



WithSecure Exposure Management

Contents

Chapter 1: Introduction to the WithSecure Elements solution.....	4
1.1 Using WithSecure Elements Security Center.....	5
Chapter 2: Elements Exposure Management overview.....	38
2.1 Why Exposure Management matters.....	39
2.2 Exposure Management.....	40
2.3 Key features.....	40
2.4 Attack surface coverage.....	41
Chapter 3: Getting started.....	42
3.1 Quick start.....	43
3.2 Create the first WithSecure business account.....	44
3.3 Logging in to Elements Security Center.....	44
3.4 Create administrator accounts.....	45
3.5 Grant existing users the Exposure Management role.....	45
Chapter 4: Asset onboarding.....	46
4.1 Device onboarding	47
4.2 Cloud account onboarding.....	60
4.3 Network asset onboarding.....	65
4.4 Identity onboarding.....	66
Chapter 5: Managing scans.....	67
5.1 Device scans.....	68
5.2 Cloud account scans.....	74
5.3 Network asset scans.....	76
5.4 Identity scans.....	77
Chapter 6: Managing exposures.....	78
6.1 Exposure dashboard.....	79
6.2 Recommendations.....	81
6.3 Findings.....	83
6.4 Exposure management for operational technology.....	84
Chapter 7: Reporting.....	86

7.1 Create vulnerability management reports.....	87
7.2 Add widgets to My report.....	89
7.3 View vulnerability management reports.....	89
7.4 Create exposure management reports.....	90
7.5 Configure email reports.....	90
7.6 Create a custom view for security events.....	91
7.7 Edit the settings of an existing report.....	91
7.8 Clone an existing report.....	91
7.9 Update contents of existing reports.....	92
7.10 View Executive summary.....	92
7.11 Delete reports.....	92
Chapter 8: General management.....	93
8.1 Device assets.....	94
8.2 Scan nodes.....	97
8.3 Delete cloud accounts.....	100
8.4 Users.....	100
8.5 Settings.....	101
Chapter 9: Troubleshooting.....	103
Appendix A: Using Infrastructure-as-Code tools.....	105
A.1 Implement infrastructure with Terraform.....	106
A.2 Implement infrastructure with CloudFormation.....	106
Appendix B: Authenticated scanning.....	108
B.1 Windows authenticated scanning (WinRM).....	110
B.2 Windows authenticated scanning (RPC).....	118
B.3 Linux authenticated scanning.....	124
B.4 Windows SSH scanning.....	129
Glossary.....	132
Index.....	138



Chapter 1

Introduction to the WithSecure Elements solution

Topics:

- Using WithSecure Elements Security Center

Introduction to the WithSecure Elements solution

Overview of the WithSecure Elements solution and its offering.

WithSecure Elements overview	WithSecure Elements is our single modular solution made up of a full range of cyber security applications that offer end-to-end business and cloud coverage. The product includes our award-winning technologies in vulnerability management, patch management, endpoint protection, and endpoint detection and response. In today's unpredictable, ever-changing business environment, our all-in-one security solution helps to build and ensure a resilient business.
The WithSecure Elements offering	WithSecure Elements has been specifically designed to support the modern agile business environment, which constantly needs to adapt not only to the external threat landscape, but also to the changing business needs. To highlight some of the main benefits: • Centralized and streamlined cyber security management to improve productivity • All the needed software components integrated into one for smooth deployment • Available as a fully managed service or as a self-managed cloud solution The solution also offers flexible licensing options, which means that you can pick and choose which of WithSecure Elements applications your business needs.
Supported languages	The Elements Security Center supports the following languages: • English (US), Finnish, French, German, Italian, Japanese, Polish, Portuguese (Brazil), Spanish (Latin America), Swedish Endpoint products support the following languages: • English, Czech, Danish, Dutch, Estonian, Finnish, French, French (Canadian), German, Greek, Hungarian, Italian, Japanese, Norwegian, Polish, Portuguese, Portuguese (Brazilian), Romanian, Russian, Slovenian, Spanish, Spanish (Latin America), Swedish, Turkish, Traditional Chinese (Hong Kong), Traditional Chinese (Taiwan), and Simplified Chinese (PRC).
WithSecure Elements training	For an introductory Elements training session, log into the WithSecure Academy via the Partner Portal.
Accessing the WithSecure Elements Security Center	You can access Elements Security Center as follows: WithSecure Elements Security Center

1.1 Using WithSecure Elements Security Center

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

This chapter describes the following tasks:

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

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

1.1.1 Get started with WithSecure Elements Security Center

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

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

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



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

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

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

1. Log in to Elements Security Center.

- a) Log in at WithSecure Elements Security Center sign-in page with your Business Account credentials. For the login options, see [Logging in](#).
- b) If you manage more than one company, switch between them with the scope selector, as described in [Move between the managed companies](#).

2. Set up multi-factor authentication (MFA).

- a) Turn on MFA for your account, as described in [Choose multi-factor authentication](#).
- b) Choose an authentication method that fits your needs. For the available methods, see [MFA methods](#).

3. Add administrator accounts.

- a) Invite additional administrators and assign their roles, as described in [Invite Security Administrator to company organization](#).

4. Assign a subscription and deploy a product.

- a) Assign a subscription key for the company, as described in [Assign a subscription key for a customer company](#).
- b) Download the installer for the product that you want to deploy, as described in [Download software from Elements Security Center](#).

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

1.1.2 Logging in

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

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

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

Log in to non-federated domains

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

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

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



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

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

Log in to federated domains

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

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

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

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



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

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

Multi-factor authentication

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

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



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



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

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

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

MFA methods

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

The methods include the following:

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



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



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

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



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

Choose multi-factor authentication

Chooses one or more multi-factor authentication methods.

Before you choose a multi-factor authentication method:

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

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



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

To choose one or more multi-factor authentication methods:

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



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



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

*The **Multi-Factor Authentication Settings** window opens.*

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



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

Remove a multi-factor authentication

Removes a multi-factor authentication method.

To remove a multi-factor authentication method:

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



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

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

Use device biometrics

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

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

To use device biometrics, do the following:

1. In Elements Security Center, select



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

*The **My settings** window opens.*

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

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

1.1.3 User management

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

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

About access rights

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

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

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

Access rights by role

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

Exposure Management – Exposure

- | | |
|---------------------|--|
| Full editing | Allows access to the following Exposure Management features: |
| | <ul style="list-style-type: none"> • Environment: Devices, Cloud, Network, Exposure, Identities • Security configurations • Reports • Management • Cloud onboarding |



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

Audit logs entry: cspm: admin

Exposure Management – Vulnerabilities

Management

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



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

Audit logs entry: vm: administrator

Team member

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

Audit logs entry: vm: team_member

Read-only

View-only access with no permission for managing users.

Audit logs entry: vm: readonly_team_member

Collaboration Protection

Admin

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

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

Audit logs entry: cpo365:admin

Read-only

Grants view-only access to the Collaboration Protection views.

Audit logs entry: cpo: readonly

Quarantine manager

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

Audit logs entry: cpo365:quarantine_mgr

Collaboration Protection – Management

Admin

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



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

Audit logs entry: fusion_admin

Endpoint Protection

No access

No access to Endpoint protection features including:

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



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

Endpoint Protection - Computers and mobiles

Full editing Allows the access to the following features:

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



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

Audit logs entry: epp: manage_computers_mobiles_only

or epp: manage_all

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

Audit logs entry: epp: manage_servers_only

or epp: readonly

Endpoint Protection - Servers

Full editing Allows the access to the following features:

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



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

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

Audit logs entry: epp: manage_servers_only

or epp_manage_all

Read-only

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

Audit logs entry: epp: manage_computers_mobiles_only

epp: readonly

Extended Detection and Response - Toggle off

No access

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

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

Extended Detection and Response - Broad Context Detections

Full editing Permission to manage:

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

Limited access to:

Devices view

Cloud view

Subscription view

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



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

Audit logs entry: elements:xdr-incident-full

Read-only

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

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

Access to the Subscription view is limited.

Audit logs entry: elements:xdr-incident-read

Extended Detection and Response - Response

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

Extended Detection and Response - Event Search

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

Elements Administration

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

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

Move between the managed companies

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

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

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

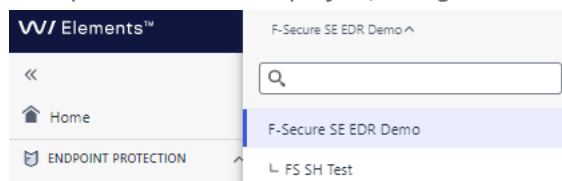
To use the scope selector to focus on a particular company:

1. Select the



icon at the title bar.

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



2. Select the desired company or write its name in the Search field, and then select **Enter**.

The name of the selected company is shown with a blue background color and the page is updated to show the relevant information for the selected company.

Elements Identity and Access Management (IAM) role

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

Overview

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

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

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

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

Benefits

The IAM role provides several benefits, including the following:

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

Claiming the IAM role

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

Elements IAM role properties

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

IAM administrators can do the following:

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

Acquiring the IAM role

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

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

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

Migration of IAM permissions

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

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

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



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

When IAM administrator candidate cannot be identified

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

Frequently asked questions about IAM roles

Answers to frequently asked questions about IAM roles.

Question

Can partners (SOP/SEP) create IAM roles for all companies under them?

What should a company administrator do if the company misses the IAM deadline (end of April 2025)?

When creating a new user using the self-registration portal, does the first administrator get an IAM role automatically?

What happens if someone accidentally selects Decline when claiming the highest-level administrative role?

Can an Endpoint Protection administrator user who selects **Decline** still add other Endpoint Protection administrator users?

Can one organization have multiple IAM administrator users?

Why are the Claim and Decline options not displayed for some administrator users?

How can I identify who in my organization has claimed an IAM role?

Answer

Yes, IAM administrators at the partner level can fully manage their own organization and organizations under them excluding companies that have chosen to isolate their XM/CP access from SOPs.

The company administrator must contact their Service partner for assistance or reach out to WithSecure support.

Yes, the first administrator is granted the IAM role automatically.

If a user accidentally declines the IAM role claim, any other IAM administrator can still assign them an IAM role, if necessary.

Yes, for time being, this is still possible. In the future, all user management action rights will be restricted to IAM role holders only.

Yes, there is no limit to the number of IAM administrators that an organization can have.

In the first stage, the IAM Claim button is shown to users who have full administrator rights on all products for which the organization has subscriptions. For example, if a company has subscriptions for Elements Endpoint Protection and Collaboration Protection, the IAM Claim button is shown to users with full administrator roles on both products.

The IAM role is shown, and users with the role can be filtered in a table under **Management > Security Administrators**.

Add a new administrator

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

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

To create an administrator account:

1. Under **Management**, select **Organization Settings** on the sidebar.

The **Organization Settings** page opens.

2. Select the **Security Administrators** tab.



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

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



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

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



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

8. Select **Next**.

The *Summary screen* opens.

9. Check that the administrator details the selected roles are correct, and then select **Add** to complete adding the new administrator.

A new administrator account is created.



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

Add a new service partner

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

To create a service partner account:

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

The service partner account is created.

Edit or remove administrators

You can edit or remove administrators accounts.

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

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



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

The administrator account is deleted.

Create an API client

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

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

To create an API client:

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



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

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

A new API client is created.

Delete an API client

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

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

To delete an API client:

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

Recover your password

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

To recover your password:

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

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

Change your account details

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

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



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

To change your user name:

1. Select



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

2. Under **Details**, enter a new user name.
3. Select **Save**.

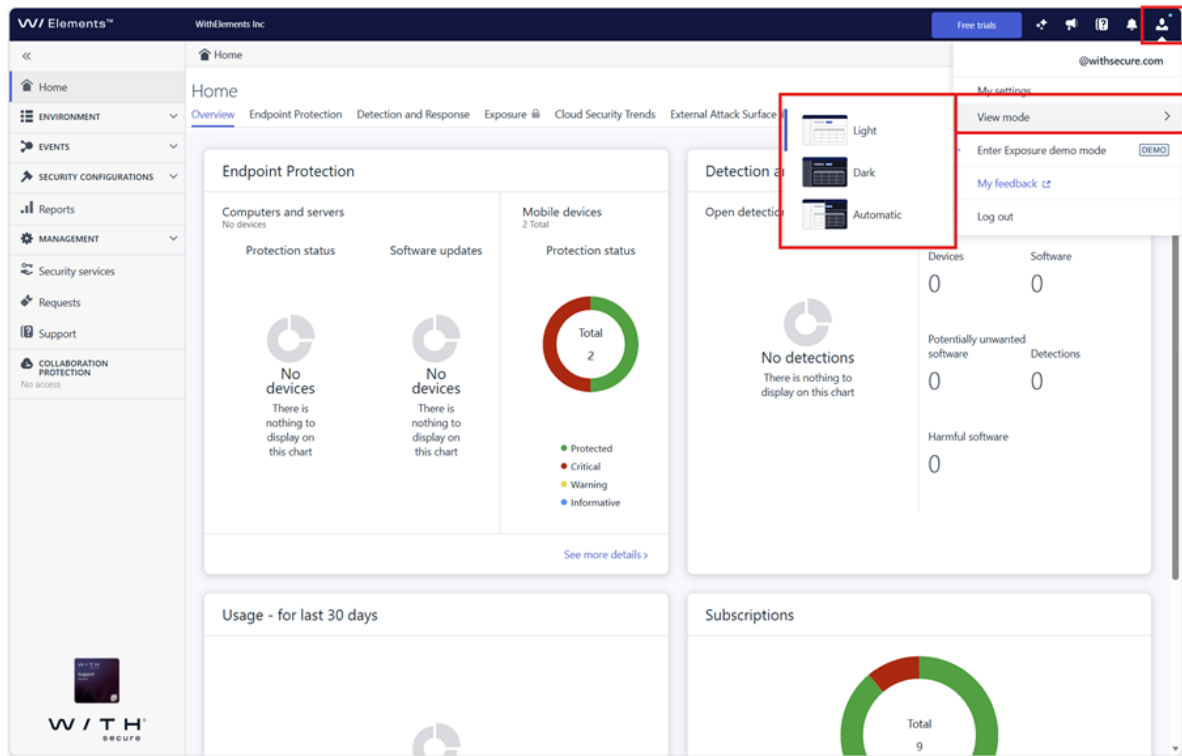
1.1.4 Change the view mode

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

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

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

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



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

1.1.5 Taking Elements products into use

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

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



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

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



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

Adding a customer company

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



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

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



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

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

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

Assign a subscription key for a customer company

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

You need to consider the following:

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



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

To assign a subscription key:

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

The new subscription key is added to the company account.

Order products for an existing customer company

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



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

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

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



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

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

2. On the main page, select **My Customers**, and then select the name of the customer company for which you are ordering products.
3. In the **Order** column, select either **New SaaS Order** or **New Yearly Order**.

*The **Welcome to Ordering** window opens.*

4. Under **New Order**, enter a reference number for your order.
5. Under **Order Products**, select **Add Products**.
6. Select the required products and follow the ordering instructions.

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

Order products for a new customer company

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



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

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

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



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

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

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

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



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

View available product subscriptions

To view the available subscriptions:

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

1. Under **Management**, select **Subscriptions**.

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



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

2. You can use filtering to find the following:

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

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



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

Change the subscription key

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

To change the subscription key:



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

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



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

The new subscription key is applied to the selected devices.

Upgrading your subscriptions

Options for upgrading your WithSecure Elements subscriptions.

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

Upgrading your subscriptions

You can upgrade your subscription in two ways:

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

You have the following options in upgrading your subscriptions:

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



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

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

1.1.6 Federated single sign-on

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

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

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

Prerequisites

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

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



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

Before implementing single sign-on (SSO)

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

Why is plus addressing problematic?

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



IMPORTANT:

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

Frequently asked questions

How to avoid users losing access to remove federation?

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

How does SSO change the login process?

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

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

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

Global impact of SSO

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

Hierarchy-level considerations

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

Handling Microsoft Entra ID account removal

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

Set up federated single sign-on with Microsoft Entra ID

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

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

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

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



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

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

1. Log in to WithSecure Elements Security Center sign-in page.
2. Under **Management > Organization Settings > Security Administrators**, select **Configure federated single sign-on**.

*The **Configure federated single sign-on** window opens showing the status of the domain that matches your email address.*

3. Select **Log in to Microsoft**
4. In the pop-up window that opens, enter your password for the Entra tenant, and select **Sign in**.
5. Select **Consent on behalf of your organization** and then select **Accept**.

*The **Single Sign-on Access Federation** window is refreshed and shows **Validation successful**.*



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

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

Link user identities

Links user identities in Elements Security Center for federated domains.



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

Make sure you have the following:

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



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

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

To link identities:

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



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

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

Remove federation from a domain

Removes single sign-on federation from a domain.

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

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



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

To remove federation:

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

1.1.7 Adding devices for management

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

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



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

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

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



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

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

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



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

Distributing WithSecure software

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

- You can install the following software using the same WithSecure Elements Agent for Computers installation package. The subscription key determines which software is installed:

- WithSecure Elements EPP for Computers (Windows and Mac)
- WithSecure Elements EDR and EPP for Computers (Windows and Mac)
- WithSecure Elements EDR for Computers (Windows, Mac, and Linux)



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

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



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

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

Send an installation link via email

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



NOTE: The installation link is valid for 30 days.

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

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

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

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

2. Select



next to **Devices**.

A menu is displayed.

3. From the menu, select **Add new device**.

*The **Add new device** page opens.*



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

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

To send multiple invitations, under **Import from CSV file**, select **Choose file** to select a CSV file from which you want to import data. Multiple email addresses must be separated by commas.

7. Select **Send**.

The listed recipients receive an email that contains a link to the download site and instructions for downloading and installing the product that you selected.



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



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

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

Download software from Elements Security Center

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

To download the software:

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

The **Downloads** page opens.

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

The available buttons depend on the operating system:

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

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

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



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

After downloading the software, you need to deploy it.

Manage automatic deletion of devices

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



NOTE: This feature does not apply to mobile devices.



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

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

To turn on automatic deletion of devices:

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

The **Devices** page opens.

2. Select  next to **Devices**.

A menu is displayed.

3. From the menu, select **Manage automatic deletion**.

The **Manage automatic deletion** page opens.

4. Turn on **Automatically delete devices...**

5. In the box, enter the number of days for a device to be offline before it is deleted.



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

6. Select **Save**.



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

Manage invitations

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

To manage the invitations:

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

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

2. Select



Manage device invitations.

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

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

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

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



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

1.1.8 Enhancing device management with custom labels

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

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

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

Add device labels

You can add device labels in three different ways.

You can add device labels in the following ways.



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

Add device labels in one of the following ways:

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

1.1.9 Managing devices in Elements Security Center

How to manage the selected devices in WithSecure Elements Security Center

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

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

Managing asset groups

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

You can assign devices to asset groups in two ways:

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



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

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

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

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

Create asset groups

Creates an asset group at the company level.

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

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

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

Add devices to asset groups

Adds devices to one or more asset groups.

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

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

5. Select **Assign**.

Remotely manage a device

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

To remotely manage a device:

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

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

2. Select one of the following tabs:

- **Computers** - shows devices with WithSecure Elements EPP for Computers and WithSecure Elements EPP for Servers
- **Mobile devices** - shows devices with WithSecure Elements Mobile Protection
- **Connectors** - shows devices with WithSecure Elements Connector
- **Unmanaged devices** - shows devices in a customer Active Directory (not in EPP)

3. Select the checkbox next to the name of the device.

A menu is displayed at the bottom of the page.

4. Select the desired operation from the menu.



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

The instruction is sent to the selected device.

Automatically delete devices

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



NOTE: This feature does not apply to mobile devices.



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

To manage automatic deletion:

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

*The **Devices** page opens.*

2. Select next to **Devices**.

A menu is displayed.

3. Select **Manage automatic deletion**.

*The **Manage automatic deletion** page opens.*

4. Turn on the **Automatically delete device...** option.

5. In the box, enter the number of days for a device to be offline before it is deleted.



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

6. Select **Save**.



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

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

View devices based on the Active Directory structure

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

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

To view devices based on the Active Directory structure:

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

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

2. Select the



icon at the top-left corner.

A drop-down menu is displayed, listing all the customer companies associated with your account.

3. Select the desired company.

4. Then, select the



icon next to **All devices**.



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

A drop-down menu shows the Active Directory structure of the selected company.

5. Select the desired Active Directory group to view all the devices in that group.



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

Customize the Devices view

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

To customize the Devices view:

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

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

2. Above the table, from the drop-down menu, select the name of a column for filtering the devices and the desired value for the selected column.



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

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

3. At the right corner above the table, select



A drop-down menu opens showing the Visible columns list.

4. Select the columns that you want to be visible in the table.

The columns that you selected appear in the table.

5. To change the order of the columns in the table:

- a) Point to the name of a column that you want to move.
- b) Depending on where you want the column to appear, drag it up or down in the list.

6. To define the number of rows shown in the table per page, do the following:

- a) At the right corner above the table, select



- b) From the drop-down menu, select the desired number of rows.

The number of rows changes according to your selection.

7. If there are more devices than can be shown in the table per page, use the navigation arrows



located above the table to go to the previous or next page.

8. Select **View:** > **Save as** at the top-right corner to save the view that you have customized.



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

Request diagnostic data

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

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



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

To request diagnostic data:

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



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

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



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

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



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

1.1.10 Elements data recovery

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

No actions are required from you.



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

Chapter 2

Elements Exposure Management overview

Topics:

- Why Exposure Management matters
- Understanding WithSecure Elements Exposure Management
- Key features
- Attack surface coverage

Elements Exposure Management overview

WithSecure Elements Exposure Management helps you identify, assess, and reduce cyber risks across your *attack surface*.

WithSecure Elements Exposure Management (XM) identifies and reduces cyber risks before attackers exploit them. It helps organizations protect assets and maintain business continuity.

The solution gives you a broad view of cyber risks. Its artificial intelligence (AI)-powered recommendations show your *attack surface*:

- *External attack surface* (EAS)
- Cloud services
- Identities
- Managed devices
- Network

Use the recommendations to fix vulnerabilities with the highest risk of intrusion.

WithSecure Elements Exposure Management helps you:

- Find your digital perimeter and its most critical assets and identities.
- Get recommendations based on threat intelligence, *attack paths*, business context, and security findings.
- Assess potential exposures from inside out and outside in. Use the results to reduce business risk and prioritize actions that improve your *security posture*.
- Explain exposure risks clearly to business leaders.

2.1 Why Exposure Management matters

Organizations face risks from *vulnerabilities*, setup errors, and changing threats that can expose sensitive data.

Navigating this detailed threat landscape is critical, and increasing visibility across your digital perimeter is essential. The typical modern company information technology (IT) environment is complex. It covers identities, workstations, and cloud services among many other asset types. Every asset can be a source of exposure – including vulnerabilities and misconfigurations. Attackers can exploit any of these to target an organization's assets and business operations.

Many organizations use hybrid environments without traditional perimeters. This makes it hard to see cloud and on-premises assets together. As organizations expand, their *attack surface* grows. New connected assets add complexity and need active management. The external threat landscape also changes as artificial intelligence (AI)-enabled cyberattacks emerge.

Threats evolve constantly, including AI-enabled cyberattacks and sophisticated malware. *Shadow IT* refers to systems deployed without central IT oversight. It can improve productivity but also adds business and compliance risks.

Interconnected assets and evolving threats make security and exposure management difficult. Each vulnerability is a potential gateway to sensitive data or critical systems. Attack paths expose internal assets to cyberattacks. Attackers may use these paths to reach important company assets, for example, during a ransomware attack. Detecting and securing these paths is important.

2.2 Understanding WithSecure Elements Exposure Management

WithSecure Elements Exposure Management (XM) helps you find, assess, and reduce security risks across exposed digital assets.

Exposure Management helps you:

- Find attack paths to critical assets before attackers exploit them.
- Give security teams a full view of their digital assets.
- Continuously check an organization's digital assets.

Security posture analysts run the 24/7 service. They investigate vulnerabilities, setup errors, and anomalies using technical indicators, industry best practices, and threat intelligence.

WithSecure Elements Exposure Management helps you:

- Identify possible attack surfaces.
- Get a ranked action list that helps improve your security posture and prevent serious incidents.
- Reduce your attack surface by managing assets that are exposed and accessible to attackers.
- Identify and address the parts of your information technology (IT) infrastructure most vulnerable to cyber threats.

2.3 Key features

In this section, we examine the key features of the WithSecure Elements Exposure Management solution.

The solution comprises the following service elements:

Exposure dashboard	The Exposure summary view gives you a risk-based overview of the identified weaknesses in your attack surface. Using the exposure score, you can start prioritizing the remediation from the assets that cause the most severe risk of exploitation. Our AI-powered recommendation engine gives you recommendations to help prioritize remediation. The Exposure view shows also the product's coverage of a selected organization's assets. It shows which assets - such as managed and unmanaged devices, network, identities, and cloud resources - are in use or not subscribed. Color coding helps to identify different issues: green indicates successful onboarding, orange indicates incomplete configuration or onboarding, and gray indicates that the organization lacks the required licenses for onboarding.
Environment view	The Environment view helps you discover and manage your assets. A single view shows you a centralized listing of assets and allows you to manage them per asset type. You can discover more assets and navigate and address risks that are related to a particular asset type.
Exposure risk	Exposure risk score shows you what is the exposure risk level of your company and assets. It works on three levels: • The exposure risk score of a company represents relative business risk that the current state of the company's digital asset cause. • The risk level is calculated separately for each asset type to highlight where the issues are. • Each asset instance has an exposure risk score which is calculated from various elements, such as attack path mapping, business context, and threat intelligence. • Attack path visualization, where available, highlights the potential risks if the provided recommendations are ignored.

By validating the attack path, exposure risk score ensures that you protect the path to the most critical assets. It also allows you to flexibly manage your business context values and benefit from our unique threat intelligence data.

2.4 Attack surface coverage

Exposure Management combines multiple scanning methods to make sure that your entire attack surface is covered.

In addition, the attack path simulation technology - integrating several scanning methodologies - creates a combined scanning approach of its own. Below is a list of the data-collection and scanning types that are used in attack path modeling.

Managed devices and network

Elements Agent.

- Agent-based scan - automatically scan Windows workstations and servers
- Device service data - collect system configuration and login information
- Patch management - monitor system and third-party patch status and perform automated updates via Software Updater



NOTE: This requires a license for WithSecure Elements Endpoint Protection (part of WithSecure Elements Endpoint Security).

Local/cloud scan node.

- Discover scan - identify and map all assets within your network
- System scan - scan all IP (Internet Protocol) systems for vulnerabilities and misconfigurations
- Authenticated scan - log into systems to gather detailed vulnerability data such as system versions, missing patches, and misconfigurations



NOTE: Authenticated scanning is not available through a cloud scan node.

- Web scan - scan and test custom web applications for vulnerabilities

External attack surface, identity, and cloud services

External attack surface.

- Internet discovery - identify your organization's internet-facing systems
- External assets - evaluate the security posture of externally exposed assets

Identity integrations.

- Entra ID - discover potential threats associated with identities in Entra ID
- Account breach - identify breached account information

Cloud integrations.

- Azure - assess the security and compliance posture of your Azure accounts
- AWS - assess the security and compliance of your AWS accounts



NOTE: Scans for cloud integrations are included in the WithSecure Elements Exposure Management for Cloud license, while the other scan types are included in the WithSecure Elements Exposure Management for Business license.

Chapter 3

Getting started with WithSecure Elements Exposure Management

Topics:

- Get started with WithSecure Elements Exposure Management
- Create the first WithSecure business account
- Log in to Elements Security Center and start asset onboarding
- Create administrator accounts
- Grant existing users the Exposure Management role

Getting started with WithSecure Elements Exposure Management

Getting started with WithSecure Elements Exposure Management covers creating a business account, logging in, and setting up administrator access.

To start using WithSecure Elements Exposure Management, create a WithSecure business account and log in to Elements Security Center. You then create administrator accounts, or grant the Exposure Management role to existing administrators, so that your team can access the service.

3.1 Get started with WithSecure Elements Exposure Management

Gets started with WithSecure Elements Exposure Management by creating an account, onboarding assets, and managing exposures.

You need either a partner-provided email with a login link or a subscription key from your WithSecure partner to create your WithSecure Business Account.

This quick start guide walks you through the three main steps to start using WithSecure Elements Exposure Management: create your account, onboard your assets, and manage your exposures in Elements Security Center.

1. Create your WithSecure Business Account and give your team access to Elements Security Center.
 - a) Create the first WithSecure Business Account, either from the email that your partner sent you or by self-registering with your subscription key. For instructions, see [Creating the first WithSecure business account](#).
 - b) Log in to Elements Security Center as described in [Logging in to Elements Security Center](#) and starting asset onboarding.
 - c) Create administrator accounts for your team. For instructions, see [Creating administrator accounts](#).
 - d) To let existing administrators use Exposure Management, grant them the role as described in [Granting existing users the Exposure Management role](#).
2. Onboard the assets that you want WithSecure Elements Exposure Management to monitor.
 - a) Install the WithSecure Elements Agent on your Windows devices, as described in [Installing new WithSecure Elements Agents](#).
 - b) If you already use Elements Endpoint Protection on your Windows devices, turn on scanning for those devices under **Environment > Devices > Computers** instead of installing the agent again. For details, see [Existing WithSecure Elements Agents](#).
 - c) To scan devices that have no agent, deploy a scan node on a Windows server (Installing scan nodes on Windows server) or a Linux server (Installing scan nodes on Linux servers), or use a cloud scan node.
 - d) Onboard your cloud accounts by adding an Azure tenant (Adding an Azure tenant) or an AWS account (Adding an AWS account in Elements Security Center).
 - e) Onboard your external attack surface under **Security Configurations > Scans** to monitor your internet-facing assets. For details, see [External attack surface scans](#) and [Identifying internet-facing systems](#).
3. Review and manage your exposures from the **Exposure** dashboard.
 - a) On the **Home** page, open the **Exposure** dashboard to see your organization's exposure score and top recommendations. For an overview, see [Managing exposures](#).
 - b) Select the highest-impact recommendation and review its affected assets, findings, and attack paths, as described in [Recommendations](#).

- c) Apply the suggested fixes and set the status of each finding to track your progress. For details, see Findings.
- d) Monitor your exposure score as you remediate findings over time.

3.2 Create the first WithSecure business account

Creates the first administrator account for your organization.

Make sure that you have the following:

- Access to the email address for the first administrator
- Either a partner-provided email with a temporary password and login link, or a subscription key that you received from your WithSecure partner
- Internet access

If your WithSecure partner created the business account for you, you have received an email from WithSecure containing a temporary password and a link to log in to Elements Security Center.

If you received a subscription key but no account, follow the steps below to create the first administrator account:

1. Go to the WithSecure Elements self-registration page at WithSecure Elements Security Center
2. On the self-registration page, enter the email address for the first administrator and the subscription key provided by your partner.



NOTE: As a partner creating the account on behalf of a customer, use the Not-for-Resale (NFR) subscription key instead.

3. To allow your subscription partner to manage the product on your behalf, leave the **Restrict Partner access to my organization** option unchecked.



NOTE: To restrict access so that only your own administrator accounts can manage the product, turn on this option.

4. Follow the instructions on the screen to complete company registration. Choose a strong password for the administrative account when prompted and submit the form.
5. Log in to Elements Security Center using the email and password that you set or the temporary password that you received from the partner email if the partner created the account for you.



NOTE: If you used a temporary password, change it at first login to a secure permanent password.

The first administrator account for your organization is created.

Next, log in to Elements Security Center and administer the product.

3.3 Log in to Elements Security Center and start asset onboarding

After creating the business account, log in to WithSecure Elements Security Center and administer the product.

To log in to Elements Security Center:

1. Go to Elements Security Center.
2. To log in, use your business account and the temporary password that you have received.

3. To subscribe Exposure Management for Users, do the following:
 - a) Install Elements Agent and turn on Elements Agent scanning on existing devices.
 - b) Onboard the Azure tenant to integrate identity data into Elements Exposure Management.
 - c) Configure Cloud Scan nodes to detect and assess internet-facing assets.
 - d) Configure External Attack Surface to detect internet-facing assets (EASM).
 - e) Install and configure Elements Scan nodes to scan all non-internet-facing devices.
4. To subscribe Exposure Management for Cloud, do the following:
 - a) Onboard the Azure tenant, if you have not done it already.
 - b) Onboard the AWS tenant.
 - c) Configure and schedule cloud accounts scans.

Next, create additional administrator accounts.

3.4 Create administrator accounts

Creates additional administrator accounts in WithSecure Elements Exposure Management.

To add administrator accounts in WithSecure Elements Exposure Management:

1. In Elements Security Center, from the sidebar, select **Management > Organization settings > Security Administrators**.
2. Select **Add administrator**.
3. Under **Administrator details**, enter the user's email address, select the desired language, and then select **Next**.
4. Under **Roles**, do the following:
 - For Exposure Management for User, under **Exposure Management**, select **Full Editing**, and then select **Next**.
 - For Exposure Management for Cloud, under **Exposure Management**, select **Full Editing**, and select **Next**.
5. Under **Summary**, review the information and select **Add**.
A new administrator account was added.
6. Select **Done**.
7. Under **Environment**, select **Devices** and from the  icon, select **Add new device**.
8. Select the subscription to use and select **Next**.
9. Follow the steps in the wizard and select **Send** to send an email invitation to one or more users with a download link to the installer.

Next, grant the Exposure Management role to an existing administrator.

3.5 Grant existing users the Exposure Management role

Grant the Exposure Management role to an existing administrator in Elements Security Center.

To grant the Exposure Management role to an existing administrator:

1. In Element Security Center, from the sidebar, select **Management > Organization settings > Security Administrators**.
2. Locate the administrator who needs the Exposure Management access and select their email address.
3. In the **Summary** view, under **Roles**, select **Exposure Management > Exposure > Full editing**.
4. Click **Save** to apply the changes.

Chapter 4

Asset onboarding

Topics:

- Device onboarding
- Cloud account onboarding
- Network asset onboarding
- Identity onboarding

Asset onboarding

Onboarding assets - services and technologies such as devices, cloud, and identities - increases coverage and helps you evaluate your organization's digital perimeter.

As organizations transition to cloud-based infrastructure and adopt hybrid work models, they face a critical challenge: a diminishing understanding of their digital assets and perimeter. This lack of visibility makes it harder to protect against cyber threats. Customers need new ways to protect their data and systems as threats keep evolving.

4.1 Device onboarding

Onboarding devices brings them under continuous vulnerability management by installing WithSecure Elements Agent or using scan nodes.

To bring your endpoint devices under continuous vulnerability management, onboard them to Elements Exposure Management. You can install WithSecure Elements Agent on supported devices, or use scan nodes to scan devices that cannot run the agent.

4.1.1 Existing WithSecure Elements Agents

If you are using Elements Endpoint Protection on Windows devices in your network, you do not need to install WithSecure Elements Agent on them. This applies if you want to run vulnerability scans on those devices.

In such cases, go directly to **Environment > Devices > Computers** and select those devices for vulnerability scanning.



NOTE: You only need to install the standalone WithSecure Elements Agent with Exposure Management (XM) capabilities on devices not already using Elements Agent for other services.

4.1.2 Install new WithSecure Elements Agents

Installs WithSecure Elements Agent on your devices.

WithSecure Elements Agent requirements:

WithSecure Elements Agent supports the following operating system versions:

- Microsoft Windows 11 (64-bit edition)
- Microsoft Windows 10 (all 32-bit and 64-bit editions), ARM-based tablets are not supported

You can find the list of supported Windows server versions.

System requirements:

- Processor: Intel Pentium 4 2GHz or higher (processor must support SSE2).
- Memory: 1 GB on 32-bit systems / 2 GB or more on 64-bit systems
- Disk space: 2 GB free disk space
- Display with a resolution of 1024 x 768 or higher
- Internet Connection: An Internet connection is required to confirm your subscription, receive product updates, and use the cloud-based detection
- Javascript must be turned on in the browser settings to use active block pages
- Windows Update Agent (WUA): The Windows Update service and API must be accessible and not blocked by security policies, firewalls, or third-party endpoint protection software. This is required for

assessing security patch compliance. The service is enabled by default in most environments, so no action is usually needed.

Supported browsers:

- Microsoft Edge (the latest versions)
- Google Chrome (the latest versions)
- Mozilla Firefox (the latest versions)
- Safari (the latest versions)

To install WithSecure Elements Agent:

1. In Elements Security Center, select **Management > Downloads**.
2. Under **WithSecure Elements Agent**, select **Download**.



NOTE: The downloaded exe file includes the subscription key.

The installation file is downloaded.

3. Locate the downloaded installation file and double-click it to start the installation.

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

```
ElementsAgentInstaller[AB12-CD34-EF56-GH78].exe
```



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

4. Select the language and restart options that you want to use for installation, and select **Next**.
5. Read the license agreement. To accept the agreement and continue, click **Accept**.
6. On the **Subscription key** screen, enter your subscription key that you can copy from under **Settings > General settings > Subscription details** in Elements Security Center, and select **Next**.
7. Follow the on-screen instructions to complete the installation.

The WithSecure Elements Agent is installed on the device.

Turn on or off WithSecure Elements Agent scanning on devices

WithSecure Elements Agent is a Windows application that offers an alternative method for conducting vulnerability scans on devices within your network.

To obtain vulnerability scan results for endpoint devices in your network, you must turn on scanning on those devices.



NOTE: By default, scanning is turned on automatically after WithSecure Element Agent is installed with an Exposure Management subscription key.

1. To turn on vulnerability scanning, do the following:
 - a) In Elements Security Center, under **Environment**, select **Devices Computers** to view a list of the detected devices with WithSecure Elements Agent installed.
 - b) Select the devices for which you want to turn on vulnerability scanning, and from the action bar that appears, select **Vulnerability Management scan > Enable scanning**.

This activates vulnerability management on the device and initiates the initial scan. It also generates a scanning schedule based on your organization's settings, for example, running a vulnerability scan every six hours.

- c) Select the **Vulnerability Assets** tab and verify that the activated devices are listed.

Initially, device details include only basic telemetry data such as IP address, hostname, and MAC address. Over time, vulnerability findings from the WithSecure Elements Agent scan begin to appear on the **Vulnerabilities and findings** tab of the device's **Asset details** page.

After the initial scan, WithSecure Elements Agent runs a new scan whenever major changes are made to the software that is installed on the device.

2. To turn off vulnerability scanning, do the following:

- a) In Elements Security Center, under **Environment**, select **Devices > Computers** to view a list of the detected devices that have WithSecure Elements Agent installed.
- b) Select the devices for which you want to turn off vulnerability scanning, then in the action bar that appears toggle the **Enable or disable scanning** switch and select **Disable scanning**.

Change the frequency for endpoint status updates

You can set how often Elements Agent sends updated status information on vulnerabilities in the devices in your network to Elements Security Center.



NOTE: In addition to the scheduled status updates, endpoints automatically send any information to Elements Security Center from scans that are triggered by changes to the installed software.

1. Under **Management**, select **Vulnerability Settings > General settings**.
2. Under **Miscellaneous**, choose the update frequency that you want in the **Vulnerability data refresh schedule on endpoints** drop-down field.
3. Click **Save**.

4.1.3 Devices without WithSecure Elements Agent

Devices without WithSecure Elements Agent can be scanned with a local or cloud scan node.

To discover and scan devices on a local network, you need a local Scan Node to run your scans.

We recommend installing Elements Agent for your Windows devices whenever possible. Devices with WithSecure Elements Agent installed on them have better scanning coverage. In case you cannot or do not want to install Elements Agent on your devices, you can scan them using a local scan node.

For scanning devices that are visible on the public internet, we recommend using WithSecure cloud scan nodes.

Local scan nodes

For local networks, we support scan nodes that can be installed on Windows or Linux servers. There is also a limited support (beta) for Windows 10 and Windows 11 installations.

Connectivity to operational technology and other isolated networks

In operational technology (OT) and other isolated networks, scan nodes are deployed locally within each network segment and scan only nearby hosts. The scan nodes do not require internet access; instead, all communication with WithSecure backend services could be routed through a centrally deployed Elements Connector over ports 80/443. This approach minimizes firewall changes, preserves network isolation, and allows secure scanning of segmented and restricted environments.

Cloud scan nodes

For devices visible in the internet, we offer you a robust collection of scan nodes at no additional cost. Using a discovery scan, you can identify devices that are exposed to the public internet, and with a system scan, you can scan them for vulnerabilities.

Security products may identify scan traffic as malicious. Add the IP addresses in 46.228.135.0/26 to the allow lists of protection mechanisms such as firewalls and intrusion prevention systems (IPS). This helps prevent false scan results.

Cloud scan nodes are available directly when you are configuring scans.

Set up labeling rules for unmanaged devices

You can set up automatic labeling rules for unmanaged devices to categorize network assets, such as cameras, printers, and PoS terminals based on various criteria.

You must have access to WithSecure Elements Center.

Use automatic labeling to identify unmanaged devices - devices that are present on the company network but do not run a WithSecure endpoint agent. Labels can be assigned automatically based on criteria such as IPv4 ranges, allowing you to group devices by type, location, or other relevant attributes. This feature lets you apply profile assignment rules to both managed and unmanaged devices.

1. In WithSecure Elements Center, go to **Security Configurations > Profiles > Profile assignment rules**.
2. Scroll to **Unmanaged devices labeling rules** to view existing labeling rules.
3. Select **Add labeling rule**.



NOTE: You can add labeling rules only on the Company level.

4. In the **Add rule** pane, from the **Condition** drop-down menu, select one of the following:
 - IPv4
 - DNS
 - Host name
5. Enter the value for the condition.
For IPv4, this may be a single address or an IP range, for example, 10.0.0.0/24.
6. The client type is automatically set to **Unmanaged device**.
7. From the **Add labels** drop-down menu, select one or more labels.
Labels may represent device type (camera, printer, PoS), location, or any other classification used in your environment.
8. Select **Add rule** to save the settings.

Devices that match the defined condition are automatically assigned the selected labels. You can use these labels to filter and organize unmanaged devices across WithSecure Elements Security Center.

4.1.4 Installing scan nodes on Windows server

Scan nodes are used to perform the actual discovery and network vulnerability scans.

A scan node can be installed with one or more of the following scanning engines:

- Discovery scan is a network discovery and port scanning engine
- System scan is able to scan IP addresses for known vulnerabilities
- Web scan is designed to scan custom web applications for vulnerabilities

Scan node requirements (Windows)

Supported operating systems.

- Latest Windows Server (minimum: Windows Server 2019)
- Windows 10/11 desktop (Beta)



NOTE: Note: The recommended operating system for Scan Node installation is Windows Server (2019, 2022, or 2025). Windows 11 is also supported, and no differences in performance or result accuracy are expected. However, our pre-release testing primarily targets server operating systems, so the same level of quality assurance cannot be guaranteed for Windows desktop versions.

Software requirements.

- Microsoft .NET Framework: recommended version 4.8 (minimum version: 4.7.2)
- npcap
- Microsoft Visual C++ 2015-2022 Redistributable Package (x86)
- User account: Local or Active Directory account with administrative rights required during installation



NOTE: The installer automatically downloads and installs all required third-party components. However, Microsoft Visual C++ is included with the Windows operating system, and the version available depends on the specific Windows OS you are using.

Hardware requirements.

- Minimum 4 GB RAM (recommended: 8GB or more)
- Minimum 2 GHz processor
- Minimum 30 GB disk space

Network requirements - access to the following URLs:

- <https://sn-api.radar-prd.fsapi.com>, <https://gateway.radar-prd.fsapi.com>, and <https://updates-api.radar-prd.fsapi.com> (Elements Vulnerability Management Update Service)
- <https://api.radar-prd.fsapi.com> (Elements Vulnerability Management API)
- If you are using a proxy server, it must allow the following HTTP request methods: GET, HEAD, and POST towards the mentioned web services



NOTE: Antivirus software may detect and block vulnerability scans as malicious activity. If the scan node has antivirus software, we recommend adding the entire scan node installation directory to the allow list. Scheduled antivirus scans can also interfere with Elements Vulnerability Management scans and stop them before completion.

Install a scan node on Windows

Download and install a scan node on Windows from Elements Security Center.

Download and install a scan node on a Windows server from the Elements Security Center.

1. Download the scan node installation package and the scan node license file:



NOTE: You can download Scan Node installers for Windows and Linux from Elements Security Center under **Management > Downloads**.

- a) In Elements Security Center, under **Security Configurations**, select **Scans > Scan nodes** and then select **Add new scan node**.
- b) Select **Request a new scan node > Next**.
- c) Enter a name and description for the scan node, then select **Request**.

The resulting page includes the download link and basic instructions. The license information included in the installation package is valid for 14 days.

2. Run the scan node installer (executable) and follow the installation wizard steps.

The installation wizard checks that all prerequisites are installed and installs any missing software if necessary.

3. After successful installation, verify that the scan node appears in the list of scan nodes in Elements Security Center.

Verify installation

Verify that a new scan node runs, downloads its scan engines, and connects to Elements Security Center. After installing a scan node on Windows, verify that it started successfully and can reach Elements Security Center.

1. Verify that the Windows Service *WithSecure Radar Agent* is installed and running.

You can use the Task Manager or Windows Services to verify if the service is running.

2. Verify that the scanning engines and plugins can be downloaded.

After the installation, wait 5-10 minutes for the Radar .Scan .Daemon to download all the binaries. Once completed, you should see the following folders:

- [drive]:\Program Files (x86)\F-Secure\RadarScanAgent\binaries_ds
- [drive]:\Program Files (x86)\F-Secure\RadarScanAgent\binaries_ws
- [drive]:\Program Files (x86)\F-Secure\RadarScanAgent\binaries_ss



NOTE: If a scan engine module is deactivated, its binaries will not be downloaded.

3. Verify that the scan node can connect to the Elements Security Center:

- a) Log in to Elements Security Center.
- b) Under **Security Configurations**, select **Scans > Scan nodes**.

It should always be less than one minute since the scan node attempted to connect to the Elements Security Center. If **Last seen** is longer, see the troubleshooting section.

4. Review the log files in [drive]:\Program Files (x86)\F-Secure\RadarScanAgent\logs for other errors.

5. Run a few test scans.

For example:

- a) Run a Discovery Scan using the Host Discovery mode.
- b) Run a System Scan with a limited port range (e.g. TCP/80,443).
- c) Run a Web Scan with **Run attacks** disabled.

Configure scan nodes

Configure an Elements Exposure Management scan node through the control center application to set its update interval, scan engines, and scan limits.

Scan nodes can be configured via the control center application.

1. Find the scan node installation directory (e.g. [drive]:\Program Files (x86)\F-Secure\RadarScanAgent\).
2. Start the control center application FSRadarAgent.Tray.exe.
3. Go to the **Settings** tab and review the configuration options.

The most important configuration options are:

Table 1: Scan node configuration options

ID	Name	Value (recommended)	Description
4	SCANNODE.ModuleLoopInterval	14400000	How often the scan node should check for updates in milliseconds. The default is every 4 hours.
10-12	Module.{ScanEngineName}.Enabled	True	Defines which scan engines are enabled on the scan node.
13-15	Module.{ScanEngineName}.ScanNodeId	GUID	The unique identifier for each scan engine module. The IDs are used when new scan nodes are added to Elements Security Center.
19-21	Module.{ScanEngineName}.MaxSimultaneousScans	DiscoveryScan: 10 SystemScan: 30 WebScan: 5	These values control the maximum number of simultaneous scans that the scan node is allowed to run. Too high values might result in open ports being missed during port scanning.
127	Communication.WebService.Updates. SkipSSLCertificateValidation	False	Skip certificate validation while connecting to Elements Vulnerability Management Update Service.
128	Communication.WebService.SecurityCentre. SkipSSLCertificateValidation	False	Skip certificate validation while connecting to Elements Security Center.

4.1.5 Installing scan nodes on Linux servers

Scan nodes are used to perform the actual discovery and network vulnerability scans.

A scan node can be installed with one or more of the following scanning engines:

- Discovery scan is a network discovery and port scanning engine.
- System scan is able to scan IP addresses for known vulnerabilities.
- Web scan is designed to scan custom web applications for vulnerabilities.

Scan node requirements (Linux)

- Any stable LTS release up to Ubuntu 24.04 (64-bit only). Available for download at Ubuntu Server downloads), or
- Any stable LTS release up to Debian 13 (64-bit only). Available for download at Debian downloads)
- SSH (GUI is not needed, the required X11 libraries are installed automatically as .deb package dependencies)
- Network access to the following:
 - <https://sn-api.radar-prd.fsapi.com>, <https://gateway.radar-prd.fsapi.com> and <http://guts2.fsapi.com/>
 - <https://updates-api.radar-prd.fsapi.com> (Elements VM Update Service API)
- Network access to Elements Vulnerability Management as follows:
 - <https://api.radar-prd.fsapi.com> for accounts with a paid subscription
 - URI assigned during the installation process for on-site installations
 - If you are using a proxy server, it must allow the following HTTP request methods: GET, HEAD, and POST towards the mentioned web services
- Hardware
 - Minimum 4 GB RAM (recommended: 8GB)
 - Minimum 2 GHz processor / 2 CPU in AWS
 - Minimum 30 GB disk space

Install a scan node on Linux

Follow these steps to install a scan node on your Linux system.

Download and install a scan node on a Linux server from the Elements Security Center.

1. Download the scan node installation package.

Using an installation package with automatically applied license information:

- a) In Elements Security Center, under **Security Configurations**, select **Scans > Scan nodes** and then select **Add new scan node**.
- b) Select **Request a new scan node > Next**.
- c) Enter a name and description for the scan node, then select **Request**.

The resulting page includes the download link and basic instructions. The license information included in the installation package is valid for 14 days. You do not need to apply the license manually when you use this type of installation package, although an internet connection is required during installation. If you encounter any issues when applying the license, follow the steps given for applying it manually.

Using an installation package for manually applied license information:

- a) Download the scan node installation package from the Elements Security Center downloads page. Alternatively, you can also download Scan Node installers for Windows and Linux from Elements Security Center under **Management > Downloads** or use the following command to download the installation package:

```
wget -P ~ --content-disposition
https://download.withsecure.com/SNA/withsecure-xm-scannodeagent-netinstaller_amd64.deb
```

- b) In Elements Security Center, under **Security Configurations**, select **Scans > Scan nodes** and then select **Add new scan node**.

- c) Select **Request a new scan node > Next**.
- d) Enter a name and description for the scan node, then select **Request**.
- e) Copy the URL under **Download scan node license** to the clipboard.

The URL is valid for 14 days and should have the following format: `https://updates-api.radar-prd.fsapi.com/api/2.9/organizations/productLicenses/order?token=2Ub3Tfd(...)`.

- f) Use the following command to download the license file to your Linux system, replacing <URL> with the URL that you copied from the Elements Security Center:

```
wget -O ~/license.fsr1 <URL>
```

2. If you need to use a proxy server for communication with external networks, set the `FSECURE_HTTP_PROXY_HOST` and `FSECURE_HTTP_PROXY_PORT` environment variables.

These settings are used both for normal scan node operations and for maintenance purposes (installing and updating the scan node).

- a) Run the following commands to set the variables using the `/etc/environment` file:

```
echo "FSECURE_HTTP_PROXY_HOST=www.proxy.example.com" | sudo tee -a /etc/environment
echo "FSECURE_HTTP_PROXY_PORT=8080" | sudo tee -a /etc/environment
```

- b) Log out for the changes to take effect and then log in again.

3. Run the following commands to install the prerequisites:



NOTE: In the command, replace the OS distribution name and version with the desired ones if you want to deploy the scan node on another operating system. The link in the command should refer to the appropriate *.deb file located in the following repository: Microsoft Linux package repository.

```
wget -q https://packages.microsoft.com/config/ubuntu/22.04/packages-microsoft-prod.deb
sudo apt install ./packages-microsoft-prod.deb
sudo apt update
```

4. Run the following command to install the Scan Node Agent:

```
sudo apt install ./withsecure-xm-scannodeagent-netinstaller_amd64.deb
```



NOTE: In the license selection screen, press **Tab** to move between the panes, the **Up** and **Down** arrow keys to scroll through the lists, and **Space** to select the file that you want to use.

The installation directory is `/opt/fsecure/radar-scannodeagent`. The Linux daemon (service) name is `f-secure-radar-scannodeagent`.

If this is the very first installation, you are asked to provide a license file (`.fsr1`).

After successful installation, verify that the scan node appears in the list of scan nodes in Elements Security Center.

Verify Linux scan node installation

After you have installed the Linux scan node, follow the steps listed here to make sure that it is installed and running successfully.

1. In Elements Security Center, under **Security Configurations**, select **Scans > Scan nodes** and check that your new scan node is synchronized and has received engine updates.
2. On the scan node, check the logs under the `/opt/f-secure/radar-scannodeagent/logs/` directory.
3. Check that the `/opt/f-secure/radar-scannodeagent/Engines/` directory is not empty.
This directory contains the scanning engines, which are required to run scans. It should contain at least some files.
4. Run the following command to verify that the Linux daemon (service) is in active state:

```
sudo systemctl status f-secure-radar-scannodeagent
```

5. Run the following commands to check the current settings:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent get-config | more
```

6. If you applied the license file, but the scan node agent has not recognized it, run the following command to restart the service:

```
sudo systemctl restart f-secure-radar-scannodeagent
```

Linux scan node paths

The stored scan node data can provide useful information for troubleshooting and maintenance purposes.

Linux scan nodes use the following paths to store their operation data:

- `/opt/f-secure/radar-scannodeagent/Scans/<scan_type>/<scan_id>` contains files related to currently running scans
- `/opt/f-secure/radar-scannodeagent/Engines/` contains the scan engine binaries
- `/opt/f-secure/radar-scannodeagent/Updates/` contains temporary update files for scan engines
- `/opt/f-secure/radar-scannodeagent/logs/` contains the scan node's log files
- `/opt/f-secure/radar-scannodeagent/scannode.db` is used for storing configuration data and information on currently running scans

Configure Linux scan nodes

Commands for viewing or changing Linux scan node settings after installation.

You have already installed the Linux scan node.

Use these commands to view or change scan node settings after installation, without reinstalling the agent.

1. Run the following command to go to the Scan Node Agent installation directory:

```
cd /opt/f-secure/radar-scannodeagent
```

2. Use the following commands to edit the settings:

To get all settings:

```
sudo ./ScanNodeAgent get-config
```

To get a single setting, for example, to check whether the Scan Node Agent sends its private IP address to Elements Security Center:

```
sudo ./ScanNodeAgent get-config HidePrivateIp
```

To modify multiple settings using a file, for example `custom_config`:

```
sudo ./ScanNodeAgent set-config < custom_config
```



NOTE: The `custom_config` file that you use must follow the same format as the output of the `get-config` command.

To modify a single setting, for example the maximum number of simultaneous system scans:

```
sudo ./ScanNodeAgent set-config SystemScan.MaxSimultaneousScans 12
```

Apply the scan node license manually

To apply a new `.fsrl` license file to an already installed WithSecure Elements VM Scan Node Agent, you need to copy the file to the installation directory.

You have already installed the WithSecure Elements VM Scan Node Agent.

Use this if you received a license file separately from the installation package, or want to apply a license for a single scanning module instead of the whole scan node.

1. Run the following commands to apply the new license file:

```
cd /opt/f-secure/radar-scannodeagent && sudo ./ScanNodeAgent apply-license ./license.fsrl
```

2. To apply a known WithSecure Elements VM Scan Node Agent license ID for a particular scanning module, you can apply the license ID directly to the Scan Node Agent configuration.

For example, for the system scan module, run the following commands:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config SystemScan.License 85f95bbf-15cf-4d06-8347-e91a1eb539b8
sudo ./ScanNodeAgent set-config SystemScan.Enabled true
sudo ./ScanNodeAgent update-engines
```



NOTE: If the installation directory (`/opt/f-secure/radar-scannodeagent`) already contains a `.fsrl` file, the data from that license file is applied when you restart the agent, overwriting the manual changes.



NOTE: If the installation directory contains more than one `.fsrl` file, you can run the following command to check which one is in use: `sudo ./ScanNodeAgent get-config LicenseFileName`

Set up encryption keys for authenticated scanning

Both Windows and Linux authenticated scanning is supported on Linux scan nodes.

Windows authenticated scanning is supported using WinRM. Select the **Specify credentials explicitly** option when creating the system scan template.

For Linux authenticated scanning, you need to once set up the encryption keys to transfer the credentials securely.

Apart from adding the encryption keys allowing the secure credentials flow for Linux authenticated scanning, you can also manage the already existing keys:

1. To list all encryption keys, run the following command:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent list-private-keys
```

2. To remove an existing key, run the following command:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent remove-private-key NameOfTheKeyPair
```

Redirect traffic to a proxy server

As WithSecure Elements VM Scan Node Agent sends requests to the Elements Security Center and Update Service, you need to configure the appropriate proxy address to redirect the traffic.



NOTE: WithSecure recommends using the Elements Connector, which is optimized for proxying traffic to WithSecure backend services. This is especially useful in isolated network environments where routing multiple scan nodes through firewalls is undesirable.

Run the following commands:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config SecurityCenterProxyUri http://proxy.example.com:8080
sudo ./ScanNodeAgent set-config UpdateServiceProxyUri http://proxy.example.com:8080
```



NOTE: If you used environment variables to set proxy settings (FSECURE_HTTP_PROXY_HOST and FSECURE_HTTP_PROXY_PORT) before installation, then these should be already applied automatically.

To reset the proxy setting, use the following commands to set the value to none:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config SecurityCenterProxyUri "(none)"
sudo ./ScanNodeAgent set-config UpdateServiceProxyUri "(none)"
```

To use the system proxy settings instead of setting the proxy configuration explicitly, run the following commands:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config UseDefaultProxySettingsForSecurityCenter true
sudo ./ScanNodeAgent set-config UseDefaultProxySettingsForUpdateService true
```

Disable SSL certificate validation

If you use a proxy server or host your local Elements Security Center using a self-signed SSL certificate, you can disable certificate validation by setting the appropriate configuration keys.

Run the following commands:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config SkipSecurityCenterSslCertificateCheck true
sudo ./ScanNodeAgent set-config SkipUpdateServiceSslCertificateCheck true
```



IMPORTANT: WithSecure recommends against disabling the SSL certificate validation check, especially for Radar Update Service communication.

Install a local CA certificate

For network vulnerability scans to correctly validate SSL/TLS certificates signed by a local certification authority (CA), you have to install the root certificate on the scan node server. System scans use the same certificate store as OpenSSL.

To install the rootCA.crt certificate file on Debian or Ubuntu distributions:

1. Run the following command to create a directory for your own trusted CA certificates:

```
sudo mkdir /usr/local/share/ca-certificates/extra
```

2. Copy the root certificate to the new directory:

```
sudo cp rootCA.crt /usr/local/share/ca-certificates/extra/
```

Make sure that the certificate has the .crt extension.

3. Run the following command to update the system certificates:

```
sudo update-ca-certificates
```

Limit the maximum number of simultaneous scans

If the default limits for simultaneous scans cause performance issues, you can customize the limits.

Run the following commands to change the default limits:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent set-config DiscoveryScan.MaxSimultaneousScans 3
sudo ./ScanNodeAgent set-config SystemScan.MaxSimultaneousScans 10
sudo ./ScanNodeAgent set-config WebScan.MaxSimultaneousScans 3
```

Update scan engines manually

By default, the scan node agent checks for engine updates automatically every 4 hours, but you can also check for updates and install them manually.

Run the following commands to manually update the scan engines:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent update-engines
```

Reset scan engines

If there are any issues with the scan engine directory integrity, you can reset the engines to download fresh instances.

Run the following commands to reset the scan engines:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent reset-engines
```

To reset a specific scan engine, you can use the engine type as an argument:

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent reset-engines DiscoveryScan
sudo ./ScanNodeAgent reset-engines SystemScan
sudo ./ScanNodeAgent reset-engines WebScan
```



NOTE: It might take a few minutes to reset the scan engines. We do not recommend using this operation to update the engines - use the `sudo ./ScanNodeAgent update-engines` command instead.

4.2 Cloud account onboarding

Onboarding cloud accounts lets the solution scan your cloud resources for security issues and provide remediation steps.

Onboarding cloud accounts lets the solution scan your cloud resources for security issues and provide you with recommendations and remediation steps to fix them.

Cloud accounts, or subscriptions, are used to access and manage the cloud-based resources, such as identities, virtual machines, storage, and databases. Onboarding these cloud accounts to the solution the is quick process and requires minimal permissions and configuration.



NOTE: The solution supports Microsoft Azure (Azure) and Amazon Web Services (AWS) accounts.

To use Exposure Management, you need to connect cloud accounts to the service. Once connected, the service scans your cloud assets and services for security risks, misconfigurations, and compliance violations. You can view and manage these accounts in Elements Security Center (ESC). When connecting cloud accounts, you grant the service the necessary permissions to access and scan your resources and data.

4.2.1 Add an Azure tenant

Connect an Azure tenant to WithSecure Elements Security Center.

To add a new Azure tenant:

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

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



IMPORTANT: You must configure the Identity Inventory capability before you add any other capabilities. See Connecting Identity Inventory for a tenant.

4.2.2 Connect Identity Inventory for a tenant

Connect the Identity Inventory capability for an Azure tenant.



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

To connect Identity Inventory:

1. Under **Security capabilities**, select **Identity Inventory**.
2. Select **Connect now**.
3. Read the introduction and instructions, select the checkbox to confirm, and select **Start**.
4. Grant the required permissions for the Identity Inventory capability.
 - If you are the Azure tenant administrator, select **Accept Permissions**, then approve the required permissions.
 - If you cannot grant permissions, select **Copy URL** to copy the URL and send it to your Azure administrator.

4.2.3 Adding Azure subscriptions

You can connect one or more Azure subscriptions to the service.

Each company can have multiple Azure tenants, and each tenant can include Azure subscriptions with different resources. When you add an Azure subscription, you typically need to onboard the corresponding Azure tenant to link the subscription.



NOTE: Azure tenant accounts are created only once. If you are onboarding an Azure subscription and a connection to the corresponding tenant already exists, only a subscription account is added. If no connection exists, both tenant and subscription accounts need to be created.

Azure prerequisites

Before creating the first Azure cloud connections for Exposure Management, you must make sure that the following prerequisites are met.

- You have signed in as a Global Administrator on the Azure account to run the script in Azure Cloud Shell
- You have your Azure subscription IDs, tenant IDs, or both ready. For instructions, see Get subscription and tenant IDs in the Azure portal.

You can add multiple cloud connections at once or a single one using the wizard. If you are adding multiple Azure subscriptions, you must prepare a CSV file.

Connect and activate Cloud Security Posture Management for a tenant

Connects and activates Cloud Security Posture Management for a tenant.

To connect and active Cloud Security Posture Management:

1. Under **Environment**, select **Cloud > Microsoft Tenants and Azure Subscriptions**.
2. From the Display name list, select a tenant.

3. On the tenant details page, under Cloud Security Posture Management, select **Connect now**.
4. Review the instructions and select **I have read the instructions and I am ready to proceed** to confirm.
5. Grant the required permissions for the Cloud Security Posture capability.
 - If you are a Microsoft Tenant administrator, select **Accept Permissions**, then approve the required permissions.
 - If you are not a Microsoft Tenant administrator, follow these steps:
 - a. Select **Copy URL** to copy the URL to your clipboard.



NOTE: You can send the URL to your Azure administrator via email along with a link to this guide.

- b. Request that the Azure administrator does the following:
 - Accept the permissions for the WithSecure Enterprise application WithSecure-CSPM-Scanner-MTA.
 - Assign the **User administrator** role to the corresponding application registration.
- c. After the Azure administrator confirms that Cloud Security Posture has been enabled, verify that the Cloud Security Posture status shows **Active** (green).

Add an Azure subscription in Elements Security Center

Onboards an Azure subscription in Elements Security Center.

To onboard an Azure subscription:

1. Open Elements Security Center at WithSecure Elements Security Center.
2. Use the scope selector to select the organization to which you want to add a new subscription.



NOTE: Adding subscriptions is only available on company level.



NOTE: The scope selector is visible only at the Solution Provider (SOP) and Service Partner (SEP) levels. If your Elements Security Center (ESC) account only has company level access, you do not see a scope selector.

3. Under **Environment**, select **Cloud > Microsoft Tenants and Azure Subscriptions**.
4. Select **Add Azure subscription**.

The **Add new Azure subscription** wizard opens.

5. In the **Subscription information** screen, do the following:
 - a) Enter a name for the subscription.
 - b) Select the tenant ID that the subscription belongs to.
 - c) Select **Next**.



NOTE: If Cloud Security Posture Management has not yet been connected for the selected tenant a warning message appears. You can still create the subscription, but you are not able to activate Cloud Security Posture Management for that subscription until Cloud Security Posture Management is active for the corresponding tenant.

6. In the **Subscription importance** screen, enter information about the importance and business context of the account.
7. Select **Next**, and then do the following:
 - a) On the **Security Capabilities** page that opens, under **Cloud Security Posture Management Subscription**, select **Connect now**.



NOTE: If the **Connect now** button is grayed out, it means that the Cloud Security Posture Management for tenant has not yet been connected.

- b) In the window that opens, review the user agreement, check the agreement box, and select **Enable now**.
The Connect Cloud Security Posture Management window opens explaining the next steps, including how to download and run the script on Azure to activate the connection.
 - c) Select **Finish** on the view to return to the **Cloud Security Posture Management Subscription** view.

8. Under **Onboarding files**, select **Download onboarding files** (powershell_[UUID].ps1).

The Azure subscription is added and the onboarding files are downloaded.

Next, run the downloaded onboarding script in the Azure portal.

Run the Azure onboarding script

Run the onboarding PowerShell script from Elements Security Center in the Azure portal to complete the subscription onboarding.

You have added the Azure subscription in Elements Security Center and downloaded the onboarding files.

Run the PowerShell script in the Azure portal:

1. Select **Go to Azure portal** or navigate to Azure portal and sign in to the portal.
2. Launch **Azure Cloud Shell** from the top navigation of the Azure portal. For instructions, see Getting started with Azure Cloud Shell.
3. Select **Manage files > Upload** at the top of the shell screen to upload the PowerShell script file that you already downloaded and extracted from the zip file.
A File Explorer window opens in which you can select a file for uploading to the current Cloud Shell session. The file is uploaded to the current working directory.
4. Select the PowerShell script that you downloaded earlier and select **Open**.



NOTE: You can also double-click the file from File Explorer. The Azure portal notifies you with a 'Successfully uploaded a file' message.

5. Run the uploaded script by entering the following command:

```
./powershell_[UUID].ps1
```

The script requests you to authenticate at the Microsoft device login page with the code that is displayed in the shell. After successful authentication, the script completes the deployment.

The Azure subscription is onboarded.

4.2.4 Add an AWS account in Elements Security Center

Connects an AWS cloud account with the service.



NOTE: For a video on how to connect Elements Security Center to your AWS account, watch the AWS connection video.

1. Open Elements Security Center.
2. Under **Environment**, select **Cloud**.
3. Select **Add accounts**.

The **Add a new cloud account** wizard opens.

4. On the **Primary account information** page, enter the following details.
 - a) Select the organization where to add the new account.



NOTE: The scope selector is visible only at the Solution Provider and Service Partner levels.

- b) Select **AWS** as the cloud provider.
 - c) Choose whether you want to add a single account or multiple accounts at the same time.
5. Select **Next**.
6. Add your AWS account name and copy the account ID from the AWS portal.
If you are adding multiple accounts, upload the CSV file with the account information.



NOTE: You can add multiple accounts only if you selected the option to add multiple accounts at the same time.

The CSV file should use the following format: `name,account id;importance,business context`.



NOTE: The name field is optional.

- a) Open the AWS Management Console.
 - b) Select your role name at the top right of the management console.
The drop-down menu shows the Account ID.
7. Select **Next**.
8. On the **Summary** page, make sure that the information you have added is correct and select **Add**.
9. On the **Result** page, select **Download Cloud Formation template** to download the file that you use to deploy the service to the AWS account.

The AWS account is added and the CloudFormation template is downloaded.

Next, deploy the downloaded CloudFormation template to link the IAM role to your AWS account.

4.2.5 Deploy the IAM role to AWS

Use the CloudFormation template from Elements Security Center to deploy the IAM role that links the AWS account to the service.

You have added the AWS account in Elements Security Center and downloaded the CloudFormation template.

Deploy the IAM role for the service to the AWS account.

1. Open the AWS Management Console with root user privileges.
2. Go to the **CloudFormation** service.
3. Select **Create Stack**.
4. In the **Create stack** wizard, upload the Cloud Formation template file that you downloaded from Elements Security Center.
5. Select the uploaded template file.
6. Select **Next**.
7. Enter a name for the stack, and select **Next**.
8. Review and confirm the stack settings.
9. Select **Create stack** to start the process.

The AWS account is linked to the service.



NOTE: For configuring multiple accounts at once, use the CloudFormation template and apply it to your Terraform configuration structure.

4.2.6 Validate cloud account status

Validates that a cloud account's connection status shows as active.

To validate the cloud account status:

1. Wait up to a minute and then select **Validate status** in the **Actions** section of the cloud account details to see the connection status change to **Active** (green check mark).
2. Under **Environment > Cloud > AWS Accounts and Security Posture**, select the associated cloud account name and then follow the same steps to validate its status.

The cloud account status shows as **Active** (green check mark).

4.3 Network asset onboarding

By onboarding network assets (external assets), you get an understanding what an attacker sees when targeting your organization from the outside.

Our scanners enumerate and discover more assets relating to your organization, which improves your visibility across all areas. The core asset types discovered are domains, subdomains, IPv4 addresses, and CIDR blocks. Ownership of new assets is confirmed through other data points, such as certificates and registration details stored within WHOIS. Therefore, this requires minimal configuration.

4.3.1 Add a new network asset

Adds a network asset to Elements Exposure Management by internet discovery or CSV import.

You can add network assets to **External assets** either by internet discovery or by importing asset data from a CSV file.

1. Open the WithSecure Security Center.
2. Under **Environment**, select **Network > Add new asset**.
3. Select the CSV file that contains the asset data that you want to add.



NOTE: The data in the file must be comma separated on separate lines, for example, <asset_name>, <asset_type>, <asset_importance>, <business_context>. The asset name must clearly identify the selected asset. Asset types are case sensitive. They can be as follows: Domain, Subdomain, Ipv4Address, or CIDR. Asset importance can be

Low, Medium, or High. Importance is optional with the default value of Medium. Business context is an optional text property that is limited to 256 characters. It can be used to describe the asset or to provide extra context to the importance rating. For example:

- domain.com, Domain, Low, Business context
- test.domain.com, Subdomain, Medium
- 192.158.1.38, Ipv4Address, High
- 192.168.0.1/24, CIDR

4.4 Identity onboarding

Onboard identity assets to find identity-related risks, such as missing multifactor authentication (MFA) and leaked credentials.

Microsoft Entra ID is currently supported. Onboard Microsoft Entra ID identities from Identity inventory. Identity-related scans start immediately after onboarding.



NOTE: For newly onboarded companies, identities and associated breach data appear within minutes. The exact time depends on the scanning and processing queues. For companies already onboarded, new identities, Microsoft Entra ID updates, and breach data can take up to 36 hours to appear.

Chapter 5

Managing scans

Topics:

- Device scans
- Cloud account scans
- Network asset scans
- Identity scans

Managing scans

Scanning your devices, cloud accounts, networks, and identities with Elements Exposure Management to find vulnerabilities and exposures.

Elements Exposure Management scans your environment to find vulnerabilities and exposures. You can scan devices, cloud accounts, networks, and identities.

5.1 Device scans

Elements Agent-based, discovery, and system scans for devices.

The scanning process

First, the discovery scan uses automatic device discovery to map the available network. It shows the active hosts, ports, and services that are available for further scanning and helps you choose which components to include.

Later, all selected hosts, ports and services are scanned for vulnerabilities with the system scan and web scan, before presenting the data in Elements Security Center. The reporting tool will take you from complete overview to extreme technical detail, giving you all the information you need for the remediation phase, where you assign and manage your security issues.

Verification scans confirm that issues have been handled. Point-and-click controls and benchmarking history help you verify the results.

Detailed descriptions

A security audit usually starts by identifying the assets to scan for vulnerabilities. *Discovery scan* maps the devices and services in the target network.

In WithSecure Elements Exposure Management, all *system scan* and *web scan* targets are stored in logical containers called *scan groups*. The scan groups serve multiple purposes:

Organize your assets	For example, you can organize your assets based on your network ranges, physical locations, or by system owners.
Apply scan templates	to assets within the scan group.
Apply scheduling	to assets within the scan group.
Select scan nodes	used to perform the network vulnerability scans.
Control email notifications	for the entire scan group.

5.1.1 Discovery scans

Discovery scans help you to identify all systems and their exposed ports (services) within your network. They give you a quick overview of the items that you may want to include in the network vulnerability scan.

A discovery scan identifies the systems and exposed ports on your network, giving you a quick overview of the items to include in a network vulnerability scan. You add, configure, run, and review discovery scans.

Add discovery scans

You can add a new *discovery scan* on the **Discovery scans** page.

To add a new *discovery scan*:

1. Under **Security Configurations**, select **Scans > Discovery scans**.

2. Select , and then select **Add discovery scan**.
3. Select either the **Host discovery** or **Port scan** mode.
 - *Host discovery* identifies if hosts are online or offline. The scan procedures include ARP resolution (in local segments), ICMP PING, and a limited scan for default SSH, HTTP, and HTTPS ports, as well as for Remote Desktop services.
 - *Port scan* finds the open ports on the hosts and reports the services (for example, database and web services) that are running on each one.
4. Enter the IP ranges to include in the scan or select **Upload targets from file** to upload targets in CSV format.
 - Enter a name for each IP range that you enter. Click **Add** to add more IP ranges to the same scan.
 - You can exclude an IP range within the included range by adding it to the **Excluded IP ranges** field.

For example: 192.168.1.0/24
5. Select the *Scan node* to use for the scan.
6. Click **Next**.
7. Select the template to use for the scan.
8. Define the scan scheduling if you want the scan to run automatically, for example once a month.
9. Configure the email notifications if you want to receive alerts on certain events.
10. Click **Finish**.

Configure discovery scan templates

Scan templates store a set of options that you want to use across several *discovery scans*.

1. Under **Security Configurations**, select **Scan templates**.
2. Select **Add discovery scan template**.
3. Enter a name and a description for the template.
4. Select **Next**.
5. Define settings for the template. Choose a scan mode between host discovery or one of the port scan options:
 - **Host discovery** mode is extremely fast at identifying hosts on a network. It is mainly used on internal networks where all hosts reply to an ICMP ping. The host discovery mode is fast because its only purpose is to identify hosts on the network. It does not care about how many open ports a given system has.
 - **Port scan** mode will attempt to detect hosts on a network and their open ports within the specified port range. Port scan is mainly used to identify hosts and services on Internet-facing systems.
 - a) To select *Port scan*, select the port range to scan:
 - **Top 100** scans each IP for the 100 most common open ports.
 - **Top 1000** scans each IP for the 1000 most common open ports.
 - **Full range** scans the full TCP and UDP range from 0 to 65535.
 - **Custom** allows you to select your own range. For example, TCP 0 - 10000 and UDP 0 - 5000.
 - b) Select **Detect operating system** to attempt to detect the operating system based on the information gathered during the port scan.
 - c) Select **Proceed if no PING** to force the *discovery scan* to port scan an IP even if it does not reply to PING. If this option is disabled, the port scan might go faster, but some open ports might not be detected.

6. Select the Scanning performance.

This setting controls the timeout, which means how long the *discovery scan* should wait for a reply before it moves on to the next port number. Note that aggressive settings may cause a *Denial of Service* condition on the target host itself or the intermediate network equipment, such as a firewall.

7. Select the Number of threads.

This setting defines how much resources are used to scan a single IP address. A higher amount of threads increases the overall scan speed, but it should be used carefully - especially if the scanning performance settings are above normal. Such optimized configuration might decrease the scan precision.

8. Turn Double check on or off.

This setting forces the *discovery scan* to scan each port twice. Use this option when scan accuracy is more important than scan speed, or if the network is slow or unstable.

9. Turn Fragmented scan on or off.

The fragmented scan mode can be used to fragment IP packets in an attempt to bypass low-quality or misconfigured firewalls.

10. Click Finish to save the template.

The discovery scan template is saved and available for use in scan groups.

Run discovery scans

You can run any of your available *discovery scans* on the **Discovery scans** page.

To run a *discovery scan*:

1. Select the checkboxes of the scans that you want to run.

The action bar appears at the bottom of the page.

2. Select Start scanning from the action bar.

TIP: You can click the **Play** button in the **Status** column to run a single scan.

3. While the scan is running, you can follow its progress by checking the Status column.

A scan can have one of the following statuses:

- **Idle** - the scan has never been started before.
- **Initialized** - the scan has been accepted by the scan node and will start shortly.
- **Queued** - the scan is waiting for an available slot on the scan node.
- **Running** - the scan is in progress on the scan node, and you can move your cursor over the progress bar to see more detailed information.
- **Completed** - the scan has finished.

4. When the scan is completed, click the name of the scan to view the results.

View the discovery scan results

The *discovery scan* results page contains a summary of the scan details, such as scan time and overall statistics, as well as a list of the identified hosts.

The discovery scan results page summarizes the scan and lists the assets it found.

1. On the Discovery scans page, click the name of the scan that you want to view.

This opens the report for the selected scan. The actual scan results are listed below the filter and scan summary. This list contains detailed information about each IP, such as its MAC address, reverse DNS hostname, the potential operating system, and the open ports found. Some IPs are marked with a green

checkmark icon while others are not. Hosts that are already added to a system scan for network vulnerability scanning are marked with a green checkmark icon.

2. If you want to narrow down the list of hosts displayed:

a) Click **Filter**.

This helps you remove irrelevant hosts if the scan covered a wide IP range and a large number of hosts were discovered, as the full list of hosts can be overwhelming.

b) Specify the filtering parameters that you want to apply.

c) Click **Apply**.

3. To add listed hosts to a scan group:

a) Select the hosts that you want.

b) Click **Add to network vulnerability scan group** at the bottom of the page.

c) Select the target network scan groups.

d) Click **Finish**.



NOTE: You can also add the discovery scan as a source for a scan group, after which new hosts are automatically added to the scan group.

5.1.2 System scans

System scan is a network-based vulnerability scanner that can scan any system with an IP for common vulnerabilities.

System scan's vulnerability detection is based on both active and passive vulnerability checks. For example, it will attempt to identify the service (product) and its version number. Once that is identified, the system scan checks if that particular software has any known vulnerabilities. In addition to passive scanning based on banner grabbing, system scans also run active checks in an attempt to confirm the existence of certain vulnerabilities or system misconfigurations. It can also identify missing security patches and outdated software if authenticated scanning has been enabled.



NOTE: System scan is non-disruptive and designed not to cause Denial of Service conditions on your systems.

When you start a *system scan*, it first performs a port scan of the target and once all the open ports (services) have been identified, they will be assessed for vulnerabilities. Examples of systems that can be scanned by the *system scan* include:

- Web servers
- Firewalls
- Email servers and gateways
- Routers and switches
- Domain controllers
- DNS servers
- Antivirus gateways
- Workstations

The checks that the scanner runs include the following:

- Detect services and operating systems discovery (UDP / TCP / ICMP)
- Testing for vulnerabilities and misconfigurations in services
- Testing for vulnerabilities and misconfigurations in operating systems

- Testing for vulnerabilities and misconfigurations in network devices
- Secure configuration testing (SSL / SSH)
- Default passwords discovery (operating systems / services / network devices)

All vulnerabilities are reported with a CVSSv2 score, CVE, BID, BugTraq, and other references when available.

Add system scans

We recommend that you add a new *system scan* by adding hosts to a scan group based on the results of a *discovery scan*, but you can also add a new *system scan* to the scan group separately.

If you need to add a new *system scan* manually:

1. Under **Security Configurations**, select **Scans > Network scans**.
2. Select  and then select **Add system scans**.
*The **Scan targets** window opens.*
3. In **IP range**, enter the list of scan targets.



TIP: If you have a large list of scan targets, click **Upload targets from file** to upload a plain-text file in CSV format. Separate hostname or IP address, name, and virtual hostname in three different columns in the file.

4. Click **Finish**.

Configure system scans

You can use templates to configure multiple system scans at a time (recommended), or you can configure individual scans.

A scan template is assigned to a *scan group* and the template is applied to all hosts within that group.

To configure *system scans*, define the desired port range to scan and if needed, modify the performance settings.



TIP: We recommend that you use the default settings.

To configure a *system scan*:

1. To configure a single system scan:
 - a) Under **Security Configurations**, select **Scans > Network scans**.
 - b) Select  and then select **Add system scans**.
 - c) Define the TCP/UDP **Port range** to scan. Keep the default **Scanning performance** setting unless your environment requires a change.
 - d) Click **Finish**.
2. To configure a system scan template:
 - a) Under **Security Configurations**, select **Scan Templates**.
 - b) On the **Network scan templates** tab, select **Add system scan template** or select the menu icon in the actions column and select **Create a new template based on this** to edit an existing template.



NOTE: Elements Exposure Management has some built-in templates that cannot be edited.

- c) Define the TCP/UDP **Port range** for the template. Keep the default **Scanning performance** setting unless your environment requires a change, then save the template.
- d) On the **Network scans** tab, select **Group view**.
- e) Select the menu icon next to the group name and select **Edit scan group**.
- f) Select **Next** to go to the **System scans** page.
- g) Select the template that you created or edited, and decide if you want to overwrite the existing scan configuration.
- h) Select **Next** until you reach the **Summary** page, then select **Finish** to save your changes.

The system scan configuration is saved and applied to the scan group.

System scan configuration options

You can use the tooltips next to any of the options in the UI to see more information about them.

General

- Define a **Template name**. We recommend that you make this as descriptive as possible.
- Define the TCP/UDP **Port range** that you want to scan. We recommend that you perform a full TCP/UDP port scan to ensure full coverage.
- **Scanning performance** decides the delay between packets sent (during the port scan).
- **Skip backported software** decides if the system scan should skip reporting certain vulnerabilities on operating systems that support backported software.



NOTE: Backporting is the action of taking parts from a newer version of software and porting them to an older version of the same software. When this approach is used for applying security patches on Linux distributions like Red Hat, Ubuntu, Debian and others, the software's version number does not change. System scans will therefore continue to see the software as outdated and report false positives. The best way to avoid such false positives is to configure authenticated scanning, which will enable system scans to verify the actual patch level on the system being scanned. Unfortunately, it is not always possible to run authenticated scans, which is why you can use the **Skip backported software** setting. This allows you to decide if system scans should report vulnerabilities in backported software or not.

- **Extended scan log**. Only enable this option if you need to debug a scan.

Plugin selection

You can choose specific plugins that you want to scan for. You can define a scan configuration that will either exclude or include the scanning of certain plugins. The most common scenario is when new critical vulnerabilities are announced to the public and you would like to scan for that specific vulnerability. For example, you can create a scan template that will only scan for the "Heartbleed" vulnerability.

For inspiration, go to **Templates > Network scan templates** to view some of the built-in scan templates.



NOTE: It is recommended that you always scan with a complete set of plugins. A scan that covers a limited number of plugins gives a false security status of the scanned system and may affect the vulnerability remediation status known to Elements Vulnerability Management. For example, already detected vulnerabilities can disappear on the latest report and be considered fixed.

Authentication In addition to regular network-based scanning, where the host's ports are scanned and the exposed services are reviewed for flaws, you can also run a system scan in authenticated mode, which enables it to authenticate the target host. Authenticated scanning helps the scanner eliminate potential false positives and check patch levels and other misconfigurations.

5.2 Cloud account scans

WithSecure Elements Exposure Management scans allow you to assess the security and compliance posture of your cloud accounts.

Scans check your cloud assets and services for potential risks, such as misconfigurations, vulnerabilities, or violations of best practices and regulatory standards. By using scans, you can gain visibility into your cloud security posture, identify and prioritize findings, and take remediation actions. Scans also help you to show the compliance of your cloud accounts with various frameworks and standards.

Scans are run periodically and can be run on demand.

5.2.1 Add cloud account scans

Adds a new *cloud account scan* that checks selected accounts against a rule group on a recurring schedule.

A cloud account scan checks the accounts you select against a rule group on a recurring schedule and reports compliance findings.

1. Under **Security Configurations**, select **Scans > Cloud scans**.
2. Go to the **Scans** view.

The **Scans** view shows the list of scans that you have configured for your cloud accounts. Each scan checks your cloud resources for compliance with the rules that you have selected for that scan.

Name	The name of the scan. Click the name to edit it.
Latest scan status	The status of the most recent scan.
Scan results	The number of findings that were detected by the scan, divided by their severity level. The severity level indicates how critical the finding is and how urgently it should be resolved.
Cloud accounts	The number of cloud accounts that are included in this scan.
Followed findings	The number of findings that you have marked as Prioritized for this scan. Followed findings are the ones that you want to track and resolve.
Rule group	The name of the rule group for which this scan belongs. Click the name to edit the rule group.
Scan frequency	The frequency at which this scan is performed automatically.
Next scheduled scan	The date and time of the next scan that will be performed automatically based on the scan frequency.

3. Select **Add scan**.
*The **Add new scan** wizard opens.*
4. On the Scan information page, choose the rule group and the scan frequency.

Name	Enter the descriptive name for the new scan.
Organization	Select the organization the scan is linked to.

Rule group	Select the rule group that contains rules and compliance frameworks that you want to scan.
Scan frequency	Select when and how often the scan runs based on your security and operational needs. Scans can be set to run daily, weekly, or monthly at specific times.

5. Select **Next**.

*The **Cloud accounts** page opens.*

6. Select cloud accounts which are scanned when the scan is run.

7. Select **Next**.

*The **Summary** page opens.*

8. Review the scan details on the summary page. Select **Next** when you are ready to finish.

9. Select **Done**.

The scan runs automatically the next scheduled time.

Create a new rule group

A rule group is a collection of rules that define the security posture for a specific need or purpose. You can use rule groups to customize the scope and criteria of your scans.

You can add either predefined or custom rules to the new rule group. Predefined compliance framework rules cover different sets of rules, which you can also customize or you can create completely new custom rule groups by selecting the rules that you want to include from the **Rule** list.



TIP: When you are creating a new rule group, we recommend that you group rules by similar characteristics.

Create a rule group as follows:

1. Go to the **Scans** view.

2. Select **Add rule group**.

*The **Rule group settings** wizard opens.*

3. Type a descriptive name for the new rule group to identify it.

4. Select compliance frameworks and rules that apply to this rule group.

Compliance frameworks provide guidelines and best practices for organizations to meet certain regulatory requirements:

Toggling these frameworks on or off selects or deselects the rules that are associated with each compliance framework in your rule group.

5. Select **Save** to finish editing the rule group and save your changes.

The new rule group is created and available for use in a scan.

Add a new scan to take the new rule group into use.

5.2.2 Scan cloud accounts

Typically all scans are run at scheduled times. To get scan results immediately, you can run a scan manually.

Manual scans use the same scan configuration as the scheduled scans. Running a scan manually does not affect the schedule of the automatic scans. For example, if you run a manual scan on a weekly scan configuration, the next automatic scan will still run on the preferred day and time that you have scheduled.

You can start multiple manual scans at the same time.

1. Under **Security Configurations**, select **Scans > Cloud scans**.
2. Select the scan that you want to run.
The action panel opens.
3. Select **Start scan**.

You can see the status of all your manual and scheduled scans in the **Cloud scans** tab in the **Scans** view.

5.3 Network asset scans

With the network assets, you get an understanding what an attacker sees when targeting your organization from the outside.

Network asset scans reveal your external attack surface: the internet-facing systems and services that an attacker can see when targeting your organization from outside.

5.3.1 Identify internet-facing systems

You can find your organization's internet-facing systems in Elements Exposure Management with internet discovery.

The internet discover feature uses the Shodan.io search engine API, which employs crawling and port mapping to allow you to collect data on public systems. You can search for data based on location, top-level domain, pay-level domain, keywords, hostname, and IP address.

You can add the discovered hosts to a scan group for network vulnerability scanning using either passive or active scanning. Passive scans check for vulnerabilities without connecting to the target host. Active scanning runs a regular system scan on the host. You can also add hosts to be scanned as part of External attack surface (EAS) scans.

1. Go to the **Internet discovery** page.
2. Open **Filter**.
3. Enter your search query using the following format:
 - Use `country:<country code>` to search for hosts in a specific country
 - Use `tld:<top-level domain>` to search for hosts using a specific top-level domain
 - Use `pld:<domain>` to search for hosts within a specific pay-level domain
 - Use `host:<search string>` to search for hostnames that contain a specific string
 - Use `keyword:<search string>` to search for hosts that contain a specific keyword
 - Use `ip:<IP address>` to search for hosts that use a specific IP address.
4. Click **Apply**.
5. Do one of the following:
 - Select the hosts that you want to add and then select **Add to scan group**.
 - Choose the type of scan that you want to run, select the scan groups for the hosts, and then select **Add > Add to External assets**. The host is now set to be scanned by the External Attack surface (EAS) scan.

5.3.2 External attack surface scans

External attack surface (EAS) scans monitor your internet-facing assets that have been onboarded for known EASM risks, such as the risk of sub-domain takeover.

The initial scan starts within a few minutes after you add a seed assets that are known to be owned by you such as domain or subdomain names. Subsequent scans will follow on frequent basis.

5.3.3 Cloud scan nodes

While Cloud Scan Nodes are part of device scans, they can also discover and scan externally visible network assets, that is, the external attack surface.

Cloud scan nodes are scan nodes hosted by WithSecure. In addition to taking part in device scans, they can discover and scan your externally visible network assets, that is, your external attack surface, without you having to deploy your own scan node.

5.4 Identity scans

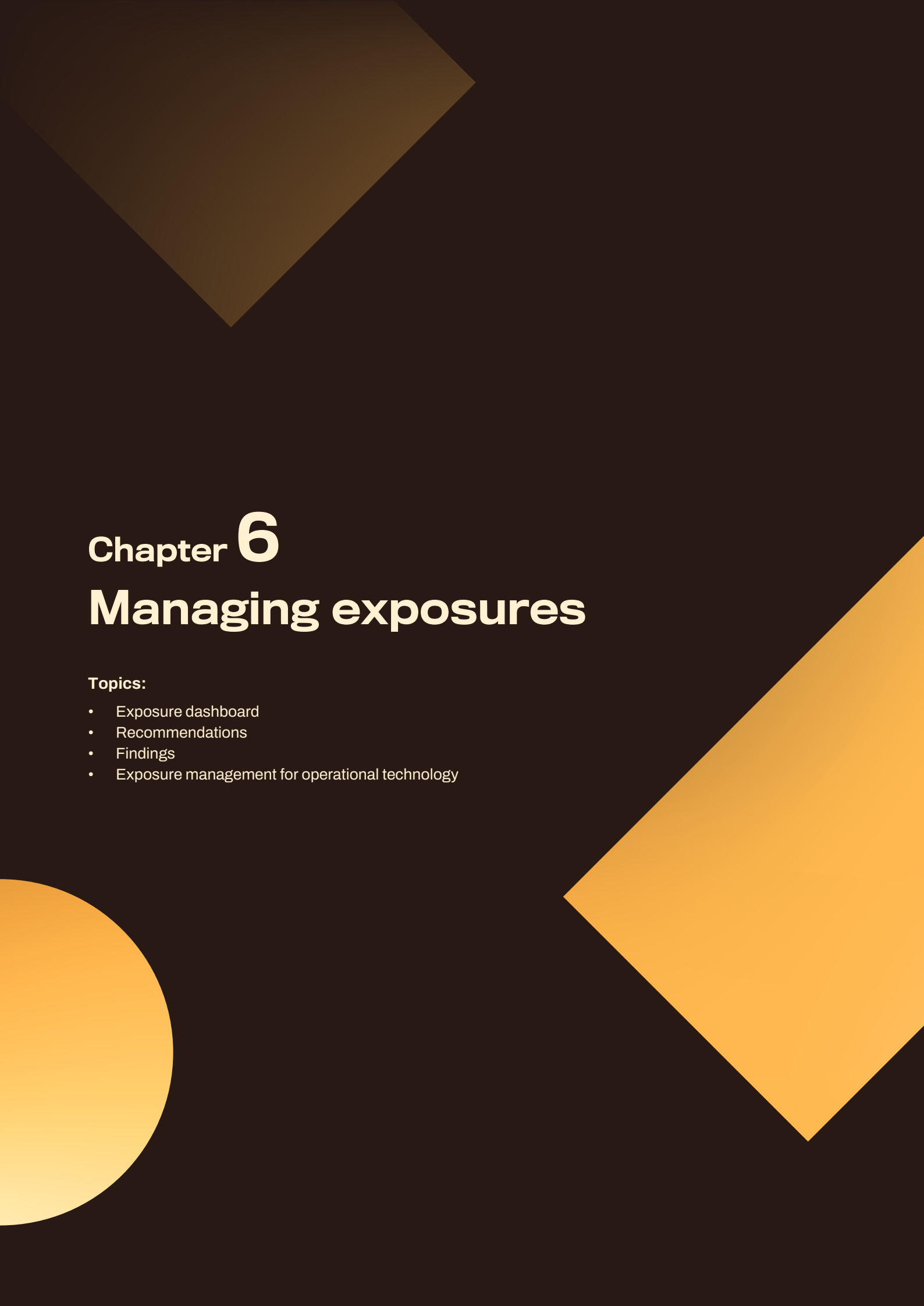
Identity scans are essential for identifying risk of unauthorized access to sensitive information and systems.

WithSecure Elements Exposure Management currently includes two types of identity scans which produce findings and recommendations:

- EntraID scans
 - Missing Multifactor Authentication (MFA)
 - Old password
 - EntraID risky users
- Leaked scans
 - Leaked credentials

In addition, the scans populate the **Identities** page under **Environment** in Elements Security Center with following the details:

- Personal information that is sourced from EntraID, including names, email addresses, and locations
- Account details such as UPN (User Principal Name), time of the last password change, M365 license plan, and multi-factor authentication (MFA) status
- Security findings, including detected leaked credentials
- Assessment of identity risks based on exposure findings from multiple sources
- Last login device information with timestamp and device status, if you have onboarded the Elements Endpoint Protection solution



Chapter 6

Managing exposures

Topics:

- Exposure dashboard
- Recommendations
- Findings
- Exposure management for operational technology

Managing exposures

The following describes the WithSecure Elements Exposure Management workflow.



NOTE: Descriptions for Exposure recommendations are now generated by a large language model (LLM). By default, these recommendations are generic and identical across all organizations, and no organization-specific data is sent to the LLM. Organizations that choose to opt in to sharing their data with the LLM receive recommendation descriptions that are tailored to their specific environment rather than the generic LLM-generated version.

Managing exposures typically includes the following steps:

1. Review the dashboard at **Home > Exposure**. It highlights the areas that need your immediate attention.
2. Select the top recommendation from the Highest impact recommendations list to view the details.
3. Review the recommendation details. Each recommendation shows the following:
 - Assets - affected resources
 - Findings - identified issues
 - Attack path visualization - how an attack could progress
 - Required actions - steps to address the issues
4. Recommendations contain remediation instructions that you can apply. When applicable, you can also:
 - Look for patches: Search for and install the required updates through the Elements Security Center
 - Elevate to WithSecure: Ask the WithSecure team for help
 - Copy instructions: Copy the steps and share them with the team handling the issue
5. After you apply the recommended actions and the related scan finishes, the dashboard shows the updated recommendation status and exposure score.

6.1 Exposure dashboard

The Exposure Dashboard serves as the entry point for reviewing Exposure Management. It highlights areas that require immediate attention.

The Exposure Dashboard is composed of multiple sections, each presenting a different aspect of exposure data.

Coverage

The **Coverage** widget displays the organization's threat exposure management status across various asset groups: **Unmanaged Devices**, **Managed Devices**, **Network**, **Identities**, **AWS Cloud**, and **Azure Cloud**. Each asset group includes a state indicator that reflects its onboarding and licensing status:

- **In use** (Green): The asset group is fully onboarded to WithSecure Elements Exposure Management, and scans are actively running.
- **Onboard now** (Orange): The organization has the necessary licenses, but onboarding or configuration is incomplete. Click the area to see the relevant view to complete the setup.
- **No Subscription** (Grey): The organization does not have the required licenses for this asset group. To proceed, contact your sales representative for licensing options.

Organization exposure risk

The Organization Exposure Risk Chart shows your company's exposure risk in comparison to the average exposure risk of other companies.

The exposure risk of a company represents the relative business risk posed by the current state of the company's digital assets. The asset exposure risk score is calculated based on various factors, including attack path mapping, business context, and threat intelligence.

The average company exposure risk is calculated as the average of the exposure risks for all companies using WithSecure Elements Exposure Management. This average is updated regularly.

Highest impact recommendations

The Highest Impact Recommendation List displays the top 5 active recommendations with the greatest potential for risk reduction. Our AI-powered recommendation engine analyzes your environment and prioritizes the most significant actions you can take to improve your security posture.

To view the full list of recommendations, navigate to **Environment > Exposure > Recommendations**.

Exposure risk by category

The **Exposure risk by category** chart displays calculated exposure risk values segmented by asset type. This breakdown helps identify which asset categories contribute most significantly to overall risk for targeted remediation efforts.

Assets with the highest exposure risk

The **Assets with highest exposure risk** list identifies the top five assets ranked by their calculated exposure risk. This list is intended to help administrators focus on the most vulnerable and significant assets within the environment.

Each asset's exposure risk score is derived from a combination of the following contributing factors:

- Likelihood of attacker exploiting asset findings
- Likelihood of attacker exploiting findings to reach this asset
- Asset business context
- Lateral movement to critical assets in case the asset is compromised

Executive summary (beta)

The **Executive summary (beta)** feature allows you to generate a customer-facing report that summarizes organizational risk levels and key security activities performed during a selected reporting period. The report is exportable as a PDF and is designed to support transparency and demonstrate progress in risk management.

Report contains:

- Text that you can edit to summarize the actions and their impact.
- Company exposure risk as a visual grade with reference to how you are doing compared to other companies using WithSecure XM.
- Exposure risk shows company exposure risk trend line for the selected time period.
- Recommendation fixed – number of recommendations with closed status ("Done", "False positive") per week (snapshot).
- Exposure risk by asset type showing the exposure risk comparisons for the start and end of the reporting period split by asset type.

6.2 Recommendations

An AI-powered engine analyzes threat intelligence, attack paths, business context, and security findings to generate specific remediation guidance.

Recommendation list

The **Recommendation list** shows all active remediation recommendations for the organization. Recommendations are prioritized to support efficient risk reduction and resource allocation.

Recommendations are sorted primarily by **Remediation impact** and secondarily by **Remediation effort**.

Recommendation details

The **Recommendation details** page provides in-depth information about a specific recommendation, including remediation guidance, related findings, and available actions. It helps to understand the context of the recommendation and take appropriate action.

Remediation instructions are step-by-step guidance powered by Luminen, the WithSecure AI assistant, to help you address the issue directly.

Findings and assets tables provide detailed lists of affected findings and associated assets. These tables help identify where action is required and may vary depending on the recommendation type.

Attack path is a graphical representation of how an attacker could exploit the issue.

- **Green node:** Initial access point (for example, public-facing service or phishing email).
- **Red nodes:** Vulnerabilities related to the current recommendation.
- Selecting an asset node opens a pane with its related findings and its role in the attack path.



TIP: Use the checkbox panel to toggle between different attack paths. Select **Show details** to view each step, including involved assets, tactics and techniques, and specific findings.

The left sidebar provides additional tools and actions:

- **Look for Patches** – Search for and install relevant updates directly via the Elements Security Center.



NOTE: Requires an Elements EPP license with WithSecure Software Updates (SWUP).

- **Elevate to WithSecure** – Request assistance from the WithSecure team.



NOTE: This service is currently free of charge

- **Status** – Change the recommendation status. Available statuses include:
 - Open
 - Acknowledged
 - Accepted Risk
 - False Positive
 - Done
- **Notes** – Add supplementary information such as ticket IDs, responsible personnel, or progress updates.

6.2.1 Recommendation impact, effort, and status

What the remediation impact, remediation effort, recommendation status, and status badge values mean for an Exposure Management recommendation.

Remediation impact

Remediation impact refers to the proportion of overall organizational risk that can be reduced by addressing specific security findings through the recommended actions. It quantifies how much risk mitigation is achievable if the recommendation is implemented.

This value is calculated using a combination of factors, including:

- the nature and severity of the findings,
- the criticality of affected assets,
- business context and operational importance,
- known attack paths, and
- relevant threat intelligence.

Based on this analysis, remediation impact is classified into four levels:

- **Critical** – Significantly reduces overall risk
- **High** – Substantially reduces risk
- **Low** – Minimally reduces risk
- **Inconclusive** – Not enough data to determine impact

Remediation effort

Remediation effort indicates the estimated level of work required to address all security findings associated with a specific recommendation. This helps administrators assess the resource commitment needed for implementation.

Remediation effort is categorized into three levels:

- **Low** – Minimal effort required
- **Medium** – Moderate effort required
- **High** – Significant effort required

Recommendation status

Each recommendation is assigned either an **Active Group** or **Closed Group** status that reflects its current state in the remediation process.

Active Group indicates that the recommendation is still under consideration or action:

- **Open** – The recommendation has been identified but not yet addressed.
- **Acknowledged** – The issue has been recognized, but remediation has not started.
- **Accepted Risk** – The organization has chosen to accept the risk without remediation.

Closed Group indicates that the recommendation has been resolved or dismissed:

- **False Positive** – The finding was determined to be incorrect or not a true risk.
- **Done** – The recommendation has been fully implemented and the issue resolved.

By default, only **Active** recommendations are shown. To view **Closed** recommendations, adjust the filter settings in the recommendation list.

Setting Recommendation Status manually

You can manually assign a status to each recommendation based on the assessment of the associated security findings. The available statuses and their intended use are as follows:

- **Open** – Indicates that the recommendation requires attention and has not yet been addressed.
- **Acknowledged** – Indicates that the recommendation has been reviewed and remediation efforts are currently in progress.
- **Accepted Risk** – Indicates that the related security findings have been reviewed and, although the findings are valid, there is a justified reason for not mitigating them. The risk is formally accepted.
- **False Positive** – Indicates that the related security findings have been reviewed and determined to be incorrect or they were triggered in error.

Recommendation Status badges

Status badges are small colored indicators displayed next to the status of a recommendation in the recommendation list. The following badge types are used:

- **Red** – Indicates that the recommendation has been issued within the past 30 days and has a **Remediation Impact** greater than **Inconclusive**.
- **Orange** – Indicates that the recommendation has transitioned from a **Closed** to an **Active** state due to an increase in its **Remediation Impact** from a lower tier to a higher tier.
- **Green** – Indicates that the recommendation has transitioned from **Active** to **Closed** because its **Remediation Impact** has decreased to **Inconclusive**.

This typically occurs when all significant security findings associated with the recommendation have been resolved, either manually or automatically, and the findings are no longer detected in subsequent scans.



NOTE: If you change the status of a recommendation that has a badge, the badge is removed.



NOTE: Red and orange badges appear only with recommendations that have a **Open** status and green badges appear only with recommendations that have a status of **Done**.

6.3 Findings

A finding is a single instance of a vulnerability, misconfiguration, or other security issue that is relevant to the organization's attack surface or compliance posture.

Finding list

The **Finding list** shows all identified security findings across the organization. Each entry provides key details to help assess and prioritize remediation efforts.

The table includes the following information:

- **Finding Type** – The category of the issue
- **Asset Type** – The type of asset affected
- **Affected Asset** – The specific asset where the finding was detected
- **State** – The current status of the finding
- **Last Seen** – The most recent date the finding was detected.

Finding details

The **Finding details** page provides comprehensive information about a specific security finding, along with available actions and contextual insights to support remediation.

The left sidebar offers additional tools and actions, when applicable:

- **View related recommendations** – Shows a list of recommendations associated with this finding.
- **View assets with this finding** – Lists all assets where this finding has been detected.
- **Status** – Allows you to update the status of the finding. Available statuses include:
 - Open
 - Acknowledged
 - Accepted Risk
 - False Positive
 - Done



NOTE: Findings that are **False Positive** or **Done** are excluded from scoring calculations.

6.4 Exposure management for operational technology

The following describes a non-intrusive, repeatable process to reduce cybersecurity risks in operational technology (OT) environments without disrupting operations.

The workflow focuses on the most important risks first and combines identity hardening, attack path analysis, controlled scanning, and guided remediation. It is designed to be repeated on a regular cycle.

1. Secure identities with access to OT.

Protect all user identities and accounts that can access OT systems:

Prioritize identities	Mark personnel with OT access as high-priority assets.
Connect frontline workers	Assign a frontline add-on license where applicable to bring them under management.
Limit access	Make sure that these identities have only the permissions required for their role.

2. Eliminate attack paths leading to OT.

Identify and remove ways an attacker could move from IT into OT:

Prioritize connecting assets	Mark IT assets that connect to OT interface assets as high priority.
Simulate attack paths	Run attack path simulations in the IT environment to verify whether OT interfaces can be reached.

3. Secure the external attack surface of OT.

Understand what is exposed to the internet and reduce unnecessary exposure:

Scan from outside	Run a controlled external exposure scan to identify internet-facing services related to OT.
--------------------------	---

4. Run controlled scans inside OT.

Use low-impact discovery and assessment to avoid disrupting operations:

Install a scan node	Place a scan node inside the OT environment to keep traffic local and controlled.
Catalog unmanaged devices	Use an internal discovery scan to find devices that are not yet inventoried.
Label and search	Tag discovered devices for future reviews.
Assess for known weaknesses	Run a system scan to check for known issues and configuration gaps.



NOTE: The system scan is an extensive scan and it should be scheduled to minimize operational risk.

5. Take remediation actions.

Address issues in a prioritized and safe way:

Review findings	Use expert guidance or a human-in-the-loop assistant to understand the impact and urgency.
Escalate when needed	Use WithSecure Elevate to get more instructions and detailed recommendations.

Exposure management is an ongoing process. Revisit these steps on a defined schedule and after any changes in your OT or connected IT environments. Each cycle should reduce attack paths, improve identity hygiene, and tighten your external and internal exposure.



TIP: Document your scan windows, stakeholder contacts, and change-control approvals to keep the process safe and predictable for operations.

Chapter 7

Reporting

Topics:

- Create vulnerability management reports
- Add widgets to My report
- View vulnerability management reports
- Create exposure management reports
- Configure email reports
- Create a custom view for security events
- Edit the settings of an existing report
- Clone an existing report
- Update contents of existing reports
- View Executive summary
- Delete reports

Reporting

Reporting is a vital part of WithSecure Elements Security Center. You can generate customized reports that suit the needs of your manager, system administrator, or your third-party service provider.

You can start creating reports as soon as your scans are completed.

You can download the reports to your computer in the following formats:

XML report grouped by hosts	Download the raw report data in XML format, organized by host.
Excel report grouped by vulnerabilities	Contains all the technical details of the hosts in scope and gives you the freedom to use the features available in Excel.
Word report grouped by hosts	Contains all the technical details of the hosts in scope, organized by host. This is useful when your scope does not cover a large number of hosts.
Word report grouped by vulnerabilities	Contains all the technical details of the hosts in scope, organized by vulnerability type. This gives you a smaller report if the scope is very large.
Word report, executive summary	Designed to be a light-weight report with few pages even if the report scope covers thousands of hosts.
Word report, preliminary PCI	This report helps your organization to proactively identify issues that need to be addressed to ensure the compliance state of your systems with the Payment Card Industry (PCI) standards.

Vulnerabilities detected during multiple scans can be combined into one report.

Exposure management reports can be scheduled to be sent via email periodically.

Once the report is created, it is added to the list on the **Reports > Email notification and report** page. As soon as reports are run, they appear as report instances under the report. Only 10 latest report instances can be downloaded from the portal. This means that generating a new report removes the oldest report instance from the list.

7.1 Create vulnerability management reports

You can create your own report on the **Reports** page.

You can start creating reports once your scans are completed. If there are no scans run yet, you can start your first agent-based scan on the **Environment > Devices > Device Discovery** page, or in the WithSecure Elements Security Center, go to **Security Configurations > Scans > Network scans** start a network-based scan.

To create a report:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Select the **Email notification and report** tab and then select **Add vulnerability report**.
*The **Vulnerability report** page opens.*
3. Give the report a descriptive name (required) and a description. You can also select the language of the report.
4. If you want to define a schedule for the report, turn on **Schedule** and enter the following details:

Option	Description
Report frequency	Based on the values you select, the time of the next report is shown beneath the report frequency fields.

Option	Description
Time Zone	The time zone comes from your profile. If you wish, you can change it for this report.
Email notifications (optional)	If you wish, you can specify that the report is automatically sent to email addresses of your choice. Separate the email addresses by commas. • Report format shared via email - Select the format of the report (.xml, .xlsx or .docx) and how the data is presented on the report. • Link to the report expires after - Define when the link to the report in the email expires.



NOTE: If you wish, you can later disable the schedule for the report by clicking its **Scheduler** column on the **Reports > Email notification and report** page.

5. Select **Next**.

*The **Scan scope** page opens.*

6. Select the report scope from one of the following options (at least one scan or asset must be chosen):

- **Assets** - Note that this is the primary choice if you mainly run agent-based scans. Not valid for network scans nor network scan groups.
- **Network vulnerability scan groups**
- **Tags**
- **Individual network vulnerability scans**



NOTE: If you wish, you can also use tags assigned to the scan type or group to narrow down the scan scope of the report.

7. Select **Next**.

*The **Include vulnerabilities with** page opens.*

8. Define the vulnerability scope of the report:

- Select the statuses and severities of the vulnerabilities to be included in the report.
- Under **System scan vulnerabilities**, select the categories and attack vector types of vulnerabilities to be included in the report.
- Under **Web scan vulnerabilities**, select the categories of vulnerabilities to be included in the report.



NOTE: If you wish, you can also use tags to narrow down the vulnerabilities included in the report.

9. Select **Next**.

*The **Report options** page opens.*

10. Select what information is shown on the report and then select **Next**.

*The report **Summary** page opens.*

11. Review the report details. You can still go back and make changes to the report settings by selecting **Previous**.



NOTE: By default, the **Generate a report now** checkbox is ticked. This means that the new report is generated as soon as you have selected **Finish**. If you don't want to generate the report immediately but according to the schedule that you have defined, untick the **Generate**

a report now checkbox before selecting **Finish**. However, if you later edit the report settings, you need to tick the **Generate a report now** checkbox if you want that the report is generated immediately.

12 To complete the report wizard, select **Finish**.

The report is added to the list of reports on the **Reports >** page. As soon as the report is run and complete, a snapshot of the current state of vulnerabilities, or report instance, is shown under the report on the **Reports > Email notification and report** page. If you wish, you can immediately download the report in desired format to your computer.

7.2 Add widgets to My report

My report is a dashboard on the **Reports** page, made up of individual widgets that you choose and arrange yourself.

My report is different from the scheduled reports on the **Email notification and report** tab. Instead, you build your own dashboard from widgets, each one showing live data from a source that you choose.

To add a widget to **My report**:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Go to the **My report** tab.
3. Select **Add widget**.
*The **Add widget** dialog opens.*
4. Enter a name for the widget in the **Name** field.
5. From **Data source**, select the data that the widget shows: **Devices**, **Security Events**, **Broad Context Detections**, **Patch Management**, or **AI-generated Summaries**.
6. Select **Create**.

The widget is added to **My report**.



NOTE: To start from a named layout instead of adding widgets one by one, select **New view template** on the **My report** tab.

7.3 View vulnerability management reports

Instructions how to access and view vulnerability reports for completed scans in the Elements Security Center.

Follow the steps to select and view reports, start new scans if needed, and manage report instances.

1. To view the vulnerability report for a single scan in the Elements Security Center, select **Security Configurations > Scans > Network scans**.
2. Select the name of the desired completed scan.



NOTE: If there are no scans run yet, you can start your first agent-based scan by going to **Environment > Devices > Computers**, selecting the desired devices, and then selecting **Vulnerability Management scan Enable scanning** from the action bar. Alternatively, you can go to **Security Configurations > Scans > Network scans** and start a network-based scan.

Once the report is created, it is added as a report instance to the list on the **Reports > Email notification and report** page.



NOTE: Only 10 latest report instances can be downloaded from the portal. This means that generating a new report removes the oldest report instance from the list.

7.4 Create exposure management reports

You can create exposure management reports on the **Reports** page.

The exposure management reports list recommended security actions that should be taken.

To create an exposure management report:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Go to **My Report**.
3. Open **View template** and select **Exposure Management**.
4. To define a schedule for the report, open **Email notification and report** and select **Add email report**.
5. Give the report a name and set data source to **My report**.
6. Select **Exposure Management** as the template.
7. Select **Save**.

The exposure management report is created and listed on the Reports page.

7.5 Configure email reports

You can configure automated email reports in the **Email notification and report** tab under **Reports**.

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

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

1. To add a new email report and configure it, do the following:
 - a) Select **Reports** on the left-hand navigation pane.
 - b) On the **Reports** page, go to the **Email notification and report** tab.
 - c) Select **Add email report**.
*The **Add new email report** pane opens.*
 - d) Enter a name for the report (for example, **XM report**).
 - e) From the **Data source** drop-down menu, select **Security Events**.



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

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



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

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

3. Select **Save**.

The scheduled email report is saved.

7.6 Create a custom view for security events

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

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

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

7.7 Edit the settings of an existing report

You can edit the settings of an existing report.

To edit the report settings:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Select the report whose settings you want to edit.
3. In the **Actions** column of the selected report, click the menu button and select **Edit**.

The **Report details** page opens.

4. Follow the steps in the wizard and make the desired changes to the report settings until the **Summary** page opens.
5. If you want to run the report with the edited settings immediately, tick the **Generate a report now** checkbox and select **Save and close**.

The report settings have now been saved.

Next time when the report is run, the report instance is based on the new settings. The report instances with the old settings will still remain downloadable on the **Reports > Email notification and report** page until they are gradually replaced by the new report instances as each report can have up to 10 instances at a time.

7.8 Clone an existing report

You can clone a report to reuse the settings of an existing report.



NOTE: The report instances, however, are not cloned.

To clone an existing report:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*

2. Select the report that you want to clone.
3. In the **Actions** column of the selected report, click the menu button and select **Clone**.

The report is added to the list of reports on the **Reports** page.

4. If you want to make changes to the settings of this report, click the menu button in the **Actions** column and select **Edit**.

A copy of the report is created and listed on the Reports page.

7.9 Update contents of existing reports

You can refresh the contents of existing reports to reflect the current state of vulnerabilities.

To update existing reports:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Select the report(s) whose data you want to refresh.
The action bar opens.
3. Select **Generate a report now**, and to confirm the action, select **Generate a report now**.

The data of the selected report or reports are refreshed to reflect the current state of vulnerabilities.

7.10 View Executive summary

In the Executive Summary page, you can see the exposure grade of your company and the global distribution of exposure grades in all companies that use Exposure Management.

The page also shows the exposure risk level of your company, the exposure risk by asset type, and the number of fixed made to comply with the recommendations.

To view and download the executive summary:

1. Under **Home > Exposure**, select **Executive Summary**.
*The **Executive Summary** page opens showing your company's exposure grade and risk level.*
2. Use the calendar at the top of the page to select the time period for which you want to view data.
3. Select **Download PDF report** to save the displayed data as a PDF file on your device.

7.11 Delete reports

You can delete reports that you don't need any more.

To delete reports:

1. From the left navigation pane, select **Reports**.
*The **Reports** page opens.*
2. Select reports that you want to delete.
The action bar opens.
3. Select **Delete**, and to confirm the action, select **Remove**.

The selected report or reports disappear from the **Reports > Email notification and report** page.

Chapter 8

General management

Topics:

- Device assets
- Scan nodes
- Delete cloud accounts
- Users
- Settings

General management

Managing your assets, scan nodes, cloud accounts, users, and product settings in Elements Exposure Management.

After you onboard and scan your environment, you manage it from Elements Security Center. Management covers your assets, scan nodes, cloud accounts, the users who can access Elements Exposure Management, and the product settings.

8.1 Device assets

Elements Exposure Management keeps an inventory of all the assets, such as servers, computers, printers, routers, IoT devices, etc. within your network environment, discovered by Elements Exposure Management during the Discovery scan or a network as well as agent-based vulnerability scan.

The Discovery scan maps your whole network and all its assets.

You get the full benefit from the assets inventory with Authenticated scanning; the non-authenticated scans will provide only a limited set of information about each asset.

On the **Environment > Devices > Vulnerability assets** page, you can:

- view the complete list of assets discovered in your environment;
- filter the list of assets to see the asset data that is most relevant to you;
- see detailed information about individual assets, such as the device's hardware details and the software installed on it;
- assign custom tags and criticality rating for each asset for improved prioritization of vulnerabilities.

To view the data of an individual asset, go to the **Environment > Devices > Vulnerability assets** page and click the asset name.

8.1.1 View device assets

There are several ways to view the assets in your network, and you can use filters to see the data that is most relevant to you.

On the **Environment > Devices > Vulnerability assets** page, you can view the data in the following two modes:

- **List view** - Shows all assets in a flat list which can be sorted by various criteria, such as asset name, vulnerability, criticality, etc.
- **Grouped by** - Allows you to group the assets by one of the following attributes: Department, Business owner, Hardware type, Operating system, Country, or Asset tags.



NOTE: You can group assets by manually-added asset tags only.

The standard Elements Exposure Management filtering can be used to filter the assets. Click the chevron next to **Filter** to see the available options for filtering the assets. For example, the **Asset source** option allows you to filter the assets to see only the assets which have been scanned by the authenticated network vulnerability scan.

To view the data of an individual asset:

1. On the **Environment > Devices > Vulnerability assets** page, click the asset name.

*The **Asset details** page opens, with all available information about the asset.*

- If you want to manually edit or add data to the asset details, the various attributes assigned to the asset in the **Description** tab, or the data in the **Notes** tab, click the pen icon in the top-right corner of the respective tab, edit or add the desired data and select **Save**.



NOTE: To see the latest network vulnerability scan report for the asset in question, click the link icon next to the vulnerability ratings.

Tracking asset changes

Assets can be filtered also by the following attributes: First discovered, Last seen, Last scanned and Last updated.

Use these attributes together with scheduled Discovery scans to see the changes, if any, that have taken place in an asset in your network.

Table 2: Asset change tracking attributes

Attribute	Meaning
First discovered	Indicates when the asset in question was detected by the system for the very first time. The source of information can be any type of scan, including a Discovery scan.
Last seen	Indicates when the asset in question was last seen. The source of information can be any type of scan, including a Discovery scan.
Last scanned	Indicates when the asset in question was last scanned for vulnerabilities.
Last updated	Indicates when the information about the asset in question was last updated in Elements Exposure Management. This takes place once the system detects new information about the asset and the reliability of the information source is high enough. For example, information gathered during the port scan of the asset is less reliable than that collected during an authenticated network scan.

8.1.2 Manage device asset attributes

On the **Environment > Devices > Vulnerability assets** page, you can manually supplement the asset data with various attributes.

Once an asset is discovered by a scan, all available data about the asset will be obtained automatically. Later on, you can manually edit the data or add more details to the asset.

To manage attributes related to an asset:

- On the **Environment > Devices > Vulnerability assets** page, select the checkbox of the asset (or assets) whose data you want to manage.

The action bar appears at the bottom of the page.

- Select **Manage attributes** from the action bar.

- From the drop-down, select the attribute you want to manage.

Depending on the type of attribute, a field or set of fields is displayed.

4. Enter the data you want to add.
5. Select **Save**.

The data can now be seen in the asset details in the **Description** tab where the data can also be edited.

8.1.3 Manage asset tags

On the **Environment > Devices > Vulnerability assets** page, you can add tags to assets and remove tags from them.

To add or remove tags related to an asset or assets:

1. On the **Environment > Devices > Vulnerability assets** page, select the checkbox of the asset (or assets) whose tags you want to manage.
The action bar appears at the bottom of the page.
2. Select **Manage tags** from the action bar.
3. If you want to add tags to the assets:
 - a) Select **Add the following tags to assets** and select **Next**.
 - b) Click the field and either select an existing tag from the tags list displayed or enter a new tag to add it to the assets and select **Add**.
4. If you want to remove tags from the assets:
 - a) Select **Remove the following tags from assets** and select **Next**.
 - b) Click the field and, from the tags list displayed, select the tag that you want to remove from the assets, and then select **Remove**.



NOTE: You can add tags to an individual asset also through the **Asset details** page.

8.1.4 Update notes

If you wish, you can add notes to the selected assets.



NOTE: When you update notes, the existing notes already assigned to the selected assets will be overwritten.

There are two ways you can add notes to an asset:

- On the **Asset details** page of the selected asset, select the **Notes** tab and click the pen icon in the top-right corner of the tab, enter the desired data and select **Save**.
- On the **Environment > Devices > Vulnerability assets** page:
 1. Select the checkbox of the asset (or assets) whose notes you want to update.
The action bar appears at the bottom of the page.
 2. Select **Update notes** from the action bar.
 3. Enter the data you want to add to notes and select **Save**.

You can view the notes in the **Notes** tab in the **Asset details** page.

8.1.5 Delete device assets

On the **Assets** page, you can immediately delete assets from your inventory.



NOTE: When you delete an asset, it will also remove the network vulnerability scans associated with the asset.

To remove an asset or assets:

1. On the **Environment > Devices > Vulnerability assets** page, select the checkbox of the asset (or assets) that you want to delete.

The action bar appears at the bottom of the page.

2. Select **Delete assets** from the action bar.
3. Select **Delete**.

The selected asset or assets together with the associated vulnerability scans are deleted from Elements Exposure Management.



NOTE: You can also configure Elements Exposure Management to delete archived assets automatically after a specified time.

8.1.6 Delete archived assets

If you have configured Elements Exposure Management to archive old assets, you can configure it also to delete the archived assets automatically after a specified time.

If you have configured Elements Exposure Management to archive old assets, they are archived based on the time they were last seen by any of type of scan.

To delete the archived assets automatically:

1. Go to **Management > Vulnerability Settings > General settings > Miscellaneous**.
2. Under **Archive assets**, use the drop-down to specify when assets will be archived based on the time last seen.

The options are: Never, 1 month, 1 quarter, Half a year, 1 year, or 2 years.

3. Under **Store assets**, use the drop-down to specify for how long the archived assets are stored before they are automatically deleted.

The options are: Forever, 1 month, 1 quarter, Half a year, 1 year, or 2 years.

4. Select **Save**.

All assets that meet the specified criteria will be deleted automatically from Elements Exposure Management.

8.2 Scan nodes

Security Configurations > Scans > Scan nodes is used to manage all scan nodes available in your Elements Exposure Management account.

The table shows the following information for each listed scan node:

- **Type** indicates the type of scan associated with the scan node (discovery scan, system scan, or web scan).
- **Name** contains a descriptive text for the node. You can hover over the name to see more details.
- **Current load** tells the maximum capacity of the scan node and how many scans are currently running on the node.
- **Engine update** tells when the scanning engine itself was last updated. Note that some scanning engines are updated more often than others. For example, you should expect daily updates for System Scan, but less frequent updates for the other engines.
- **Last seen** shows when the scan node last contacted the WithSecure Elements Security Center. By default, the scan nodes are configured to connect every 60 seconds.
- **Status** indicates whether the node is **Active** or **Inactive**.



TIP: Click the **arrow down** icon to view more details for the scan node.

8.2.1 Add new scan nodes

To use a new scan node, you need to either request a new license or register an already installed scan node in WithSecure Elements Security Center.



NOTE: You can download Scan Node installers for Windows and Linux from Elements Security Center under **Management > Downloads**.

1. Go to the **Scan nodes** page.
2. Select **Add new scan node**.

If you need a new scan node license:

- a) Select **Request a new scan node** and click **Next**.
- b) Enter a name and description (optional) for the scan node and click **Request**.

*When your request is approved, the license file automatically starts to download. Follow the steps on the **Summary** page to install the scan node.*

- c) Click **Done**.

If you already have a scan node license file:

- a) Select **Register a previously requested scan node** and click **Next**.
- b) Enter a name and description (optional) for the scan node.

Use a name that identifies the scan node server such as a hostname and preferably the source IP, so that other Elements Vulnerability Management users can see from which IP the node will be scanning.

- c) Use the switches to select the node types that you want to register and enter the corresponding module identifiers.

Log in to the scan node server and open the scan node control center application. Under the **Settings** tab, you will find the scan node identifier.

Make sure the scan node type matches the node identifier.

- d) **Connection type**. Defines how the scan node and the WithSecure Elements portal communicate. By default, the scan node starts the connection. If a so-called "reverse connection scan node" has been installed, the WithSecure Elements portal must start the connection.

8.2.2 Uninstalling scan nodes

Uninstalls a scan node from a Windows or Linux host.

When you no longer need a scan node, uninstall it from the host. The uninstallation procedure differs between Windows and Linux systems, so use the procedure that matches the host operating system.

Uninstall scan nodes from Windows

Follow these steps to uninstall a scan node from your Windows system.

To uninstall a scan node:

1. Go to **Control Panel > Programs > Programs and Features**.
2. Check the list of programs.

If you see **WithSecure Elements Scan Node Agent**:

- a) Double-click **WithSecure Elements Scan Node Agent**.

- b) Type **y** and press **Enter** to confirm that you want to remove Scan Node Agent.

Scan Node Agent no longer appears in the list of installed programs.

If you cannot find **Scan Node Agent**, it means that your version of Scan Node Agent is older than 2.6.1.1174. To uninstall earlier versions:

- a) Open an elevated command prompt.
- b) Change the directory to `C:\Program Files (x86)\F-Secure\RadarScanAgent`.
- c) Uninstall the Scan Node Agent's Windows service by running the following command: `FSRadarAgent.exe -u`.
- d) Delete the scan node folder `C:\Program Files (x86)\F-Secure\RadarScanAgent`.
- e) Remove the following registry key: `HKLM\Software\Wow6432Node\F-Secure\SN`.

The Scan Node Agent files and registry key are removed.

To remove any remaining files:

1. Log in to Elements Security Center.
2. Under Security Configurations, select **Scans > Scan nodes**.
3. Use the action menu to unregister the scan engines.

Uninstall scan nodes from Linux

Follow these steps to uninstall a scan node from your Linux system.

To uninstall a scan node:

Run the following command to uninstall the scan node:

```
sudo apt remove --purge f-secure-radar-scannodeagent-installer
```

8.2.3 Troubleshooting scan node issues

These checks help you resolve common scan node problems in Elements Exposure Management.

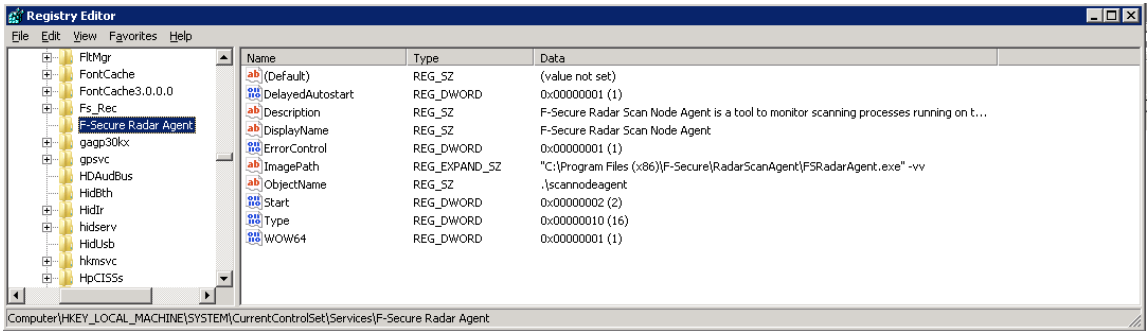
To resolve scan node issues, try the following checks:

1. Ensure that the scan node Windows service is running.
2. Open **Scan Node - Control Center** and check that the scan node is active and that scanning engines were downloaded (revision is greater than 0).
3. Review the scan node log files (`C:\Program Files (x86)\F-Secure\RadarScanAgent\logs`).
4. Perform a connection test. Run the following command as the same user that runs the service:
`C:\Program Files (x86)\F-Secure\RadarScanAgent>FSRadarAgent.exe -test`
5. Run the scan node agent in debug mode:
 - a) Via the command line with the following command: `FSRadarAgent.exe -c -vv`. For example: `C:\Program Files (x86)\F-Secure\RadarScanAgent>FSRadarAgent.exe -c -vv`.



NOTE: Remember to run the command line as the user running the "Scan Node Agent" service.

- b) Alternatively, run it as a service. To do this, add the -vv argument to the service startup command. The service startup parameters can be modified in the system registry.



NOTE: Editing the system registry is a very sensitive operation. Proceed with caution if you use this approach.

6. Check **Windows Event Viewer** for possible errors.

If none of these checks resolves the issue, contact Elements Vulnerability Management support. When sending your support request, describe your problem in detail and always attach log files (at least the log from the date when the issue occurred).

8.3 Delete cloud accounts

Deletes a cloud account that has been added to the service.

Delete a cloud account when you no longer want WithSecure to monitor it.

1. Open Elements Security Center.
2. Under **Environment**, select **Cloud**.
3. Select the account that you want to delete.
The action panel opens.
4. Select **Remove**.



NOTE: To turn off scanning for an account temporarily, select **Disable scanning** instead.

The cloud account is removed from the service.

8.4 Users

Management > Organization Settings > Vulnerability users allows you to control user access to WithSecure Elements Exposure Management using Role-Based Access Control (RBAC) principles.

User management in Elements Exposure Management involves three concepts: **Users**, **User groups**, and **Roles**.

Users The **Management > Organization Settings > Vulnerability users** page shows you a list of all users with access to your Elements Exposure Management account. On this page you can review the users and what they have access to, and add and remove users.

User groups User groups act as containers for one or more users. With groups, you can control the permissions (roles) for the set of users. The **User groups** column shows you which groups each listed user belongs to.

Roles Roles are used to define what a user can access. For example, you can create roles like: View only, System owner, Administrator. To view and edit the roles for your Elements Exposure Management account, go to **Management > Organization Settings > Vulnerability users** and select **Manage roles**.

8.5 Settings

You can control how your Elements Exposure Management account behaves across all users on the **Management > Vulnerability Settings** page.

General settings

Contact details	This sections contains the contact details of the selected organization.
Subscription details	This section provides information about the subscription of the selected organization.
Product customization	This section is used to manage the product customization if it is enabled.
Scanning restrictions	This section can be used to control what IP ranges Elements Vulnerability Management is allowed to scan, and also to control when starting certain scans is allowed or denied.
Encryption keys	This section is used to manage the encryption keys that are used as a part of the Linux authenticated scanning feature.
Vulnerability statuses	Use this section to define whether open and closed vulnerability statuses affect PCI compliance. You can also include or exclude these statuses from the vulnerability counts and statistics on the Home > Vulnerabilities page.
Workflow	Use this section to define what to do with automatically closed or reopened tickets. You can also choose whether and when to notify participants about ticket deadlines, whether to flag new assets for internet exposure, and whether to mark duplicate findings automatically.
Miscellaneous	This section can be used to define the default time zone for the organization, to specify for how long reports are stored, to define when to mark assets as archived, to specify for how long archived assets are stored, and to define how often vulnerability scans are triggered on endpoints.

Security settings

Isolate my organization	When enabled, users that belong to the upper entities in the organization hierarchy will not be able to access this organization. Only users present in the Account Management list will be able to see data from this organization.
Restrict login based on IP address	This setting can be used to control who has permission to authenticate to your Elements Exposure Management account based on the source IP address. For example, you can enhance the security of your account by only permitting a list of trusted IP addresses.
Force two-factor authentication	If enabled, this enforces two-factor authentication for all users. If disabled, two-factor authentication becomes optional. Users can choose to enable two-factor authentication manually via the My profile page.



NOTE: Two-factor authentication supports Google Authenticator, Microsoft Authenticator, and any other mobile authentication app that supports the TOTP (Time-based One-Time Password) algorithm.

User can reset password without login	If enabled, unauthenticated users are allowed to reset their password with the Forgot password? link. If disabled, only existing (authenticated) users and administrators can reset the password of another user.
Default security stance	This setting affects the default permissions of newly created users: • Permit means that everything that is not explicitly forbidden is permitted. • Deny (default) means that everything that is not explicitly permitted is forbidden.
Email notifications include	This setting defines how many details are allowed to be communicated via email, which is often unencrypted and in general considered unsafe.

Notification settings



NOTE: Notification settings apply to your personal user account only. In other words, they do not apply to the entire organization.

Event log

The event log allows you to review all the events performed by any user. You can use the filter to view only events of a specific type, for a specific date range, or a specific user. The event log is very useful to track who started or deleted specific scans, or made certain changes in the Elements Exposure Management.



Chapter 9

Troubleshooting

Troubleshooting

Help for solving technical issues with Elements Exposure Management is available in the WithSecure Community knowledge base.

Most technical issues with Elements Exposure Management involve scan nodes. Common scan node problems include:

- The scan node does not start.
- The scan node does not download its scan engines.
- The scan node cannot connect to Elements Security Center.

The scan node troubleshooting steps cover these problems. For other issues, see the Elements Exposure Management knowledge base.



Appendix **A**

Using Infrastructure-as-Code tools

Topics:

- Implement infrastructure with Terraform
- Implement infrastructure with CloudFormation

Using Infrastructure-as-Code tools

Infrastructure-as-Code (IaC) tools such as Terraform and CloudFormation for provisioning Elements Exposure Management scanning infrastructure.

You can provision and manage Elements Exposure Management scanning infrastructure with Infrastructure-as-Code (IaC) tools. Use Terraform for multi-cloud environments, or CloudFormation for AWS-only environments.

A.1 Implement infrastructure with Terraform

You can use a Terraform template to manage resources in your cloud environment.

You have installed Terraform and initialized a working directory (`terraform init`).

Elements Security Center generates a Terraform template with the account permissions Exposure Management needs; applying it keeps the setup consistent and tracked in your infrastructure-as-code workflow instead of granting permissions manually.

1. Open Elements Security Center.
2. Under **Environment**, select **Cloud > AWS Accounts and Security Posture**.
3. Select accounts that you want to edit.
The action panel opens.
4. Select **Create Terraform template**.
5. Copy the template to the directory where it has been initialized.
6. Run `terraform apply` in the directory with the template.

A.2 Implement infrastructure with CloudFormation

You can use a CloudFormation template to manage your AWS resources.

Elements Security Center generates a CloudFormation template with the account permissions Exposure Management needs; deploying it through CloudFormation keeps the setup consistent and version-controlled instead of granting permissions manually in the AWS console.

1. Open Elements Security Center.
2. Under **Environment**, select **Cloud > AWS Accounts and Security Posture**.
3. Select AWS accounts that you want to edit.
The action panel opens.
4. Select **Create CloudFormation template**.
5. Log in to your AWS account.
6. Go to the **AWS CloudFormation** console.
7. Choose **Create stack** and select **With new resources**.
The Create stack page opens.
8. Under **Specify template**, choose **Upload a template file** and browse to your CloudFormation template file.
9. Select **Next**.
The Specify stack details page opens.
10. In the **Stack name** field, enter a unique name for the stack.
11. Review the template parameters and enter values for those required in your AWS environment.

12 Select **Next**.

*The **Configure stack options** page opens.*

13 Review the stack options and add tags, permissions, or notifications required for your AWS environment.

14 Select **Next**.

*The **Review** page opens.*

15 Review your stack settings and choose **Create stack**.

Appendix **B**

Authenticated scanning

Topics:

- Windows authenticated scanning (WinRM)
- Windows authenticated scanning (RPC)
- Linux authenticated scanning
- Configuring Windows authenticated scanning (SSH)

Authenticated scanning

In addition to regular network-based scanning, where the host's ports are scanned and the exposed services are reviewed for flaws, you can also run *system scans* in authenticated mode, which enables it to authenticate the target host.



NOTE: You can only run authenticated scans for Linux and Windows system scan targets that are configured to use private scan nodes that are installed in the customer network. Authenticated system scans do not work if they are configured to use cloud scan nodes.

Network-based system scans can reveal hidden services and vulnerable products and configurations. However, a vast majority of known vulnerabilities (with or without a CVE number) affects some particular versions of a software package. The network scanning cannot always determine exact product versions, which is why WithSecure Elements Exposure Management combines the external vulnerability scanning results with the internal - "authenticated" - results.

Authentication method on Windows

Use an endpoint agent for the best authenticated scanning method with Windows targets. When WithSecure Elements Agent is installed on the target server, it sends the scanning results to WithSecure Elements Security Center. In this mode, remote management interfaces can be disabled and no additional credentials are necessary.

If you cannot use the endpoint agent, configure the scan authentication via Windows Remote Management (WinRM). When you configure it to use the Scan Node service account, which scans hosts in the same AD domain, no credentials are stored in the WithSecure Elements Security Center database.

The authenticated scan requires administrator privileges on Windows targets.

Authentication method on Linux

WithSecure Elements Exposure Management uses the industry-standard SSH protocol to perform the authenticated scanning on Linux-based hosts. We recommend that you set up a key-based SSH authentication, but the password-based authentication method is also supported.



NOTE: Credentials are stored in WithSecure Elements Security Center in an encrypted form. To perform the authenticated scans, generate a "transfer" key pair, upload the public key to the Elements Security Center and the private key to the Scan Node Agent. This key pair keeps the credentials encrypted while they are stored or transferred. The decryption is only possible on the Scan Node Agent with appropriate public key when a scan starts.

The authenticated scan does not require superuser access, but without it some system details are hidden, which may make the scanning results incomplete.

Managing credentials

Follow security policies and procedures of your organization when setting up the authenticated scanning.

It is up to the organization to perform a risk assessment and evaluate the need to split the systems into smaller groups with different credentials for scanning. From the technical point of view, it is possible to configure single credentials for the whole group of scans or for each scan separately.

Using a single user that is dedicated to authenticated scanning has its pros and cons. It can be set up, identified in logs, and deactivated if it is misbehaving. On the other hand, if a threat actor gains access to the account, they would gain access to a significant number of assets.

We do not recommend that you disable the user that is used for authenticated scans outside the scan schedule. Based on our experience, it does not improve the security posture significantly but can cause issues when the scanning takes longer than expected or scan has to be redone, for example.

B.1 Windows authenticated scanning (WinRM)

Prepares your internal network for authenticated scanning using Windows Remote Management (WinRM).

WithSecure Elements Exposure Management supports two ways of authenticating to Windows systems:

- If the scan node is deployed on a Windows computer, use the scan node service account credentials (recommended)
- Specify credentials explicitly in WithSecure Elements Security Center

WithSecure Elements Exposure Management uses WinRM to check for missing Windows patches and detect vulnerabilities related to common third-party software. WinRM obtains the list of Windows patches from Windows Update Agent using one of the following sources:

- Microsoft's own Windows Update Service (internet access required)
- An internal network WSUS service
- A Windows Updates database file

These options can be turned on or off in the WithSecure Elements Exposure Management scan templates.

If you choose the first option (Windows Update Service), you can also select the **Check for other Microsoft products** option. This allows you to retrieve updates not only for Windows systems, but also for other Microsoft products (such as Microsoft Office).



NOTE: Windows 10, Windows Server 2016, or newer target systems that do not have the **Receive updates for other Microsoft products when you update Windows** option turned on in Windows Update settings may not include the service required for finding updates for other Microsoft products. To mitigate this, Elements Exposure Management adds the service source ID to the target if necessary. Although Elements Exposure Management cannot undo this change, it does not affect any functionality of Windows Update Service or the settings for automatic updates on a scanned machine.

The third option (Windows Updates database file) can be used as a failover option if the target Windows systems do not have network access to Windows Update Service or WSUS. If it is taken into use, WithSecure Elements Exposure Management can check for missing Windows patches by uploading the Windows Updates database file (wsusscn2.cab) onto the target system's temp folder (%SystemRoot%\Temp\MBSA\Cache\). Once uploaded, WUA uses this file to check for missing Windows patches without accessing the internet.

Besides checking for missing Windows patches, WithSecure Elements Exposure Management also detects vulnerabilities related to common third-party software. WinRM fetches the list of third-party software from Windows Registry.

B.1.1 Preparing for Windows authenticated scanning (WinRM)

Before applying changes, WithSecure recommends that you discuss all potential changes with your network administrator.

The following summarizes the requirements for enabling WinRM authenticated scanning for Windows:

- If a Linux scan node is in use, a user account must meet the following requirement:
 - Local user account added to the **Administrators** group

- If a Windows scan node is in use, there are two options for user accounts:
 - An Active Directory user account added to the **Administrators** group
 - Local user account added to the **Administrators** group
- Target host configuration requirements:
 - WinRM service is running and WinRM HTTP or HTTPS listener is created



NOTE: For a scan node on Linux, we recommend that you use only HTTPS because of known authentication issues with unencrypted connections between Linux and Windows.

- Operating systems with Windows Firewall with Advanced Security component installed (introduced in Windows Vista), where a firewall exception for WinRM traffic is enabled
- Basic authentication allowed on the WinRM service (for scan nodes deployed on Linux only)
- Scan node configuration requirements:
 - For HTTP protocol only: target host is added to the **TrustedHosts** list



NOTE: When a Windows Updates database file is used for scanning, the scan node will copy the database file to the %SystemRoot%\Temp\MBSA\Cache\ folder during the scan and delete it once the scan has completed (for scan nodes deployed on Windows only).

Most of the configuration commands require a PowerShell console run with administrative privileges.

Update PowerShell

The configuration requires PowerShell version 5.0 or newer, although we recommend updating PowerShell to the latest version.

To check the PowerShell version and update it:

1. Open a PowerShell console with administrative privileges.
2. Run the following command to check the installed version of PowerShell:

```
Get-Host | Select-Object Version
```

3. If the reported version is earlier than 5.0, download and install PowerShell 5.0 or later from Microsoft Download Center.

PowerShell 5.0 or later is installed.

4. Restart the computer.

Create a dedicated user account

We recommend that you create a dedicated user account for Elements Exposure Management with access to WinRM.

To create a new user account:

1. Go to **Control Panel > Administrative Tools > Computer Management > Local Users and Groups > Users**.
2. Add a new user account.
3. Add the new user account to the **Administrators** group.

Configure the WinRM service to use HTTP on individual hosts

You can configure the WinRM service used for authenticated scanning to handle network traffic over HTTP.



NOTE: Using HTTP for WinRM is not recommended outside a domain environment where the NTLM protocol does not provide a sufficient level of protection for credentials. This also means that using HTTP is particularly inadequate when using scan nodes that are deployed on Linux computers.



NOTE: In larger domain environments, it is highly recommended to configure the WinRM service via Group Policy.

1. On the target computer where you want to run the WinRM service, run the following command to set up the remote management configuration:

```
Set-WSManQuickConfig -Force
```



NOTE: If the computer is on a public network, use the additional `-SkipNetworkProfileCheck` parameter, which enables a firewall rule for public networks.

This command ensures that the WinRM service is running and is set up to start automatically, creates an HTTP listener to accept WinRM requests, and creates a firewall exception for WinRM traffic.

2. On the scan node, run the following command to add the target host to the **TrustedHosts** list:

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value '{IpAddress}'
```



NOTE: Use the IP address of the target computer. Use the wildcard character (*) instead of an IP address to add all computers.

Configure the WinRM service to use HTTP through GPO

For larger domain environments, we recommend that you configure the WinRM service via Group Policy.



NOTE: Using HTTP for WinRM is not recommended outside a domain environment where the NTLM protocol does not provide a sufficient level of protection for credentials. This also means that using HTTP is particularly inadequate when using scan nodes that are deployed on Linux computers.

1. Create a new Group Policy object:
 - a) Select **Start > Administrative Tools > Group Policy Management**.
 - b) Right-click **Domains** and select **Create a GPO in this domain, and link it here**.
 - c) Enter **Elements Exposure Management** as the required name and click **OK**.
 - d) Right-click the GPO that you created (**Elements Exposure Management**) and select **Edit**.
2. Allow remote server management through WinRM:
 - a) Select **Computer Configuration > Policies > Administrative Templates > Windows Components > Windows Remote Management (WinRM) > WinRM Service**.
 - b) Right-click **Allow remote server management through WinRM**, select **Enabled**, and enter suitable IPv4 and IPv6 filters.

3. Switch on the WinRM service:

- Select **Computer Configuration > Preferences > Control Panel Settings**.
- Right-click **Services** and select **New > Service**.
- Select **Automatic** as the **Startup** type and **WinRM** as the **ServiceName**.

4. Add a firewall rule to allow traffic:

- Select **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security**.
- Right-click **Inbound Rules** and select **New Rule**.
- Select **Windows Remote Management** as the **Predefined** rule type and click **Next**.
- Select the appropriate rule for your network profile and click **Next**.
- Select **Allow the connection** and click **Finish**.

5. On the scan node, run the following command to add the target host to the **TrustedHosts** list:

```
Set-Item WSMan:\localhost\Client\TrustedHosts -Value '{IpAddress}'
```



NOTE: Use the IP address of the target computer. Use the wildcard character (*) instead of an IP address to add all computers.

Configure the WinRM service to use HTTPS with a publicly signed certificate

After creating the dedicated WinRM user account for Elements Exposure Management, you need to configure the WinRM service on the machine where you want to run it.

You have already created the dedicated WinRM user account for Elements Exposure Management.

To set up the remote management configuration on a computer that uses a publicly signed certificate:

1. Run the following command:

```
Set-WSManQuickConfig -UseSSL -Force
```



NOTE: When the computer is on a public network, use the additional -SkipNetworkProfileCheck parameter, which enables a firewall rule for public networks as well.

This command ensures that the WinRM service is running and is set up to start automatically, creates an HTTPS listener to accept WinRM requests, and creates a firewall exception for WinRM traffic.

2. If you are using Linux scan nodes, enable WinRM basic authentication:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Configure the WinRM service to use HTTPS without a publicly signed certificate

If the computer does not use a publicly signed certificate, you need to perform some additional steps.

On a computer running Windows 8, Windows Server 2012, or newer that does not use a publicly signed certificate, do all the following steps on the target Windows computer using PowerShell:

1. Start the WinRM service and set it to start automatically:

```
Set-Service -Name "WinRM" -StartupType Automatic -Status Running
```

2. Generate a new self-signed certificate:

- a) Use the following PowerShell command to create the certificate:

```
$Cert = New-SelfSignedCertificate -CertstoreLocation ^  
Cert:\LocalMachine\My -DnsName "{ipAddress}"
```

- b) Use the following command to check the certificate's thumbprint, which you need when creating the WSMAN HTTPS listener:

```
$cert.Thumbprint
```

3. Add a new WSMAN HTTPS listener:

```
New-Item -Path WSMAN:\LocalHost\Listener -Transport HTTPS -Address * ^  
-CertificateThumbPrint $Cert.Thumbprint -Force
```

4. Add a new firewall rule to allow WinRM HTTPS traffic:

```
New-NetFirewallRule -DisplayName "Windows Remote Management ^  
(HTTPS-In)" -Name "Windows Remote Management (HTTPS-In)" -Profile ^  
Any -LocalPort 5986 -Protocol TCP
```

5. If you are using Linux scan nodes, run the following PowerShell command on the target Windows computer to allow basic WinRM authentication:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Configure the WinRM service to use HTTPS without a publicly signed certificate on older Windows versions

On Windows versions older than Windows 8 or Windows Server 2012, configure the WinRM service to use HTTPS by importing a certificate created on a newer computer.

You have created a certificate on a separate computer running Windows 8, Windows Server 2012, or newer, using the IP address of this target computer, and exported it to a file.

On a target computer running a Windows version older than Windows 8 or Windows Server 2012 that does not use a publicly signed certificate, do all the following steps:

1. Start the WinRM service and set it to start automatically:

```
Set-Service -Name "WinRM" -StartupType Automatic -Status Running
```

2. Copy the exported certificate to the target computer and import it into the Personal certificate store:



NOTE: To view certificates in the local machine store, you must use administrator privileges.

- a) Type `mmc` and press Enter.
- b) Select **File > Add/Remove Snap In**.
- c) In the **Available snap-ins** dialog box, select **Certificates**.
- d) Click **Add**.

- e) In the **Certificates snap-in** dialog box, select **Computer account** and then click **Next**.
- f) In the **Select Computer** dialog box, click **Finish**.
- g) In the **Add/Remove Snap-in** dialog box, click **OK**.
- h) Select **Certificates (Local Computer) > Personal**, right-click and select **All Tasks > Import**.
- i) Browse for the copied certificate, then click **Next**.
- j) Enter the password for the certificate, then click **Next**.
- k) Click **Finish**.

3. Add a new WSMAN HTTPS listener:

```
New-Item -Path WSMAN:\LocalHost\Listener -Transport HTTPS -Address * ^
-CertificateThumbPrint $Cert.Thumbprint -Force
```

4. Add a new firewall rule to allow WinRM HTTPS traffic:

- a) Go to **Control Panel > Windows Firewall > Advanced settings**.
- b) Add a new rule for inbound traffic that allows TCP port 5986 for the selected network profiles.

5. If you are using Linux scan nodes, run the following PowerShell command on the target Windows computer to allow basic WinRM authentication:

```
winrm set winrm/config/service/auth '@{Basic="true"}'
```

Create and export a certificate for a legacy Windows target

Windows versions older than Windows 8 or Windows Server 2012 cannot create a self-signed certificate locally, so create one on a separate, newer computer and export it to a file.

You need a computer running Windows 8, Windows Server 2012, or newer.

Use the IP address of the target computer.

On the separate computer, run the following commands:

```
$cert = New-SelfSignedCertificate -CertstoreLocation ^
Cert:\LocalMachine\My -DnsName "{ipAddress}"
$password = ConvertTo-SecureString -String "{password}" -Force ^
-AsPlainText
Export-PfxCertificate -Cert $cert -FilePath "{filePath}" -Password ^
$password
```

The certificate is exported to the specified file, ready to copy to the target computer.

B.1.2 Troubleshoot Windows authenticated scanning (WinRM)

It is recommended that you verify the functionality of the new account from a remote host before using the account for Windows authenticated scanning.



NOTE: Run the following commands directly on the target machine. This verifies that Windows Remote Management (WinRM) is configured properly on that machine and has sufficient permissions so that Windows is ready for the authenticated scan.

1. Make sure that PowerShell 5 or newer is installed:

```
Get-Host | Select-Object Version
```

2. Check the WinRM permissions for user groups or the individual user account:

```
(Get-PSSessionConfiguration -Name Microsoft.PowerShell).Permission
```

3. Make sure that the WinRM service is running:

```
Get-Service -Name "WinRM"
```

4. Make sure that the WinRM HTTPS listener is configured:

```
winrm enumerate winrm/config/listener
```

5. Check the detailed WinRM configuration:

```
winrm get winrm/config/service
```

6. Run the corresponding PowerShell script for your configuration from a remote host (for example, from the WithSecure Elements Scan Node if possible):



NOTE: If possible, run this command on a machine with Scan Node Agent installed. This shows you if it is possible to set the remote session and run the command from a Scan Node to a target Windows IP (\$ip) using the credentials for the authenticated scan account.

- Windows scan node with explicit credentials and WinRM HTTPS listener in use:

```
$ip = "{ip}"
$user = "{username}"
$pass = "{password}" | ConvertTo-SecureString -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential ($user, $pass)

$pso = New-PSSessionOption -SkipCACheck -SkipCNCheck
Invoke-Command -ComputerName $ip -Credential $cred -Authentication Negotiate -Port 5986 -UseSSL -
SessionOption $pso {
    if ((Get-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').Property.
Contains('ProductName'))
    {
        (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' -Name 'ProductName').
ProductName
    }
}
```

- Linux scan node with explicit credentials and WinRM HTTPS listener in use:

```
$ip = "{ip}"
$user = "{username}"
$pass = "{password}" | ConvertTo-SecureString -AsPlainText -Force
$cred = New-Object System.Management.Automation.PSCredential ($user, $pass)

$pso = New-PSSessionOption -SkipCACheck -SkipCNCheck
Invoke-Command -ComputerName $ip -Credential $cred -Authentication Basic -Port 5986 -UseSSL -
SessionOption $pso {
    if ((Get-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').Property.
Contains('ProductName'))
    {
        (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' -Name 'ProductName').
ProductName
    }
}
```

- Windows scan node with explicit credentials and WinRM HTTP listener in use:

```
$ip = "{ip}"
$user = "{username}"
$pass = "{password}" | ConvertTo-SecureString -AsPlainText -Force
```

```
$cred = New-Object System.Management.Automation.PSCredential ($user, $pass)

$pso = New-PSSessionOption -SkipCACHek -SkipCNCheck
Invoke-Command -ComputerName $ip -Credential $cred -Authentication Negotiate -Port 5985 -SessionOption
    $pso {
        if ((Get-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').Property.
Contains('ProductName'))
        {
            (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' -Name 'ProductName').
ProductName
        }
    }
}
```

- Windows scan node with scan node service account credentials and WinRM HTTPS listener in use:

```
$ip = "{ip}"

$pso = New-PSSessionOption -SkipCACHek -SkipCNCheck
Invoke-Command -ComputerName $ip -Authentication NegotiateWithImplicitCredential -Port 5986 -UseSSL
    -SessionOption $pso {
        if ((Get-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').Property.
Contains('ProductName'))
        {
            (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' -Name 'ProductName').
ProductName
        }
    }
}
```

- Windows scan node with scan node service account credentials and WinRM HTTP listener in use:

```
$ip = "{ip}"

$pso = New-PSSessionOption -SkipCACHek -SkipCNCheck
Invoke-Command -ComputerName $ip -Authentication NegotiateWithImplicitCredential -Port 5985 -
SessionOption $pso {
    if ((Get-Item -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion').Property.
Contains('ProductName'))
    {
        (Get-ItemProperty -Path 'HKLM:\SOFTWARE\Microsoft\Windows NT\CurrentVersion' -Name 'ProductName').
ProductName
    }
}
}
```

Each of these scripts outputs the OS version of the target host.



NOTE:

Known issues:

- Scanning for Windows updates fails on Windows 10 (versions 1703, 1709 and 1803) - Due to a bug related to Windows updates, scanning for Windows updates may fail. It results in the `Microsoft Windows updates scanning failed (1023713)` finding in the System Scan report and `Access is denied (0x80000000)` in the System Scan log file. To solve the issue, install the recent cumulative update on the target machine. The issue is not present in the earlier and later versions of Windows 10.
- While connecting to a target machine if the `Access is denied` error is logged when scanning Windows updates on a target machine (older versions should not be affected by this issue) by using a local administrator account and the WinRM Agent is in use, make sure that the `HKEY_LOCAL_MACHINE\SOFTWARE\Microsoft\Windows\CurrentVersion\Policies\SystemLocalAccountNames` registry value is set to 1 in the target system registry.

B.2 Windows authenticated scanning (RPC)

Prepares your internal network for authenticated scanning using Remote Procedure Call (RPC), a deprecated method being replaced by WinRM.



WARNING: The authenticated scanning using RPC is a deprecated method for Windows authenticated scanning. This authentication method will be decommissioned soon, and we do not recommend its use any more. We suggest that you start using Windows authenticated scanning (WinRM) instead.

WithSecure Elements Exposure Management support two ways of authenticating to Windows systems:

- Use the scan node service account credentials (recommended)
- Specify credentials explicitly in WithSecure Elements Security Center

WithSecure Elements Exposure Management uses Windows Update Agent API (WUA) to check for missing Windows patches. To check which patches are missing, WUA must get the list of available patches from one of the following sources:

- Microsoft's own Windows Update Service (internet access required)
- An internal network WSUS service
- A Windows Updates database file

The first two options (Windows Update Service and WSUS) can be turned on or off in the WithSecure Elements Exposure Management scan templates. If allowed, the scanned Windows system will decide (based on its configuration) which of the two methods to use.

The third option (Windows Updates database file) can be used as a failover option if the target Windows systems do not have network access to Windows Update Service or WSUS. When it is on, WithSecure Elements Exposure Management can check for missing Windows patches by uploading the Windows Updates database file (wsusscn2.cab) onto the target system's temp folder (%SystemRoot%\Temp\MBSA\Cache\). Once uploaded, WUA uses this file to check for missing Windows patches without accessing the internet.

Besides checking for missing Windows patches, WithSecure Elements Exposure Management can also detect vulnerabilities related to common third-party software. The list of third-party software is fetched from Windows Registry. You must give the scan node the permission to read registry keys and turn on **Remote Registry Service** on the target Windows systems to use this feature.

B.2.1 Preparing for Windows authenticated scanning (RPC)

Before applying changes, WithSecure recommends that you discuss all potential changes to the *Group Policy* with your network administrator. For more information about *Group Policy*, refer to your Microsoft documentation on *Group Policy* deployment.

The following summarizes the requirements for enabling authenticated scanning for Windows:

- A user account must meet one of the following requirements:
 - An Active Directory user account added to the local administrators group (recommended)
 - Built-in administrator user account
 - Local user account added to local administrators group with **Admin Approval Mode** disabled
- Windows configuration requirements (preferably managed via GPOs)
 - Inbound network traffic to the RPC Endpoint Mapper
 - Inbound network traffic to the RPC Dynamic Ports

- Inbound network traffic to TCP 445 (SMB / CIFS) and TCP 135 (RPC)
- Optional (only required to check for vulnerabilities in third-party software):
 - Enable Remote Registry Service (or allow the scan node to start the service automatically during the scan)
 - Grant read access to registry keys
- Optional (only required when a Windows Updates database file is used for scanning):
 - The network share name ADMIN\$ must point to %SystemRoot% (e.g. C:\Windows). Use the net share command to verify this.



NOTE: During the scan, the scan node will copy the database file to the %SystemRoot%\Temp\MBSA\Cache\ folder and delete it once the scan has completed.

Create a Windows domain account

To create a new domain account, you may use the command given here, which must be executed using administrator credentials.

Windows authenticated scanning uses a dedicated domain account to log in to the scanned systems, separate from your own administrator credentials.

1. Log in as an administrator and open a command prompt with administrative privileges.
2. Adjust the following command to fit your organization by replacing ORGANIZATION, COM, and PASSWORD with your domain components and a password, and then run it:

```
dsadd user "cn=radar_account,cn=users,dc=ORGANIZATION,dc=COM" -samid \
  radar_account -upn radar_account@ORGANIZATION.COM -pwd PASSWORD \
  -pwdneverexpires yes -mustchpwd no -fn radar_account -ln \
  fsecure_radar -display "Radar Account" -disabled no
```

3. If your organization's password policy allows it, keep the -pwdneverexpires yes option in the command so that the account password does not expire.

It is recommended that you use this domain account to run the Windows Service (WithSecure Elements Scan Node Agent) and authenticate to the scanned Windows systems.

Disable Admin Approval Mode

This step can be skipped if you are using a domain account (recommended) or a built-in local administrator account to authenticate to Windows systems.

This step is only required if WithSecure Elements Exposure Management is configured to use a local user account and added to the local administrator's group. To disable the **Admin Approval Mode**, do the following:

1. Start secpol.msc.
2. Go to **Security Settings > Local Policies > Security Options** and disable the **User Account Control: Run all administrators in the Admin Approval Mode** policy.
3. Restart the computer.

Group Policy best practices for authenticated scanning

The best practice Group Policy settings for authenticated scanning of Windows systems are described in this section.

Consult your network administrator before changing Group Policy because the changes may affect network operations. The effect depends on your network configuration and security policy. Detailed documentation for many of the following settings is available online in the Group Policy Editor.



IMPORTANT: We highly recommended that you discuss any potential changes to the Group Policy with your network administrator before implementing any alterations, as your local network configurations may depend on certain settings being in place. This service does not verify that these settings are appropriate for your network. If you do make any Group Policy changes, it may take several hours before the changes take effect on the client.

For more information, see the Microsoft documentation on Group Policy deployment.

It is recommended that you create a dedicated Windows user account (such as "WithSecure_Elements_Vulnerability_Management_account") to be used only by WithSecure VM scan nodes.

Create a new Group Policy object

Create a Group Policy object (GPO) to apply the Windows authenticated scanning settings to the computers that Elements Exposure Management scans.

The GPO you create here holds the firewall, registry, and account settings needed for Windows authenticated scanning.

1. Go to **Start > Administrative Tools > Group Policy Management**.
2. Right-click **Domains** and select **Create a GPO in this domain, and link it here**.
3. Enter **Elements Exposure Management** as the required name and click **OK**.
4. Right-click the created GPO (**Elements Exposure Management**) and select **Edit**.

You can now edit this GPO in the Group Policy Management Editor, where you should perform the next steps.

Remember to add all computers to be scanned to your security filtering.

Add rule to allow traffic to the RPC Endpoint Mapper

Add a firewall rule that lets the scan node reach the RPC Endpoint Mapper on Windows targets scanned by Elements Exposure Management.

1. Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules**.
2. Right-click and choose **New Rule**.
3. Choose **Custom** and click **Next**.
4. Choose **This Program Path** and enter `%systemroot%\system32\svchost.exe`.
5. Choose **Customize**.
6. Choose **Apply to this service**, then select **Remote Procedure Call (RPC)** with the short name **RpcSs** and click **OK**.
7. Click **Next** and accept the pop-up warning.
8. Select **TCP** as the **Protocol type**.
9. Select **RPC Endpoint Mapper** as the **Local Port** and click **Next**.

10. Specify the IP address of the scan node on the remote IP addresses list or choose **Any IP address** and then click **Next**.
11. Select **Allow the connection** and click **Next**.
12. Select the checkboxes that fulfill the machine connection conditions and click **Next**.
13. Specify **Radar RPC Endpoint Mapper** as the name and click **Finish**.

Add rule to allow traffic to the RPC Dynamic Ports

Add a firewall rule that lets the scan node reach the RPC dynamic ports on Windows targets scanned by Elements Exposure Management.

1. Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules**.
2. Right-click and choose **New Rule**.
3. Choose **Custom** and click **Next**.
4. Choose **All programs** and click **Next**.
5. Select **TCP** as the **Protocol type**.
6. Select **RPC Dynamic Ports** as the **Local Port** and click **Next**.
7. Specify the IP address of the scan node on the remote IP addresses list or choose **Any IP address** and then click **Next**.
8. Select **Allow the connection** and click **Next**.
9. Select the checkboxes that fulfill the machine connection conditions and click **Next**.
10. Specify **Radar RPC Dynamic Ports** as the name and click **Finish**.

Add rule to allow traffic to SMB/CIFS and RPC

Add a firewall rule that opens the SMB/CIFS and RPC ports on Windows targets scanned by Elements Exposure Management.

To add a firewall rule to allow TCP/445 (SMB/CIFS) and TCP/135 (RPC):

1. Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Windows Firewall with Advanced Security > Windows Firewall with Advanced Security - LDAP > Inbound Rules**.
2. Right-click and choose **New Rule**.
3. Choose **Port** and click **Next**.
4. Choose **TCP** and at specific local ports enter 135, 445, then click **Next**.
5. Select **Allow the connection** and click **Next**.
6. Choose **Domain** (or other, depending on your knowledge), then click **Next**.
7. Specify **Radar Scanning** as the name and click **Finish**.

Enable Remote Registry service

Enable the Remote Registry service on Windows targets so that Elements Exposure Management can read their registry during authenticated scans.

To configure the Remote Registry service:

1. Log on using an account with local administrator rights.
2. Press the Windows key + R to open the Run command window.
3. Type `services.msc` and press Enter.
4. Right-click **Remote Registry** service and then select **Properties** from the menu

5. In the **General** tab, open the **Startup Type** drop-down menu and select **Automatic**.
6. Select **Apply** and then select **Start**.
7. Click OK after the **Remote Registry** service has started.

The Remote Registry service is enabled and running.

Grant read access to registry keys

Grant the scan account read access to the Windows registry keys that Elements Exposure Management needs for authenticated scanning.

You have already created and selected the domain or local user account that is used to authenticate to the target Windows systems.

1. Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Registry**.
2. Right-click and select **Add**.
3. Select `MACHINE\System\CurrentControlSet\Control\SecurePipeServers\winreg`.
4. Add read permission for the already selected (domain or local) user account used to authenticate to Windows systems.
5. Click **OK** and select **Propagate inheritable permissions to all sub keys**.
6. Click **OK**.

Add a scan node to the domain

To run Windows authenticated scans, the scan node must belong to your domain and use the scan account as a local administrator.

The scan node must be a part of your domain and the Radar_account must be set as a local administrator on the scan node.

To do this, enable the following settings:

1. Open **Administrative Tools > Group Policy Management** and select your domain.
2. Right-click and select **Create a GPO in this domain, and link it here**.
3. Enter a name, for example Scannode-Admin, and click **OK**.
4. Select the created GPO and add the computer on which the scan node will be running to the proper **Security Filtering**.
5. Right-click and select **Edit**.
6. Edit the GPO in the **Group Policy Management Editor**:
 - a) Go to **Computer Configuration > Policies > Windows Settings > Security Settings > Restricted Groups**.
 - b) Right-click and select **Add Group**.
 - c) Select **Administrators** and click **OK**.
 - d) Next to **Members of this group**, click **Add**.
 - e) Browse for the user to be used for running the scan node and accept it.
 - f) Refresh the GPO by running `gpupdate.exe`.

Configure a network scan template for Windows authenticated scanning

Configure a network scan template in Elements Security Center to run Windows authenticated scans with Windows credentials.

You have already created the domain account, the Group Policy object (GPO), and the required firewall rules for Windows authenticated scanning.

1. Log in to Elements Security Center.

2. Go to **Templates** and open the **Network scan templates** tab.
3. Select **Add network scan template** or select the menu icon in the **Actions** column and select **Edit** to edit an existing template.
4. Select **Windows credentials** from the **Authentication method** drop-down menu.
5. Specify which credentials should be used:
 - Use the scan node's service account
 - Specify credentials explicitly
6. Choose which sources the WUA can use when checking the Windows system for missing patches:
 - Microsoft Update Server or Windows Server Update Services (WSUS)
 - Windows Updates database file

If **Windows Updates database file** is enabled, you must also specify a network share where the Windows patch database can be uploaded.
7. Apply the scan configuration to a scan group or an individual scan target and run the scan.

B.2.2 Troubleshoot Windows authenticated scanning (RPC)

It is recommended that you verify the functionality of the new account from a remote host before using the account for Windows authenticated scanning (RPC).

The scanning engine requires access to the network share and the registry to perform authenticated scanning of Windows hosts.



NOTE: It may take several hours before Group Policy changes take effect.

1. Run the following command from the scan node to verify connectivity to the target system that you are trying to scan:

```
telnet TARGET_IP 135
telnet TARGET_IP 445
```

When a connection is made, you can send any information and the connection will be closed.

2. Test access to the **Remote Registry** service.

Before testing access to the **Remote Registry** service, ensure that you have already tested the access to the network shares. Run the following PowerShell script to test the **Remote Registry** access:

```
$Target = "IP_ADDRESS"
$Reg = [Microsoft.Win32.RegistryKey]::OpenRemoteBaseKey('LocalMachine', $Target)
$RegKey= $Reg.OpenSubKey("SOFTWARE\Microsoft\Windows NT\CurrentVersion")
$Result = $RegKey.GetValue("ProductName")
echo $Result
```

If the test was successful, the command should return the operating system name.

3. Test the authenticated scan.

*When the authenticated scan has finished, it is possible to check if authentication was successful or not by reviewing the informational finding named Microsoft Windows authentication succeeded/failed. The **Findings** field displays useful information if the authentication failed.*



NOTE:

Known issues:

Scanning for Windows updates fails on Windows 10 (versions 1703, 1709 and 1803)

Due to a bug related to accessing WMI remotely in these versions of Windows 10, scanning for Windows updates may fail. It results in the Microsoft Windows authentication failed (1013914) finding in the System Scan report and Access is denied (0x80070005) errors in the System Scan log file. To solve the issue, install the recent cumulative update on the target machine. The issue is not present in the earlier and later versions of Windows 10.

B.3 Linux authenticated scanning

Configuring Elements Exposure Management to run Linux authenticated scans using SSH for more detailed system information.

By default, WithSecure Elements Exposure Management runs scans over the network in an unauthenticated context and detects issues based on the exposed services on a given host. Although a lot of information can be collected over the network, it is not as detailed as gathering information from a so-called authenticated context. With Linux authenticated scanning, WithSecure Elements Exposure Management is able to authenticate using SSH and gather more detailed information about the system.

Prerequisites

The following WithSecure Elements Exposure Management components are required to perform Linux authenticated scanning:

- WithSecure Elements Scan Node version 2.3.2.646 or higher. To check the version number, go to the tray application of the scan node, under **Security Configurations**, select **Scans** and then the **Settings** tab and find the `SCANNODE.ScanNodeVersion` key. You can also check the version number in WithSecure Elements Security Center by going to **Scan nodes** and expanding the details for a scan node.

Linux authenticated scanning in WithSecure Elements Exposure Management supports the following distributions:

- CentOS
- Debian
 - Testing release (bookworm)
 - Unstable release (sid)
 - Debian 11 (bullseye)
 - Debian 10 (buster)
 - Debian 9 (stretch)
 - Debian 8 (jessie)
 - Debian 7 (wheezy)
- Oracle Linux (version 5 and higher)
- Red Hat
- Ubuntu 6.06 LTS and above
- Amazon Linux
- SUSE Linux 10 and above
- AlmaLinux

B.3.1 Preparation steps

WithSecure Elements Exposure Management ensures that the credentials needed to perform authenticated scans are stored in a safe manner.

Note that the steps in this section are only for setting up the secure credentials flow within WithSecure Elements Exposure Management; that is between the portal and a scan node. Credentials used for authentication to a target Linux system are described elsewhere in this documentation. Therefore, apart from this, you need to configure the authentication method as well.



NOTE: While using the recommended key-based authentication, you need to secure a private key along with an optional passphrase. In an authenticated Linux scan, two key pairs are used: the first one is used to authenticate to the target system and the second one to secure the flow of the first key pair with the WithSecure Elements Exposure Management parts.

Once credentials are sent to WithSecure Elements Exposure Management, they are encrypted with a public key and can only be decrypted directly on the scan node with a counterpart private key. This section describes how to configure the custom public/private keys.

Create new encryption keys

First, a public/private key pair has to be created and later installed in Elements Security Center and the scan node.

The keys are used to establish an encrypted communication channel between Elements Security Center and the scan node in question.



NOTE: The steps given here are for creating the encryption keys on Windows computers. However, the same `openssl` commands for generating the keys should also work on Linux systems.

1. Download the OpenSSL toolkit for Windows from the GnuWin32 OpenSSL package page.
2. Extract the zip file.
3. From the Windows command prompt, navigate to the `bin` directory inside the OpenSSL folder.
For example: `cd x:\openssl-{version}\bin`
4. Generate a public/private key pair by running the following commands:
Generate the private key:
`openssl genpkey -algorithm RSA -out private_key.pem -pkeyopt rsa_keygen_bits:4096`
For older versions of OpenSSL, use the following command:
`openssl genrsa -out private_key.pem 4096`
Extract the public key:
`openssl rsa -pubout -in private_key.pem -out public_key.pem`

Next, upload the public key to Elements Security Center.

Upload encryption keys to WithSecure Elements Security Center

Once the public/private key pair has been created, the public key can be uploaded to WithSecure Elements Security Center.

You have already created the public/private key pair.

Elements Security Center stores the public key and matches it by name to the corresponding private key uploaded to the scan node.

1. Log in to Elements Security Center.
2. Under Management, select **Vulnerability Settings > General settings**.
3. Open **Encryption keys** and click **Add encryption key**.
4. Specify a name and a description (optional) for the public key.



NOTE: The public key name that you enter in WithSecure Elements Security Center must match the name entered for the private key name on the scan node. Also, the entered name can only be a combination of numbers, letters and underscore characters ("_"). Other types of characters are not allowed. The key file names do not need to match the entered name value. However, the extension `.pem` is obligatory for both.

This information is needed whenever you upload a new public key. The name value is used to identify which public and private keys belong together. We recommend using a descriptive name, as it helps you to distinguish the keys from other key pairs that you may want to use for other purposes.

5. Click **Browse** and select the file to upload.

Upload encryption keys to WithSecure Elements VM scan node

After uploading the public key, you also need to upload the private key to the scan node that you want to use.

You have already uploaded the public key to Elements Security Center.

Elements Security Center only needs the public key; the scan node that runs the scan needs the matching private key to authenticate to Linux targets.

1. Log in to the WithSecure Elements Vulnerability Management scan node.
2. For Windows scan nodes:

- a) Start the **WithSecure Elements VM Scan Node - Control Center**.

You can find this via the **Start Menu** after unfolding the **WithSecure** group, or by launching `F-Secure Radar.Scan.Daemon.Tray.exe`, located in the scan node installation directory.



WARNING: Control Center has to be opened by a local administrator or have at least a `SeImpersonatePrivilege` to encrypt the private key.

- b) Go to the **Encryption Keys** tab and click **Add**.
- c) Enter the same key name as used in Elements Security Center, upload the private key and click **Save**.



NOTE: The names of the public key and private key must match for the authentication to work.



NOTE: Encryption keys are stored safely in a user account context. You will be asked for credentials to the account on which the scan node service is running, as this account might be different from the account that the *Scan Node Control Center* is running.

3. For Linux scan nodes:

- a) Run the following commands to apply an already generated private key, saved as `./private_key.pem`:



NOTE: Replace `NameOfTheKeyPair` with the name of your encryption keys from Elements Security Center.

```
cd /opt/f-secure/radar-scannodeagent
sudo ./ScanNodeAgent add-private-key NameOfTheKeyPair ./private_key.pem
```

Prepare the user account for Linux authenticated scanning

To allow WithSecure Vulnerability Management to log on to a target Linux system, it is recommended to create a specific user account on each target to be scanned.

This means that such a user account would be used only for scanning purposes.

To create the user account:

1. Run the following command to create a new account:
`sudo useradd radar-user -m`
2. Add the following line to the `/etc/sudoers` file to avoid the user form asking for a password:
`radar-user ALL=(ALL) NOPASSWD: ALL`
3. Disable the `requiretty` option by adding the following line to the `/etc/sudoers` file:
`Defaults:radar-user !requiretty`
4. Start the SSH service.

The user account is ready to be used for authenticated scanning.

B.3.2 Authentication methods

The scan nodes can log on to Linux systems using passwords or keys (recommended).

Linux authenticated scanning supports two authentication methods: password authentication and key-based authentication. Key-based authentication is recommended. Configure the method that matches your environment.

Set up password-based authentication

You need to configure all the Linux systems that should be scanned to allow password authentication over SSH.

You have already created the dedicated Linux user account for scanning and, if required, set up the credential encryption key in Elements Security Center.

Password-based authentication is a less secure alternative to key-based authentication for Linux authenticated scanning; use it only when key-based authentication isn't an option.

1. Make sure that the following line is present in the `/etc/ssh/sshd_config` file:
`PasswordAuthentication yes`
2. Run the following command:
`sudo passwd radar-user`
3. Under **Security Configurations**, select **Scan Templates > Network scan templates**.
4. Create a new scan template or edit an existing one.

5. Enable **Linux authenticated scanning using a password as authentication method** by selecting **SSH with password** and entering the target SSH port. Then, specify the credential encryption key, user name and password that were set up in the preparation steps.
6. Save the template.
7. Under **Security Configurations**, select **Scans > Network scans** and in the **Group view**, find the scan group that you want to set up for authenticated scanning.
8. Click the menu icon and select **Edit scan group**.
9. Configure the scan group to use the scan node and template that has been prepared for Linux authenticated scanning.
10. Save the changes.

The scan group is configured for Linux authenticated scanning.

Set up SSH keys on the Linux system

Create an SSH key pair and configure the target Linux system to allow key-based login before setting up Linux authenticated scanning in Elements Security Center.

You have already created the dedicated Linux user account for authenticated scanning and can log on to the target system with it.

1. Log on to the Linux system with the WithSecure Elements Exposure Management user account and create a new key pair using the following command: `ssh-keygen -t rsa -b 4096 -f targetKey`



NOTE: With OpenSSH version 7.8 or newer, use following command:

```
ssh-keygen -t rsa -b 4096 -m PEM -f targetKey
```

The file name of the private key must include the `.pem` extension. The key is generated in the correct format, so you only have to rename the file to add the extension: `mv targetKey targetKey.pem`.

We recommend protecting the key with a passphrase.



TIP: Alternatively, you can use the `openssh` command to create the encryption keys.

2. Use the following command to add the new public key to the `authorized_keys` file:

```
cd /home/radar-user/.ssh
touch authorized_keys
chmod 600 authorized_keys
cat targetKey.pub >> authorized_keys
```



NOTE: To use the same key on several systems, you need to copy `targetKey.pub` there and repeat this step on each target.

3. Verify that the key-based authentication works by logging in from a different system using the private key `targetKey.pem`.

You can do this on Windows machines with the PuTTY app or on Linux by running the following command:

```
ssh -i targetKey.pem radar-user@<target-ip>.
```

Key-based SSH login to the Linux system works.

Configure key-based authentication in Elements Security Center

Enable key-based authentication for Linux authenticated scanning in Elements Security Center using the SSH key you created.

You have set up SSH keys on the Linux system and verified that key-based login works.

1. Under **Security Configurations**, select **Scan Templates > Network scan templates**.
2. Create a new scan template or edit an existing one.
3. Enable **Linux authenticated scanning using keys as authentication method** by selecting **SSH with keys** and entering the target SSH port. Then, specify the credential encryption key and the user name that were set up in the preparation steps. Finally, upload the private key that you created when you set up SSH keys on the Linux system, and enter its passphrase if available (in the **SSH key password** field).
4. Save the template.
5. Under **Security Configurations**, select **Scans > Network scans** and in the **Group view**, find the scan group that you want to set up for authenticated scanning.
6. Click the menu icon and select **Edit scan group**.
7. Configure the scan group to use the scan node and template that has been prepared for Linux authenticated scanning.
8. Save the changes.

The scan group is configured for Linux authenticated scanning.

B.3.3 Troubleshooting

After a scan has completed with Linux authenticated scanning turned on, the scan report will contain an **Informational** finding, stating whether the scanning succeeded or failed. In the event of a failure, the **Findings** shows details about why the authenticated scanning failed.

When a scan with Linux authenticated scanning finishes, open the **Informational** finding in the scan report. Check whether authentication succeeded. If it failed, the **Findings** details explain the reason. Correct the authentication configuration and run the scan again.

B.4 Configuring Windows authenticated scanning (SSH)

Windows authenticated scanning over SSH requires configuration on both the target host and each scan node.



NOTE: Before applying changes, we recommend that you discuss all potential changes with the network administrator.

Enabling SSH authenticated scanning for Windows has these requirements:

- Target host configuration requirements:
 - The OpenSSH Server feature must be enabled on the target host.
- Scan node configuration requirements:
 - Add the private key to each scan node that runs Windows SSH authenticated scans, on both Linux and Windows scan nodes. The scan node uses the key to decrypt the scan credentials that the Elements Security Center portal sends.

B.4.1 Enable the OpenSSH Server on the target host

Enable the OpenSSH Server feature on each Windows target host before you run SSH authenticated scans.

Windows Server 2019 and later include the OpenSSH Server as a built-in feature. Use these steps to install the feature if it is missing, start the service, and allow SSH traffic through the firewall.

1. Open PowerShell as an administrator and check whether the OpenSSH Server feature is available:

```
Get-WindowsCapability -Online | Where-Object Name -like 'OpenSSH.Server*'
```

2. If the state is NotPresent, add the feature:

```
Add-WindowsCapability -Online -Name OpenSSH.Server~~~~0.0.1.0
```

3. Start the SSH service and set it to start automatically at startup:

```
Start-Service sshd
Set-Service -Name sshd -StartupType Automatic
```

4. Allow inbound SSH connections on the default port (TCP 22) by creating a firewall rule:

```
New-NetFirewallRule -Name "OpenSSH-Server" `
-DisplayName "OpenSSH Server (sshd)" `
-Enabled True `
-Direction Inbound `
-Protocol TCP `
-Action Allow `
-LocalPort 22
```

5. Check that the service is running:

```
Get-Service -Name sshd
```

The status must be Running.

6. From a remote machine, connect to confirm SSH access:

```
ssh <username>@<server-ip>
```

For example: `ssh administrator@192.168.1.10`

7. We recommend that you set up key-based authentication. Generate an SSH key pair or use an existing one, then append the public key to the `C:\ProgramData\ssh\administrators_authorized_keys` file:



NOTE: Standard users use the personal `C:\Users\<username>\.ssh\authorized_keys` file. For accounts with administrator permissions, use the global `administrators_authorized_keys` file instead.

Confirm that the correct key is present and that the file is formatted correctly:

```
ssh-keygen -l -f "C:\ProgramData\ssh\administrators_authorized_keys"
```



IMPORTANT: Use only Unix line endings (`\n`) in the key file.

Check that the file permissions are correct:

```
icacls "C:\ProgramData\ssh\administrators_authorized_keys"
```

The output must show only these two entries:

```
NT AUTHORITY\SYSTEM:(F)
BUILTIN\Administrators:(F)
```

Confirm that key authentication works:

```
ssh -i <private_key> <username>@<server-ip>
```

For example: `ssh -i .ssh/id_ecdsa administrator@192.168.1.10`

B.4.2 Scan settings for Windows update sources

When you configure a Windows SSH authenticated scan, choose how WithSecure Elements Exposure Management checks the host for missing updates.

The Windows Update Agent (WUA) gets the list of available patches from one of these sources:

Windows Server Update Services (WSUS)	Checks the host against the WSUS server that manages it. WSUS reports only the updates that it has approved, so the results match what WSUS would install. The host must be set to use a WSUS server and able to reach it.
Windows Update Server	Checks the host online against Microsoft's update service. On its own, it reports only Windows operating-system updates. The host needs internet access to Microsoft Update. Use this option for hosts that a WSUS server does not manage.
Check for other Microsoft products	Extends the online check to other Microsoft products alongside Windows, such as Office, SQL Server, Exchange, and .NET. If the target is not set up to receive these updates, Elements Exposure Management enables the required update source automatically. This option applies only when you select Windows Update Server.
Use Microsoft Updates database file	Performs an offline check using Microsoft's update catalog file (wsusscn2.cab). Elements Exposure Management uploads the file to the host over the existing SSH connection using SFTP, so no extra firewall rules are needed. It then checks for missing updates and removes the file. The host needs no WSUS server or internet access, so this is the best choice for isolated or air-gapped systems. It is the slowest of the three methods, and it requires scan nodes that are deployed on Windows.

When all options are selected

The methods are not combined. They are tried in priority order, and the first one that succeeds is used:

1. WSUS
2. Windows Update Server
3. Microsoft Updates database file

If a method cannot run, Elements Exposure Management falls back to the next one. For example, the host might have no WSUS server or no internet access. The database file is the final fallback for hosts that can reach neither WSUS nor Microsoft Update.

Selecting all three gives the widest coverage and the best chance of getting patch results from every host. The reported results depend on which method succeeded. WSUS reports only the updates approved on the WSUS server, while Windows Update Server reports all updates available from Microsoft.

Glossary

Access Control

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

Active Directory (AD)

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

Agent

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

Antivirus

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

Asset Management

Asset management is the process of tracking, maintaining, and managing an organization's IT assets, including hardware, software, and digital resources.

Attack Path Visualization

A graphical representation of how an attack could progress within an organization's infrastructure.

Automation

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

Backdoor

An undocumented way of gaining access to a computer system.

Breach

A breach is a security incident in which confidential or protected data is accessed, disclosed, or stolen by an unauthorized party.

Business Context

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

Certificate

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

Certificate Authority (CA)

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

Cloud Account

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

Cloud Security

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

Cloud Service

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

Configuration Keys

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

Connector

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

Containment

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

Criticality

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

Custom Labels

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

Customer Company

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

Detection

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

Discovery Scan

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

Encryption

Encryption is the process of converting data into a secure format using cryptographic algorithms, ensuring confidentiality and protection against unauthorized access.

Encryption Keys

Encryption keys are cryptographic values used to encrypt, decrypt, or otherwise secure protected data and communications.

Endpoint Detection and Response (EDR)

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

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

Endpoint Protection

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

Endpoint Security

Endpoint security is the protection of end-user devices — such as laptops, servers, and mobile devices — from threats through prevention, detection, and response controls.

Entra ID

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

Exploit

Objects or methods that take advantage of a flaw in a program to make it behave unexpectedly. Doing so creates conditions that an attacker can use to perform other harmful actions.

Exposure Management

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

Exposure Score

A dynamic metric that quantifies an organization's cybersecurity risk based on detected vulnerabilities, attack paths, and mitigation actions.

External Attack Surface (EAS)

The collection of internet-facing assets, services, and vulnerabilities that an attacker can exploit.

False Positive

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

Federated Single Sign-On (FSSO)

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

Firewall Rules

Firewall rules are individual allow, block, or filtering directives that define how firewall traffic is handled.

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.

Highest Impact Recommendations

A prioritized list of security findings that require immediate attention to reduce cyber risks.

IAM Role

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

Identity and Access Management (IAM)

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

Identity Management

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

Identity Provider (IdP)

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

Identity Scans

Automated scans to detect leaked credentials, misconfigurations, and vulnerabilities in identity systems such as Active Directory or cloud identity providers.

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.

Infrastructure-as-Code (IaC)

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

Intrusion Prevention System (IPS)

An Intrusion Prevention System (IPS) is a security control that inspects network traffic in real time and automatically blocks detected malicious or policy-violating activity.

Lateral Movement

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

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an open protocol for accessing and managing directory information, such as users, groups, and devices, over a network.

Linux Authenticated Scanning

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

Malware

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

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.

Network Isolation

Network isolation is a containment action that restricts or blocks a device's network communication to prevent further malicious activity or spread.

Organization Hierarchy

An organization hierarchy is a structured arrangement of organizations or sub-organizations that defines visibility, inheritance, or management relationships.

Passphrase

A passphrase is a secret, typically longer than a password, used to protect a private or encryption key — for example, an SSH key used in authenticated scanning.

Patch Management

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

Phishing

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

Privacy

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

Profile Assignment

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

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.

Remote Monitoring and Management Integration (RMM)

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

Reputation Service

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

Risk Assessment

Risk assessment is the process of identifying, analyzing, and evaluating risks to systems and data in order to prioritize and guide mitigation efforts.

Role Assignment

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

Role-Based Access Control (RBAC)

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

Scan

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

Scan Node

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

Scan Templates

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

Scheduled Scan

A scheduled scan is a scan configured to run automatically at defined times, intervals, or system conditions without needing a user to start it manually.

Scope Selector

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

Secure Shell (SSH)

Secure Shell (SSH) is a cryptographic protocol used to securely access and manage remote devices over an unsecured network.

Secure Sockets Layer (SSL)

Secure Sockets Layer (SSL) is a now-deprecated cryptographic protocol for securing network communications; it has been succeeded by Transport Layer Security (TLS).

Security Administrator

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

Security Administrator Role

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

Security Cloud

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

Security Events

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

Security Group

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

Security Policy

A set of rules that define how product settings are managed, protected and distributed. Primarily used in Policy Manager, but also appear in other admin-level corporate products.

Service Account

A service account is a special type of account used by applications, scripts, or automated processes to interact with systems and services, often with predefined permissions.

Service Partner

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

Severe Risk

The highest detection risk-level band, indicating malicious activity that could cause severe damage and requires immediate response.

Severity

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

Software Updater

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

Solution Provider

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

Subscription Key

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

System Scan

A system scan is a scan that examines a device, host, or system target to identify malware, weaknesses, or other security-relevant conditions.

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 Intelligence

Threat intelligence is evidence-based knowledge about existing or emerging threats — such as attacker tactics, indicators, and motivations — used to inform defensive decisions.

Transport Layer Security (TLS)

Transport Layer Security (TLS) is a cryptographic protocol that provides secure communication over networks by encrypting data transmissions and verifying identities.

Trojan

A Trojan is malicious software that disguises itself as a legitimate program to trick users into running it, then performs harmful actions such as stealing data or opening a backdoor.

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.

Windows Management Instrumentation (WMI)

Windows Management Instrumentation (WMI) is a Microsoft framework that enables system administrators to manage and monitor Windows-based devices using scripts or remote commands.

Index

A

- access management 16–17
- access rights 5, 10, 17, 19
- account 27
- account creation 18
- account deletion 100
- account details 20
- account levels 15
- account linking 25
- account settings 101
- account status 65
- Active Directory 35
- AD groups 35
- adding devices 28, 30, 33
- Admin Approval Mode 119
- administrator account 5–6, 10, 17–18, 44–45
- Agent 44, 47–49
- Agent for Computers 29
- Agent for Servers 29
- Agent for Windows 36
- API client 19
- archived assets 97
- asset attributes 95
- asset changes 95
- asset deletion 96–97
- asset filtering 94–95
- asset groups 33
- asset inventory 94
- asset management 94
- asset notes 96
- asset onboarding 44, 47
- asset tags 96
- assets 47
- attack path 81, 84
- attack surface 41
- audit logs entry 10
- authenticated scanning 57, 109
- authenticator app 8
- Authenticator applications with Time-Based One-Time Password (TOTP) 8
- automatic deletion 31, 34
- Azure 61, 106
- Azure Cloud Shell 63
- Azure portal 60
- Azure subscription 61–63
- Azure tenant 60–61

B

- backup 37
- biometric authentication 9
- business account 44
- Business Account 6

C

- CA certificate 59
- Center 50
- certificate 113–115
- change name 20
- change subscription 24

- clone report 91
- cloud account 60–62, 64–65, 100, 106
- cloud account scan 74–75
- cloud accounts 47
- cloud connection 61
- cloud scan node 49, 77
- Cloud Security Posture 61
- Cloud Security Posture Management 61–62
- CloudFormation 64, 106
- company level 33
- Company level 34
- compliance posture 74, 83
- credentials 109, 119, 125
- custom labels 32
- custom view 91
- customer company 10, 21–22

D

- dark mode 20
- dashboard 89
- data recovery 37
- delete API client 19
- Denial of Service 69
- device 48
- device asset 94–96
- device assignment 33
- device biometrics 9
- Device biometrics 8
- device commands 34
- device filters 35
- device grouping 32–33
- device invitations 32
- device labels 32
- Device list 32
- device management 28, 31–35
- device onboarding 47
- device scan 68, 77
- device view 33, 35
- devices 24, 34, 47
- Devices page 33
- Devices view 35
- diagnostic data 36
- digital perimeter 47
- discovery scan 68–70, 94
- discovery scan results 70
- domain 122
- domain account 119
- domain federation 26
- downloading software 30
- Downloads page 30

E

- edit administrator 18
- edit profile 20
- EDR 24, 30
- EDR and EPP for Computers 24
- EDR and EPP for Computers Premium 24
- EDR and EPP for Servers 24
- EDR and EPP for Servers Premium 24
- EDR for Computers 24, 30

- Element Agent 48
- Element Security Center 45
- Elements API 19
- Elevate 84
- email address 25
- email aliases 26
- email invitation 30, 32
- email notification 90
- email report 90
- encryption keys 57, 125–126
- endpoint status updates 49
- engine update 59
- Enterprise 61
- EPP for Computers 24, 34–35
- EPP for Computers Premium 24
- EPP for Servers 24, 34–35
- EPP for Servers Premium 24
- EPP subscription 24
- event log 101
- Executive Summary 92
- existing customer company 22
- exposed assets 40
- exposed ports 68
- exposure 79
- Exposure Dashboard 79
- exposure grade 92
- Exposure Management 43, 125–126
- Exposure Management for Cloud 45
- Exposure Management for Cloud, do the following: 44
- Exposure Management for User 45
- Exposure Management for Users 44
- exposure management report 90
- Exposure Management role 45
- exposure risk 79
- external attack surface 41, 65, 76–77
- external attack surface scan 76

F

- federated domain 7, 27–28
- federated single sign-on 25–26
- finding 83, 129
- fingerprint 9
- firewall rule 120–121
- forgot password 20
- FSSO 25

G

- getting started 43
- GPO 120
- Group Policy 112, 118, 120
- Group Policy object 120

H

- host 70, 72
- Host discovery 68

I

- IAM administrator 15–17
- IAM role 10, 15–17, 64
- identities 47
- identity 61
- Identity and Access Management 15

- identity asset 66, 77
- Identity Inventory 61
- identity onboarding 66
- identity provider 25
- identity scan 77
- Infrastructure-as-Code 106
- installation 47, 51, 54
- installation link 30, 32
- installation package 29–30
- installation verification 52, 56
- internet discovery 76
- internet-facing systems 76

K

- key features 39–40
- key pair 125
- key-based authentication 127, 129

L

- label assignment 32
- labeling rules 50
- light mode 20
- Linux 54, 56, 98–99
- Linux authenticated scanning 124–125, 127, 129
- Linux scan node 56
- Linux server 53
- local scan node 49
- logging in 6
- login 7, 20, 44
- login credentials 6–7
- login security 7

M

- managed companies 15
- MFA 7–9
- MFA methods 8
- Microsoft Entra Admin Center 25
- Microsoft Entra ID 7, 25–27
- Microsoft Updates database file 131
- misconfiguration 39, 83
- Mobile Protection 28–29, 34, 36
- multi-factor authentication 6–9
- Multifactor Authentication 66
- My report 89
- My settings 9, 20

N

- network asset 50, 65
- network asset scan 76
- network scanning 109
- network vulnerability scan 50, 53, 68, 71
- new customer company 23
- non-federated domain 7
- notification settings 101

O

- offline devices 31, 34
- onboarding 43, 60–62, 64–65
- onboarding script 63
- OpenSSH 129–130
- operational technology 84

ordering products 22–23
 Organization Settings 17–19, 33

P

partner 17–18
 Partner Portal 21–23
 password authentication 127
 password recovery 20
 patch management 5
 pending invitations 32
 permissions 10
 Phone number for Short Message Service (SMS) messages
 with One-Time Passwords (OTP) 8
 plugin selection 73
 Port scan 68–69
 PowerShell 63, 111
 Premium subscription 24
 prerequisites 61
 private key 126
 product deployment 21
 profile assignment 35
 profile assignment rules 33
 proxy server 58
 public key 125
 Push notifications with Auth0 Guardian authenticator 8

Q

quick start 6, 43

R

read access 122
 recommendation 79, 81
 recommendation status 82
 registry keys 122
 remediation 81
 remediation effort 82
 remediation impact 82
 remote device management 34
 Remote Procedure Call 118
 Remote Registry service 121
 remote request 36
 remove administrator 18
 removing federation 28
 removing MFA 9
 report 87, 90–92
 report deletion 92
 report settings 91
 reset password 20
 role 10
 role assignment 10
 role permissions 16
 Role-Based Access Control 45, 100
 roles 100
 RPC dynamic ports 121
 RPC endpoint mapper 120
 rule group 75

S

scan configuration 68, 73
 scan engine 59
 scan group 72
 scan groups 68

scan limits 59
 scan management 68
 scan node 49–54, 56–59, 97–99, 104, 109, 122, 124–126,
 129
 Scan node 68
 Scan Node Agent 57–59
 scan node configuration 52, 56
 Scan Node Control Center 126
 scan node data 56
 scan node license 57, 98
 scan report 129
 scan results 89
 scan schedule 75
 scan scope 75
 scan settings 131
 scan target 127
 scan template 69, 72
 scanning methods 41
 scope selector 5, 15, 17, 22–23, 30, 33–34
 Secure USB keys 8
 security administrator 10, 17
 Security Administrators 18
 Security Center 5–10, 15, 17, 20–23, 25–26, 28, 30–36, 43–
 45, 47, 49–52, 54, 56, 58, 60, 62, 64–65, 68, 77,
 87, 89–90, 94, 97–98, 100, 104, 106, 109–110, 118,
 122, 124–125, 129
 security configurations 97
 security events 91
 security posture 74–75
 security risk 40
 security roles 15
 security settings 101
 self-signed certificate 115
 service 37
 service partner account 18
 simultaneous scans 59
 single sign-on 7, 26, 28
 Smartphones or other devices 8
 software distribution 29
 software installation 30
 Solution Provider 15, 21–22
 SSH 124, 127, 129–130
 SSH authentication 127
 SSH key 129
 SSL certificate 58
 SSL/TLS certificate 59
 status badges 82
 subdomain takeover 76
 subscription 6, 21–23, 28, 31
 subscription assignment 22
 subscription key 21–24, 29
 subscription upgrade 24
 subscriptions 21, 23
 Subscriptions view 23
 support 36
 system scan 68, 70–73, 109
 system scans 72

T

table columns 35
 target host 130
 tenant 61
 Terraform 106
 terraform apply 106
 threat 39
 troubleshooting 99, 104, 115, 123, 129

two-factor authentication 7

U

unauthorized access 77

uninstallation 98–99

unmanaged devices 50

upgrading options 24

user account 111, 127

user groups 100

user identity linking 27

user management 10, 45, 94, 100

user name 20

V

view mode 20

Vulnerabilities role 10

vulnerability 39, 71, 83, 92

vulnerability management 5, 47, 94

Vulnerability Management 50, 53, 73, 98–99, 101

vulnerability management report 87

Vulnerability Management: 16

vulnerability report 87, 89

vulnerability scan 47–48, 94

W

web scan 68

widget 89

Windows 51–52, 98

Windows authenticated scanning 110–112, 115, 118–123, 129–131

Windows Remote Management 110

Windows server 50

Windows Update Agent 47

Windows Update Server 131

WinRM 110–111, 115

WinRM service 112–114

WithSecure 5–7, 15–17, 21, 36, 44, 49–50, 58, 126

WithSecure-CSPM-Scanner-MTA 61

workflow 79

WSDIAG file 36