

WithSecure Elements Mobile Protection for Android

Administrator's guide

Contents

| | |
|---|-----------|
| Chapter 1: Introduction..... | 4 |
| 1.1 Why WithSecure Elements Mobile Protection?..... | 5 |
| 1.2 Key features..... | 5 |
| 1.3 System requirements..... | 6 |
| Chapter 2: Deploying the app..... | 7 |
| 2.1 Deploying the app on endpoint devices..... | 8 |
| 2.2 Installing and activating the app on Android devices..... | 8 |
| Chapter 3: Scanning for harmful content..... | 9 |
| 3.1 Manual scanning..... | 10 |
| 3.2 Automatic scanning..... | 10 |
| Chapter 4: Protecting internet traffic..... | 11 |
| 4.1 Turning on network protection..... | 12 |
| 4.2 Turning on Browsing Protection..... | 12 |
| 4.3 Turning on Tracking protection..... | 12 |
| 4.4 Selecting app exceptions..... | 12 |
| 4.5 Viewing the protection statistics..... | 12 |
| Chapter 5: Managing mobile device profiles..... | 14 |
| 5.1 Creating a new mobile device profile..... | 15 |
| 5.2 Turning on Network Gateway..... | 15 |
| 5.3 Turning on reputation-based browsing..... | 15 |
| 5.4 Selecting web content to block..... | 16 |
| 5.5 Allowing and blocking websites..... | 16 |
| 5.6 Selecting app exceptions..... | 16 |
| 5.7 Turning on malware protection..... | 17 |
| 5.8 Turning on metered scan..... | 17 |
| 5.9 Selecting action on infections..... | 17 |
| 5.10 Scheduling scans..... | 18 |
| Chapter 6: Support..... | 19 |
| Appendix A: Exporting log files..... | 20 |
| A.1 How to export log files..... | 21 |
| Appendix B: Using MDM..... | 22 |

| | |
|---|----|
| B.1 Before you begin..... | 23 |
| B.2 Deployment using Google Workspace MDM..... | 23 |
| B.2.1 Adding the Android app to Google Workspace Endpoint Management..... | 23 |
| B.3 Deployment using VMware Workspace ONE MDM..... | 24 |
| B.3.1 Adding the Android app to VMware Workspace ONE MDM..... | 24 |
| B.3.2 Viewing the managed applications..... | 25 |
| B.3.3 Deploying Android Enterprise with VMware Workspace ONE..... | 25 |
| B.4 Deployment using Microsoft Intune MDM..... | 27 |
| B.4.1 Deploying the Android app with Microsoft Intune MDM..... | 27 |
| B.5 Deployment using IBM MaaS360 MDM..... | 29 |
| B.5.1 Deploying Android Enterprise with IBM MaaS360 MDM..... | 30 |
| B.6 Deployment using Ivanti Endpoint Management..... | 31 |
| B.6.1 Deploying the Android app with Ivanti Endpoint Management..... | 31 |
| B.6.2 Android Enterprise deployment with Ivanti Endpoint Management..... | 33 |
| B.7 Deployment using Miradore MDM..... | 33 |
| B.7.1 Adding the Android app to Miradore MDM..... | 34 |
| B.8 Deployment using Samsung Knox..... | 34 |
| B.8.1 Deploying the Android app with Samsung Knox..... | 35 |

Chapter 1

Introduction

Topics:

- [Why WithSecure Elements Mobile Protection?](#)
- [Key features](#)
- [System requirements](#)

This guide gives you general information about the WithSecure Elements Mobile Protection app and its key features.

It gives you instructions on how to activate and administer the app and how to deploy it with an MDM solution.

We socialize and work on our mobile devices – wherever, whenever. The line between work and personal devices is blurry. We use our mobile devices to run daily business operations and take care of personal matters. Mobile devices are also continuously connected to the internet, which makes them an attractive attack vector for cyber criminals

WithSecure (formerly known as F-Secure Business) Elements Mobile Protection is a proactive, streamlined protection solution for your mobile devices. You can prevent cyber-attacks and defend against mobile threats by using our latest innovations in mobile security technology. With the solution, you can fight off phishing attempts coming through various social apps and SMS links, protect your employees from accessing harmful websites, block malware, and keep your business-critical data safe.

WithSecure Elements Endpoint Protection is a module of the WithSecure Elements cyber security platform. The cloud-based platform provides effective protection against ransomware and advanced attacks. Elements brings together vulnerability management, automated patch management, dynamic threat intelligence, continuous behavioral analytics, and security for your cloud collaboration services and infrastructure. You can use individual solutions for specific needs or combine them all seamlessly for maximum defense.

1.1 Why WithSecure Elements Mobile Protection?

Protection against modern mobile threats

With Elements Mobile Protection, you can prevent employees from accessing malicious websites and running risky applications with real-time threat intelligence and security analytics. It provides advanced protection against malware, phishing attacks, and other malicious threats. As an administrator, you can block or allow specific websites and receive detailed reports on blocked URLs.

Unified experience across all your devices

The renewed application supports the latest Android versions. With Network Gateway, you can bridge the gap between different mobile platforms and ensure that all users benefit from our robust security framework, advanced controls, and enhanced network performance. Moreover, all resource-intensive operations have been moved to the cloud, which gives your devices a longer battery life.

Simple and efficient management

Via WithSecure Elements Security Center or your MDM solution, you can easily deploy and manage Elements Mobile Protection. It is easy to install and use, with a user-friendly interface. You have full visibility and control when deploying the app and managing security settings. The solution offers you a centralized visibility for identifying vulnerable and end-of-life operating systems. You receive detailed security event reports that allow you to quickly identify and address potential threats.

1.2 Key features

This section describes the key features of WithSecure Elements Mobile Protection.

Browsing protection

Browsing Protection is a key security layer that proactively prevents end-users from visiting phishing and malicious sites. This early intervention greatly reduces overall exposure to malicious content, and thus attacks.

It is fully browser agnostic, as it works at the network level. This ensures that it provides protection even if the end-user is not using company-sanctioned browsers. It protects end-users who are tricked into accessing seemingly legitimate phishing sites, accessing malicious sites through an email link, or getting infected through malicious third-party advertisements on otherwise legitimate sites.

Browsing Protection works by leveraging real-time threat intelligence and fetching the latest reputation checks of the websites and their files from WithSecure Security Cloud, based on various data points, such as IP addresses, URL keywords, and site behavior.

Virus and threat protection

With our Network Gateway, mobile devices are automatically protected against malware and malicious content. Network Gateway, together with our Security Cloud, scans the traffic at the network level, utilizing the full extent of our security analytics. This allows us to provide better security than traditional mobile security solutions for the following reasons:

- Security level is not compromised by limited mobile device resources.
- Resource-intensive operations are processed in the cloud.
- Network-level scanning proactively blocks contact with malicious content making sure that your system stays secure from the very beginning
- Apps and files are scanned using real-time threat intelligence and security analytics.

Network gateway

Using Network Gateway, Elements Mobile Protection can check every website visited, and by using WithSecure Security Cloud, it can limit access to those sites. Security Cloud provides a URL reputation service, powered by machine learning, which analyses many millions of URLs to check what kind of content those provide. Network Gateway is then used to evaluate the reputation of URLs before they are loaded.

- Harmful sites are fully blocked.
- Sites containing certain categories of content, for example adult or gambling content, can be optionally blocked. These sites are reported to the Elements Security Center so that the administrator can decide if further action is needed.

Note: Visibility of a URL may be restricted in the Security Center due to local legislation related to employee privacy. It is your responsibility as your organization's administrator to ensure the compliance with the local legislation.

- The innovative architecture of Network Gateway eliminates latency and buffering, ensuring a seamless browsing experience.
- Network Gateway provides enhanced security and advanced control by offering a variety of features to protect devices from malicious websites and content.

Simplified management

Our lightweight solution is simple and easy to manage in the cloud. It gives you control over security settings and profiles, and also offers visibility during the deployment:

- The invitations that you send are visible until the installation is done.
- Each email link is unique and allows a single installation within the next 30 days.
- The user interface allows you to easily re-send an invitation or generate a new one with an updated link when the previous one expires.

Flexible deployment methods

WithSecure Elements Mobile Protection integrates seamlessly with all popular Mobile Device Management (MDM) solutions, allowing for comprehensive policy management, such as enforcing minimum operating system versions and device encryption.

1.3 System requirements

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

Supported operating systems

Android 11 and later

Supported languages

The WithSecure Elements Mobile Protection app and documentation are localized into the following languages:

Chinese (Taiwan), Finnish, French, German, Italian, Polish, Portuguese (Brazilian), Spanish (Latin American), and Swedish

Supported MDMs

VMware Workspace ONE, Google Workspace Endpoint Management, IBM Security MaaS360, Microsoft Intune, Miradore, Ivanti Endpoint Management, Samsung Knox

Note: Certificate activation is supported only in the production environment.

Note: User interface optimization is pending for Android tablets.

Chapter 2

Deploying the app

Topics:

- [Deploying the app on endpoint devices](#)
- [Installing and activating the app on Android devices](#)

Instructions on how to install and activate the WithSecure Elements Mobile Protection app.

The app can be activated in Android devices through the WithSecure Elements portal or using an MDM.

Note: For detailed instructions how to deploy the product using a third-party MDM, see the appendix [Using MDM](#) on page 22.

2.1 Deploying the app on endpoint devices

Instructions on how to deploy the app to endpoint devices.

To install WithSecure Elements Mobile Protection on endpoint devices, you must add the new devices to the WithSecure Elements portal and enter user information such as email address and first and last name.

Note: The portal shows the first and last names if they have been added. If they have not been added, the system checks for email address and alias. If none of the information is available, the UUID is shown.

2.2 Installing and activating the app on Android devices

Instruct the users to follow these steps to install the app on their Android devices.

Note: In the following steps, "you" refers to end users.

You receive an email from your administrator instructing you to install the app. The email contains a link for installing the app on one device and a link to activate your license.

To install the app:

1. Open the invitation email.

2. Select the link next to Android.

You are redirected to Google Play Store where you can download and install the WithSecure Mobile Protection app.

3. After you have installed the app on your device, go back to the installation email and select **Activate for Android** to activate the subscription.

Note: The activation link is valid for 29 days, but you can only use the link once. If you log in to the app using the username and password that are provided in the email, but you do not manage to activate the license, you can try using the activation link. If you, however, first select the activation link and, for some reason, it does not work, you can no longer manually enter the credentials.

The WithSecure Mobile Protection app opens.

4. When asked, select **Allow** to give the app the required permissions.

Note: The app needs permission to access your photos, media, and files to be able to scan for harmful items.

Chapter 3

Scanning for harmful content

Topics:

- [Manual scanning](#)
- [Automatic scanning](#)

The product scans your device for harmful content and other threats to your device and data.

3.1 Manual scanning

You can scan your device for viruses and other threats at any time.

To manually scan files on your device:

1. On main the view, select **Malware protection**.
2. Tap **Scan**.
The scan starts.
3. After the scan is finished, the product shows the following information:
 - Total files checked - the number of the files that were scanned
 - Total apps checked - the number of applications that were scanned


Note: By selecting **Scan history**, you can see the dates and times of the manual and automatic scans.

3.2 Automatic scanning

By default, the app automatically scans your device for viruses and other threats.

When the Antivirus option is on, the app automatically scans the device, for example, every time an installed app is updated, when the device restarts, or an SD card is mounted.

To automatically scan files on your device:

1. On the main view, select .
2. On the **Settings** view, select **Malware Protection**.
3. Turn on **Antivirus is ON**.
The app automatically scans new apps and files daily.
4. Turn on **Metered scan ON** if you want the app to scan your device even when the device is on a metered network connection.

Note: Turning this option on may result in increased data traffic.

Protecting internet traffic

Topics:

- [Turning on network protection](#)
- [Turning on Browsing Protection](#)
- [Turning on Tracking protection](#)
- [Selecting app exceptions](#)
- [Viewing the protection statistics](#)

Network Gateway is used to evaluate the reputation of URLs before they are loaded.

By using WithSecure Security Cloud, it can limit access to those sites. Security Cloud provides a URL reputation service that is powered by machine learning, which analyses millions of URLs to check what kind of content they provide.

Network Gateway gives you advanced control over URL blocking and allowlisting. You can block entire categories of websites to prevent access to specific types of content, such as adult, gambling, or social media sites. Additionally, you can allowlist specific URLs, allowing users to access approved websites that may be blocked by default.

With Network Gateway, all users, regardless of their device and mobile platform, benefit from our security framework and network performance. Whether you are using our Network Gateway directly or relying on a third-party service, it provides unified protection and accelerated performance. All users are shielded from harmful websites and equipped with advanced control over their online experiences.

Additionally, Network Gateway provides enhanced security and advanced control for Android devices. It offers a variety of features to protect devices from malicious websites and content.

4.1 Turning on network protection

When you turn on the protection, Elements Mobile Protection evaluates the reputation of URLs before the websites are loaded..

To turn on Network Protection:

1. On the main view, select **Network Protection**.
The **Network Protection** screen opens.
2. Tap **Protection OFF** to activate protection.


Your network is now protected.

4.2 Turning on Browsing Protection

Browsing Protection blocks web sites that are suspicious or known to be malicious.

Note: To use Browsing Protection, Network Protection must be on.

To turn on Browsing Protection:


1. On the main view, select **Network Protection**.
The **Network Protection** view opens.
2. Select .
3. On the view that opens, turn on **Browsing protection**.

4.3 Turning on Tracking protection

Tracking protection blocks advertisers from monitoring your online behavior.

Note: To use Tracking protection, Network Protection must be on.


To turn on Tracking protection:

1. On the main view, select **Network Protection**.
The **Network Protection** view opens.
2. Select .
3. On the view that opens, turn on **Tracking protection**.

4.4 Selecting app exceptions

Instructions on how to select apps that you want to connect to the internet directly, bypassing the protection of Network Gateway.

To select the apps:

1. On the main view, select **Network Protection**.
The **Network Protection** screen opens.
2. At the top-right corner, select , and then select **App Exceptions**.
3. On the view that opens, from the list of apps, select those that you want to connect to the internet directly.

The apps that you selected connect directly to the internet, bypassing the protection of Network Gateway.

4.5 Viewing the protection statistics

On the Traffic Protection view, you can see how many threats the app has blocked.

Note: The number of blocked tracking attempts and harmful sites is shown only if Browsing protection and Tracking protection are on. Whether these features are on or off depends on the profile that is assigned to the device.

To view the statistics:

1. Open the app.
2. Tap **Network Protection**.
3. On the **Network Protection** screen, tap **Internet traffic protected**.
The **Traffic Protection** screen shows you how many tracking attempts and harmful sites the app has blocked.
4. Turn on **Record tracking details** to start logging.
Note: The logging lasts for 24 hours. The log is automatically erased after three days. It is also erased every time you start recording a new log.
5. To view the log, tap **Last recorded logs**.

Chapter 5

Managing mobile device profiles

Topics:


- [Creating a new mobile device profile](#)
- [Turning on Network Gateway](#)
- [Turning on reputation-based browsing](#)
- [Selecting web content to block](#)
- [Allowing and blocking websites](#)
- [Selecting app exceptions](#)
- [Turning on malware protection](#)
- [Turning on metered scan](#)
- [Selecting action on infections](#)
- [Scheduling scans](#)

Information on how to manage mobile device profiles in the WithSecure Elements Endpoint Protection portal.

5.1 Creating a new mobile device profile

You can create profiles that can be assigned to specific mobile devices.

To create a new profile:

1. Log in to the WithSecure Elements portal.
2. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
3. Select the **For Mobile** tab.
4. Select  next to an existing profile, and select **Clone profile**
The **Profile for Mobile Protection** page opens.
5. Enter a name and description for the new profile, and select a type for the new profile.
6. Make desired changes to the settings, and then select **Save and Publish**.
The new profile is created.

5.2 Turning on Network Gateway

Network Gateway keeps mobile phone apps safe by checking their internet traffic for threats and blocking malicious requests.

To turn on Network Gateway:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
3. Under **Network Protection**, turn on **Network Gateway**.
Note: You can select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.
4. Select **Save and Publish**.
Your changes are saved and published to the current profile.

5.3 Turning on reputation-based browsing

Reputation-based browsing blocks websites that are suspicious or known to be malicious.

To turn on Reputation-based browsing:


1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
4. Under **Network Protection**, turn on **Reputation-based browsing**.
5. Under **Reputation-based browsing**, you can turn on the following:
 - **Block access when website is rated harmful**
 - **Block access when website is rated as suspicious**
 - **Block access when website is rated as prohibited**
 - **Block access when website contains trackers****Note:** Select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.
6. Select **Save and Publish**.
Your changes are saved and published to the current profile.

5.4 Selecting web content to block

You can select the types of web content that you want to block.

Web content control blocks websites based on their content.

Note: Turning on the Unknown category blocks access to websites whose reputation is unknown.

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
4. From the menu on the left, select **Network Protection**, and scroll down to **Web content control**.
5. Turn on **Web content control**.
6. Select  next to **Web content control**.
The list of web content categories opens.
7. In the **Disallowed** column, turn on the categories that you want to block for mobile devices.
8. In the **Alert** column, turn on the categories for which you want a security event to be sent.

Note: If you turn on **Block everything except allowed sites**, it overrides your selections in the **Web content control** table.

9. Select **Save and Publish**.

5.5 Allowing and blocking websites

You can add websites to the allowed and denied websites list.

To allow or block websites:


1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the desired profile.
The **Profile for Mobile** page opens.
4. From the menu on the left, select **Network Protection**, and scroll down to **Website exceptions**.
5. Under **Web site exceptions**, do the following:
 - a) To allow a website, under **Allowed sites**, select **Add site** and enter the website URL in the **Address** field.
 - b) To block a website, under **Denied sites**, select **Add site** and enter the website URL in the **Address** field.

Note: You can enter a description in the **Notes** field.

5.6 Selecting app exceptions

Instructions on how to select apps that you want to connect to the internet directly, bypassing the protection of Network Gateway.

To select the apps:

1. On the main view, select **Network Protection**.
The **Network Protection** screen opens.
2. At the top-right corner, select , and then select **App Exceptions**.
3. On the view that opens, from the list of apps, select those that you want to connect to the internet directly.
The apps that you selected connect directly to the internet, bypassing the protection of Network Gateway.

5.7 Turning on malware protection

When on, malware protection scans files and applications.

Note: This applies only to Android devices.

To turn on malware protection:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
4. From the left pane, select **Malware Protection**.
5. Turn on **Malware Protection**.

Note: Select the lock icon next to a setting to lock or unlock it. When a setting is locked, it prevents users from changing it.

6. Select **Save and Publish**.
Your changes are saved and published to the current profile.

5.8 Turning on metered scan

A metered network connection has a limit on how much data can be used.

You can allow scanning over metered connections. Exceeding the limit may incur extra costs.

Note: This applies only to Android devices.

To turn on metered scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
4. From the left pane, select **Malware Protection**.
5. Turn on **Metered scan**.
6. Select **Save and Publish**.
Your changes are saved and published to the current profile.

5.9 Selecting action on infections

You can select an action for infected objects.

Note: This applies only to Android devices.

To select an action:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
4. From the menu on the left, select **Malware Protection**.
5. From the **Action on infections** drop-down menu, select the desired action for infected objects:
 - Delete - this option automatically removes the infected objects from your device
 - Ask after scan - you need to manually remove the infected objects from your device

5.10 Scheduling scans

Set your device to scan and remove malware and other harmful applications automatically periodically to make sure that your device is secure.

Note: This applies only to Android devices.

To schedule a scan:

1. Under **Security Configurations**, select **Profiles** on the sidebar.
The **Profiles** page opens.
2. Select the **For Mobile** tab.
3. Select the profile that you want to edit.
The **Profile for Mobile** page opens.
4. From the menu on the left, select **Malware Protection**, and scroll down to **Scheduled scanning**.
5. Turn on **Scheduled scanning**.
6. Select the arrow next to **Scheduled scanning**.
The **Scan frequency** drop-down menu appears.
7. From the drop-down menu, select how often you want to scan your device automatically.

| Option | Description |
|------------------|--|
| Daily | Scan your device every day. |
| Weekly | Scan your device on selected days of the week. Select the weekday from the list. |
| Every four weeks | Scan your device on a selected weekday at four-week intervals. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday. |
| Monthly | Scan your device on a selected weekday every month. Select the weekday from the list. The scan starts on the next occurrence of the selected weekday. |

8. Select **Save and publish**.
Your changes are saved and published to the current profile.

Chapter 6

Support

We are looking forward to receiving comments and feedback on the product functionality, usability, and performance.

You can report any technical issues through the WithSecure support website [here](#).

Appendix A

Exporting log files

Topics:

- [How to export log files](#)


If you have a technical issue, the technical support may ask you to export and send log files for investigation.

This section explains how to export log files on activated and non-activated apps on mobile devices.

A.1 How to export log files

Instructions on how to export a log file on an activated or non-activated app on Android devices.

If you are reporting a technical issue, attach the log file to the feedback as follows:

1. Open the Elements Mobile Protection app.
2. On the main view, tap .
The **Settings** view opens.
3. Tap **About App**.
The **About App** view opens.
4. Under **Mobile Protection**, tap the version number seven times.
The **Send log** button appears.
5. Follow the instructions on the screen.

Appendix

B

Using MDM

Topics:

- [Before you begin](#)
- [Deployment using Google Workspace MDM](#)
- [Deployment using VMware Workspace ONE MDM](#)
- [Deployment using Microsoft Intune MDM](#)
- [Deployment using IBM MaaS360 MDM](#)
- [Deployment using Ivanti Endpoint Management](#)
- [Deployment using Miradore MDM](#)
- [Deployment using Samsung Knox](#)

This section describes how the WithSecure Elements Mobile Protection app can be integrated with MDM.

WithSecure Elements Mobile Protection is perfect for organizations that want to provide additional security for their mobile devices on top of the basic security features that their existing MDM solution already provides. The solution greatly enhances your security against malware, phishing, and data theft, among others.

WithSecure Elements Mobile Protection can be integrated with the following MDMs: Google Workspace Endpoint Management, VMware Workspace ONE, Microsoft Intune, IBM Security MaaS360, Ivanti Endpoint Management (formerly known as MobileIron Cloud), Miradore, and Samsung Knox.

You can deploy WithSecure Elements Mobile Protection per profile enrolment, which means that if the end device has both personal and work profiles, you need to install the app on both profiles.

Tip: We strongly recommend that you test the enrolment on one device first.

Note: Variables are usually defined when WithSecure Elements Mobile Protection is configured on an MDM platform. The variables define whether the app is registered with an email address, username, or UUID. For example:

- If you do not configure the app, it uses the UUID, which shows under the device name in the WithSecure Elements portal.
- If you configure email addresses, they show under the device name in the portal.

Once you have configured the app on an MDM platform, you should not change it. If you do decide to change it, you need to first remove the devices from the WithSecure Elements portal and also remove the app from the MDM agent because it will create duplicates.

B.1 Before you begin

The app can be activated in mobile devices by using an MDM or through the WithSecure Elements portal by inviting users.

B.2 Deployment using Google Workspace MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with Google Workspace MDM to Android devices.

B.2.1 Adding the Android app to Google Workspace Endpoint Management

Instructions on how to add WithSecure Elements Mobile Protection as an allowed app to Google Workspace MDM in Android devices.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

To add the product to Google Workspace MDM:

1. Log in to your Google Workspace Admin console.
2. On the Dashboard, select **Apps > Web and mobile apps**.
3. On the **Web and mobile apps** page, select **Add App > Add private Android app**.
4. On the **Managed Android apps** page, select **Search Play Store** and enter `mobile protection elements` in the search box.
5. Select the app and then select **Approve > Select**.
6. Under **User access**, select your preferred option and select **Continue**.
7. Under **Access method**, select your preferred options and select **Finish**.

The Android app is added to Google Workspace MDM.

Configuring the Android app

Instructions on how to configure the Android app.

Note: Google Workspace does not support variables. However, the Registration key field accepts a subscription key as a variable in standard format. Therefore, enter the subscription key as is, but do not enter an email address. If you do, all your devices are shown with the same email address in the WithSecure Elements Endpoint Protection portal. When you leave the email address empty, the devices that have WithSecure Elements Mobile Protection installed are shown with a Device UUID.

1. On the **Admin Console** page, under **Managed configurations**, select **Add managed configuration**.
2. On the Managed configuration page, enter a name for the configuration and do the following:
 - a) In the Registration key field, enter the product subscription key.
You can find the subscription key in the WithSecure Elements Security Center under **Endpoint Protection Subscriptions**.
 - b) Enter your first and last name in the respective fields (optional).
 - c) In the Alias field (optional), enter an alternate name.
 - d) In the Email address field (optional), enter your email address.
 - e) In the Environment field (optional), enter 2.
3. Select **Save**.

B.3 Deployment using VMware Workspace ONE MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with VMware Workspace ONE (formerly known as Airwatch) MDM to Android and iOS devices.

Note: These instructions do not include information on how to create and configure users and devices.

B.3.1 Adding the Android app to VMware Workspace ONE MDM

Instructions on how to add the WithSecure Elements Mobile Protection Android app to VMware Workspace ONE MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

1. On the VMware Workspace ONE administration portal, go to **Apps and Books** and select **Native**.
2. Next, in the Public tab, select **Add application**.
3. On the Add Application page, do the following:
 - a) From the **Platform** drop-down menu, select **Android**.
 - b) In the **Source** field, select **Search App store**.
 - c) In the **Name** field, enter WithSecure Elements Mobile Protection.
 - d) Select **Next**.
4. In the Apps view, select **WithSecure Elements Mobile Protection**.
5. In the **WithSecure Elements Mobile Protection** view, select **Approve > Select**.
6. In the Edit Application view, select the **Terms of Use** tab.
7. From the **SDK** drop-down menu, select **MP strings@ WithSecure**.
8. Select **Save and assign**.

B.3.2 Viewing the managed applications

Instructions on how to view managed applications in VMware Workspace ONE MDM.

1. In the VMware Workspace ONE console window, select **Apps&Books** and then under **Applications**, select **List View**.
The List View page opens
2. Select the **Public** tab.
The WithSecure Elements Mobile Protection app appears in the Apps list on the VMware Workspace ONE administration portal.

B.3.3 Deploying Android Enterprise with VMware Workspace ONE

This chapter contains instructions on how to deploy the WithSecure Elements Mobile Protection app in the Android Enterprise context with VMware Workspace ONE.

Setting up Android Enterprise in VMware Workspace ONE MDM

Instructions on how to set up the WithSecure Elements Mobile Protection Android app in the Android Enterprise context.

To deploy the app in the Android Enterprise context, the company must have Google Administrator account. All the users must have accounts there, either predefined or generated during the enrollment.

The domain administrator has to generate an EMM token and a certificate, and bind VMware Workspace ONE as an EMM provider.

To set up Android Enterprise:

1. Log into the VMware Workspace ONE administration portal.
2. Go to **Groups and Settings** and select **All Settings**.
3. In the Settings view, under **Devices and Users**, select **Android**.
4. Under **Android**, select **Android EMM Registration**.
5. Select the account icon at the top right corner and select **Manage your Google Account**.
6. Log in with your email and password.
7. On the Bring Android to Work page, select **Get started**.
The Android EMM Registration page opens.
8. When the service account is set up, accept the settings in the **Enrollment Settings** and **Enrollment Restrictions** tabs, and select **Save**.
The settings are saved.

Adding profiles in VMware Workspace ONE

Instructions on how to add profiles.

1. On the VMware Workspace ONE administration portal, go to **Apps & Books > All Apps & Books Settings**
The Settings page opens.
2. On the navigation pane, select **Settings and Policies > Profiles**.
The Profiles view opens.
3. Select **Add Profile > SDK Profile > Android**
The Add a New Android Profile page opens.
4. Select **General**, enter a name and description for the new profile, and select **Save**.

Adding the Android app

Instructions on how to add the WithSecure Elements Mobile Protection Android app in the Android Enterprise context to VMware Workspace ONE MDM.

1. On the VMware Workspace ONE administration portal, go to **Apps & Books > Applications > Native**.

The List view opens

2. Select the **Public** tab, and then **Add application**.
3. In the Add Application view, do the following:
 - a) From the **Platform** drop-down menu, select **Android**.
 - b) Enter the application name: `mobile protection elements`.
 - c) Select **Next**.
The **Apps** page opens.
4. Select **WithSecure Elements Mobile Protection**.
5. In the WithSecure Elements Mobile Protection view, select **Approve > Select**.
The Edit application view opens.
6. Select the **SDK** tab, and from the **Application Profile** drop-down menu, select **MP strings @ WithSecure**.
7. Select **Save and assign**.
The WithSecure Elements Mobile Protection - Assignment page opens.
8. Select **Distribution** and do the following:
 - a) In the Name field, enter a name for the distribution, for example, `alldevices`.
 - b) In the Assignment groups, select your preferred device distribution group.
9. Next, select **Application Configuration** and do the following:
 - a) In the **Registration key** field, enter the product subscription key.

Note: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Endpoint Protection > Subscriptions**.
 - b) In the First name (optional) field, enter **{FirstName}**
 - c) In the Last name (optional) field, enter **{LastName}**
 - d) In the Alias (optional) field, enter **{EnrollmentUser}**
 - e) In the Email (optional) field, enter **{EmailAddress}**
 - f) Select **Create**.
The Assignments tab opens.
10. Select **Save**.
The Preview Assigned Devices page opens.
11. Select **Publish**.

Configuring the Android app

Instructions on how to configure the WithSecure Elements Mobile Protection Android app in VMware Workspace ONE MDM in the Android Enterprise context.

To configure the Android app:

1. On the VMware Workspace ONE administration portal, select the **Edit Application** page.
2. Select the **Assignment** tab and define the assignment group.
3. Select **Send Application Configuration**.
4. Under **Configuration Key**, add values to the following configuration entries:

Note: The reseller provides you with the values.

- `fate_registration_key` - the license key
- `first_name` (optional) - a name that makes it easier to identify the user in the WithSecure Elements Endpoint Protection portal
- `last_name` (optional) - a name that makes it easier to identify the user in the WithSecure Elements Endpoint Protection portal

For the optional keys, select **Insert Lookup Value** and select respective variables. The fields are automatically filled when the application is deployed to user devices.


5. Fill the rest of the app settings under **Details and Assignment**, and select **Save and Publish** to add the app to **List View**.

Using certificates to register devices

Instructions on how to register devices using a certificate.

Note: You must have a subscription for WithSecure Elements Mobile Protection with External MDM to do this.

To register a device using a certificate:

1. Log in to the WithSecure Elements Endpoint Protection portal with your company administrator account.
2. Under **Subscriptions**, select  and then select **External MDM server configuration**
3. Download and save the certificate file.
4. On the VMware Workspace ONE administration portal, go to **Resources Profiles & Baselines > Add new Profile**.

Note: You can also use an existing profile to pre-configure the certificate.

5. Under **Credentials**, select **Add** to upload the certificate that you downloaded from the WithSecure Elements Endpoint Protection portal.
6. Select **Save and publish**.
7. Assign the profile to your devices.

B.4 Deployment using Microsoft Intune MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with Microsoft Intune MDM to Android and iOS devices.

B.4.1 Deploying the Android app with Microsoft Intune MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with Microsoft Intune MDM.

Adding the Android app to Microsoft Intune MDM

Instructions on how to add the WithSecure Elements Mobile Protection Android app to Microsoft Intune MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

1. Log into your Microsoft Intune portal.
2. Select **Apps > Android > Add**.

- The **Select app type** pane opens.
3. From the **App type** drop-down menu, select **Managed Google Play app**, and then select **Select**.
 4. In the **Managed Google Play** view, in the Search field, enter `WithSecure Elements`.
The **Apps** view opens.
 5. Select **WithSecure Elements Mobile Protection**.
 6. On the view that opens, select **Approve > Approve**.
 7. In the **Approval settings** tab, select **Keep approved when app requests new permissions**, and select **Done**.
The **Managed Google Play** view opens.
 8. Select **Sync** at the top left corner.
The **Android Apps** view opens.
 9. Select **Refresh** and then select **WithSecure Elements Mobile Protection**.
The **WithSecure Elements Mobile Protection** view opens.
 10. Under **Manage**, select **Properties**.
The **WithSecure Elements Mobile Protection Properties** view opens.
 11. Next to **Assignments**, select **Edit**.
The **Edit Application** view opens.
 12. In the **Assignments** tab, do the following:
 - a) Under **Required**, select **Add all users**.
 - b) Select **Review + save**.
 - c) In the **Review + save tab**, select **Save**.

The WithSecure Elements Mobile Protection app has been added to Microsoft Intune MDM.

Next, add the app configuration policies.

Adding the Android app configuration policies

Instructions on how to add the WithSecure Elements Mobile Protection configuration policies for managed Android devices.

1. Select **Apps**.
The Apps overview pane opens.
2. Under **Policy**, select **App configuration policies**.
3. Select **Add > Managed devices**
The Create app configuration policy pane opens.
4. In the **Basics** tab, do the following:
 - a) In the **Name** field, enter `WithSecure Mobile Protection`.
 - b) From the Platform drop-down menu, select **Android Enterprise**.
 - c) From the Profile type drop-down menu, select **Personally-Owned Work Profile Only**.
 - d) Next to **Targeted app**, select **Select app**.
The Associated app pane opens.
 - e) Select **WithSecure Elements Mobile Protection**, and select **OK > Next**.
The Settings tab opens.
5. Do the following:
 - a) Under **Configuration Settings**, from the Configuration settings format drop-down menu, select **Use configuration designer**.
 - b) Select **+Add**.
 - c) On the pane that opens at the right, select the following:
 - Registration key
 - Alias (optional)
 - Email address (optional)
 - Environment (optional)
 - d) Select **OK**.
 - e) Select the value types and enter the configuration values for the following configuration keys:

- `fate_registration_key`: value type: **String**; configuration value: [WithSecure Elements Mobile Protection subscription key].

Note: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Management > Subscriptions**.

- `alias`: value type: **String**; configuration value: { {username} }
- `email`: value type: **String**; configuration value: { {mail} }
- `env`: value type: **Integer**; configuration value: 2

Note: The `env` configuration key and its value define where the VPN endpoint connects to.

- Select **Next**.
The **Assignments** tab opens.
- Under **Included groups**, select **Add all users** and select **Next**.
The **Review + create** tab opens.
- Select **Create**.

The app configuration policy was created and assigned.

You need to install the app on an Android device.

Granting permissions to an app

Instructions on how to grant permission to an app for a silent activation.

1. Log in to the Microsoft Endpoint Manager administrator center.
2. Select **Apps > App configuration policies > Add > Managed devices**.

Note: You can choose to add either managed devices or managed apps. For more information, see [Apps that support app configuration](#).

3. On the **Basics** page, enter the following details:
 - Name - a name for the profile that is shown in the portal
 - Description - a description for the profile that is shown in the portal
 - Device enrollment type - the default option is **Managed devices**
4. Under **Platforms**, select **Android Enterprises**.
5. Next to **Targeted app**, choose **Select app**.
The **Associated app** pane opens.
6. On the **Associated app** pane, select the managed app that you want to associate with the configuration policy, and select **OK**.
7. Select **Next > Add**.
The **Add permissions** pane opens.
8. Select the permissions that you want to override.

Note: The granted permissions override the default app permissions policy for the selected apps.
9. Set a permission state for each permission. You can select from the following options:
 - Prompt - ask the user to accept or deny
 - Auto grant - automatically approve without notifying the user
 - Auto deny - automatically deny without notifying the user
10. Select **Review + save**.
Your settings are saved.

B.5 Deployment using IBM MaaS360 MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with IBM MaaS360 MDM to Android and iOS devices.

B.5.1 Deploying Android Enterprise with IBM MaaS360 MDM

This chapter contains instructions on how to deploy the WithSecure Elements Mobile Protection app in the Android Enterprise context with IBM MaaS360 MDM.

Configuring Android Enterprise

Instructions on how to configure Android Enterprise.

Note: Prior to enrolling devices, you need to configure Android Enterprise.

1. On the IBM MaaS360 administration portal, select **Setup > Services**.
2. Under **Mobile Device Management, Enable Android Enterprise Solution Set Enable via Managed Google Play Accounts (no G-suite for business)**, select **here**.
The **Confirm Android Managed Google Play Accounts Enablement** window.
3. Select **Enable**.
4. In the **Security Check** window, enter your password and select **Confirm**.
Google Play opens.
5. On the **Bring Android to work** page, select **Get started** and do the following:
 - a) Enter the name of your business and select **Next**.
 - b) On the Contact details page, enter your name, email, and phone number (optional), select **I have read and agree to the Managed Google Play agreement** option, and then select **Confirm**.
6. Select **Complete Registration**.
You have completed the setup.

Next, you need to add the WithSecure Elements Mobile Protection app.

Adding the WithSecure Elements Mobile Protection app

Instructions on how to add the WithSecure Elements Mobile Protection app to IBM MaaS360 MDM.

1. On the IBM MaaS360 administration portal, select **Apps > Catalog**.
2. On the App Catalog page, select **Add > Android > Google Play App**.
3. In the Search box, enter `WithSecure Elements Mobile Protection`.
4. Select **WithSecure Elements Mobile Protection**, and select **Select**.
5. In the Approve Permission window, select **Approve** to add the app.

Next, you need to configure the app.

Configuring the app

Instruction son how to configure the WithSecure Elements Mobile Protection app.

1. In the Add Google Play App window, in the **Configuration** tab, select **Configure App Settings** and do the following:
 - a) In the Registration field, enter the product subscription key.
Note: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Endpoint Protection > Subscriptions**.
 - b) Enter your first and last name in the respective fields (optional).
 - c) In the Alias field (optional), enter an alternate name.
 - d) In the Email address field (optional), enter your email address
 - e) In the Environment field (optional), enter 2.
2. Select **Add**.
The **Security Check** window opens.
3. Enter your password and select **Confirm**.
The app was added.

Distributing the app

Instructions on how to distribute the app to the selected targets.

1. On the App Catalog page, under **WithSecure Elements Mobile Protection**, select **View**.
2. On the page that opens, at the top-right corner, select **Distribute**.
The Distribute App window opens.
3. From the Target drop-down menu, select one of the options:
 - Specific device
 - Group
 - All devices
4. Select **Distribute**.

B.6 Deployment using Ivanti Endpoint Management


Instructions on how to deploy the WithSecure Elements Mobile Protection app with Ivanti Endpoint Management (formerly known as MobileIron Cloud MDM) to Android and iOS devices.

B.6.1 Deploying the Android app with Ivanti Endpoint Management

Instructions on how to deploy the Android app with Ivanti Endpoint Management.

You can configure WithSecure Elements Mobile Protection in one of the following ways:

- Configure the app manually by adding the subscription key and other variables in Ivanti Endpoint Management under **App Configurations Managed Configurations for Android**.
- Configure the app using MDM server configuration certificates that you can download from the

WithSecure Elements portal. You can find the certificate by going to **Subscriptions** and selecting  at the end of the WithSecure Elements Mobile Protection row.

Adding the WithSecure Elements Mobile Protection Android app to Ivanti Endpoint Management

Instructions on how to add the WithSecure Elements Mobile Protection Android app to Ivanti Endpoint Management MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

To add the Android app to Ivanti Endpoint Management:

1. In the Ivanti Endpoint Management MDM administration portal, go to **Apps** and select **Add**.
2. From the menu, select **Google Play**.
3. Search for `WithSecure Elements Mobile Protection`.
4. Select the app, and then click **Select**.
5. Check that the app category is correct. Optionally, you can add app information in the Description box.
6. Select **Next**.
7. Select whether you want to delegate the app to all spaces, and select **Next**.
8. Select the preferred distribution group and press **Next**.

Next, you need to configure the app.

Manually configuring the Android app management

Instructions on how to manually configure the Android app management.

1. Under **App Configurations** > **Managed Configurations for Android**, select the plus icon. The **Configuration Setup** view opens.
2. Do the following:
 - a) Enter a name for the configuration.
 - b) Under **Managed Configurations**, select **Auto-launch on install**.
 - c) Make sure that **Only push settings with values defined** is selected.
 - d) Next to **Registration key**, enter the subscription key.

Note: You can find the subscription key in the WithSecure Elements portal.
 - e) In the Email address field, enter `#{userEmailAddress}` as a value.
 - f) Select **Manage Permissions**. The **Select Permissions** window opens.
 - g) Select all the options, and then click **Select**.
 - h) Under **Runtime Permissions**, go through all the drop-down menus, and select **Auto Grant**, and then select **Next**. The **App Configurations** page opens
3. Next to **Install on device**, select the plus icon, and do the following:
 - a) Enter a name for the configuration setup.
 - b) Turn on **Device Installation Configurations**.
 - c) Select the **App Update Mode** option, and from the drop-down menu, select **High Priority**.
 - d) Select **Next**. The **App Configurations** page opens.
4. Next to **Promotion**, select the plus icon, and do the following:
 - a) Enter a name for the configuration setup.
 - b) Select **Featured List**.
 - c) Select **Next**.
5. Next to **Delegated Device Permissions**, select the plus icon, and do the following:
 - a) Enter a name for the configuration setup.
 - b) Select **Manage App Configurations**.
 - c) Select **Next**
6. Select **Done**. The WithSecure Elements Mobile Protection is added to the App Catalog.

Configuring the Android app using certificates

Instructions on how to configure the Android app using certificates.

1. On the **Ivanti Endpoint Management** administration portal, go to the **Configurations** page and select **Add**.
2. Select **Certificate**.

3. Enter a name for the certificate.
4. Upload the WithSecure Elements certificate for WithSecure Elements Mobile Protection.
Note: You can find the certificate in the WithSecure Elements portal.
5. Select **Next**.
6. On the next page, select the preferred option for deploying the certificate, and then select **Done**.
Note: The certificate must be deployed to the device, manually or automatically, to activate WithSecure Elements Mobile Protection.

B.6.2 Android Enterprise deployment with Ivanti Endpoint Management

This chapter contains instructions on how to deploy the WithSecure Elements Mobile Protection app in the Android Enterprise context with Ivanti Endpoint Management.

Adding the WithSecure Elements Mobile Protection app

Instructions on how to add the WithSecure Elements Mobile Protection app to Ivanti Endpoint Management.

1. In the Ivanti Endpoint Management administration portal, select **Admin** > **Google** > **Android Enterprise**. The Android Enterprise page opens.
2. Under **Begin Recommended Setup**, select **Authorise Google**.
3. Select **Complete sign-up**.
4. Select **Apps** > **App Catalog**, and select **+Add**. The Add App wizard opens.
5. In the Choose view, from the drop-down menu, select **Google Play**.
6. In the Search the Google Play store... box, enter WithSecure Elements Mobile Protection.
7. Select the app and then select **Approve** > **Approve**.
8. Select **Done** > **Select** > **Next**.
9. In the Describe view, select **Next**.
10. In the Delegate view, select **Next**.
11. In the Distribute view, select your preferred option and select **Next**.
12. In the Configure view, next to **Managed Configurations for Android**, select the plus icon. The Configuration Setup page opens.
13. In the Name field, enter a name, and under **Managed Configurations**, do the following:
 - a) In the Registration key field, enter the product subscription key.
Note: You can find the WithSecure Elements Mobile Protection subscription key in the WithSecure Elements Security Center under **Management** > **Subscriptions**.
 - b) Enter your first and last name in the respective fields (optional).
 - c) In the Alias field (optional), enter an alternate name.
 - d) In the Email address field (optional), enter your email address.
 - e) In the Environment field (optional), enter 2.
14. Under **Distribute this App Config**, select **Everyone with App**, and select **Next**.
15. On the App Configurations page, select **Done**. WithSecure Elements Mobile Protection is shown on the **App Catalog** page.

B.7 Deployment using Miradore MDM

Instructions on how to deploy the WithSecure Elements Mobile Protection app with Miradore MDM to Android and iOS devices.

Note: These instructions do not include information on how to create and configure users and devices.

B.7.1 Adding the Android app to Miradore MDM

Instructions on how to add the WithSecure Elements Mobile Protection Android app to Miradore MDM.

Miradore MDM can provide the license information to the app either by using an XML file or the Install Referrer service of the Google Play store. Select the method that you want to use before you start adding the app to the MDM.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

1. In the Miradore administration portal, select **Management > Applications** from the left pane menu.
2. In the **Actions** menu on the right, select **Add > Android application**.
The Add application wizard opens.
3. In the Add application wizard, do the following:
 - a) In step 1, select **Google Play store** and then **Next**.
 - b) In step 2, enter the following details:
 - **Name:** WithSecure Elements Mobile Protection for Android
 - **Package name:** com.fsecure.mp.ucf
 - **Description:** Enter any description that you want to use.
 - **Notification to user:** Enter any information that you want users to see.
 - **Add shortcut to home screen:** Select to create a shortcut to the app.
 - c) Add the following information to the **Install referrer** field:
 - If you want to use the Install Referrer service to deliver the license information, use the install referrer string that can be found from WithSecure Elements service. Look for **Google Play download URL** with the WithSecure Elements Mobile Protection activation string. Copy the latter part of the string, starting from utm-medium. If you want to send additional information to the app, you can add extra elements to the activation string.
4. Select **Create**.
5. In step 4, make sure the information is correct and select **Close**.

B.8 Deployment using Samsung Knox

Instructions on how to deploy the WithSecure Elements Mobile Protection app with Samsung Knox to Android devices.

Note: The instructions do not include information on how to create and configure users and devices.

B.8.1 Deploying the Android app with Samsung Knox

Instructions on how to deploy the Android app with Samsung Knox.

Adding the Android app to Samsung Knox

Instructions on how to add the WithSecure Elements Mobile Protection Android app to Samsung Knox.

Before you integrate WithSecure Elements Mobile Protection with your MDM, make sure that the following prerequisites are met:

- You have enrolled your end device
- You have set the profile with policy restrictions

Note: WithSecure does not provide support for or instructions related to profiles and policies, unless specifically mentioned.

- An internet connection for setting up the VPN and permissions for the files
- A valid WithSecure Elements Mobile Protection subscription

The integration consists of the following:

- Adding the app to the MDM from Google Play Store
- Assign the app and configure it with the subscription key that WithSecure provides, or
- Download the MDM server configuration certificate from WithSecure Elements portal. You can download the certificate by logging in to the portal, going to **Management > Subscriptions** and selecting first the relevant company, then the three dots next to WithSecure Elements EPP for Mobiles, and then **MDM server configuration**

Note: In some MDMs, you can integrate the app only by using the certificate. For more details see the instructions for the relevant MDM.

To add the Android app to Samsung Knox:

1. Log in to your Samsung Knox console.
2. Select **Application**.
The Application page opens.
3. Select **Add**.
4. On the Select Application Type screen, select **Android platform > public Managed Google Play**, and then select **OK**.
5. On the Add Application page, enter `WithSecure Elements Mobile Protection` and search for the application.

Note: To change the country of the selected platform, select the check box next to **Set Country** and then select the country.

6. In the search results, first select the application that you want to add and then **Select**.
7. Edit the following imported information, if necessary:
 - Name - enter the name of the application
 - Category - select the category for the application. By selecting **Manage category**, you can add or edit the application categories.
 - Description - enter a description for the application
8. Choose one of the following options to continue:
 - Select **Save & Assign** to save the information and proceed to assign the application by selecting **Continue**.
 - Select **Save** to save the information and return to the application list. You can assign this application later.

Assigning and configuring the Android app

Instructions on how to assign and configure the Android app.

Important: When you assign a profile to a parent organization, its sub-organizations inherit the profile. However, sub-organizations do not inherit Applications and Contents.

To assign and configure the Android app on Samsung Knox:

1. Select **Application**.
The Application page opens.
2. Select **WithSecure Elements Mobile Protection** and then select **Assign**.
The Assign Application page opens.
3. Configure the following assignment settings:
 - Target device - you can select one of the following options: **Android Enterprise**, **Android Legacy**, or **Android Enterprise + Legacy**.
 - Installation area- shows the designated installation area
 - Installation type - select one of the available options:
 - **Manual** - allows device users to install the application manually
 - **Automatic (Removable)** - sets the application to be installed automatically. Device users are allowed also to manually remove the application.
 - **Automatic (Non-Removable, Android Management API only)**
 - Auto-run after installation (Non-Android Management API) - you can select to set the application to start immediately after installation.
 - Auto update model - the available options are **Default update**, **High Priority**, and **Postponed (90 days)**.
4. Next to Managed Configuration, select **Set configuration** and do the following:
 - In the Managed configuration field, enter a descriptive name, for example, `work`.
 - In the Registration key field, enter the WithSecure Elements Mobile Protection subscription key.
 - In the Alias field, enter the following: `$username$`.
 - In the Email address field, enter `$emailaddress$`.
 - In the Environment field, enter `2`.

Note: Registered devices to WithSecure Elements will be shown with Email Address when you configure the value `$ emailaddress$`.
5. Select **Save** to save the changes.
6. Under Target, select the group to which you want to assign the application.