

# **WithSecure Elements Collaboration Protection**

**Administrator guide**

# Contents

|                                                                                              |           |
|----------------------------------------------------------------------------------------------|-----------|
| <b>Chapter 1: Introduction.....</b>                                                          | <b>4</b>  |
| 1.1 Solution overview.....                                                                   | 5         |
| 1.2 System requirements.....                                                                 | 5         |
| 1.3 Features.....                                                                            | 6         |
| <b>Chapter 2: Getting started.....</b>                                                       | <b>8</b>  |
| 2.1 Creating a new administrator account.....                                                | 9         |
| 2.2 Logging in to WithSecure Elements Security Center.....                                   | 9         |
| 2.2.1 Adding administrator accounts.....                                                     | 9         |
| 2.3 Logging in to the WithSecure Elements Collaboration Protection portal.....               | 10        |
| <b>Chapter 3: Setting up the WithSecure Elements Collaboration Protection portal.....</b>    | <b>11</b> |
| 3.1 Switching between the managed companies.....                                             | 12        |
| 3.2 Setting up the portal.....                                                               | 12        |
| 3.3 Changing your user name.....                                                             | 12        |
| 3.4 Creating a default policy.....                                                           | 12        |
| 3.5 Connecting WithSecure Elements Collaboration Protection to the Microsoft Office 365..... | 13        |
| 3.6 Setting up Exchange protection.....                                                      | 14        |
| 3.7 Setting up SharePoint protection.....                                                    | 14        |
| 3.8 Setting up OneDrive protection .....                                                     | 15        |
| 3.9 Setting up Teams protection.....                                                         | 15        |
| 3.10 Restricting partner access.....                                                         | 15        |
| 3.10.1 Requesting access.....                                                                | 16        |
| 3.10.2 Approving partner access request.....                                                 | 16        |
| <b>Chapter 4: Administering the product.....</b>                                             | <b>17</b> |
| 4.1 Manual application creation.....                                                         | 18        |
| 4.2 Checking the overall status of the managed companies.....                                | 19        |
| 4.3 Managing cloud services.....                                                             | 19        |
| 4.3.1 Viewing cloud service properties.....                                                  | 20        |
| 4.3.2 Changing the assigned policy for a deployed cloud service.....                         | 20        |
| 4.3.3 Disconnecting a cloud service.....                                                     | 21        |
| 4.3.4 Removing a cloud service.....                                                          | 21        |
| 4.4 Managing detections.....                                                                 | 21        |
| 4.4.1 Filtering detections.....                                                              | 21        |
| 4.4.2 Viewing detections details.....                                                        | 22        |
| 4.4.3 Updating detection status.....                                                         | 23        |
| 4.4.4 Adding comments.....                                                                   | 23        |

|                                                                                             |           |
|---------------------------------------------------------------------------------------------|-----------|
| 4.4.5 Viewing comments.....                                                                 | 23        |
| 4.5 Managing compromised accounts.....                                                      | 24        |
| 4.5.1 Viewing compromised accounts.....                                                     | 24        |
| 4.5.2 Remediation of compromised accounts.....                                              | 25        |
| 4.6 Managing policies.....                                                                  | 26        |
| 4.6.1 Setting up the General options.....                                                   | 26        |
| 4.6.2 Setting up privacy options.....                                                       | 26        |
| 4.6.3 Setting up notifications.....                                                         | 26        |
| 4.6.4 Setting up the Exchange general options.....                                          | 29        |
| 4.6.5 Setting up the SharePoint general options.....                                        | 30        |
| 4.6.6 Setting up malware scanning.....                                                      | 30        |
| 4.6.7 Setting up Exchange URL scanning.....                                                 | 31        |
| 4.6.8 Setting up Exchange inbox rules scanning.....                                         | 32        |
| 4.6.9 Setting up the Exchange compromised accounts options.....                             | 32        |
| 4.6.10 Setting up Exchange notifications.....                                               | 33        |
| 4.7 Managing quarantined items.....                                                         | 33        |
| 4.7.1 Filtering quarantined items.....                                                      | 33        |
| 4.7.2 Deleting quarantined items.....                                                       | 34        |
| 4.7.3 Releasing quarantined items.....                                                      | 34        |
| 4.8 Managing system events.....                                                             | 36        |
| 4.8.1 Filtering system events.....                                                          | 36        |
| 4.9 Managing reports.....                                                                   | 37        |
| 4.9.1 Generating scheduled report tasks.....                                                | 37        |
| 4.9.2 Editing scheduled report tasks.....                                                   | 37        |
| 4.9.3 Downloading and viewing reports.....                                                  | 38        |
| 4.9.4 Cloning scheduled report tasks.....                                                   | 38        |
| 4.9.5 Deleting scheduled report tasks.....                                                  | 38        |
| <b>Chapter 5: Support.....</b>                                                              | <b>39</b> |
| <b>Appendix A: Specifying Microsoft Azure Active Directory tenant<br/>name and ID .....</b> | <b>40</b> |
| A.1 Determining the tenant name of your Azure Active Directory and Office 365.....          | 41        |
| A.2 Locating the Microsoft Azure Active Directory tenant ID.....                            | 41        |
| <b>Appendix B: Reporting false positives and false negatives.....</b>                       | <b>42</b> |
| B.1 Submitting a sample.....                                                                | 43        |
| <b>Appendix C: Manual scanning of suspicious items.....</b>                                 | <b>44</b> |
| C.1 Manually scanning suspicious Exchange items.....                                        | 45        |
| C.2 Manually scanning suspicious SharePoint items.....                                      | 45        |

# Chapter 1

## Introduction

---

### Topics:

- [Solution overview](#)
- [System requirements](#)
- [Features](#)

This guide gives you general information about WithSecure Elements Collaboration Protection (formerly known as WithSecure Cloud Protection for Microsoft Office 365).

## 1.1 Solution overview

---

WithSecure Elements Collaboration Protection is a cloud-based solution to detect, protect from, and respond to security threats in Microsoft Office 365.

WithSecure Elements Collaboration Protection protects Exchange items, such as email messages, tasks, calendar appointments, contacts, sticky notes from malicious content, and it provides advanced protection against Inbox rule-based attacks. The solution also provides real-time protection for SharePoint, OneDrive, and Teams content.

Combined with WithSecure's award winning endpoint protection, detection, and response capabilities, the solution provides more comprehensive protection for your business than any email security solution alone. Cloud-to-cloud integration makes the solution easy to deploy and manage.

## 1.2 System requirements

---

This section contains important information about the WithSecure Elements Collaboration Protection. We strongly recommend that you read the entire document before you start using the product.

### Supported browsers

The WithSecure Elements Collaboration Protection portal supports the latest versions of the following browsers:

- Mozilla Firefox
- Google Chrome
- Microsoft Edge
- Safari

### Supported languages

The WithSecure Elements Collaboration Protection portal and documentation are localized into the following languages:

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

### Supported Microsoft 365 and Office 365 plans

The WithSecure Elements Collaboration Protection solution supports a variety of Microsoft 365 and Office 365 plans including the following:

- Microsoft 365 enterprise plans:
  - Microsoft 365 E3
  - Microsoft 365 E5
  - Microsoft 365 F1
- Microsoft 365 business plans:
  - Microsoft 365 Business Basic (formerly Office 365 Business Essentials)
  - Microsoft 365 Business Standard (formerly Office 365 Business Premium)
  - Microsoft 365 Business Premium (formerly Microsoft 365 Business)
- Microsoft 365 educational plans:
  - Microsoft 365 A1
  - Microsoft 365 A3
  - Microsoft 365 A5
- Office 365 enterprise plans:
  - Office 365 E1
  - Office 365 E3

- Office 365 E5
- Office 365 educational plans:
  - Office 365 A1
  - Office 365 A3
  - Office 365 A5

## 1.3 Features

---

Some of the main features of WithSecure Elements Collaboration Protection are described here.

|                                      |                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                          |
|--------------------------------------|--------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Compromised account detection</b> | Email is one of the biggest threat vectors for companies of all sizes. Access to user email accounts often grants access to a wide range of other company services and gives attackers an opportunity to steal company and customer data. A breached account is an easy way for the attacker to get into an organization. The attacks done using a breached account, such as phishing campaigns or impersonation, are hard to detect because they use a legitimate company user account. The Compromised account detection feature detects compromised accounts as soon as information about the breach is available. It informs users and administrators to take action to remediate the accounts by changing the password or by taking other security measures, such as turning on the multi-factor authentication to avoid further exploitation of the breached data. |
| <b>Inbox rule scanning</b>           | Inbox rules in Outlook work as a trigger to perform specific actions on incoming emails automatically. After gaining access to a mailbox, an attacker creates inbox rules to carry out different types of attacks, such as auto-forwarding and auto-deleting of emails. The scanning feature analyzes all the inbox rules in a mailbox. This analysis helps detect any suspicious rules that may indicate a compromise of the account. It also notifies the owner of the mailbox and the administrators to take action.                                                                                                                                                                                                                                                                                                                                                  |
| <b>File and URL protection</b>       | Whenever an end user receives or creates a Microsoft Outlook item, such as email, appointment, task, contact, or note in their mailbox, all included attachments and URLs are analyzed for harmful content, such as malware, Trojans, ransomware, or phishing.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                           |
| <b>Multilayered security</b>         | WithSecure Elements Collaboration Protection leverages WithSecure Security Cloud, which combines award-winning multi-engine antivirus, machine learning-based heuristic analysis, and threat intelligence database updated in real-time. WithSecure Security Cloud finds instantly emerging and unseen malware variants as well as detects broader range of malicious features, behavior patterns and trends.                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Advanced threat detection</b>     | Advanced threat detection runs suspicious files in an isolated virtual environment (known as a sandbox) that mimics a normal computer. As the file is detonated - that is, allowed to run in the sandbox - the process examines its behavior for any harmful actions. It then returns a verdict on whether the file is clean or harmful. Clean files are allowed to run normally, while harmful files are blocked.                                                                                                                                                                                                                                                                                                                                                                                                                                                       |
| <b>Advanced analytics</b>            | Advanced security analytics gives full visibility into analyzed content and ensures fast and efficient response capabilities.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                            |
| <b>Worry-free administration</b>     | As a product administrator, you can configure settings, detections, user notifications, and actions in accordance with your company security policies. The WithSecure Elements Collaboration Protection portal allows you to manage detections and quarantined items for multiple Microsoft Office 365 tenants. WithSecure partners can administer the solution for multiple end customers.                                                                                                                                                                                                                                                                                                                                                                                                                                                                              |
| <b>Seamless integration</b>          | WithSecure Elements Collaboration Protection supports cloud-to-cloud integration without additional software to be installed or changes made to server or client side. The protection is totally platform agnostic and capable of detecting threats regardless of which device or application is used by the end user.                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                                   |

|                                      |                                                                                                                                                                                                                                                                                                                                                                                    |
|--------------------------------------|------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Quarantine management</b>         | Microsoft Office 365 user mailbox items, such as emails, calendar appointments, notes, contacts, and groups which contains harmful files, harmful URLs, or both can be quarantined immediately. Later on you can review and restore them using quarantine management.                                                                                                              |
| <b>Reporting</b>                     | WithSecure Elements Collaboration Protection allows you to generate scheduled reports to provide a holistic overview of the secured environment which can be shared to show the value provided by the solution over a certain period of time.                                                                                                                                      |
| <b>Microsoft Exchange protection</b> | The solution protects your Exchange items, such as email messages, tasks, contacts, and more.                                                                                                                                                                                                                                                                                      |
| <b>SharePoint protection</b>         | The solution protects the content in your SharePoint sites. Whenever you store files in SharePoint, WithSecure Elements Collaboration Protection analyzes the files for harmful content, such as malware, Trojans, ransomware or phishing. Advanced SharePoint protection is included in the product and can be used with no additional charge.                                    |
| <b>OneDrive protection</b>           | The solution protects the content in your OneDrive drives. Whenever you store files in OneDrive or share them in private or group chats in Teams, WithSecure Elements Collaboration Protection analyzes the files for harmful content, such as malware, Trojans, ransomware or phishing. OneDrive protection is included in the product and can be used with no additional charge. |
| <b>Teams protection</b>              | The solution protects the files that you share in your Team channels.                                                                                                                                                                                                                                                                                                              |

# Chapter 2

## Getting started

---

### Topics:

- [Creating a new administrator account](#)
- [Logging in to WithSecure Elements Security Center](#)
- [Logging in to the WithSecure Elements Collaboration Protection portal](#)

Instructions on how to get started with WithSecure Elements Collaboration Protection (formerly known as WithSecure Cloud Protection for Microsoft Office 365).

## 2.1 Creating a new administrator account

---

After receiving the subscription key for WithSecure Elements Collaboration Protection, you need to create an administrator account to manage the solution.

To create an administrator account:

1. Open the following link in the web browser: <https://portal.business.f-secure.com/self-register>.
2. Enter the subscription key and your email address.

**Note:** You use the email address as your username later on to log in to WithSecure Elements Collaboration Protection.

3. Select **Submit**.  
You receive an email from WithSecure Elements Security Center with a link and temporary password to log into WithSecure Elements Security Center.
4. Follow the instructions in the email to change your login password.

**Important:** We strongly recommend that you turn on two-factor authentication (2FA) for the administrator accounts. You can set it up in account settings.

## 2.2 Logging in to WithSecure Elements Security Center

---

WithSecure Elements Security Center is a web-based user interface where you can manage administrator accounts, roles, and subscriptions of your organization.

**Note:** The Subscriptions page shows both the number of active mailboxes that are protected and the actual number of mailboxes for the subscription.

To log in to WithSecure Elements Security Center:

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

Next, you can add new administrator accounts to manage WithSecure Elements Collaboration Protection in your organization.

### 2.2.1 Adding administrator accounts

You can add more administrator accounts with different roles to manage WithSecure Elements Collaboration Protection in your organization.

To add administrator accounts:

1. In the WithSecure Elements Security Center portal, on the sidebar, select **Management - Collaboration Protection > Users**.  
The **Users** page opens.
2. Select **Add user**.
3. In the Add user screen, select the organization or a single company to which you want the new administrator to have access.
4. Select **Next**.  
The **Add email** screen opens.
5. Enter the email address of the new administrator, and select **Next**.
6. In the User roles screen, from the WithSecure Elements Collaboration Protection and WithSecure Elements Collaboration Protection drop-down menus, select the roles that you want the new administrator to have.
7. Select **Next**.  
The Confirmation screen opens.

8. Check that the user name, organization and the selected roles are correct, and then select **Confirm** to complete adding the new administrator.

The new administrator receives an email message from WithSecure Elements Security Center with temporary credentials and instructions for logging in.

## 2.3 Logging in to the WithSecure Elements Collaboration Protection portal

---

The WithSecure Elements Collaboration Protection portal is a web-based user interface to administer the WithSecure Elements Collaboration Protection application.

To log in to the WithSecure Elements Collaboration Protection portal, do the following:

- Open the following link in your web browser: <https://elements.f-secure.com/apps/cloudprotection/>.
- On the WithSecure Elements Security Center dashboard, select **WithSecure Elements Collaboration Protection**.

**Note:** WithSecure Elements Collaboration Protection is only visible if you have access to it.

The WithSecure Elements Collaboration Protection portal opens.

# Chapter 3

## Setting up the WithSecure Elements Collaboration Protection portal

---

### Topics:

- [Switching between the managed companies](#)
- [Setting up the portal](#)
- [Changing your user name](#)
- [Creating a default policy](#)
- [Connecting WithSecure Elements Collaboration Protection to the Microsoft Office 365](#)
- [Setting up Exchange protection](#)
- [Setting up SharePoint protection](#)
- [Setting up OneDrive protection](#)
- [Setting up Teams protection](#)
- [Restricting partner access](#)

Instructions on how to set up the WithSecure Elements Collaboration Protection portal (formerly known as WithSecure Cloud Protection for Microsoft Office 365).

## 3.1 Switching between the managed companies

---

Use the **scope selector** to broaden or narrow the scope of information displayed in the WithSecure Elements Collaboration Protection portal.

The scope selector shows all the companies that are managed by the reseller, even the ones with restricted access that are not visible in the portal.

In the WithSecure Elements Collaboration Protection portal, there are different account levels.

**Note:** If the account was created to manage only one company, only the company name is shown next to the portal logo instead of a drop-down menu.

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

1. Select the  icon at the top of the page next to the logo.  
A drop-down menu is displayed, listing all the companies associated with your account.
2. Click to select the desired company.

**Tip:** Use the **Search** field to narrow the list.

The page is updated to show the relevant information for the selected company.

## 3.2 Setting up the portal

---

On the My settings page, you can select the language and timezone for the portal, and help us improve the product by sending usage data.

To set up the portal:

1. Select  at the top right corner.  
The **My settings** window opens.
2. To select the language, under **Details**, from the **Language** drop-down menu, select the correct language.  
The selected language is used across the WithSecure Elements Collaboration Protection portal.
3. To select the timezone, from the **Timezone** drop-down menu, select the timezone to be used in the WithSecure Elements Collaboration Protection portal.
4. To send usage data, under **UI Analytics**, turn on **Allow the portal to collect anonymized statistics on usage**.

By allowing us to collect anonymized statistics and data about the use of the key WithSecure Elements Collaboration Protection portal features, you help us improve the product.

## 3.3 Changing your user name

---

You can change your user name in the settings.

To change your user name:

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

## 3.4 Creating a default policy

---

A policy is a set of rules and settings that define how WithSecure Elements Collaboration Protection acts when a security threat is detected.

**Important:** Before rolling out WithSecure Elements Collaboration Protection, you need to create a default policy for your company. If you do not create a default policy, WithSecure Elements Collaboration Protection uses WithSecure Policy that is created by WithSecure and cannot be modified.

To create a default policy:

1. Open the portal.
2. Select **Policies** on the sidebar.
3. Select **Add policy** at the top of the page.

**Note:** By default, a WithSecure Policy is available and you can use it as a template.

**Note:** You can create a new policy also by copying from an existing policy. To do that, select  in the Menu column next to the policy that you want to copy, and select **Copy**.

4. On the page that opens, under **General**, in the **Policy name** field, enter a name for the new policy.

**Note:** You may add also a description and enter one or more tags to make it easier to find the policy later.

5. Under **Notifications**, enter a recipient email address for sending notifications.

6. Select **Save**.

You have created a new policy

7. On the Policies page, select  in the Menu column next to the policy that you just created, and select **Set as default**.

The new policy is now the default policy. It is automatically assigned to every new cloud service that is created for a given company when you connect WithSecure Elements Collaboration Protection to your Microsoft Office 365 tenant.

Next, you need to set up the new default policy.

## 3.5 Connecting WithSecure Elements Collaboration Protection to the Microsoft Office 365

---

You can connect WithSecure Elements Collaboration Protection to the Microsoft Office 365 Exchange service and to the SharePoint service for more comprehensive protection.

To connect WithSecure Elements Collaboration Protection:

1. Select **Cloud services** on the sidebar.
2. Select **Add connection**.

**Note:** On a partner level, to add a new connection, either switch to a company level, or go to **Organization view**, select , and then select **Add new connection**.

The **Add new connection** page opens.

3. Under **Connection details**, do the following:

- a) In the **Name** field, enter a name for the new connection.
- b) In the **Specify Microsoft Azure Active Directory tenant name or ID** field, specify a name or ID for the Microsoft Azure Active Directory tenant that is dedicated for your Microsoft Office 365 service. For more information, see [Determining the tenant name of your Azure Active Directory and Office 365](#) on page 41.
- c) If you have several subscriptions, select the proper subscription key from the drop-down menu.

**Note:** If you have only one subscription, it is shown automatically.

4. Select **Next** to continue.

The **Summary** screen opens.

5. Review the information on the **Summary** page, and select **Add connection**.

The new connection is added and the **Finish** screen opens.

6. Select **Close**.

7. On the Cloud services page, do one of the following:

- To authorize and connect the new cloud service, select **Authorize** in the Exchange column, and then select **Connect**.
- To authorize and connect the new cloud service, select **Authorize** in the SharePoint column, and then select **Connect**.

- To authorize and connect the new cloud service, select **Authorize** in the OneDrive column, and then select **Connect**.
- The authorization for Teams is received by authorizing SharePoint to protect the Teams channels.

**Note:** If you are not an administrator, select **Copy URL** to get the URL that you need to finish the setup. You need appropriate rights to visit this page grant the required permissions to connect to the cloud service.

8. When prompted to accept permissions requested by WithSecure Elements Collaboration Protection, do the following:

**Note:** Your browser may block pop-up windows. In that case, the portal shows a warning and a link that you can select to open the Microsoft page manually.

- a) Make sure that the link under WithSecure Elements Collaboration Protection points to the WithSecure Elements Collaboration Protection portal.
- b) Check the WithSecure service agreement and privacy policy, and select **Accept**.

**Note:** By accepting, you allow WithSecure Elements Collaboration Protection to access data in your Microsoft Office 365 tenant.

A pending connection appears on the Cloud services page. When the connection between WithSecure Elements Collaboration Protection and the Microsoft Office 365 Exchange, SharePoint, or OneDrive service has been established, the status of the service changes to "Configure protection".

Next, you need to set up protection for the mailboxes.

#### Related tasks

[Determining the tenant name of your Azure Active Directory and Office 365](#) on page 41

The Microsoft Azure Active Directory tenant name is the primary domain that was initially created for Microsoft Office 365.

## 3.6 Setting up Exchange protection

---

Instructions on how to set up protection for the mailboxes in a configured domain.

To set up protection for the mailboxes:

1. Select **Cloud services** on the sidebar.
2. Select **Configure protection** in the row of the new connection in the **Exchange** column.
3. In the page that opens, do the following:

- Select **Protect all mailboxes** if you want to protect all the existing mailboxes in your account in Microsoft Exchange.
- Select **Customize my protection** if you want to select the mailboxes that you want to protect.

**Note:** You can turn on **Protect new mailboxes** if you want to automatically protect all the new mailboxes. If this setting is off, you must manually select the new mailboxes to add them to the list of protected mailboxes.

- To add protection for an existing unprotected mailbox on your account, select the mailbox from the mailbox list and at the bottom of the page, select **Turn on protection**. The status of the mailbox changes to "Protected".

## 3.7 Setting up SharePoint protection

---

Instructions on how to set up protection for the sites in a configured domain.

To set up protection for the sites:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **SharePoint** column.
3. In the page that opens, do the following:

- a) From the list of sites, select the sites that you want to protect.

**Note:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

- b) To add protection for an existing unprotected site on your account, select the site from the list, and at the bottom of the page, select **Turn on protection**.  
The status of the site changes to "Protected".

## 3.8 Setting up OneDrive protection

---

Instructions on how to set up protection for the user drives in a configured domain.

To set up protection for the drives:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **OneDrive** column.
3. In the page that opens, do the following:

- a) From the list of drives, select the drives that you want to protect.

**Note:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

- b) To add protection for an existing unprotected drive on your account, select the drive from the list, and at the bottom of the page, select **Turn on protection**.  
The status of the drive changes to "Protected".

## 3.9 Setting up Teams protection

---

Instructions on how to set up protection for the files shared in Teams channels in a configured domain.

To set up protection for the channels:

1. Select **Cloud services** on the sidebar.
2. In the row of the new connection, select **Configure protection** in the **Teams** column.
3. In the page that opens, do the following:

- a) From the list of channels, select the channels that you want to protect.

**Note:** You can filter the list by selecting one of the options from the drop-down menu: All, Protected, Unprotected, Unavailable, or Error.

- b) To add protection for an existing unprotected channel on your account, select the channel from the list, and at the bottom of the page, select **Turn on protection**.  
The status of the channel changes to "Protected".

## 3.10 Restricting partner access

---

If your company is managing WithSecure Elements Collaboration Protection on its own, you may restrict the partner's access to your WithSecure Elements Collaboration Protection portal.

To restrict partner access:

1. Log in to WithSecure Elements Security Center.
2. On the sidebar, select **Management - Collaboration Protection > Settings**.  
The **Settings** page opens.
3. Under Organization settings, turn on **Restrict Partner access to my organization**.  
The partner access setting now shows the status as Restricted. With restricted access, the partner cannot, for example, remove users from the company account. And in the WithSecure Elements Collaboration Protection portal, the company is no longer visible in the list of the partner's managed companies (scope selector).

## 3.10.1 Requesting access

As a partner, you can request access to the company account to which your access has been restricted.

To request access:

1. Log in to WithSecure Elements Security Center.
2. Select **Organizations** on the sidebar.
3. Select the company account to which you want to request access.
4. Select **Request access** under the **My access** column.  
The Request access window opens.
5. From the Role drop-down menu, select one of the following roles for requesting access:
  - Admin - an administrator has a full access and can fully manage the product and the account.
  - Read-only - a user with read-only access can only view but not manage the product or the account.
  - Quarantine\_Mgr - a user with quarantine manager rights has limited access to manage only quarantined items.
6. Under **Reason**, explain the reason for your access request.
7. Select **Send request**.

**Note:** The access request is valid for 72 hours. If your request is not approved within that time, you need to send another request.

Your pending request is visible for the company administrator in WithSecure Elements Security Center under Users.

## 3.10.2 Approving partner access request

Instructions on how to approve partner access request.

To approve partner access request:

1. Open WithSecure Elements Security Center.
2. Select **Users** on the sidebar.
3. In the WithSecure Elements Collaboration Protection column, select the pending request.  
The Access request window opens showing the request details.
4. Select to allow or deny access.

**Note:** If you approve the request, it gives the partner a 72-hour access to your WithSecure Elements Collaboration Protection.

# Chapter 4

## Administering the product

---

### Topics:

- [Manual application creation](#)
- [Checking the overall status of the managed companies](#)
- [Managing cloud services](#)
- [Managing detections](#)
- [Managing compromised accounts](#)
- [Managing policies](#)
- [Managing quarantined items](#)
- [Managing system events](#)
- [Managing reports](#)

This chapter contains information on how you can view the overall status of all managed companies and manage detections, policies, quarantined items, and system events.

## 4.1 Manual application creation

You can create the application fully manually.

**Note:** If you want to create the application manually, refer to the Microsoft documentation for details.

The application must have at least the following properties:

| API/Permission name          | Type        | Description                                                 |
|------------------------------|-------------|-------------------------------------------------------------|
| Azure Active Directory Graph |             |                                                             |
| Directory.Read.All           | Application | Read directory data                                         |
| User.Read                    | Delegated   | Sign in and read user profile                               |
| Exchange                     |             |                                                             |
| full_access_as_app           | Application | Use Exchange Web Services with full access to all mailboxes |
| Microsoft Graph              |             |                                                             |
| Calendars.ReadWrite          | Application | Read and write calendars in all mailboxes                   |
| Contacts.ReadWrite           | Application | Read and write contacts in all mailboxes                    |
| Mail.ReadWrite               | Application | Read and write mail in all mailboxes                        |
| User.Read.All                | Application | Read all users' full profiles                               |
| Reports.Read.All             | Application | Read all usage reports                                      |
| Office 365 Management APIs   |             |                                                             |
| ActivityFeed.Read            | Application | Read activity data for your organization                    |
| ServiceHealth.Read           | Application | Read service health information for your organization       |

**Note:** When more features and functionality are added to WithSecure Elements Collaboration Protection, you need to add more permissions. If you fail to add a permission, the product functionality becomes impaired and might stop working.

You must set the following redirect URLs in the application:

- <https://portal.cp.f-secure.com/permission-request>

- <https://portal.cp.f-secure.com/cloud-services>

## 4.2 Checking the overall status of the managed companies

Instructions what to do when you want to make sure that everything is alright in customer environments.

To view the overall status:

1. Select **Home** on the sidebar.  
The Home view opens.
2. Check the Dashboard pane.

The **Dashboard** pane keeps you informed on what takes place in the companies that you manage. Based on the currently selected scope, it shows the overview of all companies or only the selected company.

**Note:** Using the drop-down menu at the top-right corner, you can select the time period for which you want to view the overall status.

You can view the following information:

|                                        |                                                                                                                                                                                                                                                                                             |
|----------------------------------------|---------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------------|
| <b>Current detections</b>              | Shows the number of detections by their status and severity level from critical to low.                                                                                                                                                                                                     |
| <b>Subscriptions</b>                   | Shows the number of expired cloud service accounts, as well as those that expire within seven days and within 30 days.                                                                                                                                                                      |
| <b>Item status</b>                     | Shows by companies the number of protected, unprotected, and unavailable mailboxes, sites, user drives, and channels as well as those that have errors or are unavailable.                                                                                                                  |
| <b>Top affected items</b>              | Shows the number and severity of detections and additional information in the top affected mailboxes, sites, user drives, and channels.                                                                                                                                                     |
| <b>Protection trend</b>                | Shows the all-time average percentage of the unsafe content in the selected company (the gray bar), the percentage of the unsafe content from the selected period (the dark blue bar) and from the period preceding the selected period (the light blue bar).                               |
| <b>Cloud service protection status</b> | The Exchange tab shows the total number of unsafe items (attachments and URLs) out of all the scanned items, and the amount of quarantined, deleted, and detonated items. The SharePoint, OneDrive and Teams tabs each show the number of unsafe files and the amount of quarantined files. |

## 4.3 Managing cloud services

The Cloud services page shows all the cloud services that have been added and set up for a chosen level (the partner level shows all the cloud services of the partner-managed companies).

You can add new services, assign new policies to existing cloud services, view the properties of and disconnect or remove existing cloud services.

The page shows you the overall status of each cloud service. The cloud service status can be as follows:

- **Protected** - The cloud service is fully protected. The protection is based on the assigned policy settings. The Exchange column shows the number of protected, unprotected, and unavailable mailboxes as well as the number of mailboxes in error state; the SharePoint column shows the number of protected, unprotected, and unavailable sites as well as the number of sites in error state; the OneDrive column shows the number of protected, unprotected, and unavailable user drives, and the number of drives in error state; the Teams column shows the number of protected, unprotected, and unavailable channels, and the number of channels in error state.
- **Configure protection** - The service is connected to Microsoft Exchange, SharePoint, OneDrive, or Teams but is not yet fully protected. You need to set up protection for the mailboxes, sites, user drives, or channels.

**Note:** If real-time scanning under the Policy settings is turned off, the service has a "Connected" status.

- **Connect** - The cloud service is disconnected and not protected. Your attention is required.  
**Note:** You can connect a disconnected service by selecting **Connect** in the row of the cloud service or by selecting the cloud service and selecting **Connect...** at the bottom of the page.
- **Authorize** - Pending authorization - the cloud service is not yet connected, but waiting for authorization. The service is not protected and your attention is required.  
**Note:** A service in the authorization process needs appropriate permissions the grant of which can be initiated by selecting the cloud service and then selecting **Connect...** at the bottom of the page.
- **Pending** - the cloud service is not yet connected, but currently establishing a connection. The service is not protected during this process.

The page shows whether a cloud service is connected to Exchange, SharePoint, OneDrive, or Teams. It also shows the name of the policy that is in use for a given cloud service.

#### Related tasks

[Connecting WithSecure Elements Collaboration Protection to the Microsoft Office 365](#) on page 13

You can connect WithSecure Elements Collaboration Protection to the Microsoft Office 365 Exchange service and to the SharePoint service for more comprehensive protection.

### 4.3.1 Viewing cloud service properties

On the cloud service **Summary** page, you can view the properties of the selected cloud service.

To view cloud service properties:

1. Select **Cloud services** on the sidebar.
2. Select the name of the cloud service whose details you want to view.  
The **Summary** page opens. It shows the cloud service name, Exchange, SharePoint, OneDrive, and Teams status, Microsoft Azure Active Directory (tenant) ID, WithSecure (tenant) ID, the subscription key, the date when the connection was created, the name of the assigned policy, and the consent URL for Exchange, SharePoint, OneDrive, or all of them.
3. If you want to edit the name of the cloud service, enter the new name in the Name field, and select **Save**.
4. If the status of the cloud service is Disconnected or Pending, you can select **Copy URL**.

**Note:** The URL is used to initiate the connection for external cloud service administrators to grant permissions that are required for protecting the cloud service.

5. Select the **Exchange** tab.  
The Exchange page opens. It shows the setup for mailbox protection.
6. Select the **SharePoint** tab.  
The SharePoint page opens. It shows the setup for site protection.
7. Select the **OneDrive** tab.  
The OneDrive page opens. It shows the setup for drive protection.
8. Select the **Teams** tab.  
The Teams page opens. It shows the setup for channel protection.

### 4.3.2 Changing the assigned policy for a deployed cloud service

Instructions on how to assign a different policy to a cloud service that has already been deployed.

To change the assigned policy:

1. Select **Cloud services** on the sidebar.
2. Select the cloud service for which you want to change the assigned policy.
3. At the bottom of the page, select **Assign policy...**, and from the drop-down menu, select a different policy.
4. Select **Assign** to confirm the action.

The assigned policy is changed for the selected cloud service.

### 4.3.3 Disconnecting a cloud service

Instructions on how to disconnect a cloud service.

To disconnect a cloud service:

1. Select **Cloud services** on the sidebar.
2. Select the cloud service that you want to disconnect.
3. At the bottom of the page, select **Disconnect....**

**Note:** The Disconnect option is available only for cloud services the status of which is either Protected or Connected.

4. In the confirmation window, select **Disconnect** to confirm that you want to disconnect the selected cloud service.

The cloud service is disconnected and no longer protected.

### 4.3.4 Removing a cloud service

Instructions on how to remove a cloud service.

To remove a cloud service:

1. Select **Cloud services** on the sidebar.
2. Select the cloud service that you want to remove.
3. At the bottom of the page, select **Remove....**
4. In the confirmation window, select **Remove** to confirm that you want to disconnect the selected cloud service.

The cloud service is removed from the WithSecure Elements Collaboration Protection service. When you remove a cloud service, all the quarantined items, dashboard statistics, and detections that are associated with the cloud service are also removed from the system.

## 4.4 Managing detections

---

Detections give you information about current security issues.

You can manage detections by updating their status and by entering notes and comments about detections for other system users, which improves the daily management of detections.

### 4.4.1 Filtering detections

You can use filtering to find detections in the WithSecure Elements Collaboration Protection portal.

To filter detections:

1. Select **Detections** on the sidebar.  
The Detections page opens listing all the detections.
2. From the drop-down menu, select a category for filtering the detections:
  - Status
  - Time from
  - Time to
  - Severity - available values:
    - Critical
    - High
    - Medium
    - Low
  - Type of threat - available values:
    - Harmful
    - Suspicious

- Disallowed
- Suspicious inbox rule
- Breached domain account
- User
- SHA-1
- Action taken - available values:
  - Deleted
  - None
  - No action taken
  - Passed
  - Quarantined
  - Subject modified
  - Error
- Detonated in sandbox - available values:
  - Yes
  - No
- Detection ID
- Filename
- Extension
- Cloud service source
- Exchange
  - Sender
  - Subject
  - Inbox rule name
  - Item type (available values: Appointment, Contact, Contact group, Email message, Meeting message, Post item, Task)
  - URL
- SharePoint
  - Item type (available value: SharePoint file)
- OneDrive
  - Item type (available value: OneDrive file)
- Teams
  - Item type (available value: Teams file)

3. In the field next to the category drop-down menu, enter or select a value, and select **Apply**.

4. To reset the selected filter category and the value, select **Clear all**.

**Note:** You can remove a filter by selecting **x** in the text box that appears under the drop-down menu once you have applied a filter.

5. From the drop-down menu on the right, select the cloud service for which you want to view the detections.

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

## 4.4.2 Viewing detections details

You can view the details of detections in the WithSecure Elements Collaboration Protection portal.

You can also view the quarantine items that are associated with the detections.

**Note:** Furthermore, you can report as false positives any URLs that are marked as either suspicious or harmful in the URL section by selecting **Report as false positive** next to the URL which you want to report. The link is then sent to the WithSecure Tactical Defense team for evaluation.

To view detections details:

1. Select **Detections** on the sidebar.  
The **Detections** page opens listing all the detections.
2. Select the name of the detection the details of which you want to see.  
The **Detection details** page opens.

The **Detection details** page shows the details of the selected detection, including its severity and status, affected user, the action taken on the item, the message headers, possible attachments, and URLs.

### 4.4.3 Updating detection status

Instructions on how to update the detection status.

To update the detection status:

1. Select **Detections** on the sidebar.  
The Detections page opens.
2. In the ID column, select the desired detection.  
The Detection details page opens.
3. Select a new status from the Status drop-down menu:
  - New
  - Acknowledged
  - In progress
  - Closed: Resolved
  - Closed: False positive
4. Select **Save**.

**Note:** Alternatively, you can select the checkbox of the desired detection, and then at the bottom of the page, select **Update status**. From the drop-down menu that appears, select a new status and select **Update**.

### 4.4.4 Adding comments

Instructions on how to add comments.

To add a comment:

1. Select **Detections** on the sidebar.  
The Detections page opens.
2. Select the number in the Comments column in the row of the desired detection.  
The Comments window opens.
3. Enter your comment in the Enter comment box, and select **Save**.

### 4.4.5 Viewing comments

Instructions on how to view comments regarding a detection.

To view comments:

1. Select **Detections** on the sidebar.  
The Detections page opens.
2. In the Comments column, select the number in the row of a detection.

**Note:** The number shows how many comments have been entered for the detection.

The Comments window opens showing who has left the comment, the date and time when the comment was left and the actual content.

## 4.5 Managing compromised accounts

---

WithSecure Elements Collaboration Protection detects compromised company email accounts in a domain early in the breach timeline.

Early detection gives the company administrators precious time to validate the user identity and take actions before the data becomes available for broader criminal audience.

A breached account is an easy way for the attacker to get into an organization and take maximum advantage by launching attacks such as internal phishing campaigns, ransomware attacks, or impersonation-based attacks. The attacks that are done using a breached account are hard to detect because they use a legitimate company user account. Detecting compromised accounts as soon as the breach information is available is the key to reclaiming those accounts by a password change or other security measures, such as multi-factor authentication to avoid further exploitation of breached data.

As soon as you deploy the product to protect your organization's Microsoft 365 domain, it checks for possible breach information for the protected email addresses in the domain and notifies you if your company accounts have been compromised.

### 4.5.1 Viewing compromised accounts

You can view the compromised accounts and their details in the WithSecure Elements Collaboration Protection portal

To view compromised accounts:

1. Select **Compromised accounts** on the sidebar.

**Note:** If you see "N/A" in the MFA column in the Compromised accounts table view, you need to refresh the Cloud Service connection to see the MFA status. To refresh the connection, select **Cloud services** on the sidebar, select the cloud service and then select **Refresh** at the bottom of the page.

The Compromised accounts page opens showing the following information:

- The breached email account
- The domain name
- The number of breaches
- The date and time of the last password change
- Whether the breached email account has the multi-factor authorization (MFA) turned on

2. In the Breaches column, select the number.

The **Detection** view opens showing the date and time of the breach, its severity and status, the threat type, the cloud service, the user name, the number of comments, and the location.

3. Select a detection in the ID column to see the detection details.

The **Detection details** page opens showing the following information:

- Breached domain account:
  - Severity
  - Status
  - Details
  - Affected user
  - Breach occurred
  - Cloud service
  - Breach detected
  - Action taken
  - Item type
  - Comments
- Breach details:
  - Breach title
  - Breach type

- Password type
- Password change (at the time of the detection)
- Last password change
- Description

## 4.5.2 Remediation of compromised accounts

This section explains how to resolve compromised accounts.

There are different ways to resolve compromised accounts depending on their severity level.

### **Breached email address (severity level: low)**

This low-level alert indicates that an email address or an email address and a non-crackable hashed password have been breached.

The primary concern here is that the email addresses that have been included in such a breach are being actively shared online by malicious actors. A likely attack scenario would be a spear-phishing campaign.

In a spear-phishing campaign, criminals send fraudulent emails claiming to be from reputable sources to induce unsuspecting individuals to reveal personal information or to open malicious links. We recommend that you carefully examine the links in emails and turn on the multi-factor authentication for your account, if not on yet.

### **Breached email address and password (severity level: medium)**

This medium-level alert indicates that an email address and a plaintext password have been exposed in a data breach. The user has changed the password after the breach happened.

With this type of breaches, the primary concern is the password reuse. The password used for the breached service is compromised and actively shared in dark places. You must change the compromised password and never use it again. In addition, you should change all variations of the compromised password and never use them again. If an attacker has even a few characters of your password, they can crack the entire password. These types of breaches have impacted the most sophisticated users of top-technology companies because of the password reuse. This is a serious concern and often overlooked. We highly recommend that you use a password manager so that all your passwords are unique and easily managed. We also recommend that you turn on the multi-factor authentication for all your passwords.

### **Breached email address and password (severity level: high)**

This high-level alert indicates that an email address and a plaintext password have been exposed in a data breach.

With this type of breaches, the primary concern is the password reuse. The password used for the breached service is compromised and actively shared in dark places. You must change the compromised password and never use it again. In addition, you must change all variations of the compromised password and never use them again. If an attacker has even a few characters of your password, they can crack the entire password. These types of breaches have impacted the most sophisticated users of top-technology companies because of the password reuse. This is a serious concern and often overlooked. We highly recommend that you use a password manager so that all your passwords are unique and easily managed. We also recommend that you turn on the multi-factor authentication for all your passwords.

### **Infected user (severity level: critical)**

Given the source of this breach, a device that you have used has been infected with malicious software. The malicious software logs every keystroke. While your device is infected, changing your password does not solve the problem and is not recommended until the malicious software is removed. Also, while your device is infected, criminals capture every password that you use. We strongly suggest that you power off the infected device until a professional can analyze and remove the malicious software. Given that the malicious software could have been on your device for a long time, all passwords that you have used on this system are compromised. You must change all your passwords using a clean system.

We highly recommend that you use a password manager to simplify and speed up the process of protecting yourself in this situation. We also recommend that you turn on the multi-factor authentication for all your passwords.

## 4.6 Managing policies

---

WithSecure Elements Collaboration Protection uses policies to prevent security threats.

### Related tasks

[Changing the assigned policy for a deployed cloud service](#) on page 20

Instructions on how to assign a different policy to a cloud service that has already been deployed.

### 4.6.1 Setting up the General options

Instructions for setting up the general options for a new policy.

To set up the general options:

1. In the Policy name field, enter a name for the new policy.
2. You can add one or more tags and a description to make it easier to find the policy later.
3. Select **Save**.

Next, set up the privacy options.

### 4.6.2 Setting up privacy options

Instructions for setting up privacy options for a new policy.

To set up the privacy options:

1. In the General tab, select **Privacy**.
2. Select one or more of the following privacy options:
  - Select **Allow sending of non-personalized metadata with file submissions** to send non-personalized metadata together with files to support and enhance the threat analysis.
  - Select **Allow WithSecure to store suspicious executable files for further analysis** to save suspicious executable files to a long-term permanent storage where they are available for later analysis by WithSecure with automated and manual systems.
  - Select **Allow WithSecure to store suspicious non-executable files for further analysis** to save suspicious non-executable files to a long-term permanent storage where they are available for later analysis by WithSecure with automated and manual systems.
  - Select **Allow data to be sent to third-party services used by WithSecure for threat analysis** to allow the sending of file content and metadata or only metadata. The data is used by WithSecure to improve quality of protection and threat analysis.

Next, set up the notifications.

### 4.6.3 Setting up notifications

Instructions for setting up notifications for a new policy.

To set up the notifications:

1. In the General tab, select **Notifications**.
2. In the **Recipient email addresses** field, specify the email addresses of the administrator users who want to receive detection and other administrator email notifications.
3. In the **Sender email address** field, specify the email address from which the detection and other administrator notifications are sent.
4. From the **User notifications based on severity** drop-down menu, select which notifications based on their severity are sent to users: All (Low, Medium, High, Critical); Medium, High & Critical; High & Critical; Critical.
5. Select **Save**.

## Variables used in notification emails

This section lists and describes variables that are used in the user and administrator notification emails that are sent when harmful content or harmful URLs have been detected.

### Variables used in user notifications regarding harmful content

| Variable             | Description                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| \$ITEM-TO            | To whom the item was sent                                                                                       |
| \$ITEM-SUBJECT       | The subject of the item                                                                                         |
| \$ITEM-FOLDER        | The folder in which the item was detected (for example, Inbox)                                                  |
| \$ITEM-SENDER        | The email address of the sender                                                                                 |
| \$ITEM-DATETIME-SENT | The date and time when the harmful content was sent (UTC)                                                       |
| \$TAKEN-ACTION       | The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed) |
| \$QUARANTINE-ID      | The ID of the quarantined item (shown only if the Quarantine feature is turned on).                             |
| \$AFFECTED-FILENAME  | The name of the attachment in which harmful content was detected.                                               |
| \$AFFECTED-FILESIZE  | The size (in bytes) of the attachment with harmful content                                                      |
| \$ATTACHMENT-THREAT  | The type of the threat that was detected in the attachment                                                      |

### Variables used in administrator notifications regarding harmful content

| Variable             | Description                                                    |
|----------------------|----------------------------------------------------------------|
| \$USER-MAILBOX       | The user mailbox in which harmful content was detected         |
| \$ITEM-FOLDER        | The folder in which the item was detected (for example, Inbox) |
| \$ITEM-SUBJECT       | The subject of the item                                        |
| \$ITEM-SENDER        | The email address of the sender                                |
| \$ITEM-TO            | The list of email addresses to which the item was sent         |
| \$ITEM-DATETIME-SENT | The date and time when the harmful content was sent at (UTC)   |

| Variable              | Description                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| \$TAKEN-ACTION        | The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)     |
| \$PORTAL-LINK         | The link to the portal                                                                                              |
| \$QUARANTINE-LINK     | A direct link to the item in the Quarantine view in the portal (shown only if the Quarantine feature is turned on). |
| \$SECURITY-ALERT-LINK | A direct link to the Detections view in the portal                                                                  |
| \$QUARANTINE-ID       | The ID of the quarantined item (shown only if the Quarantine feature is turned on).                                 |

### Variables used in user notifications regarding harmful URLs

| Variable             | Description                                                                                                     |
|----------------------|-----------------------------------------------------------------------------------------------------------------|
| \$ITEM-TO            | To whom the item was sent                                                                                       |
| \$ITEM-SUBJECT       | The subject of the item                                                                                         |
| \$ITEM-FOLDER        | The folder in which the item was detected (for example, Inbox)                                                  |
| \$ITEM-SENDER        | The email address of the sender                                                                                 |
| \$ITEM-DATETIME-SENT | The date and time when the harmful content was sent (UTC)                                                       |
| \$TAKEN-ACTION       | The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed) |
| \$QUARANTINE-ID      | The ID of the quarantined item (shown only if the Quarantine feature is turned on).                             |
| \$AFFECTED-URL       | The defanged or non-clickable URL that triggered the Security alert                                             |
| \$URL-THREAT         | The specific threat or reason why the URL was detected                                                          |

### Variables used in administrator notifications regarding harmful URLs

| Variable       | Description                                            |
|----------------|--------------------------------------------------------|
| \$USER-MAILBOX | The user mailbox in which harmful content was detected |

| Variable              | Description                                                                                                         |
|-----------------------|---------------------------------------------------------------------------------------------------------------------|
| \$ITEM-FOLDER         | The folder in which the item was detected (for example, Inbox)                                                      |
| \$ITEM-SUBJECT        | The subject of the item                                                                                             |
| \$ITEM-SENDER         | The email address of the sender                                                                                     |
| \$ITEM-TO             | The list of email addresses to which the item was sent                                                              |
| \$ITEM-DATETIME-SENT  | The date and time when the harmful content was sent (UTC)                                                           |
| \$TAKEN-ACTION        | The action that was taken, for example, Quarantined, Dropped (i.e., deleted), or No action taken (i.e., passed)     |
| \$PORTAL-LINK         | The link to the portal                                                                                              |
| \$QUARANTINE-LINK     | A direct link to the item in the Quarantine view in the portal (shown only if the Quarantine feature is turned on). |
| \$SECURITY-ALERT-LINK | A direct link to the Detections view in the portal                                                                  |
| \$QUARANTINE-ID       | The ID of the quarantined item (shown only if the Quarantine feature is turned on).                                 |
| \$AFFECTED-URL        | The defanged or non-clickable URL that triggered the detection.                                                     |
| \$URL-THREAT          | The specific threat or reason why the URL was detected                                                              |

## 4.6.4 Setting up the Exchange general options

Instructions for setting up the Exchange general options for a new policy.

To set up the Exchange general options:

1. On the Policies page, select the policy that you just created.  
The General view opens.
2. Select the **Exchange** tab.  
The Exchange General view opens.
3. Turn **Real-time scanning** on to scan email messages and other Exchange items that are saved to user mailboxes.
4. Under **Trusted senders**, do the following to add trusted senders.
  - a) Select **ON**.
  - b) Select **Scan and create a low severity alert for trusted senders when harmful content detected** if you want the system to alert if harmful content is detected.

**Note:** When this option is selected, no action is taken and the email items are passed through.

- c) In the **Trusted email sender addresses** field, add the email addresses of those senders whose email messages are not quarantined or deleted.
  - d) In the **Trusted sender domains** field, add those sender domains that you consider trusted. Email messages coming from those domains not quarantined or deleted.
5. Under **Quarantine**, from the drop-down menu, select the amount of time after which you want old items to be automatically deleted.

## 4.6.5 Setting up the SharePoint general options

Instructions for setting up the SharePoint general options for a new policy.

1. On the **Policies** page, select the policy that you just created.  
The General view opens.
2. Select the **SharePoint** tab.  
The **SharePoint General** view opens.
3. Turn **Real-time scanning** on to scan SharePoint items on the sites in your organization.
4. Under **Quarantine**, from the drop-down menu, select the amount of time after which you want old items to be automatically deleted.
5. Select **Save**.

## 4.6.6 Setting up malware scanning

Instructions for setting up malware scanning for a new policy.

To set up malware scanning:

1. Select of the following solutions for which you want to set up malware scanning:

- Select **Exchange > Malware scanning**
- Select **SharePoint > Malware scanning**
- Select **OneDrive > Malware scanning**
- Select **Teams > Malware scanning**

2. Turn **Malware scanning** on.

**Note:** When on, malware scanning scans email messages for malware and other harmful content. It is available only when the real-time scanning is on.

3. Under **Scan files**, select which file types are scanned for malware and other harmful content: All; Included only; All except excluded.

- If you selected the Included only option, in the **Included files** field, check the list of included file extensions and if needed, add a file extension that identifies the type of file that you want to be scanned for malware and other harmful content.

**Note:** You can select  to copy the email addresses to the clipboard or **Remove all** to empty the field.

- If you selected the All except excluded option, in the **Excluded files** field, check the list of excluded file extensions and if needed, add a file extension that identifies the type of file to be excluded from scanning for malware and other harmful content.
- Select **Scan inside archive (compressed) files** if you want to scan inside archived files.
- Select **Sandbox detonation** if you want to send suspicious files to the Security Cloud to analyze the behavior of the file and decide whether it is clean or harmful.

4. Under **Action**, set up the following:

- From the drop-down menu, select the action that the system takes if malware is detected:
  - for Exchange: Move malicious attachment into quarantine; Move whole item into quarantine; Delete malicious attachment; Delete whole item; Take no action.
  - for SharePoint: Quarantine; Take no action
  - for OneDrive: Quarantine; Take no action

- for Teams: Quarantine; Take no action

**Important:** The deleted items cannot be recovered; instead they are permanently removed.

- Select **Notify the administrator** for the administrators to receive a notification when harmful content is found in user mailboxes.
- Turn **Notify the user about detections with the following severities:** on for the users to receive a notification when harmful content is found in their mailbox.

**Note:** Select **Change** if you want to change the severity level.

**Note:** This option applies only to Exchange.

- Select **Configure notification text** to go to the **Notifications** view. Under **Notifications for malware**, you can enter the text that you want to show in the notification or edit the current notification.

**Note:** This option applies only to Exchange.

5. Select **Save**.

## 4.6.7 Setting up Exchange URL scanning

Instructions for setting up URL scanning for a new policy for Exchange.

To set up URL scanning:

1. On the Policies page, select the policy that you just created.  
The General view opens.
2. Select **Exchange > URL scanning**.
3. Turn **URL scanning** on.

**Note:** When on, URL scanning scans web links (URLs) in bodies of email messages and other Exchange items.

4. Under **Action**, set up the following:

- a) From the **Malicious URL** drop-down menu, select the action that the system takes if a malicious URL is detected: Move item into quarantine; Delete item; Modify the subject; Take no action.

**Important:** The deleted items cannot be recovered, but they are permanently removed.

**Note:** If you select the 'Modify the subject' option, you can edit the message subject that is shown if a harmful link is detected. The default subject is "Malicious URL content".

- b) From the **Suspicious URL** drop-down menu, select the action that the system takes if a suspicious URL is detected: Move item into quarantine; Delete item; Modify the subject; Take no action.

**Important:** The deleted items cannot be recovered; instead they are permanently removed.

**Note:** If you select the 'Modify the subject' option, you can edit the message subject that is shown if a harmful link is detected. The default subject is "Malicious URL content".

- c) Select **Notify the administrator** for the administrators to receive a notification when a harmful or suspicious URL is found in a user mailbox.
- d) Select **Notify the user about detections with the following severities:** for the users to receive a notification when a harmful or suspicious URL is found in their mailbox.

**Note:** Select **Change** if you want to change the severity level.

- e) Select **Configure notification text** to go to the **Notifications** view. Under **Notifications for malicious URL**, you can enter the text that you want to show in the notification or edit the current notification.

5. Turn **Trusted websites** on and set up the following:

- a) Select **Allow reporting of trusted websites to WithSecure** to improve the accuracy of URL detection. The product validates all email URLs against the one defined as a trusted in a policy.
- b) In the **Websites** field, enter addresses of trusted websites to specify the websites that you want to exclude from scanning, for example, example . com or www . mywebpage . com.

If you specify a full URL, the system marks only a domain name as trusted:  
`http://foobar.example.com/?t=true > foobar.example.com.`

**Note:** If `http://foobar.example.com/?t=true` is defined as a trusted website in the Policy settings, the system processes the URLs as described below:

- `www.alpha.foobar.example.com` - passes as trusted
- `http://example.com` - is sent for further analysis

**Note:** You can select  to copy the website addresses to the clipboard or **Remove all** to empty the field.

6. Turn **Blocked websites** on and set up the following:

- a) In the **Websites** field, enter addresses of blocked websites to specify the websites that you want to block, for example, `example.com` or `www.notmywebpage.com`.

If you specify a full URL, the system marks only a domain name as blocked:

`http://foobar.example.com/?t=true > foobar.example.com.` Furthermore, none of the subdomains of the blocked subdomain are allowed.

**Note:** You can select  to copy the website addresses to the clipboard or **Remove all** to empty the field.

**Note:** The Blocked websites setting has higher priority than the trusted one.

Next, set up inbox rules scanning.

## 4.6.8 Setting up Exchange inbox rules scanning

Instructions for setting up inbox rules scanning for a new policy for Exchange.

To set up inbox rules scanning:

1. Select **Exchange > Inbox rules scanning**.
2. Turn **Inbox rules scanning** on.

**Note:** When on, inbox rules scanning detects suspicious inbox rules.

3. Select the inbox rules for which you want to turn detections on:

- Suspicious rule name
- Suspicious auto email moving
- Suspicious email deletion
- Suspicious auto auto-forwarding

4. Under **Action**, set up the following:

- Select **Notify the administrator** for the administrators to receive a notification when a suspicious inbox rule is found in user mailboxes.
- Select **Notify the user about detections with the following severities** for the users to receive a notification when a suspicious inbox rule is found in their mailbox.

## 4.6.9 Setting up the Exchange compromised accounts options

Instructions for setting up the Compromised accounts options for a new policy for Exchange.

To set up the Compromised accounts options:

1. Select **Exchange > Compromised accounts**.
2. Turn **Compromised accounts** on.
3. Under **If an account is found as compromised**, set up the following:
  - Select **Notify the administrator** for the administrator to receive a notification when an account has been detected as compromised.

- Select **Notify the user about detections with the following severities**: for the users to receive a notification when their email account has been detected as compromised.

**Note:** Select **Change** if you want to change the severity level.

**Note:** Even if a user email account has been part of a breach, it does not necessarily mean that the account users themselves have entered the email addresses to the breached site.

4. If you want to set up the user notification text, select **Configure user notification text**.

## 4.6.10 Setting up Exchange notifications

Instructions for setting up notifications for a new policy for Exchange.

To set up Exchange notifications:

1. On the Policies page, select the policy that you just created.  
The General view opens.
2. Select **Exchange > Notifications**.
3. Under **Notifications for malware** and **Notifications for malicious URL**, you can edit the malware and malicious URL email templates for both user and administrator notifications.
4. Under **Notifications for compromised accounts**, based on the severity of the breach (critical, high, medium, or low), you can edit the subject and the text of the notification that is sent to users when their email account or password or both have been detected as part of a breach.
5. Under **Notification for released quarantine item**, you can edit the subject and text of the notification that is sent to users when items are released from the quarantine.
6. Select **Save**.

## 4.7 Managing quarantined items

---

Quarantine is a safe repository for items that may be harmful.

**Note:** Quarantined items cannot spread or cause harm to the company computers. The product can place harmful items in quarantine to make them harmless. You can release items from the quarantine later if you need them. If you do not need a quarantined item, you can delete it. Deleting an item in the quarantine removes it permanently from the cloud service.

In the WithSecure Elements Collaboration Protection portal, you can view the quarantined items, use filtering to find specific ones, and release or delete quarantined items.

### 4.7.1 Filtering quarantined items

You can use filtering to find quarantined items by using different filtering criteria.

**Note:** By default, the Quarantine page is shown with the following Status filters applied: quarantined, failed, and recoverable failure,

To filter the quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, use any of the following criteria:
  - Quarantine ID - enter the quarantine ID of the quarantined message.
  - Status - select the status of the message. You can search for items that are quarantined, deleting, releasing, released, failed, or that have recoverable failure.
  - Time from - select from which date and time on you want to see the quarantined items.
  - Time to - select until which date and time you want to see the quarantined items.
  - Cloud service source: select one of the source options: Exchange, SharePoint, OneDrive, or Teams
  - Exchange
    - Message ID - enter the message ID of the quarantined message.
    - Sender - enter the email address of the message sender. You can only search for one address at a time, but you can widen the search by using the wildcards.

- Mailbox - enter the email address of the message receiver.
- Subject - enter the subject of the message to use it as a search criteria.
- SharePoint
  - Site name - enter the name of the quarantined site.
  - Site URL - enter the URL of the quarantined site.
  - File name - enter the name of the quarantined file.
  - File location - enter the location of the quarantined file.
- OneDrive
  - Drive name - enter the name of the quarantined drive.
  - Drive location - enter the location of the quarantined drive.
  - File name - enter the name of the quarantined file.
  - File location - enter the location of the quarantined file.
- Teams
  - Site name - enter the name of the quarantined site.
  - Site location - enter the location of the quarantined site.
  - File name - enter the name of the quarantined file.
  - File location - enter the location of the quarantined file.

3. Select **Apply**.

4. From the drop-down menu on the right, select the cloud service that you want to view.

The page shows a list of items that were found based on your search criteria.

## 4.7.2 Deleting quarantined items

You can delete quarantined items.

To delete quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, select the items that you want to delete from the quarantine.

**Note:** You can delete up to 200 items at a time.

3. At the bottom of the page, select **Delete**.

The selected items are gradually deleted one by one from the quarantine.

## 4.7.3 Releasing quarantined items

You can release items from the quarantine.

To release quarantined items:

1. Select **Quarantine** on the sidebar.
2. On the Quarantine page, select the items that you want to release from the quarantine.

**Note:** You can release up to 200 items at a time.

3. At the bottom of the page, select **Release**.

The selected items are gradually released from the quarantine.

## Manually recovering quarantined emails

Instructions on how to manually recover quarantined emails after the Cloud Service has been deleted.

The best practice for managing quarantined items is to remove or release them from the quarantine before removing the Cloud Service. Once you have removed a Cloud Service, you no longer can manage any quarantined items for that Cloud Service via the WithSecure Elements Collaboration Protection portal.

**Note:** Creating a new Cloud Service with the same name or Azure AD connection does not grant access to old quarantined items.

After removing a Cloud Service, you can release the quarantined items for the user by using the EWS Editor tool at <https://github.com/dseph/EwsEditor/releases> as follows:

To manually restore quarantined items:

1. Use your administrator credentials to connect to Exchange and impersonate the user.

EWS Editor - 1.21 1.21.1.29558 - EWS Editor - Exchange Service Configuration

Use Autodiscover or use Exchange Web Service URL directly:

☐ Autodiscover Email: Target mailbox. Example: myuser@contoso.com

☒ Service URL: <https://outlook.office365.com/EWS/Exchange.asmx> 365 Default  
Example: <https://mail.contoso.com/EWS/Exchange.asmx>

Note: For Autodiscover against out of network servers such as Exchange Online, you should set disable SCP Autodiscover so that only POX will be used. You can do this from the Global Options window.

EWS Schema Version: Exchange2013  
Set the version of the EWS Schema to use. This is not the same thing as the Exchange version.

☐ Use Default Credentials

☒ Use the following credentials instead of the default Windows credentials.

User Name: administrator@acme.onmicrosoft.com

Password: .....

Domain: acme.onmicrosoft.com

Use credentials of mailbox being accessed or the those of the EWS Impersonation account.  
Suggestion: Use UPN/SMTP address and no domain for Outlook 365.

☐ Use OAuth (Registration must have been completed first)

Redirect URI: <https://microsoft.com/EwsEditor>

Client App ID: 0e4bf2e2-aa7d-46e8-aa12-263adeb3a62b

Server Name: <https://outlook.office365.com>

Auth Authority: <https://login.windows.net/common>

☒ Check if using EWS Impersonation.  
Id Type: SmtptAddress  
Id: user@acme.onmicrosoft.com  
Set to mailbox being accessed using EWS Impersonation.

☐ Set X-AuthorMailbox header.  
SMTP:   
Normally set to the target mailbox when using Impersonation and when accessing a public folder.

☐ Set X-PublicFolderMailbox header.  
SMTP:   
Set when accessing a public folder.

Global Options

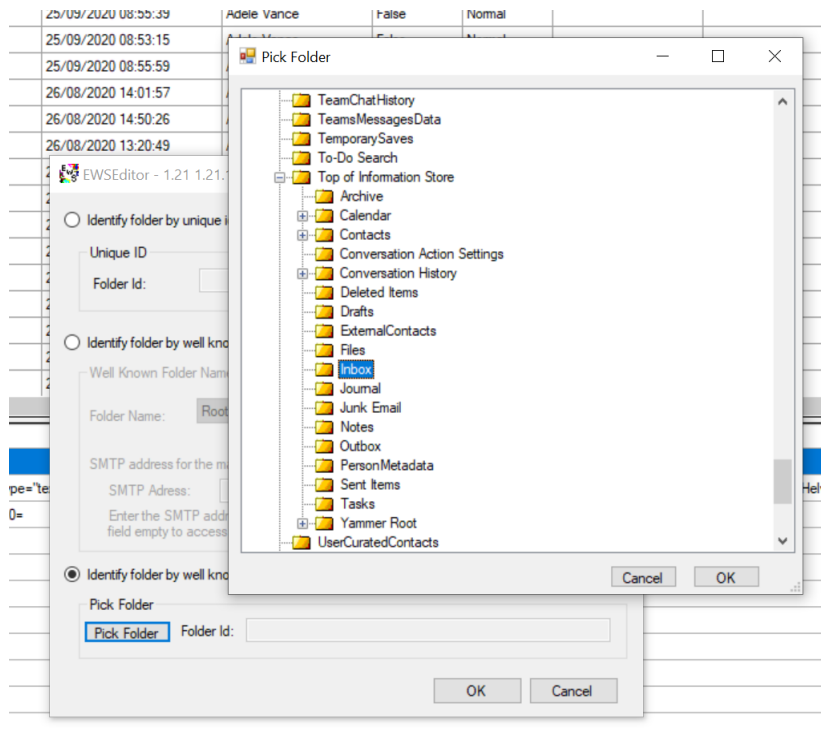
Note: For delegate access: Log in as the delegate then the tree menu select "Add Root Folder...". Use one of the options to add the folder of the mailbox to the folder tree.

Note: It's best to set the X-AuthorMailbox header for Impersonation - it resolves a lot of issue. It also can help with delegate access..

OK Cancel

2. Select **OK**.
3. After configuring the connection, when asked if you want to add the mailbox root to the tree view, select **Yes**.
4. Double-click the **WithSecure Elements Collaboration Protection** folder inside the Root folder.  
A new window that contains all the Exchange items that have been quarantined opens up allowing you to delete or restore the quarantined items.
5. To restore an item, right-click the item and select **Move Item....**
6. In the pop-up window that opens, select **Identify folder by well known name**.

7. In the pop-up window that opens, select **Identify folder by well known name** > **Pick Folder** to select the folder to which you want to restore the item. A good location would be, for example, the Inbox folder under Top of Information Store.



8. Select **OK** > **OK** to restore the item to the desired location.
9. Repeat the steps for any additional items that you want to release or remove.

## 4.8 Managing system events

System events help you understand changes in the state of your system resources or system health. Every action of adding, editing or deleting system resources generates a new system event.

### 4.8.1 Filtering system events

You can use filtering to find system events in the WithSecure Elements Collaboration Protection portal.

To filter system events:

1. Select **System events** on the sidebar.  
The System events page opens listing all the events.
2. From the drop-down menu, select one of the categories to filter the events:
  - Source
  - Level
  - Time from
  - Time to
3. In the field next to the drop-down menu, select a value, and then select **Apply**.  
For the Source category, you can select one of the following values:
  - Provisioning service
  - Policy service
  - Quarantine service
  - Authorization service
  - Email scan service
  - Reporting service

For the Level category, you can select one of the following values:

- Information
- Warning
- Error
- Critical

4. To reset the selected filter category and the value, select **Clear all**.

**Note:** You can remove a filter by selecting **x** in the text box that appears under the drop-down menu once you have applied a filter.

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

## 4.9 Managing reports

---

Scheduled reports give you information about the overall status of the WithSecure Elements Collaboration Protection portal.

On the Scheduled reports page, you can switch a scheduled report task on or off in the Active column. If the scheduled task is switched off (that is, inactive), no report is generated.

### 4.9.1 Generating scheduled report tasks

You can use the portal to generate scheduled reports.

**Note:** Generated reports show the name of the user who created the scheduled task. To change the name, select  at the top right corner, and then select **Account settings**.

To schedule a report:

1. Select **Reports** on the sidebar.  
The Reports view opens.
2. Select **Add new**.  
The **Scheduled report** screen opens.
3. Enter the following information:
  - Report name - give the report a name
  - Organization - as a company administrator, you can only generate a report for your own company  
**Note:** As a partner, you can select the company for which you want to create the report.
  - Frequency - select how often you want the report to be generated
  - Timezone - select the timezone that is used in the report
  - Contents - select which sections of the Dashboard you want to include in the report:
    - Detections by severity
    - Mailbox status
    - Top 10 affected mailboxes
    - Protection status
    - Protection trend
  - Author name - the name of the user who created the scheduled report task.
  - Summary (optional) - enter here text that you want to show in the beginning of the report
4. Select **Save**.  
The new schedule for generating a report is created.

### 4.9.2 Editing scheduled report tasks

Instructions on how to edit the scheduled report tasks.

To edit a scheduled report task:

1. Select **Reports** on the sidebar.

The **Reports** view opens.

2. In the Action column, select  next to the report that you want to edit, and then select **Edit**.  
The Scheduled report screen opens.
3. Make the changes to the report settings, and select **Save**.

### 4.9.3 Downloading and viewing reports

Instructions on how to download and view the generated reports.

To view the reports:

1. Select **Reports** on the sidebar.  
The Reports view opens.
2. Select  next to the scheduled report task that you want to view.  
**Note:** The Reports available column shows if and how many reports are available.
3. Under **Reports ready to download**, select the report that you want to download and view. You can either open the report (PDF file) or save it on your computer.

**Note:** The link shows the date of the report and in how many days the report expires.

### 4.9.4 Cloning scheduled report tasks

Instructions on how to clone schedule report tasks.

To clone a scheduled report task:

1. Select **Reports** on the sidebar.  
The **Reports** view opens.
2. In the Action column, select  next to the report that you want to edit, and then select **Clone**.  
The Scheduled report screen opens.
3. Enter a new name for the report and make any other changes, if needed.
4. Select **Save**  
The new scheduled report task was added.

### 4.9.5 Deleting scheduled report tasks

Instructions on how to delete scheduled report tasks.

To delete a scheduled report task:

1. Select **Reports** on the sidebar.  
The **Reports** view opens.
2. In the Action column, select  next to the report that you want to edit, and then select **Remove**.
3. In the window that opens, select **Remove**.  
The scheduled report is permanently removed and the action cannot be undone.

# Chapter 5

## Support

---

If you cannot find answers to your questions in this guide, you can get more information from the our Help Center, Community forums and the support website.

In our [Help Center](#), you can find user guides for all WithSecure products.

Our [Community forums](#) help you find more troubleshooting information and solutions for known issues.

Go to our [Support request](#) page for instructions on how to contact our technical support team.

# Appendix A

## Specifying Microsoft Azure Active Directory tenant name and ID

---

### Topics:

You need to specify the name and ID for the Microsoft Azure Active Directory tenant.

- [Determining the tenant name of your Azure Active Directory and Office 365](#)
- [Locating the Microsoft Azure Active Directory tenant ID](#)

## A.1 Determining the tenant name of your Azure Active Directory and Office 365

---

The Microsoft Azure Active Directory tenant name is the primary domain that was initially created for Microsoft Office 365.

To determine the tenant name:

1. Log in to [Office 365 Admin Center](#) as an administrator.
2. Under [Setup](#), select [Domains](#) and find a domain that ends with `.onmicrosoft.com`.  
This is your Office 365 tenant name.

## A.2 Locating the Microsoft Azure Active Directory tenant ID

---

Instruction on how to locate the Microsoft Azure Active Directory (AAD) tenant ID in the Office 365 Admin Center.

To locate the tenant ID:

1. Select [Azure Active Directory](#) in the navigation menu.  
The Azure Active Directory (AAD) administrator portal opens.
2. In the AAD administrator portal, select [Azure Active Directory](#)
3. Under Manage, select [Properties](#).

The tenant ID is shown in the Directory ID box.

# Appendix B

## Reporting false positives and false negatives

---

### Topics:

- [Submitting a sample](#)

Security programs sometimes unintentionally identify a program or file as harmful if it has code or behavior that resembles known harmful programs.

This is known as a false positive. False negatives are messages that are considered spam by the end user, but since they were scored below 50 by the MLX engine, they are delivered to the end user.

## B.1 Submitting a sample

---

Instructions on how to report a potentially false positive or negative to WithSecure Labs.

If you think that a file or a URL has been falsely detected, follow these steps to submit the sample to WithSecure Labs for analysis. You can submit multiple URLs or IP addresses by combining them into a text file and submitting them as a file.

**Note:** You can also report a URL as a false positive or false negative through the WithSecure Elements Collaboration Protection portal using the link in the Action column of the URL table on the Detection details page.

To submit a sample:

1. Go to our [Submit a Sample \(SAS\)](#) page.

- If you are submitting a file sample, select the **File Sample** tab. Select **Browse**, and attach your sample file.

**Note:** The maximum file size allowed for uploading is 30MB. You can submit files over 30MB via [FTP](#). You can [zip multiple files](#) if you want to submit them as one archive file.

- For URL sample submission, select the **URL Sample** tab, and enter the URL in the Suspicious URL box.

**Note:** You can submit multiple URLs or IP addresses by combining them into a text file and submitting them as a file.

2. Select the **I want to give more details about this sample and to be notified of the analysis results** option to add in more information and receive feedback on the submitted file or URL sample.

3. Type in the verification Captcha code.

4. Select **Submit sample file**.

# Appendix C

## Manual scanning of suspicious items

---

### Topics:

You can force the scanning of suspicious emails and other items.

- [Manually scanning suspicious Exchange items](#)
- [Manually scanning suspicious SharePoint items](#)

## C.1 Manually scanning suspicious Exchange items

---

Instructions on how to manually scan suspicious Exchange items.

To force the scanning of suspicious emails:

1. Create a new folder in the inbox called "manual scan".
2. Move any suspicious emails to the new folder.

The suspicious emails are automatically scanned. Depending on the action defined in the security policy, an action is taken, for example, the emails are quarantined or an email notification is sent.

## C.2 Manually scanning suspicious SharePoint items

---

Instructions on how to manually scan suspicious SharePoint items.

To force the scanning of suspicious items:

1. Create a new folder in the same location where the files that you want to scan are located.
2. Move any suspicious items to the new folder.

The items are automatically scanned. Within ten minutes, they are detonated and removed if detected as unsafe.