groups for the user, and click **Next**.

The user inherits all role assignments from the selected groups. We recommend using security groups instead of direct role assignments in the next step.

5. Optionally assign roles directly to the user, and click **Next**.



TIP:

We do not recommend direct role assignments except for root user accounts.

6. Review the invitation details on the summary page, and click **Invite**.

Verify that the organization membership is the Solution Provider and that the security group memberships are correct.

If the email address is new, the user receives an invitation email with a temporary password and must set up MFA. If the email address already existed, the user joins the organization as a member. The user becomes a member of the Solution Provider organization, is added to the selected security groups, and inherits permissions from those groups.

Invite Security Administrator to company organization

Invite a company employee as a security administrator in a specific company organization, where they become a member and can manage that company only.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The target company organization selected in the Scope Selector.
- The email address of the company employee.

Company IAM administrators use this procedure to add employees to their own company. Partners use it to add the first company administrator on behalf of a customer.

1. Go to **Access Control > Security Administrators**.

The Security Administrators tab lists the security administrators who belong to this company. It does not show partner security administrators, who belong to the partner organization even though they may have access to this company.

2. Click Invite Security Administrator.

3. In the Invitation Wizard, complete the following:

- Enter the company employee's email address.
- Select one or more security groups, if any are created in the company.
- Optionally, assign roles directly to the security administrator.



TIP:

The first company administrator usually needs a direct role assignment, because no security group exists yet to grant them access. Assign the **Elements Editing All** role so they can finish setting up the company.

d) Review the invitation details, and click Invite.

The new security administrator becomes a member of the company organization and inherits permissions from the selected security groups. They see only this company in the Scope Selector and cannot see or access other companies or partner organizations.

Create the first company administrator (Root Account)

Create the first security administrator account for a new company organization by inviting a user and assigning the Elements Editing All role directly.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the partner organization.
- The target company organization selected in the Scope Selector.
- The email address of the person who will administer the company.

A partner IAM administrator performs this procedure on behalf of a new customer. Because the company organization has no security groups yet, the role is assigned directly to the first security administrator.

1. Go to Access Control > Security Administrators.

- 2. Click **Invite Security Administrator**.
- 3. Enter the email address, and click **Next**.
- 4. Skip the security groups step, and click **Next**.
- 5. Assign the **Elements Editing All** role directly to the security administrator, and click **Next**.
- 6. Review the invitation details, and click **Invite**.

The new security administrator becomes the company's IAM administrator. From this account, they can create security groups and invite additional company employees.

Add a security administrator to security group manually

Add a security administrator to a locally-managed security group so that the administrator inherits the group's role assignments.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The organization where the security group belongs selected in the Scope Selector.
- The security administrator must already belong to the same organization as the security group.

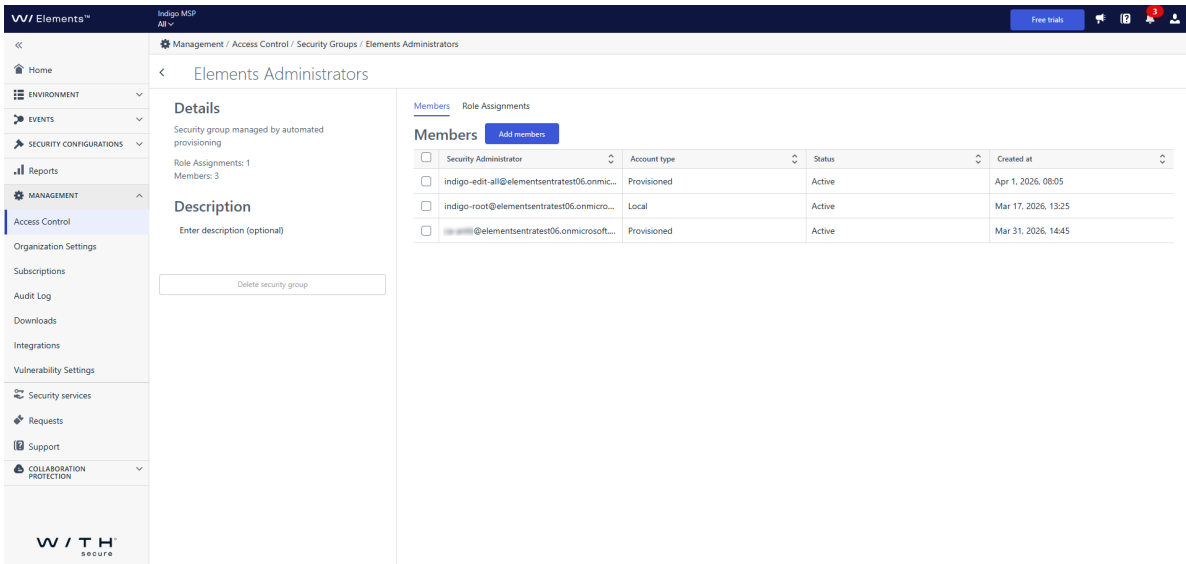
A security administrator and a security group must belong to the same organization to be linked. This procedure applies to locally-created security groups. Provisioned security groups cannot accept locally-managed members; their membership is managed exclusively in Entra ID.

You can add a security administrator to a security group from two starting points:

- From the security group's details: convenient when adding several administrators to the same group.
- From the security administrator's details: convenient when adding one administrator to several groups.

Both approaches produce the same result.

- 1. Select the organization in Scope Selector.
- 2. Go to **Access Control > Security Groups**.
- 3. Click the security group name to open its details.
- 4. Open the **Members** tab.



- 5. Click **Add Members** button.

6. Select one or more security administrators, and click **Add**.

The 'Add members' dialog box is displayed. It has a title bar with 'Add members' and a close button. Below the title bar, it says 'Elements Administrators'. The main area is divided into two sections. The left section, titled 'Add members', contains a 'Security administrators' dropdown menu with a 'Choose' button, a status 'Selected security administrators: 0', a 'Clear all selections' link, and an 'Add' button with an information icon. The right section, titled 'Added members', shows '1 / 100' members and a 'Remove all' link. It contains a message: 'These security administrators will be added to the security group once you finish the wizard.' Below this is a table with one row showing a security administrator's email address '@withsecure.com' and a 'Remove' button. At the bottom of the dialog are 'Cancel' and 'Ok' buttons.



NOTE: A security group has a maximum number of members.

7. Click **OK**.

The selected security administrators become members of the security group and inherit all role assignments granted to the group.

Alternative: adding from the security administrator's details

To start from the security administrator's details instead, follow these steps:

1. Go to **Access Control > Security Administrators**.
2. Click the email address of the security administrator to open the details.
3. Open the **Security Groups** tab.

The screenshot shows the WithSecure Elements interface. The left sidebar contains navigation links: Home, ENVIRONMENT, EVENTS, SECURITY CONFIGURATIONS, Reports, MANAGEMENT (expanded), Access Control (selected), Organization Settings, Subscriptions, Audit Log, Downloads, Integrations, Vulnerability Settings, Security services, Requests, Support, and COLLABORATION PROTECTION. The main content area shows the details of a security administrator. The 'Details' tab is active, displaying 'Elements local security administrator', 'Account status: Active', 'Security groups: 0', 'Role assignments: 1', and 'Organization: Indigo MSP (Solution Provider)'. Below this is a 'Quick actions' section with a 'Remove security administrator' button. The 'Security Groups' tab is also visible, showing a table with columns 'Security group name' and 'Description'. The table is empty, with a message 'No data found.' at the bottom.

4. Click **Add to Security Group**.

Add administrator to Security Group(s)

Security groups

Choose

Search

Select all

☐ Elements Administrators

Elements Administrators

Added security groups 2 / 50 Remove all

The security administrator will be added to these security groups when you complete the wizard.

Elements SOC	-	Remove
Elements Reporters	-	Remove

Cancel Ok

5. Select one or more security groups, and click **Add**.

6. Click **OK**.

The result is the same: the security administrator becomes a member of the selected security groups and inherits all role assignments granted to those groups.

Related reference

System limits on page 166

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Remove a security administrator from a security group manually

Remove a security administrator from a locally-managed security group to revoke the role assignments the administrator inherited through that group.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The organization where the security group belongs selected in the Scope Selector.

This procedure applies to security groups that were created locally in Elements. Provisioned security groups are managed exclusively in Entra ID, so members cannot be removed from them in the portal.

1. Select the organization in Scope Selector.
2. Go to **Access Control > Security Groups**.
3. Click the security group name to open its details.
4. Open the **Members** tab.
5. Select the checkbox next to the security administrator, and remove them from the group.
6. Confirm the removal.

The security administrator is removed from the security group and loses all role assignments inherited through that group. The administrator retains membership in any other security groups and any direct role assignments.

Remove a security administrator from an organization

Remove a security administrator from an organization to revoke their membership and all access granted through that organization.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The organization selected in the Scope Selector.
- The security administrator must belong to an organization you manage.

1. Navigate to **Access Control > Security Administrators**.
2. Locate the security administrator in the table, and select the checkbox next to their entry.
3. Click **Remove from Organization** button.
4. Confirm the removal.

The security administrator is removed from this organization's membership, from all security groups in this organization, and from all direct role assignments granted through this organization. The organization no longer appears in the security administrator's Scope Selector.

For local accounts, memberships in other organizations are not affected. The account may still exist in Elements, and the security administrator can still log in if they are a member of other organizations.

Remove a federated security administrator from all organizations (Hard Delete)

Permanently remove a federated security administrator account from all Elements organizations, including those outside your visibility.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- A federated security administrator account for an email domain that uses single sign-on (SSO) Federation.

For federated accounts, an Identity and Access Management (IAM) administrator can permanently delete the account. This removes the security administrator from every organization in Elements, including organizations that the administrator cannot see. Only federated accounts support this option.

1. Go to **Access Control > Security Administrators**.
2. In the table, find the federated security administrator and select the checkbox next to their entry.
3. Click **Remove from All Organizations**.
4. Confirm the hard deletion.

The account is removed from Elements and every organization it belonged to, including those outside your visibility.

A.3.3 Managing through Entra ID

Delegate security administrator management to Microsoft Entra ID, where you can add, update, and remove administrators in one place.

When you integrate Elements with Microsoft Entra ID, security administrators are created from your Entra ID tenant. Accounts and security group memberships synchronize automatically. Disabling or deleting a user in Entra ID also removes their access to Elements. The related topics describe daily tasks and limitations for Entra ID-managed security administrators.

Managing Security Administrators with Entra ID

When Entra ID provisioning is configured, security administrator management happens primarily in Microsoft Entra ID, and Elements automatically reflects the changes.

The recommended workflow for Entra-managed organizations is:

- In Entra ID, add or remove users, and add or remove their membership in Entra security groups.
- In Elements, define role assignments for the provisioned security groups. This is one-time setup, not a day-to-day operation.

Once role assignments are defined for provisioned groups, no day-to-day operations are needed in the Elements portal. Changes in Entra take effect in Elements within minutes, typically.

Entra ID also distinguishes between temporary and permanent removal:

Deactivation	The account is disabled in Entra ID. The security administrator cannot authenticate, but the account can be reactivated later. Use deactivation for leaves of absence, suspended employees, or investigation periods.
Deletion	The account is deleted in Entra ID and is eventually removed from Elements. Deletion is difficult to reverse. Use deletion for terminated employees or accounts that are no longer needed.

Add a security administrator through Entra ID

Onboard a new security administrator by creating or activating the user account in Microsoft Entra ID and placing it in a provisioned security group.

Before you start, make sure you have:

- System for Cross-domain Identity Management (SCIM) provisioning configured between Microsoft Entra ID and Elements.
- Permissions in Entra ID to manage user accounts and security group memberships.
- Role assignments already defined in Elements for the provisioned security groups the user will join.

In Entra-managed organizations, day-to-day onboarding happens in Entra ID, and Elements automatically reflects the change. No action is needed in the Elements portal.

1. In Entra ID, create or activate the user account.
2. Add the user to one or more security groups that are provisioned to Elements.

Entra ID syncs the change to Elements, typically within minutes. The user appears in Elements as a provisioned security administrator, becomes a member of the selected provisioned security groups, and inherits all role assignments defined for those groups.

Deactivate a security administrator through Entra ID

Disable a security administrator account temporarily by deactivating it in Microsoft Entra ID, so that the administrator cannot authenticate but the account can be reactivated later.

Before you start, make sure you have:

- System for Cross-domain Identity Management (SCIM) provisioning configured between Microsoft Entra ID and Elements.
- Permissions in Entra ID to disable the user account.

Deactivation is the temporary equivalent of removal. Use deactivation for leaves of absence, suspended employees, or investigation periods. To remove the account permanently, delete it in Entra ID instead.

1. In Entra ID, open the user account.
2. Disable the account.

The account is deactivated in Elements. The security administrator cannot log in. The account retains its memberships and role assignments so that it can be reactivated later.

Delete a security administrator through Entra ID

Remove a security administrator account permanently by deleting it in Microsoft Entra ID, so that the account is eventually removed from all organizations in Elements.

Before you start, make sure you have:

- System for Cross-domain Identity Management (SCIM) provisioning configured between Microsoft Entra ID and Elements.
- Permissions in Entra ID to delete the user account.

Deletion is the permanent equivalent of removal. Use deletion for terminated employees or accounts that are no longer needed. Deletion is difficult to reverse. For a temporary removal, deactivate the account instead.

1. In Entra ID, open the user account.
2. Delete the account.

Entra ID first deactivates the account in Elements, and the account is eventually removed from all organizations. All security group memberships and role assignments are removed. The account no longer exists in Elements.

Remove a security administrator from a security group through Entra ID

Revoke role assignments inherited through a provisioned security group by removing the security administrator from the corresponding Entra security group.

Before you start, make sure you have:

- System for Cross-domain Identity Management (SCIM) provisioning configured between Microsoft Entra ID and Elements.
- Permissions in Entra ID to manage the relevant security group.

For provisioned security groups, membership is managed exclusively in Entra ID. Use this procedure when you need to revoke only the access that comes through one specific group, without affecting other groups or direct role assignments.

1. In Entra ID, open the relevant security group.
2. Remove the user from the group.

Entra ID syncs the change to Elements, typically within minutes. The security administrator is removed from the corresponding provisioned group in Elements and loses the role assignments inherited through that group. The administrator retains membership in any other groups and any direct role assignments.

Security administrator limitations

Several constraints affect how security administrator accounts behave in Elements RBAC.

Plan security administrator management with the following constraints in mind:

The e-mail address is the account identity Elements identifies each security administrator by e-mail address. The same e-mail address always refers to the same account across the entire Elements system, and two different accounts cannot share an e-mail address. When SSO Federation is configured, the e-mail domain also determines whether the account is federated.

Removing a security administrator is scoped to one organization Removing a security administrator from an organization affects only that organization:

- The user no longer appears in the organization's security administrators list.
- All role assignments granted through that organization are removed.
- The user is removed from all security groups in that organization.
- The user's membership in other organizations is not affected.

Federated accounts can also be hard-deleted from the entire Elements system.

Cross-tenant invitations are restricted Elements enforces cross-tenant access policies to prevent phishing through invitations. An organization cannot invite a security administrator from an unrelated organization without explicit consent. This protects users from malicious organizations that would otherwise be able to invite them to fake organizations to capture their accounts.

Provisioned security administrators are immutable A security administrator synchronized from Entra ID through System for Cross-domain Identity Management (SCIM) provisioning cannot be edited or deleted in the Elements portal. All account changes must be made in Entra ID:

- Account details are managed in Entra ID.
- Security group membership is managed in Entra ID.
- Removing the user requires removing them from Entra ID, or from the provisioning scope.

Provisioned security administrators are marked as **Provisioned** in the Elements security administrators list.

A.3.4 Managing security groups

Security groups bundle role assignments to grant the same permissions to several security administrators at once.

Create security groups in Elements for teams that need shared access, and delete groups when the team they represent no longer exists. Groups provisioned from Microsoft Entra ID are managed in your tenant, not here.

Create a security group manually

Create a security group manually in Elements to group security administrators who share the same permissions.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- RBAC enabled.
- The appropriate organization selected in the Scope Selector.

Manual security groups are created and managed entirely within Elements. The Security Group creation wizard guides you through defining the group's name, description, role assignments, and initial members.

1. Go to **Access Control > Security Groups**.
2. Click **Create Security Group**.
3. On the Details page, enter a unique group name, optionally add a description, and click **Next**.

The screenshot shows the 'Create security group' wizard in Indigo MSP. The wizard is on the 'Details' page (step 1 of 5). The left sidebar shows 'Create security group' as the active option. The main area has a 'Details' section with a description of Security Groups. Below this, there is a 'Group name*' field with the value 'Administrators' and a 'Description' field with the placeholder 'Enter description (optional)'. At the bottom, there are 'Cancel' and 'Next' buttons.

4. On the Role Assignments page, select one or more roles to assign to the group, click **Add** to preview the assignments, and click **Next**.

For partner organizations, also select one or more organizations as the role scope. Role assignments at this stage are optional and can be configured later.

5. On the Members page, search for and select existing security administrators, click **Add**, and click **Next**.

Members at this stage are optional and can be added later.

6. On the Summary page, review the configuration, and click **Finish**.

The security group is created and ready for use.

Delete a security group

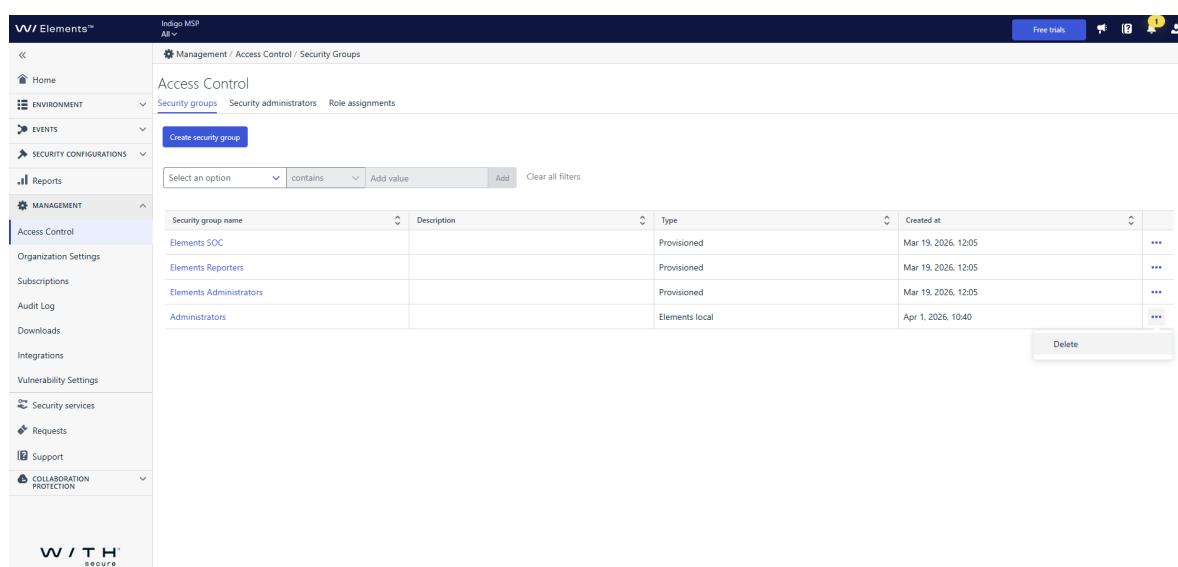
Delete a locally created security group from Elements when it is no longer needed.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The organization where the security group belongs selected in the Scope Selector.

Only locally created security groups can be deleted. Provisioned security groups are immutable in Elements and cannot be deleted through the portal.

1. Go to **Access Control > Security Groups**.
2. Locate the security group, click the three-dot menu next to its name, and select **Delete**.



3. Confirm the deletion.

The security group is deleted, and all of its role assignments are removed. Security administrators who were members of the group remain in the system but lose the permissions they inherited through the group.

A.3.5 Managing role assignments

Role assignments connect a subject (a security administrator or security group) to a role and a resource (an organization).

Role assignments let you grant access, inspect existing access, use inheritance to avoid duplicate assignments, and revoke access when it is no longer needed. The same role assignment is visible from both the member view and the organization view, and the procedures cover both entry points.

Granting access

Create role assignments either from the member's view or from the organization's view.

Assign roles to a security group when several security administrators need the same permissions (the recommended approach), or directly to a single security administrator for special cases such as the root user. The organization view is useful when you want to see and adjust everyone who has access to a specific organization.

Assign roles to a security group (Indirect Assignment)

Assign one or more roles to a security group to grant the same set of permissions to all members of the group at once.

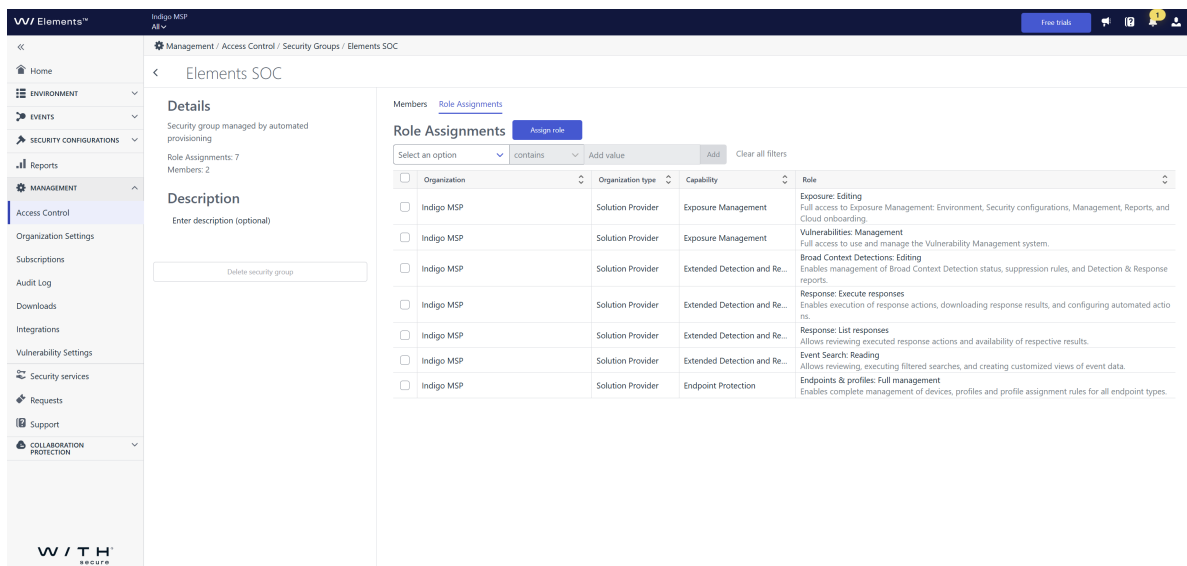
Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- A security group already created.
- Knowledge of which organizations and roles you need to assign.

This approach starts with the security group and defines where and what permissions the group has. It is the recommended approach for defining permission profiles for teams.

1. Select the organization where the security group belongs in the Scope Selector.

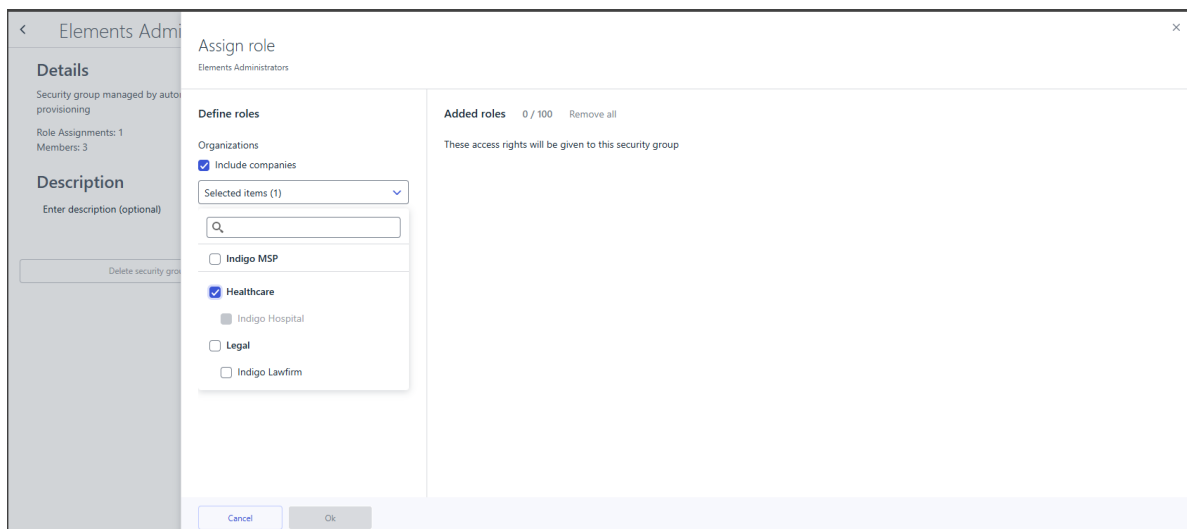
2. Go to **Access Control > Security Groups**, and click the security group name.
3. Open the **Role Assignments** tab.



The tab shows existing role assignments for the group. Inherited assignments (assignments made at a parent organization) appear here too but cannot be removed at this level.

4. Click **Assign Role**.
5. Select one or more organizations to define the role scope.

For partner organizations, choose from the Solution Provider, Service Partners, or companies. Untick **Include companies** to list only Service Partners for a simpler view. Each selected organization defines where the permissions will apply.



6. Select one or more roles to assign.

Use the **Include detailed permissions** checkbox to see granular feature-specific roles in addition to the standard roles.

7. Click **Add** to stage the assignments, and review them on the right side of the layout.

The number of role assignments created is the number of selected organizations multiplied by the number of selected roles. Selecting 3 organizations and 2 roles, for example, creates 6 role assignments.

8. Click **OK** to confirm.

The role assignments are created immediately. All members of the security group receive the assigned permissions. Revocation changes are effective within one minute. Members may need to log out and log in again to use some of the newly granted roles.

Assign roles directly to a security administrator

Grant permissions to a single security administrator by assigning roles directly to the administrator's account, without using a security group.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The organization where the security administrator belongs selected in the Scope Selector.
- Knowledge of which organizations and roles you need to assign.

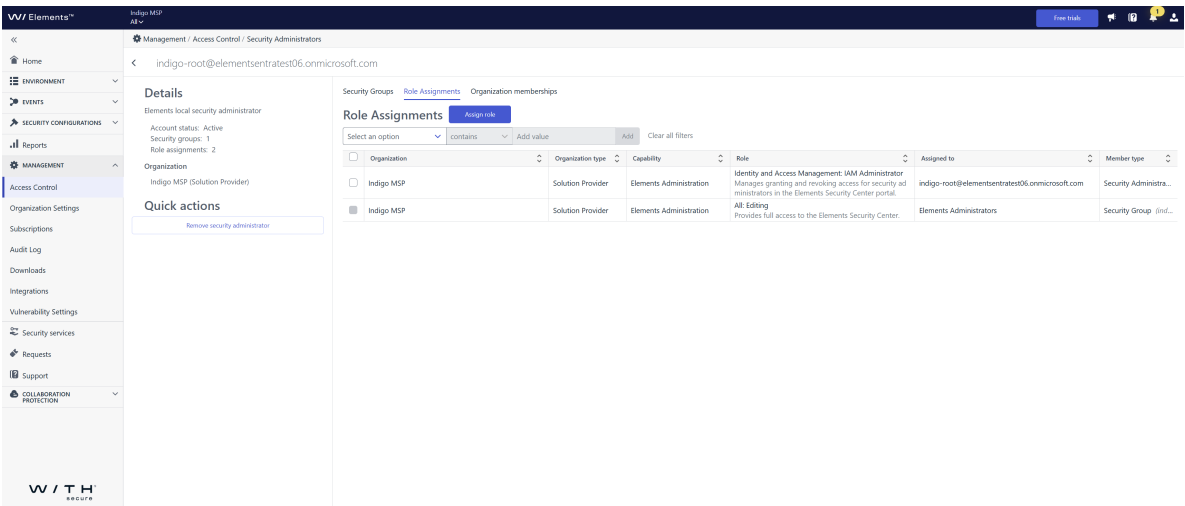


IMPORTANT:

Direct role assignments are discouraged except for special cases: root user accounts (to prevent lockout), temporary elevated access for a specific administrator, or exception cases where group membership is not appropriate. For all other cases, use security groups for scalability and maintainability.

1. Go to **Access Control > Security Administrators**.
2. Click the security administrator's email address to open the administrator details.
3. Open the **Role Assignments** tab.

The tab shows the administrator's existing role assignments. Indirect assignments (received through security group membership) and inherited assignments (from a parent organization) also appear here, but they cannot be removed from this view.



4. Click **Assign Role**.
5. Select one or more organizations to define the role scope.

For partner organizations, choose from the Solution Provider, Service Partners, or companies. Untick **Include companies** to list only Service Partners for a simpler view. Each selected organization defines where the permissions will apply.

6. Select one or more roles to assign.

Use the **Include detailed permissions** checkbox to see granular feature-specific roles in addition to the standard roles.

7. Click **Add** to stage the assignments, and review them on the right side of the flyout.

The number of role assignments created is the number of selected organizations multiplied by the number of selected roles.

8. Click **OK** to confirm.

The role assignments are created immediately and grant the selected permissions to the security administrator. Revocation changes are effective within one minute. The administrator may need to log out and log in again to use some of the newly granted roles.



TIP:

If you repeatedly assign the same roles directly to multiple security administrators, create a security group instead and assign the roles to the group once.

Add access from the organization view

Add access to an organization by selecting members and assigning them roles from the organization's Role Assignments tab.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The target organization selected in the Scope Selector.

This approach starts with the organization (the resource) and defines who has access to it. It is useful for reviewing and managing access to a specific organizational unit.

1. Select the target organization in the Scope Selector.
2. Go to **Access Control > Role Assignments**.

The tab lists all role assignments defined for this organization. Inherited assignments (those created at a parent organization) appear with an **inherited** indicator and cannot be modified or removed from this view.

Assigned to	Member type	Capability	Role	Organization type
Elements Administrators	Security Group	Elements Administration	All Editing Provides full access to the Elements Security Center.	Solution Provider (inherited)
Elements SOC	Security Group	Exposure Management	Exposure Editing Full access to Exposure Management: Environment, Security configurations, Management, Reports, and Cloud onboarding.	Solution Provider (inherited)
Elements SOC	Security Group	Exposure Management	Vulnerabilities Management Full access to use and manage the Vulnerability Management system.	Solution Provider (inherited)
Elements SOC	Security Group	Extended Detection and Re...	Broad Context Detections: Editing Enables management of Broad Context Detection status, suppression rules, and Detection & Response reports.	Solution Provider (inherited)
Elements SOC	Security Group	Extended Detection and Re...	Response Execute responses Enables execution of response actions, downloading response results, and configuring automated actions.	Solution Provider (inherited)
Elements SOC	Security Group	Extended Detection and Re...	Response List responses Allows reviewing executed response actions and availability of respective results.	Solution Provider (inherited)
Elements SOC	Security Group	Extended Detection and Re...	Event Search: Reading Allows reviewing, executing filtered searches, and creating customized views of event data.	Solution Provider (inherited)
Elements SOC	Security Group	Endpoint Protection	Endpoints & profiles: Full management Enables complete management of devices, profiles and profile assignment rules for all endpoint types.	Solution Provider (inherited)

3. Click **Add Access**.

4. For partner organizations, select the member organization type to choose where the members come from.

Three choices are available:

Solution Provider

Select from top-level partner security administrators and groups. This is the recommended choice for partner staff.

- Service Partner**

Select from Service Partner security administrators and groups. Use this when delegating IAM to a Service Partner.
- Company**

Select from company security administrators and groups. Use this when granting company access to a company administrator.

For company organizations this step is skipped. The members come from the company organization implicitly.

Assign role

Healthcare

Define roles

Select Members

Service Partner

Solution Provider

Service Partner

☐ Include detailed permissions

Choose

Selected role assignments: 0

Clear all selections

Add

Added roles

0 / 100

Remove all

These access rights will be given to selected entities

Cancel

Ok

5. Search for and select one or more members.

Security groups appear at the top of the list and security administrators at the bottom. Both are valid subjects. We recommend selecting security groups rather than individual administrators.

Assign role

Healthcare

Define roles

Select Members

Solution Provider

Choose

Security Groups

☐ Elements SOC

☐ Elements Reporters

☐ Elements Administrators

Security Administrators

☐

test3@elementsentratest06.onmicrosoft.com

Added roles

0 / 100

Remove all

These access rights will be given to selected entities

Cancel

Ok

6. Select one or more roles from the role dropdown, and close the dropdown.

Select one or more roles to assign. Multiple roles can be assigned in one operation.

Assign role

Healthcare

Define roles

Select Members

Solution Provider

Selected items (1)

Roles

☐ Include detailed permissions

Selected items (2)

☒ Broad Context Detections: Reading

☐ Broad Context Detections: Editing

☐ Response: List responses

☐ Response: Execute responses

☐ Event Search: Reading

Environment

☒ Cloud configuration: Reading

Added roles

0 / 100

Remove all

These access rights will be given to selected entities

Cancel

Ok



NOTE: Selecting several members and several roles creates one assignment for each combination, which counts toward the role assignment limits.

7. Click **Add** to stage the assignments, and review them on the right side of the flyout.

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Inspecting access

Review the role assignments that apply to a security group, to an organization, or to an individual security administrator.

Use these procedures to audit access before a change, to investigate a permissions issue, or to verify that a new security administrator has the access they need.

View role assignments for a security group

View all role assignments granted to a security group, showing where the group has access and which roles its members inherit.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

Use this procedure to audit a security group's permissions, plan changes to its access, understand the scope of its reach, or document the permission profile it represents.

1. Select the organization where the security group belongs in the Scope Selector.
2. Go to **Access Control > Security Groups**.
3. Click the security group name to open its details.
4. Open the **Role Assignments** tab.

The tab shows all role assignments for the security group, including the organizations where the group has access and the roles granted at each organization. All members of the security group inherit these assignments. Inherited assignments (those created at a parent organization) appear with an **inherited** indicator and cannot be modified here.

View role assignments for an organization

View all role assignments that grant access to a specific organization.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

Use this procedure to inspect or audit access defined for a specific organization, or to locate role assignments that you need to modify or remove.

1. Select the organization in the Scope Selector.
2. Go to **Access Control > Role Assignments**.

The table shows all role assignments defined for the selected organization.

Assigned To	The subject of the assignment: either a security group name or a security administrator's email address.
Member Type	Security group or security administrator.
Capability	The feature area covered by the role.
Role	The role name.
Organization Type	Where the assignment was created. If the assignment is inherited from a parent organization, this column shows the parent organization type with an inherited indicator.

Assignments whose Organization Type matches the selected organization were created explicitly at this level and can be removed from this view. Inherited assignments cannot be removed here; they must be removed at the parent organization where they were originally created.



NOTE:

This view does not expand security group membership. To see which security administrators belong to a security group, open the security group's details. To see the effective access of a specific administrator, use the Check Access feature.

Check a security administrator's effective access

View the complete effective access of a specific security administrator in a selected organization, combining direct, indirect, and inherited role assignments.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

Use this procedure to verify a security administrator's access before or after making changes, to audit their permissions, to troubleshoot access issues, or to investigate security incidents.

1. Select the organization in the Scope Selector.
2. Go to **Access Control > Role Assignments**.
3. Click **Check Access** in the header.

The Check Access link in the Role Assignments header allows inspecting specific user's effective permissions.

The screenshot shows the 'WZ Elements' Management console. The breadcrumb trail is 'Management / Access Control / Role Assignments'. The page title is 'Access Control'. Below the title, there are tabs for 'Security groups', 'Security administrators', and 'Role assignments'. A blue 'Add access' button is visible. A filter bar shows 'Select an option' and 'contains' with an 'Add value' button and a 'Clear all filters' link. The main table has columns: 'Assigned to', 'Member type', 'Capability', 'Role', and 'Organization type'. The table contains one entry: 'Elements Administrators' (Member type: Security Group, Capability: Elements Administration, Role: All Editing, Organization type: Solution Provider (inherited)). A tooltip for the 'All Editing' role states: 'Provides full access to the Elements Security Center. [Source: Editing]'.

4. Enter the security administrator's email address, and click **Next**.

Check access Healthcare

1

2

Search

Result

You are checking a security administrator's effective access to the Healthcare organization. All inheritance rules will be applied. You'll also see which other organizations this security administrator belongs to.

Security administrator email*

indigo-root@elementsentratest06.onmicrosoft.com

X

Cancel

Next

The results page shows two tables:

- The top table, **Effective Role Assignments**, lists all roles that the security administrator has for the selected organization. The list includes direct assignments, indirect assignments through security groups, and inherited assignments from parent organizations, giving you the complete effective access in one place.
- The bottom table, **Other Organization Memberships**, lists other organizations where the security administrator is a member. This table only shows organizations that you yourself have IAM access to. Click an organization name to switch scope and check the administrator's access in that organization.

Check access Healthcare

1

2

Search

Result

Effective access for indigo-root@elementsentratest06.onmicrosoft.com:

Effective role assignments

Select an option

contains

Add value

Add

Clear all filters

Capability	Role	Organization type	Assigned to	Member type
Elements Administration	Identity and Access Management: IAM Administrator Manages granting and revoking access for security administrators in the Elements Security Center portal.	Solution Provider <i>(inherited)</i>	indigo-root@elementsentratest06.onmicrosof...	Security Administrator
Elements Administration	All: Editing Provides full access to the Elements Security Center.	Solution Provider <i>(inherited)</i>	Elements Administrators <i>(indirect)</i>	Security Group <i>(indirect)</i>

Other organizations

This security administrator is a member of the following organizations you can manage.

Organization name	Type	
Indigo MSP	Solution Provider	...

Remove security administrator from all organizations

Previous

Close

**TIP:**

To see organization memberships only (without the effective access detail), open the security administrator's details from **Access Control > Security Administrators** and view the Organization Memberships section.

Using inheritance effectively

Assigning a role at a parent organization grants the access to all child organizations through a single role assignment. This can sharply reduce the number of assignments you need to manage.

Role assignments made at a parent organization automatically cascade to all child organizations. This means that one role assignment at a high level can serve many lower-level organizations. Any organizations added later inherit the same access without further configuration. Used well, inheritance keeps deployments compact, consistent, and auditable.

Use inheritance when:

- The same set of security administrators should have the same access across all child organizations of a parent. For example, a SOC team that monitors all managed companies under a Solution Provider.
- Access should automatically extend to new child organizations as the hierarchy grows. For example, a new company onboarded under a Service Partner should automatically be visible to the partner's incident response team.
- You want to keep the total number of role assignments low, both for ease of management and to stay within the per-tenant role assignment limit.

Do not rely on inheritance when:

- Access should be limited to specific child organizations rather than all of them. Assign the role at the specific organizations instead.
- A parent-level assignment would grant broader access than the security administrators should have at that level. The narrowest appropriate scope is always preferable.

Inheritance applies only to partner hierarchies. Company organizations have no child organizations, so inheritance does not apply to assignments made at a company.

**NOTE:**

A company organization can restrict the inheritance it receives from its managing partner. The company's Identity and Access Management (IAM) administrator does this in **Organization Settings > General > Access Policies**, by enabling **Restrict Partner access**. This disables a configurable subset of inherited partner roles for that company. Partner administrators planning role assignments should be aware that the inheritance shown at design time may be restricted by the company on the receiving end.

Partner SOC team with read access everywhere

A partner wants its SOC team to monitor the entire managed estate.

1. Create a SOC Team security group at the Solution Provider organization.

2. Assign reading roles to the group, with the Solution Provider as the resource:

Exposure Management	Reading
Vulnerability Management	Reading
Broad Context Detection	Reading

Three role assignments at the Solution Provider give every SOC team member read access through inheritance. The access covers the Solution Provider, every Service Partner, and every company. Adding a new company under any Service Partner extends the access automatically.

Healthcare team with full access to one segment

A partner manages several customer segments and wants its healthcare team to have full access to healthcare customers only, with no visibility into other segments.

- 1. Create a Healthcare Team security group at the Solution Provider organization.
- 2. Assign editing roles to the group, with the Healthcare Service Partner as the resource:

Exposure Management	Editing
Vulnerability Management	Editing
Cloud Configuration	Editing

Three role assignments at the Healthcare Service Partner give every team member full access to all healthcare companies through inheritance. The team has no access to companies under other Service Partners.

Executives with read-only access everywhere

A partner wants its executives to see the full managed estate without making any changes.

- 1. Create an Executives security group at the Solution Provider organization.
- 2. Assign the **Elements Reading All** role to the group, with the Solution Provider as the resource.

A single role assignment at the Solution Provider gives every executive read-only access across the entire estate through inheritance. It automatically covers any organization added later.

Related reference

System limits on page 166
Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Revoking access

Remove role assignments from a security administrator, from a security group, or from the organization view.

Choose the entry point that matches the change you want to make:

- Remove a direct assignment when a single security administrator should lose access.
- Remove an assignment from a security group when an entire team should lose it.
- Use the organization view when you are removing access from a specific organization.

Remove a direct role assignment from a security administrator

Remove a role assignment that was made directly to a specific security administrator, rather than granted through a security group.

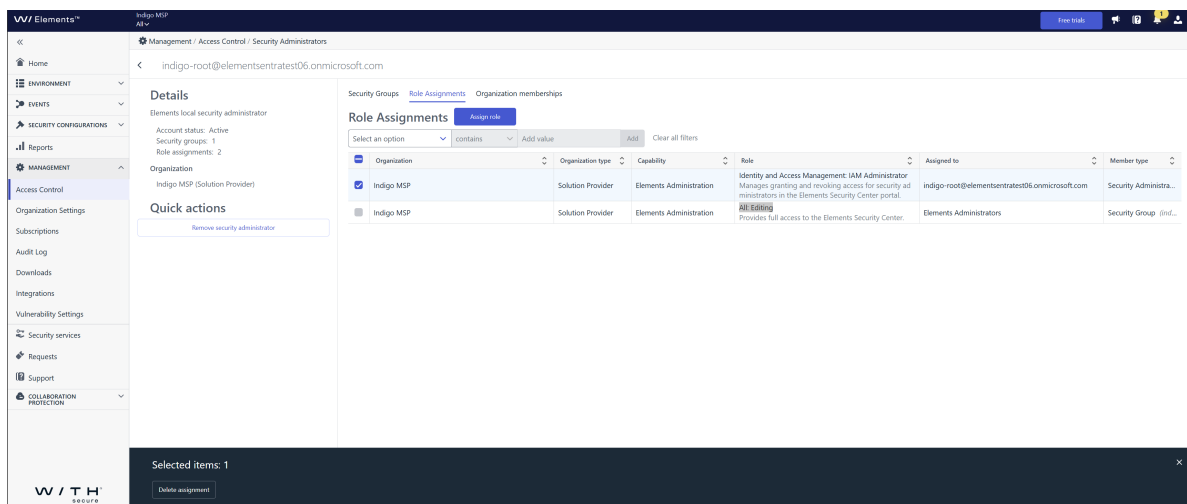
Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

This procedure removes a direct role assignment from a security administrator's Role Assignments tab. Indirect role assignments (those that the administrator receives through security group membership) appear on the same tab for visibility but cannot be removed here. To remove an indirect assignment, remove it from the security group instead.

1. Go to **Access Control > Security Administrators**.
2. Click the security administrator's email address to open their details.
3. Open the **Role Assignments** tab.
4. Select the direct role assignment that you want to remove.

Indirect assignments cannot be selected on this tab.



5. Click **Delete Assignment**, and confirm the deletion.

The role assignment is removed. The security administrator loses the corresponding access within one minute.

Remove a role assignment from a security group

Remove a role from a security group so that all members of the group lose the corresponding indirect access.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

Removing a role assignment from a security group affects every member of the group. Each member loses the corresponding indirect access at the organization where the assignment was made. If you want to remove the access for a single member only, remove that member from the security group instead, or create a separate security group with the appropriate set of members and roles.

1. Select the organization where the security group belongs in the Scope Selector.

- 2. Go to **Access Control > Security Groups**.
- 3. Click the security group name to open its details.
- 4. Open the **Role Assignments** tab.
- 5. Select the role assignment that you want to remove.
- 6. Click **Delete Assignment**, and confirm the deletion.

The role assignment is removed from the security group. All members of the group lose the corresponding indirect access within one minute. Other role assignments for the group are unaffected.

Remove a role assignments from the organization view

Remove one or more role assignments that were created at a specific organization, working from the organization's Role Assignments tab.

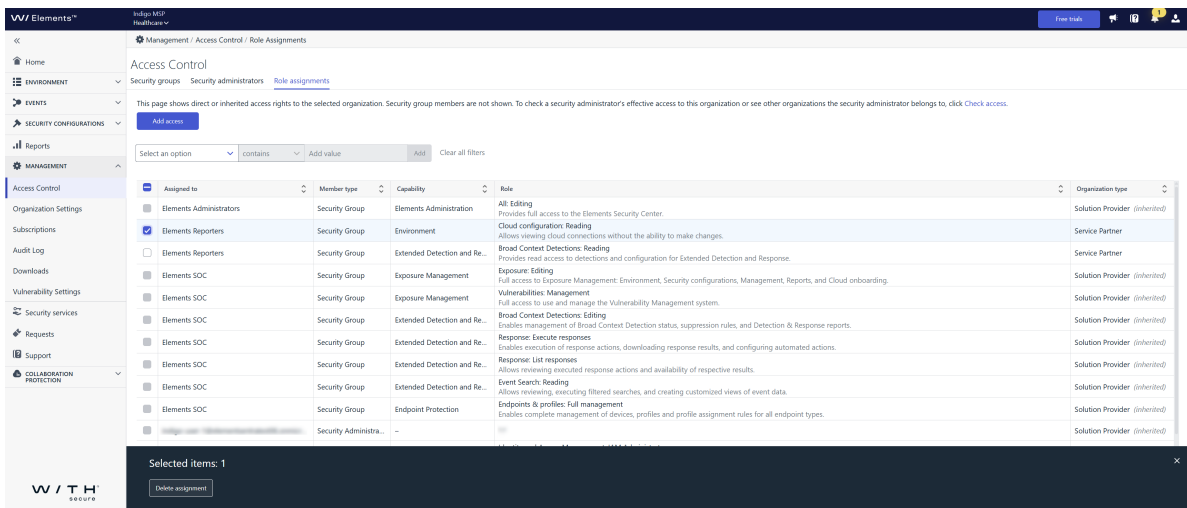
Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role.
- The target organization selected in the Scope Selector.

Use this procedure to remove role assignments at a single organization in one operation. You can select multiple assignments and remove them together. Inherited role assignments (those created at a parent organization) appear in the table but are disabled for selection. To remove an inherited assignment, remove it at the parent organization where it was originally created.

- 1. Select the organization in the Scope Selector.
- 2. Go to **Access Control > Role Assignments**.
- 3. Select one or more role assignments that you want to remove.

Inherited assignments are disabled and cannot be selected.



- 4. Click **Delete Assignments**, and confirm the deletion.

The selected role assignments are removed from this organization. The affected subjects (security groups and security administrators) lose the corresponding access at this organization within one minute. If a subject still has access through another assignment (for example, through a different security group, or through an inherited assignment at a parent organization), that access is unaffected.

Role assignment limitations

Role assignment in Elements RBAC follows four structural rules that determine what can and cannot be done when granting access through roles.

Scope is required	A role assignment must specify an organization where the role applies. For example, if a user has the Identity and Access Management (IAM) Administrator role but no assigned organization, the role assignment is incomplete. If the user has the IAM Administrator role in organization ABC, the role assignment is complete. The organization (resource) is mandatory for every role assignment.
Roles cannot be assigned partially	Roles are atomic. A role cannot be granted in part. For example, an IAM Administrator role cannot be assigned only for security groups. Either the role is assigned in full, or it is not assigned at all. When a role is broader than what is needed, the solution is to use a more granular role.
Composing granular roles is complex to manage	Combining many granular roles to create a custom permission set provides precise access control, but it is complex to set up and maintain, and it requires understanding the full set of available roles.
Large-scope roles cannot be decomposed	Elements Editing All and Elements Reading All are indivisible. You cannot exclude Identity and Access Management (IAM) from an Elements Editing All assignment or exclude specific capabilities from a large-scope role. When selective access is needed, use granular roles instead.

Assigning roles directly to individual administrators has several drawbacks:

- They do not scale, because each administrator must be managed individually.
- They are hard to audit, because there is no straightforward way to list all administrators with a specific role.
- They make consistency hard to maintain across administrators with similar responsibilities.
- They increase the total role assignment count and contribute toward reaching the tenant's role assignment limit.
- They make troubleshooting access issues more complex.

Troubleshooting role assignments

Use these suggestions to investigate the most common issues with role assignments and effective access.

A security administrator has unexpected access	1. Check indirect assignments to see whether the administrator receives the access through security group membership. 2. Check inherited assignments to see whether the access comes from a role assignment at a parent organization. 3. Use the Check Access feature to see the administrator's effective access in the selected organization.
A security administrator cannot access a feature	1. Verify that the administrator has a role assignment for that capability. 2. Check the organization scope. The administrator may have access in a different organization than expected. 3. Verify that the role assignment was not removed and that the security group membership was not revoked. 4. Check that the administrator belongs to the correct organization.

- A role assignment cannot be removed**

1. Inherited assignments cannot be removed at a child organization. Navigate to the parent organization where the assignment was created and remove it there.
 2. Indirect assignments cannot be removed from a security administrator's view. Remove the assignment from the security group, or remove the administrator from the group.
 3. Assignments on provisioned security groups require the group to be deleted in Entra ID, not in Elements.
- The role assignment limit has been reached**

1. Consolidate direct user assignments into security groups.
 2. Use inheritance. Assign roles at a parent organization instead of at each child.
 3. Remove redundant assignments.
 4. Audit role assignments and remove obsolete ones.

A.4 Setting up Microsoft Entra ID integration

Integrate Elements with Microsoft Entra ID to centralize authentication and automatically provision security administrators and security groups.

Integration has two parts. Single sign-on (SSO) federation controls how security administrators sign in. System for Cross-domain Identity Management (SCIM) provisioning keeps Elements aligned with the users and groups in your Entra ID tenant. Set up SSO federation first. Then set up provisioning. Use the limitations and best-practice topics to validate your configuration.

A.4.1 What is Microsoft Entra ID integration

Microsoft Entra ID is Microsoft's cloud identity and access management service, and integrating it with Elements automates security administrator and security group management.

Microsoft Entra ID (formerly Azure Active Directory) is Microsoft's cloud identity and access management service. Many organizations already use Entra ID to manage their users, security groups, authentication, and password policies. When Entra ID is integrated with Elements, Entra becomes the source of truth for identity, and Elements automatically reflects what Entra holds.

Integration splits responsibility between the two systems:

- Identity management: Entra ID**

Holds the user accounts and their attributes, the security groups and their memberships, and the authentication credentials. Entra is the single source of truth for who exists in the organization.
- Authorization management: Elements**

Holds the role assignments that link Entra users and security groups to Elements permissions, and defines the organizational scope of those permissions. Elements decides what each user or group can do.

The integration has two parts that can be configured independently or together:

- SSO Federation**

Authentication is delegated to Entra ID. Security administrators in a federated email domain sign in with their Entra credentials rather than with an Elements password.
- SCIM provisioning**

Identity is synchronized from Entra ID. Selected users and security groups in Entra appear automatically in Elements, and changes in Entra are reflected in Elements within minutes.

Both parts are typically used together for fully automated access management. After SSO Federation and System for Cross-domain Identity Management (SCIM) provisioning are configured, and role assignments are defined in Elements for the provisioned security groups, day-to-day onboarding, offboarding, and group-membership changes happen entirely in Entra ID. Elements requires no further intervention.



NOTE:

SCIM provisioning depends on SSO Federation. SSO Federation can be used on its own without SCIM provisioning, but provisioning cannot work without federation.

A.4.2 SSO Federation

SSO Federation connects Elements to Microsoft Entra ID for authentication, so that security administrators in a federated email domain sign in with their Entra ID credentials rather than an Elements password.

When an organization configures SSO Federation, it proves ownership of one or more email domains and links those domains to its Entra ID tenant. Security administrators whose email addresses fall in a federated domain authenticate through Entra ID. Elements does not store passwords for these administrators and redirects them to Entra at sign-in.

SSO Federation also changes how security administrator accounts are owned and managed:

- Accounts in a federated domain become federated accounts, owned by the federated organization rather than by the security administrator.
- Authentication is handled by Entra ID, including multi-factor authentication and password policies.
- Identity and Access Management (IAM) administrators in the federated organization gain full control over the account lifecycle, including hard deletion across the entire Elements system.
- Sign-in events are recorded in the Entra ID audit trail.

SSO Federation is configured per organization. A federated organization can federate one or more email domains. Each domain must be verified through Entra ID before federation takes effect.

SSO Federation can be configured on its own, or together with System for Cross-domain Identity Management (SCIM) provisioning. SCIM provisioning depends on SSO Federation, but SSO Federation does not depend on SCIM provisioning.



IMPORTANT:

The email address in Elements and the Entra ID User Principal Name (UPN) must match. The first Elements security administrator must already have an email address in a domain you intend to federate. Mismatches between Elements emails and Entra UPNs cause authentication failures.



NOTE:

An Elements account created before SSO Federation is configured for its email domain becomes a federated account once federation is in place. The reverse is not generally possible. Once an account is federated, it stays federated as long as its domain remains federated.

Configure SSO Federation

Set up federated authentication between Elements and Microsoft Entra ID so that security administrators in the federated email domain sign in with their Entra ID credentials.

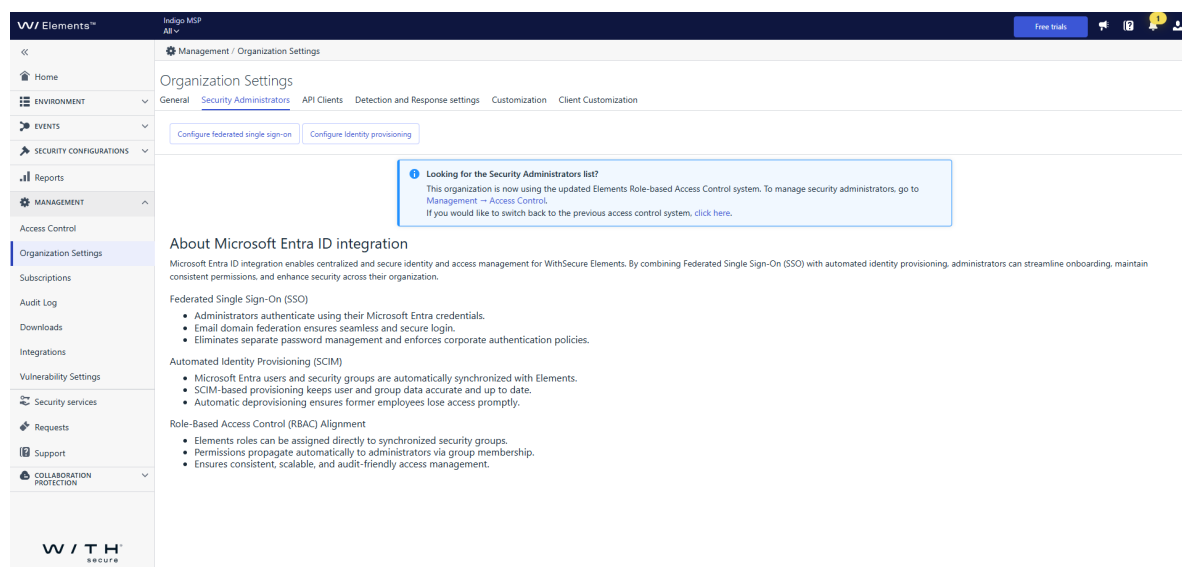
Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where you will configure federation.
- A Microsoft Entra ID tenant, and the privileges in Entra ID to list verified domains and configure single sign-on.
- Ownership of the email domain you intend to federate.
- An Elements account with an email address in the domain you intend to federate.

SSO Federation is configured per email domain, not per organization. All security administrators with email addresses in the federated domain authenticate through Entra ID. To federate multiple domains in the same organization, repeat this procedure for each additional domain.

1. Go to **Organization Settings > Security Administrators**.

After RBAC is enabled, the Security Administrators page is the location for configuring both Entra ID Federation and System for Cross-domain Identity Management (SCIM) provisioning.



2. Click **Configure Single Sign-On Federation**.

3. Review the prerequisites checklist in the wizard, and confirm that each item is satisfied.

4. Sign in to Entra ID using a privileged account to complete the federation setup.

Elements completes the federation configuration automatically, using the information returned by Entra ID.

5. Sign out of Elements.

6. Sign in with your federated email address, and enter your existing Elements password when prompted.

The first federated sign-in for an existing account requires the Elements password once, to link the local account to the federated identity. After this one-time linking, the Elements password is no longer used.

7. Complete the Entra ID authentication.

SSO Federation is active for the email domain. Security administrators with email addresses in this domain sign in through Entra ID rather than with an Elements password. Existing Elements accounts are linked to federated identities the first time each security administrator signs in.

A.4.3 SCIM provisioning

System for Cross-domain Identity Management (SCIM) provisioning automatically synchronizes security administrators and security groups from Microsoft Entra ID into Elements. User management then happens in Entra ID rather than in the Elements portal.

When an organization configures SCIM provisioning, Entra ID continuously synchronizes a configurable set of security administrators and security groups to Elements. Changes made in Entra ID are reflected in Elements within minutes. These changes include adding or removing a security administrator, changing group membership, and renaming or deleting a group.

SCIM provisioning produces two kinds of objects in Elements:

Provisioned security administrators

Synced from Entra ID users. Account ownership and authentication are controlled by Entra ID through SSO Federation. The account cannot be created or removed manually in Elements.

Provisioned security groups

Synced from Entra ID security groups. The group name, description, and membership are managed in Entra ID and cannot be modified in the Elements portal. Only role assignments are configured in Elements.

SCIM provisioning is typically configured at the top of an organization's hierarchy. For partners, this is the Solution Provider organization; for companies with their own Entra ID tenant, it is the company organization. Provisioning to lower levels is possible but requires careful planning and is not the standard configuration.



IMPORTANT:

You can provision the same Entra ID tenant to more than one Elements organization. For example, you might provision it to both a Solution Provider and one or more Service Partners. This setup is supported, but it is prone to misconfiguration. Plan the scope and filters carefully so that each organization receives only its intended security administrators and security groups. Verify the result after the first sync.

The provisioning scope and filters in Entra ID determine which security administrators and groups are synchronized. Only the in-scope administrators and groups appear in Elements. The rest remain in Entra ID and are not visible to Elements. We recommend setting filters to provision only the administrators and groups that need Elements access. Do not provision every user and group in the Entra ID tenant.

SCIM provisioning depends on SSO Federation. The federated email domains determine which users are eligible for provisioning, and the resulting accounts are always federated accounts.



IMPORTANT:

SCIM provisioning is the recommended operating mode for organizations already using Microsoft 365. Once role assignments are defined for the provisioned security groups, no day-to-day user-management operations are needed in the Elements portal. All onboarding, offboarding, and group-membership changes happen in Entra ID.

Configure SCIM provisioning

Set up automated synchronization of security administrators and security groups from Microsoft Entra ID into Elements through System for Cross-domain Identity Management (SCIM).

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where you will configure provisioning.
- SSO Federation already configured for the organization. SCIM provisioning depends on SSO Federation.
- A Microsoft Entra ID tenant, and the privileges in Entra ID to create an enterprise application and configure provisioning. See Microsoft's Entra ID documentation for the exact Entra-side permissions.

SCIM provisioning configuration spans two systems. You start in Elements to generate client credentials, then move to Entra ID to create an enterprise application and configure provisioning using those credentials.

SCIM provisioning is typically configured at the Solution Provider organization for partner deployments, or at the company organization for companies with their own Entra tenant.

1. Go to **Organization Settings > Security Administrators**.
2. Click **Configure Identity provisioning**.

The Configure Identity Provisioning flyout provides the URLs and credentials needed to set up SCIM sync with Entra ID.

Configure Identity provisioning Indigo MSP

Identity provisioning is configured for this organization: Indigo MSP
SCIM API is available for 1 client

Setup Instructions

1. In Entra ID, create an Enterprise app with the Non-gallery option. In the newly created Entra ID Enterprise app, set up 'Provisioning' with OAuth2 client credentials grant use the Tenant URL and Token endpoint from here:
 Tenant URL: <https://api.connect-stg.fsapi.com/scim/v2>
 Token endpoint: <https://api.connect-stg.fsapi.com/as/scim/token.oauth2>
2. To configure the Enterprise application you created in Step 1 within Microsoft Entra ID, you must generate client credentials. If you haven't previously generated client credentials, click the 'Add client credentials' button below to create the client ID and client secret. Copy these values and enter them into the corresponding fields in Entra ID. Keep these credentials strictly confidential, as they are security-critical, and discard them immediately after use.

[Add client credentials](#)

Description	Client ID	Created
New Indigo SCIM	fusion_e69af568b71d4b0f4a...	Mar 24, 2026, 7:06 AM

Deprovisioning Instructions

[Close](#)

3. Click **Add client credentials** to generate a client identifier and secret token for the Elements SCIM endpoint.
4. Copy the Tenant URL, the Token endpoint, the Client identifier, and the Secret token from the flyout.

You will paste these values into the enterprise application that you create in Entra ID. Keep the flyout open, or store the values securely, until the Entra-side configuration is complete.

5. In Microsoft Entra ID, create a non-gallery enterprise application.

In the Entra ID portal, go to Enterprise applications, click New application, select Create your own application, and choose Non-gallery application. Give the application a descriptive name, for example WithSecure Elements SCIM. The detailed Entra ID procedure is in Microsoft's Entra ID documentation.

6. In the enterprise application, open the Provisioning section and configure automatic provisioning using the credentials from Elements.

Select Automatic provisioning mode and OAuth 2.0 client credentials grant as the authentication method. Paste the Tenant URL and Token endpoint, then paste the Client identifier and Secret token. Click Test Connection to verify the credentials, and save the configuration.

7. Configure the attribute mappings so that every provisioned user has a populated email field.

In the Entra ID provisioning configuration, map a non-empty email attribute (for example, the work email or the User Principal Name) to the email field. Elements identifies provisioned users by email address, so users without a mapped email cannot be provisioned.



NOTE:

Microsoft Entra suggests that you map externalId to mailNickname. The mailNickname value is human-readable and recognizable in logs.

This mapping is not sufficient when multiple users share the same local part of their e-mail address (the part before the @) but have different domains. Synced Entra guest accounts are one example.

In these cases, map externalId to the Entra objectId instead. If you later migrate to a different Entra tenant, the objectId values do not carry over.

Provisioning is configured between Entra ID and Elements but is not yet active. Before users and groups synchronize, you must filter the scope of what is provisioned and then activate provisioning.

Filter which users and groups synchronize

Limit System for Cross-domain Identity Management (SCIM) provisioning to only the users and security groups that need access to Elements, using filters on the Entra ID enterprise application.

Before you start, make sure you have:

- A configured SCIM provisioning enterprise application in Entra ID.
- The privileges in Entra ID to modify the enterprise application's provisioning configuration.

Entra ID supports two ways to filter the provisioning scope: explicit group assignment, and attribute-based scoping filters. Both are configured in the enterprise application's Provisioning section.



IMPORTANT: Filter provisioning so that Elements synchronizes only the users and groups that need access. An unfiltered sync can exceed the system limits, and a group that passes the member limit stops adding members.

1. In the SCIM provisioning enterprise application in Entra ID, open the Provisioning section.
2. Set the provisioning scope to **Sync only assigned users and groups**.
3. In the Users and groups tab, assign the security groups that should be synchronized to Elements.

Assigning a security group provisions the group and its members. To provision an individual user without provisioning the whole group, assign the user directly. We recommend assigning groups rather than individual users.

4. Save the configuration.

SCIM provisioning is limited to the assigned users and security groups. When provisioning is active, only these objects are synchronized to Elements.

Using a naming convention and attribute-based filter

As an alternative to explicit assignment, you can use an attribute-based scoping filter to select security groups by name. This pattern works well when you can adopt a naming convention for Elements-related security groups in Entra ID.

1. Ensure that security groups intended for Elements share a common naming pattern. A common choice is an Elements- prefix, for example Elements-SOC-Team, Elements-Administrators, or Elements-ViewOnly.
2. In the enterprise application's Provisioning section, set the scope to **Sync all users and groups**.
3. Add a scoping filter where the displayName attribute matches the chosen pattern, for example displayName startsWith Elements-.
4. Save the configuration.

Only security groups matching the filter are synchronized to Elements. Users are provisioned through their membership in those groups.

Related reference

System limits on page 166

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Activate provisioning

Turn on System for Cross-domain Identity Management (SCIM) provisioning in Entra ID to start synchronizing the configured users and security groups into Elements.

Before you start, make sure you have:

- A configured SCIM provisioning enterprise application in Entra ID, with filters set for the users and security groups that should synchronize.
- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where provisioning was configured.
- The privileges in Entra ID to turn on provisioning for the enterprise application.

Activation is the final step in setting up SCIM provisioning. Once activation completes, Entra ID begins continuously synchronizing the in-scope users and security groups to Elements.

1. In the SCIM provisioning enterprise application in Entra ID, set the Provisioning status to **On**.

The initial sync begins immediately and may take 20 to 40 minutes to complete. Subsequent changes in Entra ID sync to Elements continuously, typically within minutes.

2. In Elements, go to **Access Control > Security Administrators** to confirm that provisioned users have started to appear.

Provisioned users appear in the list with a **Provisioned** indicator.

3. Go to **Access Control > Security Groups** to confirm that provisioned security groups have started to appear.

Provisioned security groups appear in the list with a **Provisioned** indicator.

SCIM provisioning is active. The in-scope users and security groups from Entra ID synchronize continuously to Elements. Subsequent changes in Entra ID (adding users to groups, removing them, renaming groups, deleting accounts) propagate automatically.



IMPORTANT:

Provisioned users and security groups are immutable in Elements. All changes to provisioned objects must be made in Entra ID. The only Elements-side state for provisioned objects is role assignments, which remain editable in the Elements portal.

Verify that provisioning works

Confirm that System for Cross-domain Identity Management (SCIM) provisioning is synchronizing users and security groups from Entra ID to Elements as expected.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where provisioning was configured.
- The organization where provisioning was configured selected in the Scope Selector.
- Access to the Entra ID provisioning configuration to compare it with the configuration in Elements.

Perform this verification after activating SCIM provisioning, and periodically afterwards to confirm the integration remains healthy.

1. Go to **Access Control > Security Groups** in Elements.
2. Confirm that the security groups in the Entra ID provisioning scope appear in the list with a **Provisioned** indicator.

If a security group does not appear, check the provisioning scope in Entra ID. The group must be either explicitly assigned to the enterprise application or matched by an attribute-based filter.

3. Click a provisioned security group to open its details, and open the **Members** tab.
4. Compare the members shown in Elements with the membership of the corresponding security group in Entra ID.

The two lists should match. If members are missing from Elements, the most likely cause is that those users are not in the provisioning scope. Being a member of a synchronized group is not enough; the user account itself must also be in scope.

5. Go to **Access Control > Security Administrators**, and confirm that provisioned security administrators appear with a **Provisioned** indicator.

Provisioning is working correctly when:

- The configured security groups from Entra ID appear in Elements as provisioned groups.
- The membership of each provisioned group in Elements matches the membership in Entra ID.
- The users in those groups appear as provisioned security administrators in Elements.

A.4.4 Troubleshoot Entra ID integration

Investigate and resolve common issues with SSO Federation and System for Cross-domain Identity Management (SCIM) provisioning.

Before you start, make sure you have:

- Access to the Elements Security Center.
- Access to the Microsoft Entra ID portal where SCIM provisioning was configured.

When Entra ID integration does not behave as expected, the most common causes are scope misconfiguration, sync delays, identity mismatches, or attempts to perform Entra-managed actions in Elements. Match the symptom to one of the scenarios in the example below and follow the diagnostic checks for that scenario.

1. Identify the symptom you are seeing from the scenarios in the example below.
2. Follow the diagnostic checks for the matching scenario in order.
3. If the issue is not resolved after completing the checks, contact WithSecure support with the diagnostic details you have gathered.

Common scenarios and diagnostic checks

A security administrator cannot sign in through SSO Federation

Check the following:

1. Verify that the email domain has been federated and that domain verification completed in Entra ID.
2. Confirm that the email address in Elements exactly matches the User Principal Name (UPN) in Entra ID for that account. A mismatch causes authentication to fail, even if both accounts exist.
3. If this is the security administrator's first federated sign-in for an existing local account, confirm that they have entered the Elements password once to link the account.

A user is not appearing in Elements after provisioning

Check the following:

1. Wait a few minutes. The initial sync may take 20 to 40 minutes to complete, and ongoing changes propagate within minutes.
2. Check that provisioning is active in Entra ID and not paused.
3. Check the provisioning scope in Entra ID. The user must be either directly assigned to the enterprise application or be a member of an assigned security group.
4. Confirm that the user has a populated email attribute in Entra ID. Elements requires the email field to identify users.

A security group is not appearing in Elements after provisioning

Check the following:

1. Wait a few minutes for sync to complete.
2. Check the provisioning scope in Entra ID. The security group must be either explicitly assigned or matched by an attribute-based filter.
3. If you are using an attribute-based filter (for example, displayName starts with a prefix), verify that the security group's name matches the filter pattern.

Group membership in Elements does not match Entra ID

Check the following:

1. Wait a few minutes for sync to complete.

	2. Verify that the missing members are in the provisioning scope. A user who is a member of a provisioned group in Entra ID but is not in the provisioning scope themselves is not synchronized. 3. Check the Entra ID provisioning logs for errors related to the missing users.
A provisioned user or security group cannot be edited or deleted in Elements	Provisioned objects are immutable in Elements by design. The name, description, and membership of a provisioned object can only be changed in Entra ID. The only Elements-side state that you can edit for provisioned objects is role assignments.
Too many users or security groups have been provisioned	Take these steps: 1. Tighten the provisioning scope in Entra ID so that only the intended users and groups are in scope. 2. To remove already-provisioned users and groups that should not have been synchronized, deprovision the integration and reconfigure it with the corrected scope.

A.4.5 Limitations of Entra ID integration

Entra ID integration has several hard constraints that affect how the integration can be configured and what can be changed in Elements after provisioning.

Plan and operate Entra ID integration with the following constraints in mind:

Provisioned objects are immutable in Elements	Security administrators, security groups, and security group membership that arrive in Elements through System for Cross-domain Identity Management (SCIM) provisioning cannot be edited or deleted in the Elements portal. The group's name, description, and members can only be changed in Entra ID. The only Elements-side state for provisioned objects is the set of role assignments, which remain editable regardless of the immutability of the underlying object.
Local users cannot be added to provisioned groups	A locally-invited security administrator cannot be added to a security group that was provisioned from Entra ID, because the membership of a provisioned group is managed exclusively in Entra. The reverse is allowed. A provisioned user can be added to a locally-created security group through the Elements portal.
Email addresses and Entra UPNs must match	The email address of a security administrator in Elements must match the User Principal Name (UPN) of the corresponding user in Entra ID. A mismatch causes authentication to fail through SSO Federation, even if both accounts exist on their respective sides.
Sync is one-way from Entra to Elements	Changes made in Entra ID propagate to Elements continuously, typically within minutes. Changes made in Elements do not propagate back to Entra ID. The only Elements-side state that does not have to be mirrored in Entra is role assignments. Everything else (user attributes, group membership, group names) must be changed in Entra.
Provisioning is configured at one organizational level	SCIM provisioning is typically configured at the top of an organization's hierarchy: the Solution Provider for partners, or the company organization

for a company with its own Entra ID tenant. Provisioning the same Entra tenant to multiple organizational levels is technically possible but is not the standard configuration and is prone to misconfiguration.

A.4.6 Best practices for Entra ID integration

These recommendations help organizations deploy Entra ID integration in a way that minimizes Elements portal work and maximizes the automation benefits.

Apply these practices when planning and operating Entra ID integration.

Configure SSO Federation and SCIM provisioning together	Both halves of the integration produce the most value when used together. SSO Federation alone gives you delegated authentication but still requires manual identity management. System for Cross-domain Identity Management (SCIM) provisioning depends on SSO Federation and cannot be used without it. Configure both during initial setup for fully automated access management.
Filter aggressively when configuring provisioning	An Entra ID tenant typically contains many more users and security groups than need access to Elements. Configure provisioning filters in Entra ID to sync only the users and groups that need Elements access. A common approach is to use a naming convention (for example, an Elements - prefix on security groups intended for Elements integration) and configure Entra to sync only those groups. Aggressive filtering improves sync performance, reduces visual clutter in Elements, and limits the scope of any accidental misconfiguration.
Provision at the top of the organizational hierarchy	Configure provisioning at the Solution Provider organization for partner deployments, or at the company organization for company deployments. This places the synchronized users and groups at the highest scope, where role assignments can use inheritance to reach all lower organizations.
Define role assignments once, then leave them in place	After provisioning is active, define the role assignments for each provisioned security group in Elements. Once those role assignments are in place, day-to-day onboarding, offboarding, and group-membership changes happen entirely in Entra ID. Revisit Elements role assignments only when access requirements change, when new Elements features become available, or when restructuring the security group design.

Once the integration is in place, the recommended operating model has three phases:

Initial setup (one-time)	Configure SSO Federation, configure SCIM provisioning, set up security groups in Entra ID with appropriate filtering, and define role assignments for those groups in Elements.
Day-to-day operations (in Entra ID)	Onboard new security administrators by adding them to Entra ID and to the appropriate Entra security groups. Offboard departing security administrators by removing them from the Entra groups or by deleting their Entra accounts. Elements reflects each change automatically, typically within minutes. No action is needed in the Elements portal.
Maintenance (occasionally in Elements)	Adjust role assignments for provisioned security groups when access needs change. Add role assignments for new Elements features released by WithSecure.

A.4.7 Deprovision Entra ID integration

Disconnect Elements from Microsoft Entra ID so that provisioned users and security groups become local and can be deleted. Disconnecting also lets you reconfigure or fully disable provisioning.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where provisioning was configured.
- The privileges in Entra ID to modify the System for Cross-domain Identity Management (SCIM) provisioning enterprise application, if you intend to reconfigure provisioning afterwards.

Use this procedure to fix a misconfigured provisioning setup, switch to a different identity source, or disable Entra ID integration. A misconfigured setup might synchronize too many users or groups.

The procedure has two phases. The first five steps disconnect Elements from Entra ID and let you remove unwanted provisioned objects. Steps 6 and 7 are optional and are only needed when you intend to continue using Entra ID integration with corrected settings.

1. Go to **Organization Settings > Security Administrators**.
2. Open **Configure Identity provisioning**.
3. Remove the SCIM client credentials.

Entra ID can no longer synchronize changes to Elements. Existing provisioned users and security groups remain in Elements but stay immutable until the next step.

4. Click **Deprovision Entra ID**.

Provisioned users and security groups become local objects in Elements. They can now be deleted, but they cannot be edited.

5. Delete the unwanted users and security groups from Elements.

Delete only the objects that should not have been provisioned. Any objects that are still needed can stay. When provisioning is reconfigured, Entra ID recognizes them and re-provisions them.

6. In Entra ID, update the SCIM provisioning enterprise application with the corrected scope or filters.
7. In Elements, return to **Configure Identity provisioning** and add new client credentials.

If you completed all seven steps, Entra ID resumes synchronization with the corrected scope. Users and security groups that remained in Elements after cleanup are recognized as provisioned again. Any new objects in the updated scope synchronize according to the updated filters.

If you stopped after step 5, SCIM provisioning is fully disabled. Users and security groups already provisioned remain in Elements as local objects. SSO Federation, if configured, is independent of SCIM provisioning and remains active until disabled separately.

A.5 Migrating to Elements RBAC

Migrating an organization from the previous access management model to Elements RBAC covers pre-migration planning, the migration sequence, and post-migration verification.

Migrating to Elements RBAC is a one-time activity per organization. You can perform it in a single maintenance window or gradually over time. After the migration is complete, the ongoing operations are described in the other topics of this guide.

Who should migrate

- Identity and Access Management (IAM) administrators in partner organizations, typically Managed Service Providers. They migrate their Solution Provider, Service Partners, and customer Companies to Elements RBAC.
- IAM administrators in customer Companies who need to migrate their Company organization to Elements RBAC.

If you are starting with Elements RBAC for the first time, you do not need to migrate.

A.5.1 Understanding the migration

Learn what changes when you migrate, the two migration approaches you can choose between, and how reversible the migration is.

The decisions you make when preparing for migration depend on understanding what will change in your environment and which migration approach fits your team. Understand the migration before you make those decisions.

What changes when you migrate

When you migrate to Elements RBAC, all existing access is preserved, but its structure changes. Partner security administrators no longer need company membership, and direct grants become explicit role assignments.

Migrating an organization from the previous access model to Elements RBAC does not change which security administrators have access or what they can do. All existing access is preserved. What changes is how the access is represented in the system and how it can be managed.

Security administrator memberships

In the previous access model, partner security administrators were typically added directly as members of customer Companies to gain explicit (non-inherited) access to those Companies. The membership and the access were the same operation. To have access to a Company, the security administrator had to be a member of that Company. As a result:

- Partner security administrators appeared in the Company's security administrator list.
- Company Identity and Access Management (IAM) administrators could see, and could modify the permissions of, partner staff with access to the Company.
- Partner internal staff structure was visible to Company administrators.

Elements RBAC introduces access without membership: a partner security administrator can have role assignments scoped to a Company without being a member of that Company. The two concepts are decoupled. As a result:

- Partner security administrators belong only to the Solution Provider organization.
- Partner security administrators are invisible to Company IAM administrators.
- The partner manages access to the Company through role assignments at the Solution Provider or Service Partner level.

The migration does not automatically remove partner security administrators from Company memberships. The previous membership-based access continues to work in the new model. Cleanup is recommended and is one of the seven phases of migration.

Direct role assignments instead of grants

In the previous access model, permissions were called grants and were always assigned directly to individual security administrators. Security groups did not exist, and the roles available were less granular than in Elements RBAC.

During migration, existing grants are converted to direct role assignments. The underlying access is unchanged. The assignments are now visible in the security administrator's **Role Assignments** tab, and can be managed alongside indirect (group-based) and inherited (hierarchy-based) assignments.

Direct role assignments work but do not scale. Consolidating direct assignments into security groups is recommended after migration to take advantage of group-based management. Change a group's role assignments once, and every member's effective permissions are updated.

What is preserved

Migration preserves all existing state:

- All existing access: every security administrator retains the permissions they had before migration.
- All existing security administrator accounts and their organization memberships.
- The organizational hierarchy of Solution Provider, Service Partners, and Companies.
- SSO Federation configuration, if it was set up before migration.

What needs cleanup after migration

Two cleanup activities are recommended to take full advantage of Elements RBAC:

- Remove partner security administrators from Company memberships, granting them access through role assignments instead.
- Consolidate direct role assignments into security groups for easier ongoing management.

Both activities are covered as separate phases in the migration sequence.

Migration approaches: phased or single-cutover

You can migrate to Elements RBAC in one coordinated operation (single-cutover, also called big bang) or gradually over time (phased). The choice depends on the size of the deployment and the operational constraints.

The two approaches differ in timing, not in outcome. Either approach moves the organization from the previous access model to Elements RBAC and produces the same final state.

Single-cutover migration Turn on RBAC, complete all configuration changes, and finish all cleanup in a single planned window. Configuration changes include security groups, role assignments, and Microsoft Entra ID integration. Cleanup includes removing partner administrators from Company memberships and consolidating direct assignments.

Suitable for:

- Smaller deployments that can be planned and executed within a short window.
- Organizations with strong change management discipline.
- Cases where a mixed state (some access through groups, some still through direct assignments) is undesirable.

Phased migration

Turn on RBAC to make the new operations available, then continue working with the existing access, now represented as direct role assignments. Over weeks or months,

gradually create security groups, consolidate assignments, and remove redundant partner memberships.

Suitable for:

- Larger deployments where coordinating a single migration window is impractical.
- Partners managing many customer Companies that will migrate independently.
- Organizations that prefer to validate the new model with a subset of users before extending it.

Choosing an approach

Both approaches preserve existing access at every stage, so neither is materially riskier for access continuity. The decision is primarily about operational coordination:

- Choose single-cutover if you can schedule a single window for the full migration and you want to operate in a fully consistent state immediately afterwards.
- Choose phased if you cannot afford a single coordinated window, or if you have many Companies to migrate over time. The intermediate state (where security administrators have both direct role assignments and indirect role assignments through groups) is supported by Elements RBAC.

A mixed approach is also possible. For example, a partner can perform a single-cutover migration on their Solution Provider while letting individual Companies migrate at their own pace.

Reversibility of the migration

The migration to Elements RBAC can be reverted to the previous access model. To revert, you must first remove all configuration that depends on RBAC-specific features.

Elements supports reverting an organization from Elements RBAC back to the previous access model. The revert link is on the **Organization Settings > Security Administrators** page after RBAC has been turned on.

What must be removed before reverting

The previous access model does not support the features introduced by Elements RBAC. Before you can revert, the following must be removed:

- All security groups in the organization.
- All access that does not depend on organization membership (for example, role assignments where the security administrator is not a member of the target organization).

If RBAC-specific configuration remains, the revert operation is blocked.

What is preserved after reverting

Security administrators and their organization memberships are preserved. Direct role assignments are converted back to the previous grant model. The organizational hierarchy is unchanged.

When to consider reverting

Reverting is intended as a safety mechanism, not a routine operation. Consider it only if:

- The migration encountered an operational issue that cannot be resolved within Elements RBAC.
- The organization has not yet started taking advantage of RBAC-specific features and prefers to wait.

If the migration is well underway (security groups created, access patterns adopted) reverting requires undoing all that work, which is rarely worth it.

A.5.2 Preparing for migration

Assess your current state, make the pre-migration decisions, and complete the checklist before you turn on RBAC for the first organization.

Preparing for migration produces the outputs you need to perform the migration. These outputs are an inventory of current access, decisions about your target structure, and a sequenced plan you can follow.

Related reference

System limits on page 166

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Assessing your current state

Before you begin the migration, inventory the security administrators, document their current permissions, and assess whether you can integrate with Microsoft Entra ID.

The assessment phase produces the inputs you need for the pre-migration decisions and for the migration sequence itself. Three assessment activities are recommended for every migration.

Inventory the security administrators

Build a complete list of security administrators with access to the organization being migrated. For each one, document:

- The organizations they currently belong to.
- Whether they are partner staff or Company staff.
- Whether their account is local or already federated through SSO.

Identify any partner security administrators who are members of Company organizations. These are candidates for cleanup during the migration. In Elements RBAC, partner staff should belong only to the Solution Provider, with access to Companies granted through role assignments rather than membership.

Document the current permissions

For each security administrator, document the grants (in the previous access model) they currently hold. Group security administrators with identical or similar permissions. These groupings become the basis for the security groups you will create during migration.

The output of this activity is a mapping from current permissions to planned security groups. For example, five security administrators with the same grants can become members of an SOC Team security group with the corresponding role assignments.

Assess Microsoft Entra ID integration

Determine whether Entra ID integration is available and applicable for this organization:

- Does the organization use Microsoft 365 or have an existing Entra ID tenant?
- Are there existing Entra security groups that could be reused, or will new groups need to be created in Entra?
- Are there compliance requirements that benefit from centralized identity governance?

Entra integration is strongly recommended for partners with existing Entra ID infrastructure and for Companies with more than five security administrators.

Pre-migration decisions

Before starting the migration, decide whether to integrate with Microsoft Entra ID, whether to use Service Partners, and which migration approach to follow.

The outputs of the assessment phase inform three decisions that shape the migration sequence.

Decide whether to integrate with Microsoft Entra ID

Full Entra integration uses SSO Federation for authentication and System for Cross-domain Identity Management (SCIM) provisioning for security administrator and group synchronization. It eliminates day-to-day access management in the Elements portal.

- | | |
|------------|---|
| Yes | Recommended for organizations that already use Microsoft 365 or have an Entra ID tenant. The migration sequence will include setting up SSO Federation and SCIM provisioning. |
| No | Suitable for small organizations without Microsoft 365 or with team sizes that do not justify the integration setup. Security administrators and security groups will be managed locally in Elements. |

Decide how many Service Partners to use (partners only)

Service Partners are recommended sub-organizations that group customer Companies under a Solution Provider, and every migrating partner should have at least one:

- | | |
|-----------------|--|
| Multiple | Useful for partners managing many Companies with clear segmentation by managing team, industry, service tier, or geography. |
| Single | Suitable for partners with a small portfolio of Companies or with no clear segmentation. All Companies are grouped under one Service Partner rather than sitting directly under the Solution Provider, preserving the ability to scope IAM Administrator, API Key Management, and Audit Log roles to Companies only. |

Decide the migration approach

Choose between a single coordinated migration or a gradual migration over time:

- | | |
|-----------------------|--|
| Single-cutover | Turn on RBAC, complete all configuration, and finish cleanup in a single window. |
| Phased | Turn on RBAC and continue working with existing access, then gradually create security groups and remove redundant access. |

Migration checklist

Use this checklist to confirm that the assessment and decisions are complete before starting the migration sequence.

Work through the following items before turning on RBAC for the first organization. The checklist consolidates the assessment outputs from assessing your current state and the decision outputs from pre-migration decisions.

Inventory and documentation

- Complete list of security administrators with their current organization memberships.

- List of partner security administrators who are members of Company organizations (for post-migration cleanup).
- Documented current permissions for each security administrator.
- Grouping of security administrators with similar permissions into planned security groups.
- Documented role assignments for each planned security group.

Decisions

- Decision on Microsoft Entra ID integration (yes or no).
- If using Entra integration: Entra ID tenant prepared, Entra security groups defined with a naming convention (for example, ELeMents - SOC - Team), and provisioning filters identified.
- Decision on Service Partner usage (partners only).
- If using Service Partners: planned grouping of Companies under Service Partners.
- Decision on migration approach (phased or single-cutover).
- Identified administrator who will perform the migration in each organization. This administrator must hold the Identity and Access Management (IAM) Administrator role or the Elements Editing All role.

Communication and scheduling

- Affected security administrators notified of the upcoming change.
- Migration window scheduled.
- Verification procedures planned: how you will confirm that access is preserved after each phase.

The migration sequence

The migration to Elements RBAC follows seven phases in order, starting with turning on RBAC and ending with removing partner security administrators from Company memberships.

Each phase has its own procedure. The phases are sequential, because each phase depends on the outputs of the phases before it. You can perform them back-to-back in a single-cutover migration, or spread them over time in a phased migration.

Four of the phases are specific to migration. The other three reuse existing procedures: turning on RBAC, setting up Microsoft Entra ID integration, and creating security groups.

Turning on RBAC	RBAC is enabled per organization. Existing access is preserved and converted to direct role assignments, and the new Access Control pages become available.
Reviewing existing access	The converted access is inspected to confirm the migration succeeded and to identify cleanup candidates. Examples of cleanup candidates are partner staff in Company memberships and patterns of similar permissions.
Setting up Microsoft Entra ID integration	When the planning phase chose Entra integration, SSO Federation and System for Cross-domain Identity Management (SCIM) provisioning are configured. SSO Federation precedes SCIM provisioning, because SCIM provisioning creates federated accounts.
Creating security groups for the new model	One security group is created per permission profile identified during planning. Groups are either created manually in Elements or synchronized from Entra ID.

Migrating from direct role assignments to security groups

Roles are assigned to each security group and the corresponding security administrators become members. After this phase, each administrator has both direct role assignments (from migration) and indirect role assignments (through groups).

Removing redundant direct role assignments

Direct role assignments that are now covered by indirect assignments through groups are removed. The direct **Elements Editing All** assignment for the root security administrator is kept.

Removing partner security administrators from Company memberships

Partner staff are removed from Company memberships; their access is now granted through role assignments at the Solution Provider or Service Partner level.

A.5.3 Performing the migration

Complete the migration in the specified order by reviewing access, converting direct assignments into security groups, and removing redundant access.

Perform each task in sequence. Each step depends on the outputs of the previous step, so skipping ahead is likely to produce inconsistent access.

Review existing access after turning on RBAC

Review the security administrators and their converted direct role assignments to confirm the migration succeeded and to identify candidates for cleanup.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization.
- RBAC turned on for the organization.

The review activity has three purposes:

- Confirm that all expected security administrators are present and that their grants have been converted to direct role assignments.
- Identify partner security administrators who are members of Company organizations. These are candidates for the cleanup phase.
- Identify patterns of similar permissions across security administrators. These patterns become the basis for the security groups you will create.

1. Select the organization in the Scope Selector.
2. Go to **Access Control > Security Administrators**.

The list of security administrators in the selected organization appears.

3. Confirm that the list matches the inventory from the assessment phase.

If a security administrator is missing or unexpected, investigate before proceeding to later migration phases.

4. Note any partner security administrators who appear in Company organization lists.

These are candidates for the cleanup phase.

5. For each security administrator, click the email address and open the **Role Assignments** tab.

The converted grants appear as direct role assignments, with member type **security administrator**.

6. Document the role assignments for each security administrator and identify groups of administrators with similar assignments.

The groupings are the basis for the security groups you create for the new model.

You have confirmed that the migration is in a correct state and have produced two artifacts for the next phases:

- A list of partner security administrators in Company memberships (for the cleanup phase).
- A grouping of security administrators by similar permissions (for the security group creation phase).

Migrate from direct role assignments to security groups

Assign roles to the security groups you created, and add security administrators to the appropriate groups, so that each administrator's permissions come from group membership.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization.
- The security groups already created in Elements (locally-created or Entra-provisioned).

This phase moves the permission management from direct role assignments (per security administrator) to indirect role assignments through security groups. After this phase, each security administrator has both direct role assignments (from the migration) and indirect role assignments through their security group memberships. The direct assignments are then redundant and are removed in the next phase.

1. For each security group, assign the roles that match the group's intended permission profile.

Use the role assignment mapping from the planning phase.

2. Add the corresponding security administrators to each security group.

- For locally-managed groups, add members in Elements.
- For Entra-provisioned groups, add the security administrators to the corresponding Entra groups. System for Cross-domain Identity Management (SCIM) provisioning synchronizes the membership to Elements.

3. Verify that each security administrator has the expected effective access through group membership.

Use the Check Access feature.

Each security administrator now has the same permissions as before, expressed both as direct role assignments (from the migration) and as indirect role assignments through security group membership. The direct assignments are now redundant and can be removed.

Remove redundant direct role assignments

Remove direct role assignments that are now redundant because the same permissions are granted through security group membership.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization.
- The previous phase complete, so that each security administrator has indirect role assignments through security group membership that cover the permissions they need.

After the previous phase, each security administrator has both direct role assignments (from the migration) and indirect role assignments through security groups. The direct assignments are now redundant and add unnecessary complexity to permission management. This phase removes them.



IMPORTANT:

Keep the direct **Elements Editing All** role assignment for the root security administrator in each organization. This direct assignment prevents accidental logout if security group membership becomes corrupted.

1. Go to **Access Control > Security Administrators**.
2. Click the email of a security administrator and open the **Role Assignments** tab.

The tab shows direct, indirect, and inherited assignments. Direct assignments have member type **security administrator**.

3. Compare the direct role assignments with the indirect role assignments and identify which direct assignments are now covered by indirect ones.
4. Select the redundant direct role assignments and click **Delete Assignments**.

Do not delete the direct **Elements Editing All** assignment for the root security administrator.

5. Use the Check Access feature to confirm that the security administrator still has the same effective access through indirect assignments.
6. Repeat for each security administrator.

Each security administrator's permissions now come from security group membership only, except for the root security administrator's direct **Elements Editing All** assignment. The permission model is fully consolidated and easier to maintain.

Remove partner security administrators from company memberships

Remove partner security administrators from Company memberships to keep partner staff managed solely by the Solution Provider, invisible to Company Identity and Access Management (IAM) administrators.

Before you start, make sure you have:

- The IAM Administrator role or the Elements Editing All role in the partner organization and in the Company organization.
- Role assignments in place for each partner security administrator that grant the access they currently have through Company membership. These role assignments can come either through partner security group assignments or through direct role assignments from the Solution Provider.

This is the final phase of the migration. In the previous access model, partner staff were typically added as members of Company organizations to gain explicit access. In Elements RBAC, partner staff should belong only to the Solution Provider, with access to Companies granted through role assignments.



IMPORTANT:

Before removing each partner security administrator from a Company membership, verify with the Check Access feature that they have the equivalent access through role assignments. Removing the membership before establishing role-assignment-based access will revoke the administrator's access to the Company.

1. Select the Company in the Scope Selector.

2. Go to **Access Control > Security Administrators**.

The list of security administrators who are members of this Company appears.

3. Identify the partner security administrators in the list, those who should belong only to the Solution Provider.

Use the inventory from the review phase. Partner security administrators are those who belong to the Solution Provider organization in addition to this Company.

4. For each partner security administrator, use the Check Access feature to confirm that they have role-assignment-based access to the Company.

5. If a partner security administrator does not have role-assignment-based access, configure it before continuing. Either add them to a partner security group that has role assignments to the Company, or assign them directly from the Solution Provider.

6. Select the partner security administrators that are confirmed to have alternative access, and click **Remove from Organization**.

The selected security administrators are removed from this Company's membership. They remain members of the Solution Provider and retain access to the Company through role assignments.

7. Confirm that the partner security administrators no longer appear in the Company's security administrator list. Then use the Check Access feature from the Company context to confirm that they still have the expected access.

8. Repeat for each Company that has partner security administrators in its memberships.

Partner security administrators no longer appear in Company memberships. Company IAM administrators can manage their Company's security administrators without seeing partner internal staff. Partner staff continue to manage the Company through role assignments at the Solution Provider or Service Partner level.

This completes the migration to Elements RBAC.

A.5.4 Verifying the migration

After completing the migration sequence, verify that all security administrators have the expected effective access and that cleanup is complete.

The migration preserves existing access at every phase, but verification is recommended after the migration sequence is complete. Verification confirms that the new access model produces the same effective permissions as the previous model. It also confirms that the cleanup activities did not unintentionally remove necessary access.

What to verify

Effective access for each security administrator	Compare each security administrator's current effective access against the inventory from the assessment phase. The access should be identical except where you deliberately changed it during migration.
Security group membership	Each security administrator should be a member of the security groups that grant their required permissions. For Entra-provisioned groups, confirm that the synchronization is current.
Cleanup completeness	For partner organizations, confirm that no partner security administrators remain in Company memberships, except where intentionally kept. For all organizations, confirm that direct role assignments have been removed where the same permissions are available through security groups. The

exception is the root security administrator's direct Elements Editing All assignment.

SSO and SCIM integration (if configured) Confirm that SSO Federation works for federated security administrators. Also confirm that System for Cross-domain Identity Management (SCIM) provisioning synchronizes security administrators and security groups between Entra ID and Elements.

Verification tools

Elements provides two key tools for verification:

- Check Access** Shows the complete effective access for a security administrator in a selected organization, combining direct, indirect, and inherited role assignments. Use this to confirm equivalence with pre-migration access.
- Role Assignments tab** Shows the full set of role assignments for a security administrator or security group, with member type and organization scope. Use this to inspect specific assignments.

When to verify

For a single-cutover migration, verify after the final phase is complete. For a phased migration, verify after each phase that affects access. This typically means after migrating to group-based permissions, after the cleanup phase, and after removing partner staff from Company memberships.

Verify access after migration

Use the Check Access feature to confirm that each security administrator has the same effective access after the migration as they had before.

Before you start, make sure you have:

- The Identity and Access Management (IAM) Administrator role or the Elements Editing All role in the organization where you are verifying.
- The migration sequence, or the phase you are verifying, complete.
- The pre-migration permission inventory from the assessment phase.

This task uses the Check Access feature to compare a security administrator's current effective access with the access they had before migration. Repeat the task for each security administrator, or for a representative sample if the team is large.

1. Select the organization in the Scope Selector.
2. Go to **Access Control > Role Assignments**.
3. Click the **Check Access** link in the header.
4. Enter the email address of the security administrator you are verifying, and click **Next**.

The effective role assignments for the security administrator in this organization appear, including direct, indirect (through security groups), and inherited (from parent organizations) assignments.

5. Compare the effective access against the inventory from the assessment phase.

The access should be the same. If the migration was supposed to add or remove access (for example, by removing redundant direct assignments) check that those changes match the intended outcome.

6. If the access differs from the expected outcome, investigate the cause.
7. Repeat for each security administrator, or for a representative sample.

Each verified security administrator's effective access matches the expected migration outcome. Any differences that were found and investigated are fixed.

A.5.5 Common migration issues

Common issues encountered during or after migration include unexpected access changes, role assignments that cannot be removed, and synchronization problems with Microsoft Entra ID.

If verification reveals an issue, the cause is usually one of the patterns described below.

A security administrator does not have expected access

Possible causes:

- The administrator is not a member of the security group that grants the access. Check the security group membership and add the administrator if necessary.
- The security group does not have the expected role assignment. Check the group's Role Assignments tab.
- The role assignment was made at a Company level, but the administrator needs access to a different Company. Add a role assignment at the correct scope.
- For Entra-provisioned groups, the Entra synchronization may be delayed. Wait for the next sync, or trigger one manually.

Use the Check Access feature to see the complete effective access and identify which assignments are missing.

A security administrator has unexpected access

Possible causes:

- The administrator is a member of a security group that grants the unexpected role. Review the group's role assignments.
- The administrator inherits the access from a role assignment at a parent organization. Inherited assignments cannot be removed at the child level. Go to the parent organization to remove them.
- A direct role assignment was not removed during cleanup. Remove it from the security administrator's Role Assignments tab.

A role assignment cannot be removed

Three types of role assignment cannot be removed from the security administrator's Role Assignments tab:

- Indirect role assignments (from a security group) cannot be removed directly. They are removed by removing the security administrator from the group, or by removing the role assignment from the group.
- Inherited role assignments (from a parent organization) can only be removed at the parent organization.
- Provisioned group role assignments must be managed by removing the group in Entra ID, since the Entra-provisioned group is immutable in Elements.

Partner security administrators are still visible to Company administrators after cleanup

If a partner administrator still appears in a Company's security administrator list after the cleanup phase:

- The administrator may still be a member of the Company organization. Re-run the cleanup procedure for that Company.

- If the partner administrator was added back to the Company through an invitation, remove them again.

Microsoft Entra ID synchronization is not working

If provisioned security administrators or groups do not appear in Elements as expected:

- Verify in Microsoft Entra ID that the Enterprise Application provisioning is enabled and that the connection test succeeds.
- Confirm that the provisioning filters match the names of the Entra security groups you expect to synchronize.
- Check that each Entra user has the email field populated.
- Initial synchronization can take 20 to 40 minutes after activation.

The role assignment limit is reached

If you cannot add a new role assignment because the per-security-administrator or per-security-group limit has been reached:

- Use inheritance instead of repeating the same role assignment at each Company. A single assignment at the Solution Provider or Service Partner level applies to all descendant organizations.
- Consolidate direct user assignments into security groups.
- Remove redundant or obsolete role assignments.

Related reference

System limits on page 166

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

A.6 RBAC reference

Use these tables and definitions when you need details on roles, system limits, or terminology.

The role catalogue lists every Elements role and the permissions it grants. The system limits topic gives the per-account and per-organization quotas you should plan against. The glossary defines the RBAC terms used throughout the guide.

A.6.1 Role catalogue

Elements RBAC organizes roles by capability and permission level, from broad access to precise control of specific features.

Large-scope roles

Large-scope roles are continuously maintained by WithSecure. When new features are added to Elements, these roles automatically include appropriate permissions.

Table 10: Large-scope roles

Role name	Description	Use case
Elements Editing All	Full editing access to all current and future features	Root accounts, administrators, full access users
Elements Reading All	Read-only access to all current and future features	Executive dashboards, auditors, read-only monitoring

**NOTE:**

Large-scope roles cannot be decomposed. You cannot exclude Identity and Access Management (IAM) from an Elements Editing All assignment or exclude specific capabilities from a large-scope role. If you need selective access, use granular roles instead.

Granular roles by capability

Granular roles provide precise control over specific feature areas. They are static and do not automatically expand when new features are added.

Table 11: Exposure Management (XM)

Subcategory	Access level	Description
Exposure	Editing	Full access to Exposure Management: Environment, Security configurations, Management, Reports, and Cloud onboarding
Vulnerabilities	Management	Full access to use and manage the Vulnerability Management system
Vulnerabilities	Editing	Full access to Vulnerability Management views, settings, and findings without system management permissions
Vulnerabilities	Reading	View-only access to Vulnerability Management
Vulnerabilities	Discovery scans reading	View discovery scans for hosts and networks and their results
Vulnerabilities	Discovery scans editing	View and manage discovery scans for hosts and networks
Vulnerabilities	Discovery scans start & stop	Start and stop discovery scans without viewing or managing configurations

Subcategory	Access level	Description
Vulnerabilities	Vulnerability scans reading	View vulnerability scans for hosts and applications (system and web scans)
Vulnerabilities	Vulnerability scans editing	View and manage vulnerability scans for hosts and applications
Vulnerabilities	Vulnerability scans start & stop	Start and stop vulnerability scans without viewing or managing configurations
Vulnerabilities	Reports reading	Read-only access to vulnerability reports and security findings
Vulnerabilities	Reports editing	Edit and manage summary vulnerability and vulnerability scan reports
Vulnerabilities	Tickets reading	View remediation tickets and details
Vulnerabilities	Full tickets editing	Full ticket management for vulnerability remediation (requires Tickets reading role)
Vulnerabilities	Own tickets editing	View and manage own tickets only (requires Tickets reading role)
Vulnerabilities	Settings reading	View organization-wide vulnerability management settings
Vulnerabilities	Settings editing	Manage organization-wide vulnerability management settings (requires Settings reading role)
Vulnerabilities	Account management	Vulnerability management system administrator capabilities

Table 12: Collaboration Protection (ECP)

Subcategory	Access level	Description
Collaboration Protection	Administrator	Full access to Collaboration Protection views including policy management
Collaboration Protection	Reading	View-only access to Collaboration Protection views
Collaboration Protection	Quarantine manager	Editing access to detections and quarantined files

Table 13: Endpoint Protection (EPP)

Subcategory	Access level	Description
Endpoints & profiles	Reading	View devices, security events, and Endpoint Protection profiles
Endpoints & profiles	Full management	Complete management of devices, profiles, and profile assignment rules for all endpoint types
Endpoints & profiles	Managing non-servers	Management of computers and mobile devices (servers read-only)
Endpoints & profiles	Managing servers	Management of server devices (computers and mobiles read-only)

Table 14: Extended Detection and Response (XDR)

Subcategory	Access level	Description
Broad Context Detections	Reading	Read access to detections and configuration for Extended Detection and Response
Broad Context Detections	Editing	Manage Broad Context Detection status, suppression rules, and reports
Response	List responses	Review executed response actions and availability of results
Response	Execute responses	Execute response actions, download results, and configure automated actions
Event Search	Reading	Review, execute filtered searches, and create customized views of event data

Table 15: Environment

Subcategory	Access level	Description
Cloud configuration	Reading	View cloud connections without the ability to make changes
Cloud configuration	Editing	Onboard and offboard cloud products for XDR and Exposure Management

Table 16: Elements administration

Subcategory	Access level	Description
Identity and Access Management	IAM Administrator	Manage security administrators, security groups, role assignments, API keys, and SSO federation. The holder of this role can grant all system permissions to themselves.



NOTE:

Some roles require other roles to function properly. For example, **Full tickets editing** requires the **Tickets reading** role.

Choosing between large-scope and granular roles

- Use Elements Editing All or Elements Reading All when:
- The security administrator needs comprehensive access.
 - You want automatic access to new features.
 - Simplicity is preferred over granularity.
 - The role is administrative or monitoring.

- Use granular roles when:
- You need precise feature-level control.
 - Different teams access different capabilities.
 - Compliance requires separation of duties.
 - You want explicit control over feature access.

A.6.2 System limits

Elements RBAC enforces operational limits on organizations, security groups, security administrators, and role assignments to maintain system performance and stability.

Table 17: System limits

Resource	Maximum Limit	Description
Organization memberships per user	50	Maximum number of organizations a single user account can belong to
Users per security group	500	Maximum members in a single security group
Security group memberships per user	50	Maximum number of security groups a user can belong to
Security groups per organization	100	Maximum number of security groups that can be created in one organization

Resource	Maximum Limit	Description
Role assignments per user or group	100	Maximum number of role assignments for a single directory member
User accounts per organization	1,000	Maximum number of security administrators in a single organization

Important notes

- These limits apply to both locally-managed and Entra-provisioned entities
- When using Entra ID provisioning, ensure that your provisioning filters do not exceed these limits
- For partners managing many companies: Users should belong only to the Solution Provider organization (one membership), not to individual company organizations
- Large organizations approaching these limits should contact WithSecure support to discuss architectural options

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.

Access Without Membership

The capability for a security administrator to have permissions for an organization without being a member of it, typically used by partner security administrators to manage customer companies.

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.

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.

Browsing Protection

A feature that evaluates the safety of visited websites and prevents users from unintentionally accessing harmful websites.

Browsing Protection Extension

The Browsing Protection Extension is a browser component that enables web protection features such as reputation-based site analysis and policy-based web content control.

Certificate

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

Company

A customer organization, either managed by a partner or standalone, that is the lowest level in the organizational hierarchy and has no child organizations.

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.

Direct Role Assignment

A direct role assignment grants a role to an individual account instead of granting access through group membership or another indirect path.

Discovery Scan

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

Effective Permissions

The combined set of permissions a security administrator has in a given organization, calculated as the union of all direct, indirect, and inherited role assignments that apply.

Email Sample

An email sample is an email message collected and submitted for security analysis, validation, or investigation.

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).

Event

A monitored occurrence on a device that a sensor has detected and that matches the definition of a detection.

Exclusion Rules

Exclusion rules are rules that omit specific files, paths, processes, or other items from scanning, monitoring, or enforcement.

Exposure Management

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

False Negative

A false negative is a harmful file, message, URL, or activity that a security system incorrectly fails to identify as malicious or suspicious.

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 Account

A security administrator account, owned by the federated organization and authenticated through Entra ID, where SSO Federation is enabled for the email domain.

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.

File Sample

A file sample is a file collected and submitted for security analysis, validation, or threat investigation.

Forensics

Forensics is the collection and analysis of evidence from systems, processes, files, or memory to investigate suspicious or malicious activity.

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.

Host

A device that runs a sensor and that the sensor's platform monitors.

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 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.

Indirect Role Assignment

A role assignment that a security administrator receives through membership in a security group.

Infection

An infection is the state in which a file, object, system, or workload contains or has been affected by malicious code or other harmful content.

Inherited Role Assignment

A role assignment made at a parent organization that automatically applies to all child organizations through the organizational hierarchy.

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.

Local Account

A security administrator account, owned by the security administrator and authenticated with an Elements password, created without SSO Federation.

Malware

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

Malware Protection

Malware Protection is the feature that detects, blocks, and removes viruses and potentially unwanted applications on a device.

Managed Detection and Response (MDR)

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

Member

A security administrator or security group that belongs to an organization or to another security group.

Membership

Membership is the state of belonging to a group, organization, directory, or other managed collection that affects visibility, access, or inherited permissions.

Mobile Device Management (MDM)

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

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.

OAuth

OAuth is an open standard for delegated authorization that lets an application access resources on a user's behalf without exposing the user's credentials.

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.

Organization

The container for security administrators, security groups, and role assignments in Elements RBAC; the three organization types are Solution Provider, Service Partner, and Company.

Organization Hierarchy

An organization hierarchy is a structured arrangement of organizations or sub-organizations that defines visibility, inheritance, or management relationships.

Organization Membership

The state of a security administrator belonging to an organization, visible in that organization's security administrators list and distinct from access.

Partner

An organization that manages one or more customer companies, either as a Solution Provider or a Service Partner.

Patch Management

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

Phishing

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

Potentially Unwanted Application (PUA)

A software program that may not be malicious but could introduce security risks, intrusive behavior, or unwanted advertisements.

Privacy

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

Profile Assignment

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

Quarantine

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

Ransomware

A malicious program that prevents the user from accessing their data and/or device and demands a ransom to 'restore normal access'. The program may not actually restore normal access even if the ransom is paid.

Real-Time Scanning

Real-time scanning is continuous scanning that checks content or activity as it is accessed, saved, or processed.

Remote Monitoring and Management Integration (RMM)

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

Resource

In the RBAC subject-role-resource model, the organization where a role assignment applies.

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.

Root User Account

The first security administrator in an organization, which receives the Elements Editing All role directly as a fallback for organization-level recovery; also referred to as the Root account.

Sample Submission

A sample submission is a request that sends a suspicious file, URL, or email for analysis and follow-up handling.

Sample Validation

Sample Validation is a service for submitting suspicious files, URLs, or emails for expert analysis and tracking the results of the request.

Scan

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

Scan Node

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

Scan Templates

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

SCIM

System for Cross-domain Identity Management, the protocol Entra ID uses to provision security administrators and security groups to Elements.

SCIM Provisioning

SCIM provisioning is the automated synchronization of users and groups between an identity provider and another service by using the System for Cross-domain Identity Management standard.

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.

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.

Spam

Spam messages are unsolicited email messages that are usually sent in bulk to a large list of recipients.

SSO Federation

SSO Federation is a single sign-on arrangement where authentication for a domain or service is delegated to an external identity provider.

Subject

In the RBAC subject-role-resource model, a security administrator or security group that receives a role assignment.

Subscription Key

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

Tenant

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

Threat Detection

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

Threat Intelligence

Threat intelligence is evidence-based knowledge about existing or emerging threats — such as

attacker tactics, indicators, and motivations — used to inform defensive decisions.

Trojan

A Trojan is malicious software that disguises itself as a legitimate program to trick users into running it, then performs harmful actions such as stealing data or opening a backdoor.

Unwanted Application

An application that can compromise privacy or has a severe impact on a device's security.

URL Sample

A URL sample is a submitted web address collected for security analysis, validation, or investigation.

User Invitation

A user invitation is the process or message used to add a new user or administrator to a service, organization, or managed scope.

Virus

A virus is usually a program that can attach itself to files and replicate itself repeatedly; they can alter and replace the contents of other files in a way that may damage the computer.

Virus Definition

A virus definition is a signature used to identify known viruses and other malware during a scan.

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 84, 108
 access management 22, 80, 85
 access rights 17, 23, 25
 access without membership 91
 account 14
 account creation 24
 account details 26
 account identity 120
 account levels 21
 account linking 12
 account ownership 106
 Active Directory 40
 active threat 64
 AD groups 40
 adding devices 35, 39
 administrator 108
 administrator account 17, 23–24, 48
 Advanced Endpoint Protection 76–77
 Agent for Computers 35
 Agent for Servers 35
 Agent for Windows 42
 agentic identities 70
 agentic identity visibility 68
 AI agent identities 68
 AI agents 70
 AI assets 68–70
 AI Dashboard 68
 AI Security 68–70
 AI Security dashboard 68
 AI software 69
 AI tool visibility 68
 allowlisting 45, 47
 allowlisting request 46, 51
 Android 63
 API client 25
 API credentials 75–76, 78
 API key 77
 API user 75
 approve AI asset 70
 asset groups 38–39
 audit logs entry 17
 authentication 138–139
 authenticator app 8–9
 Authenticator applications with Time-Based One-Time Password (TOTP) 8
 automated tickets 75–77
 automatic deletion 36, 40
 Autotask 75–76
 Autotask PSA 75–76
 Available WithSecure services 33

B

backup 43
 ban AI asset 70
 best practices 58, 94–96, 148
 big bang migration 151
 biometric authentication 10
 Business Account 7

C

change name 26
 change subscription 30
 Check Access 131, 160
 checklist 153
 cleanup 156–157
 company 80, 83, 93, 99–100, 103–104, 110
 company administrator 113
 company level 39
 Company level 40
 company membership 158
 company organization 91, 112
 Company scope 72
 company user 84
 ConnectWise 75–76
 ConnectWise PSA 76–77
 core concepts 80
 create request 72
 Create Request 52–54
 creating security group 121
 cross-tenant access policies 109
 custom labels 38
 customer company 17, 28
 customer isolation 80
 customer mapping 77

D

dashboard 55
 data recovery 43
 deactivation 118–119
 delete API client 25
 deleting security group 121
 deletion 118–119
 deployment 94
 deployment planning 92–93
 deprovisioning 149
 detailed roles 87
 Detection and Response Team 72
 detection quality 45
 detection update 57
 device assignment 39
 device biometrics 10
 Device biometrics 8
 device commands 39
 device filters 41
 device grouping 38
 device invitations 37
 device labels 38
 Device list 38
 device management 35–36, 38, 40–41
 device view 38, 40
 devices 30, 39
 Devices page 39
 Devices view 41
 diagnostic data 42
 diagnostic logs 64
 direct role assignment 89, 124, 135, 156–157
 directory 106
 domain federation 13
 downloading software 36
 Downloads page 36

Dropzone 58–64

E

Early Access 68
 edit administrator 24
 edit profile 26
 Editing All 88, 108, 113
 EDR 31, 36
 EDR and EPP for Computers 31
 EDR and EPP for Computers Premium 31
 EDR and EPP for Servers 31
 EDR and EPP for Servers Premium 31
 EDR for Computers 31, 36
 effective access 131, 137, 159–160
 effective permissions 90
 Elements API 25
 Elevate Requests 72
 email address 12
 email aliases 12
 email invitation 37
 email sample 51, 54, 62–63
 enterprise application 143
 Entra ID integration 138, 145, 147–149
 EPP for Computers 31, 39–40
 EPP for Computers Premium 31
 EPP for Servers 31, 39–40
 EPP for Servers Premium 31
 EPP subscription 30
 escalation 57
 existing access 156
 Extended Detection and Response 75–77

F

false negative 45–47, 57, 64
 false positive 45–47, 57, 63
 federated account 106, 117
 federated authentication 140
 federated domain 7, 14, 139
 federated single sign-on 12–13
 file sample 51–52, 58–59, 63
 file-based false negative 46
 file-based false positive 46
 filtering 143
 fingerprint 10
 forgot password 26
 FSSO 12

G

getting started 97
 granting access 122
 granular roles 162

H

Halo 75
 HaloPSA 77–78
 hard delete 117

I

IAM administrator 22, 106
 IAM role 17, 22
 Identity and Access Management 22

identity management 138
 identity provider 12
 in-product reporting 57
 Incident Readiness and Response 33
 indirect access 135
 indirect assignment 122
 indirect role assignment 89
 Infinite 72
 inheritance 82, 96, 104, 133
 inherited role assignment 89, 104
 inspecting access 130
 installation link 37
 installation package 35–36
 isolation 100

L

label assignment 38
 large-scope roles 88, 137, 162
 lifecycle management 118
 limitations 105, 120, 137, 147
 Linux 59, 61, 63–64
 local account 106
 local security group 86
 logging in 7
 login 7, 26
 login credentials 7
 login security 8

M

macOS 59, 61–62, 64
 malicious application 63
 managed companies 21
 manual management 109–110
 member view 122
 membership 85–86, 105, 108, 112, 114, 117, 150
 MFA 8–9
 MFA methods 8
 Microsoft Entra Admin Center 12
 Microsoft Entra ID 7, 12–14, 70, 86, 92–93, 99, 118–119, 138–145, 147–149, 153–154, 161
 migration 149–150, 152–161
 migration approach 150–151, 154
 migration checklist 154
 migration sequence 149, 155
 Mobile Protection 35, 39, 42, 63
 moving organization 101
 multi-factor authentication 8–10
 multi-tenancy 80
 My report 68
 My settings 9, 26
 My WithSecure services 33

N

new customer company 29
 non-federated domain 7

O

offline devices 36, 40
 onboarding 118
 open request 56
 ordering products 29

- organization 80, 82, 90, 92, 97, 100, 102–103, 105, 108, 117, 122, 130, 166
- organization hierarchy 82, 92, 95, 101, 133
- Organization Settings 23–25, 39
- organization types 83
- organization view 122, 125, 136
- organizing environment 100

P

- parent organization 133
- partner 24, 80, 92, 99, 104, 110
- partner access 100
- partner hierarchy 103
- Partner Portal 28–29
- partner security administrator 91, 104, 158
- partner user 84
- partner-company business model 80
- password recovery 26
- patch management 5
- pending invitations 37
- permission management 96
- permissions 17, 85, 87, 120–122, 124, 153, 162
- phased migration 151
- phishing 54, 60–61
- phishing false negative 46
- phishing false positive 46
- phishing prevention 109
- Phone number for Short Message Service (SMS) messages with One-Time Passwords (OTP) 8
- portal 57
- portal user 84
- pre-migration decisions 154
- pre-migration planning 149
- Premium subscription 31
- preparation 153
- prerequisites 48
- product deployment 28
- profile assignment 40
- profile assignment rules 38
- provisioned security administrator 120
- provisioned security group 86, 118
- provisioning 118, 147
- PSA integration 75–77
- PSA platform 75
- Push notifications with Auth0 Guardian authenticator 8

Q

- quarantine 59
- Quarantine Dumper 59
- quarantined files 59
- quick start 97, 99

R

- ransomware 64
- ransomware reporting 45, 58, 64
- Reading All 88
- reference 162
- remote device management 39
- remote request 42
- remove administrator 24
- removing federation 14
- removing MFA 9
- removing role assignment 135

- reputation cache 57
- request comments 56–57, 72
- request details 72
- request status 51, 55, 72
- request type 72
- request view 55
- request views 51
- reset password 26
- resource 81–82, 88, 122
- Resource 80
- response time 48
- restricting partner access 104
- revalidation 101
- reversibility 150, 152
- revoking access 116–117, 134–136
- role 17, 81, 87–88, 122, 124
- Role 80
- role assignment 17, 80–82, 88–92, 96–97, 101, 104–105, 108, 114, 116, 119–120, 122, 125, 130–131, 133–137, 150, 155–157, 161, 166
- Role Assignments tab 125, 136
- role catalogue 162
- role permissions 22
- role-based access control 80
- roles 162
- rollback 152
- root account 113
- root user 108

S

- sample collection 59
- sample gathering 58, 60, 62
- sample submission 45, 48, 51, 64
- sample type 51
- Sample Validation 45, 48, 51, 57–64
- Sample Validation request 52–56
- SCIM provisioning 138, 141–145, 148–149
- scope 96, 137
- scope selector 21, 23, 28–29, 39, 52, 100
- Secure USB keys 8
- security administrator 17, 23, 84, 87, 89–90, 99, 106, 108–112, 114, 116–121, 124–125, 130–131, 134–135, 137, 141–142, 150, 153, 156, 160
- security administrator account 106
- Security Administrators 24
- Security Center 5, 7–10, 12–14, 17, 21–23, 26, 28–29, 35–36, 38–40, 42, 45, 48, 50, 52–56, 64, 72, 75–78, 80, 84, 106, 109–110
- Security Cloud 57
- security group 80, 82, 85–86, 92–93, 96–97, 99, 111, 114, 116, 119–122, 130, 134–135, 141–145, 149, 156–157, 166
- security group membership 159
- security request 72
- security roles 22
- Security services 33
- security team 93
- service 43
- service availability 48
- service delivery 50
- service partner 83, 95, 100, 102–103, 154
- service partner account 24
- service scope 47
- Services 45
- shadow AI 68–69
- Show AI assets 69

- single sign-on 7, 12–14, 139–140
- Smartphones or other devices 8
- software distribution 35
- software inventory 69
- solution provider 83, 95, 102, 111, 158
- Solution Provider 21, 28
- spam false negative 46
- SSO Federation 138–140, 145, 148
- standard roles 87
- sub-organization 102
- subject 81, 84, 88, 122
- Subject 80
- subject-role-resource model 81
- subscription 28–29, 35–36, 48
- subscription assignment 28
- subscription key 28–31, 35
- subscription upgrade 30–31
- subscriptions 28–29
- Subscriptions view 29
- support 42, 57
- support hours 48
- synchronization 142, 144
- system limits 162, 166

T

- table columns 41
- tenant 109
- terminology 162
- third-party integration 75
- ticket creation 78
- ticket queue 76
- troubleshooting 137, 145, 161
- turning on RBAC 97
- two-factor authentication 8

U

- upgrading options 30
- URL categorization 45, 47, 53
- URL false negative 46
- URL false positive 46
- URL sample 51, 53, 60–61
- URL submission 60
- user identity linking 14
- user invitation 109–113
- user management 17, 106, 141
- user name 26

V

- verdict 57
- verification 145, 159
- viewing access 130
- virus definitions 57
- visibility 84, 100
- Vulnerabilities role 17
- vulnerability management 5
- Vulnerability Management: 22

W

- Windows 58, 60, 62, 64
- WithSecure 5, 7, 21–22, 28, 42
- WSDIAG file 42
- wsdumpqrt 59

Z

- ZIP archive 58–59