



WithSecure Elements Mobile Protection for iOS

Contents

Chapter 1: About Elements Mobile Protection.....	4
1.1 Why WithSecure Elements Mobile Protection?.....	5
1.2 Key features.....	5
1.3 System requirements (iOS).....	7
1.4 Quick start guide.....	7
1.5 Deploy Content Filter.....	9
Chapter 2: Protecting internet traffic.....	10
2.1 Turn on network protection.....	11
2.2 Content Filter inspection mode.....	11
2.3 Turn on SMS protection.....	13
2.4 Turn on Reputation-based browsing.....	14
2.5 Turn on alert notifications.....	14
2.6 Allow remote proxy server.....	15
2.7 Allow external DNS servers.....	15
2.8 Remove VPN configurations.....	15
2.9 Allow remote collection of diagnostic file.....	16
2.10 Remove protection log data.....	16
2.11 Reset counters.....	16
2.12 View the protection statistics.....	16
Chapter 3: Contact support.....	18
Appendix A: Exporting log files.....	20
A.1 Export log files (iOS).....	21
Appendix B: Using MDM.....	22
B.1 Before you begin.....	23
B.2 Content Filter MDM payload.....	23
B.3 Deployment using Google Workspace MDM.....	24
B.4 Deployment using VMware Workspace ONE MDM.....	26
B.5 Deployment using Microsoft Intune MDM.....	28
B.6 Deployment using IBM MaaS360 MDM.....	31
B.7 Deployment using Ivanti Endpoint Management.....	32
B.8 Deployment using Miradore MDM.....	34
B.9 Deployment using Jamf Pro MDM.....	35

Glossary.....	39
Index.....	43



Chapter 1

About Elements Mobile Protection

Topics:

- Why WithSecure Elements Mobile Protection?
- Key features
- System requirements
- Get started with WithSecure Elements Mobile Protection
- Deploy Content Filter

About Elements Mobile Protection

Learn about the WithSecure Elements Mobile Protection app, including its features, activation, and mobile device management (MDM) deployment.

This topic explains how to activate and manage the app and deploy it with a mobile device management (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 F-Secure Business) Elements Mobile Protection protects your mobile devices. It helps prevent cyberattacks and other mobile threats. It can block phishing links in social apps and short message service (SMS) messages, harmful websites, and malware. It also protects business-critical data.

WithSecure Elements Endpoint Protection is a module of the WithSecure Elements cybersecurity platform. The cloud-based platform protects against ransomware and advanced attacks. Elements combines vulnerability management, automated patch management, dynamic threat intelligence, continuous behavioral analytics, and security for cloud collaboration services and infrastructure. You can use individual solutions or combine them for broader protection.

1.1 Why WithSecure Elements Mobile Protection?

WithSecure Elements Mobile Protection protects mobile devices from malware, phishing, and risky apps with centralized management across platforms.

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 updated application supports the latest iOS versions. Network Gateway provides strong security controls and improved network performance across different mobile platforms. The cloud handles operations that use the most processing power, which extends device battery life.

Centralized management

Via WithSecure Elements Security Center or your MDM solution, you can deploy and manage Elements Mobile Protection. You can install and use it through the app's user 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 help you identify and address potential threats.

1.2 Key features

Key features of WithSecure Elements Mobile Protection, including browsing protection, SMS protection, and the Network Gateway.

Browsing protection	Browsing Protection prevents users from visiting phishing and malicious sites. Blocking these sites reduces exposure to malicious content and 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 using 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. Elements Mobile Protection includes a Safari extension that integrates with existing VPN setups and provides the same level of protection to iOS users regardless of their VPN preference.
SMS protection	SMS protection automatically scans incoming SMS messages for unsafe links or malicious QR codes. Messages identified as unsafe are moved to your Junk folder, keeping your device and personal data safe.
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 WithSecure 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. • Network Gateway provides enhanced security and advanced control by the Safari extension that integrates with existing VPN setups and provides the same level of protection to iOS users regardless of their VPN preference.
Simplified management	Our lightweight solution is managed 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 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 with Mobile Device Management (MDM) solutions and supports policy management, such as enforcing minimum operating system versions and device encryption.

1.3 System requirements

The devices and operating system versions that WithSecure Elements Mobile Protection supports on iOS.

Supported operating systems • iOS 17 or 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, IBM Security MaaS360, Microsoft Intune, Miradore, Ivanti Endpoint Management

Status upstream and remote notifications

- For the app to work properly, it needs to run in either background or foreground



NOTE: User interface optimization is pending for iPad tablets.

1.4 Get started with WithSecure Elements Mobile Protection

Installs, activates, and gets you started with WithSecure Elements Mobile Protection.

Your device must be running iOS 17 or later.

The app can be activated in iOS 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. Supported MDM vendors include Intune, Jamf Pro, Workspace ONE, IBM MaaS360, Ivanti, and Miradore.

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

- When you purchase the product from a WithSecure partner, the partner typically creates a business account for the first administrator in your organization. If this applies to you, you have received an email from WithSecure with a temporary password and a link to log in to Elements Security Center.
- If your account has not yet been created, but you have received a subscription key from your partner, you can use the subscription key to create a WithSecure business account for the first administrator in your organization. To do that, use the company self-registration link to WithSecure Elements Security Center.

This quick start guide walks you through installing, activating, and getting started with WithSecure Elements Mobile Protection.

1. Use the Business Account credentials to log in to WithSecure Elements Security Center at WithSecure Elements Security Center sign-in page.
2. You must add the new devices by sending an email invitation for manual installation:



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.

- a) In Elements Security Center, under **Environment**, select **Devices** > **Mobile devices**.
- b) Select  and then select **Add new device**.
- c) Select the subscription to use and select **Next**.
- d) Follow the steps in the wizard and send an email invitation to one or more users with a download link to the installer.



NOTE: Each invitation link is unique and valid for a single installation within 29 days.

3. To install the app on your mobile device:

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.



NOTE: "You" refers to end users.

- a) Open the invitation email.
- b) Select the link next to iOS.
You are redirected to AppStore where you can download and install the WithSecure Mobile Protection app.
- c) After you have installed the app on your device, go back to the installation email, select **Activate for iOS** 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.

- d) When asked, select **Allow** to give the app the required permissions.



NOTE: The app needs permission to notify you about important events.

4. Turn on the protections that you want to use.



NOTE: Turn on network protection before reputation-based browsing. Reputation-based browsing depends on network protection.

- a) Turn on network protection. For instructions, see Turning on network protection.
- b) Turn on reputation-based browsing. For instructions, see Turning on reputation-based browsing.
- c) Turn on SMS protection. For instructions, see Turning on SMS protection.



NOTE: On iOS, SMS protection requires extra configuration in the device settings.

5. To view and edit user details:

- a) On the main view, tap .
*The **Menu** view opens.*
- b) Tap **User details**.
- c) On the **User details** view, you can view and edit the following information:

- Email address.



NOTE: You cannot edit your registered email address.

- First name
- Last name
- Alias

Your changes are saved automatically.

1.5 Deploy Content Filter

Deploy the Content Filter inspection mode to your organization's supervised iOS and iPadOS devices.

Your organization already uses an MDM solution, and the target devices run iOS 17 or later.

We recommend that you pilot Content Filter with your organization's exact MDM, iOS or iPadOS version, WithSecure application build, and third-party VPN combination before a broad deployment.

1. Enroll and supervise the target devices through your organization's MDM solution.
2. Install and activate WithSecure Elements Mobile Protection.
3. Create and deploy the WithSecure plug-in Web Content Filter payload.
4. Select **Content Filter** in the assigned Elements Mobile Protection profile.
5. Confirm that Network Protection is connected and that the effective mode is **Content Filter**.
6. Validate policy enforcement, counters, recent activity, and third-party VPN operation.
7. Expand the deployment only after a successful pilot validation.
8. Monitor automatic VPN fallbacks as configuration exceptions that need investigation.

Content Filter is deployed and inspecting traffic on the target devices.

Chapter 2

Protecting internet traffic

Topics:

- Turn on network protection
- Content Filter inspection mode
- Turn on SMS protection
- Turn on Reputation-based browsing
- Turn on alert notifications
- Allow routing traffic through remote proxy server
- Allow external DNS servers
- Remove VPN configurations
- Allow remote collection of diagnostic file
- Remove protection log data
- Reset counters
- View the protection statistics

Protecting internet traffic

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 more control over URL blocking and allow lists. You can block website categories to prevent access to specific content, such as adult, gambling, or social media sites. You can also add specific URLs to an allow list so that users can 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.

Network Gateway also provides more security and control for iOS devices. The Safari extension works with existing VPN setups to provide the same protection regardless of VPN preference.

2.1 Turn 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:

On the main view, under **Network Protection**, tap **Turn on protection**.

Your network is now protected.

2.2 Content Filter inspection mode

Content Filter is an alternative inspection mode that uses Apple's on-device content-filtering framework instead of the local VPN.

To evaluate the reputation of URLs before websites load, WithSecure Elements Mobile Protection normally routes traffic through a local VPN. Content Filter is an alternative inspection mode that applies the same Browsing Protection policies, but uses Apple's on-device Network Extension filtering framework instead of the VPN.

Because Content Filter does not use the device's VPN connection slot, it can run alongside a third-party VPN provider.

Inspection modes	VPN	Uses the WithSecure local VPN configuration. Best fit: unsupervised devices, or devices without the required MDM payload.
	Content Filter	Uses Apple's on-device Network Extension content-filtering framework. Best fit: supervised, MDM-managed devices, particularly when another VPN must run at the same time.

Both modes use the same protection policy, counters, and recent-activity view.

Requirements Before you enable Content Filter, confirm the following:

- The device is enrolled in an MDM solution and is supervised.
- WithSecure Elements Mobile Protection is installed, activated, and its assigned profile is synchronized.
- An Apple Web Content Filter payload that uses the plug-in filter type and is associated with the deployed WithSecure application is installed on the device.
- No existing system-wide filter prevents activation.



IMPORTANT: Apple lets production applications create a Network Content Filter configuration only on supervised devices.

Automatic fallback to VPN

VPN is the default compatibility mode. If Content Filter cannot be activated, the app automatically selects VPN inspection and re-enables Network Protection. The user sees a notification that Content Filter is not supported on the device and that VPN-based protection was enabled instead.

Common causes of a fallback:

- The device is not supervised.
- The Web Content Filter payload is not installed yet.
- The plug-in association is incorrect.
- Another system-wide filter is active.
- The MDM profile was removed or became invalid.

After you correct the supervision, payload, or filter conflict, select Content Filter again on the device, or reapply it from the assigned profile.



IMPORTANT: A fallback preserves protection. It is a change of the effective mode, not a protection outage.

Operational considerations

- Apple allows only one content filter to run system-wide on iOS and iPadOS. Review existing security and filtering products before you deploy Content Filter.
- Traffic is evaluated through Apple's Network Extension framework instead of being routed through the WithSecure local VPN solely for inspection.
- Content Filter and VPN use the applicable Browsing Protection and website-control settings from the assigned profile.
- Protection statistics and recent activity stay available in the existing Network Protection views.
- Supported policy changes reach an active Content Filter automatically, without a restart or a manual reconnect.

2.2.1 Select the inspection mode

Choose whether WithSecure Elements Mobile Protection inspects traffic using the local VPN or the Content Filter framework.

Before you select **Content Filter**, confirm that:

- The device is enrolled in an MDM solution and is supervised.
- An Apple Web Content Filter payload for WithSecure Elements Mobile Protection is installed on the device.
- No other system-wide content filter is active.

To select the inspection mode:

1. On the main view, tap .
*The **Menu** view opens.*
2. Tap **Settings > Network protection > Inspection mode**.
3. Select **Content Filter** or **VPN**.

The selected inspection mode becomes active without requiring a restart or a manual reconnect. The active mode also appears on the main Network Protection view.



NOTE:

- If the mode remains **VPN**, confirm that **Content Filter** is selected and not overridden by the assigned profile.
- If **Inspection mode** is disabled, the assigned profile has locked the setting, or the device does not meet the requirements above.
- If policies appear stale after a change, confirm that the profile has synchronized, then check the effective mode and the Network Protection status.

2.2.2 Set the default inspection mode

Choose whether devices in a profile use VPN or Content Filter as the default traffic-inspection mode.

To set the default inspection mode for a profile:

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**, select **VPN** or **Content Filter** as the inspection mode.



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 on the device.

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



IMPORTANT: Devices use **Content Filter** only after they meet its on-device requirements — supervision, the MDM payload, and a synchronized profile.

2.3 Turn on SMS protection

When you turn on SMS protection, Elements Mobile Protection protects your devices against SMS-message phishing attempts.

To protect your SMS messages, you first need to enable Mobile Protection as a filter in the **Messages** app on your iPhone or iPad.

To turn on SMS protection:

1. Open **Settings** on your device.
2. Tap **Apps > Messages**.
3. Under **Unknown Senders**, turn on **Screen Unknown Senders**.
4. Select **Mobile Protection** as your text message filter.

5. On the main view in the Mobile Protection app, under **SMS protection**, tap **Protection: OFF** to activate the SMS protection.
6. By tapping the  icon and then **Settings > SMS protection**, you can turn on the following:

Option	Description
URL validation	Mobile Protection validates URLs in SMS messages. If a URL is identified as unsafe, the message is automatically sent to the Junk folder in your Messages app.
QR code validation	If an SMS message contains an image with a QR code that links to an unsafe URL, the message is automatically sent to the Junk folder in your Messages app.
Safety check for other messaging apps	You can perform a safety check on any message in other messaging apps (for example, WhatsApp or Telegram) using the Share button. Mobile Protection will scan the message for potential threats.

SMS protection is on.

2.4 Turn on Reputation-based browsing

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



NOTE: To use Reputation-based browsing, Network Protection must be on.

To turn on Reputation-based browsing:

1. On the main view, tap .
*The **Menu** view opens.*
2. Tap **Settings**.
3. Tap **Network protection**.
4. Turn on **Reputation-based browsing**.
5. Under **Reputation-based browsing**, you can turn on the following:
 - **Block access to websites rated as harmful**
 - **Block access to websites rated as suspicious**
 - **Block access to websites rated as prohibited**
 - **Block trackers found on websites**
 - **Block access to recently created domains**

Reputation-based browsing is on.

2.5 Turn on alert notifications

You can turn this setting on, if you want to receive alerts when the app has blocked specific content.

To turn on alert notifications:

1. In the main view, tap .
*The **Menu** view opens.*
2. Tap **Settings > Alert notification options**.
3. In the view that opens, turn on **Show alert notifications**.
4. Select which alerts you want to receive for blocked content:

- Blocklisted content blocked - notifies you when content from blocklist is blocked
- Prohibited content blocked - notifies you when content prohibited by policy is blocked
- Harmful content blocked - notifies you when an attempt to load a harmful URL is blocked
- Suspicious content blocked - notifies you when suspicious content is blocked
- Tracker blocked - notifies you when an attempt to load a tracker is blocked
- Local filter alerts - notifies you when content from a local filter is blocked
- Forbidden category blocked - notifies you when content from a forbidden category is blocked. Categories include adult, anonymizers, hacking, and more. See the full list of categories on the WithSecure page.
- Domain age alerts - notifies you when a web page was registered recently and may be suspicious or harmful

Alert notifications are on.

2.6 Allow routing traffic through remote proxy server

You can allow network gateway to route traffic through a remote proxy server.



NOTE: You can configure this in the Wi-Fi settings of your iOS device.

To allow remote proxy server settings:

1. On the main view, tap .
*The **Menu** view opens.*
2. Tap **Settings > Network protection**.
3. Turn on **Allow remote proxy servers**.

Routing traffic through a remote proxy server is allowed.

2.7 Allow external DNS servers

You can allow the use of external DNS servers.

If this option is turned on, both external and local DNS servers are used for domain name resolution; if turned off, only local DNS servers are used to resolve domain names.

To allow external DNS servers:

1. On the main view, tap .
*The **Menu** view opens.*
2. Tap **Settings > Network protection**.
3. Turn on **Allow external DNS**.

External DNS servers are allowed.

2.8 Remove VPN configurations

You can select to remove all VPN configurations that Elements Mobile Protection has done.



IMPORTANT: Use this option for troubleshooting purposes only. It turns off your protection.

To remove VPN configurations:

1. On the main view, tap .
*The **Menu** view opens.*

2. Tap **Settings**.

3. Under **More**, tap the **Remove VPN configuration** link.

All changes to the VPN configurations are removed and your protection is turned off.

The VPN configuration is removed.

2.9 Allow remote collection of diagnostic file

Turning this setting on allows administrators to remotely collect the diagnostic file from your device.

To turn the setting on:

1. On the main view, tap .

*The **Menu** view opens.*

2. Tap **Settings**.

3. Under **More**, turn on **Accept remote collection of diagnostic file**.

Remote collection of diagnostic files is allowed.

2.10 Remove protection log data

Selecting this option removes permanently all existing protection log data from your mobile device.

To remove log data:

1. On the main view, select **Network Protection**.

*The **Network Protection** view opens.*

2. Select .

3. On the view that opens, select **Remove Protection Log data**.

All protection log data is permanently removed from the device.

2.11 Reset counters

Selecting this option resets all statistic counters to zero.

To reset the counters:

1. On the main view, tap .

*The **Menu** view opens.*

2. Tap **Settings**.

3. Under **More**, tap **Reset counters**.

All statistical counters are reset to zero

2.12 View the protection statistics

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



NOTE: The number of blocked tracking attempts and harmful websites is shown only if reputation-based browsing is on. Whether this feature is on or off, depends on the profile that is assigned to the device.

To view the statistics:

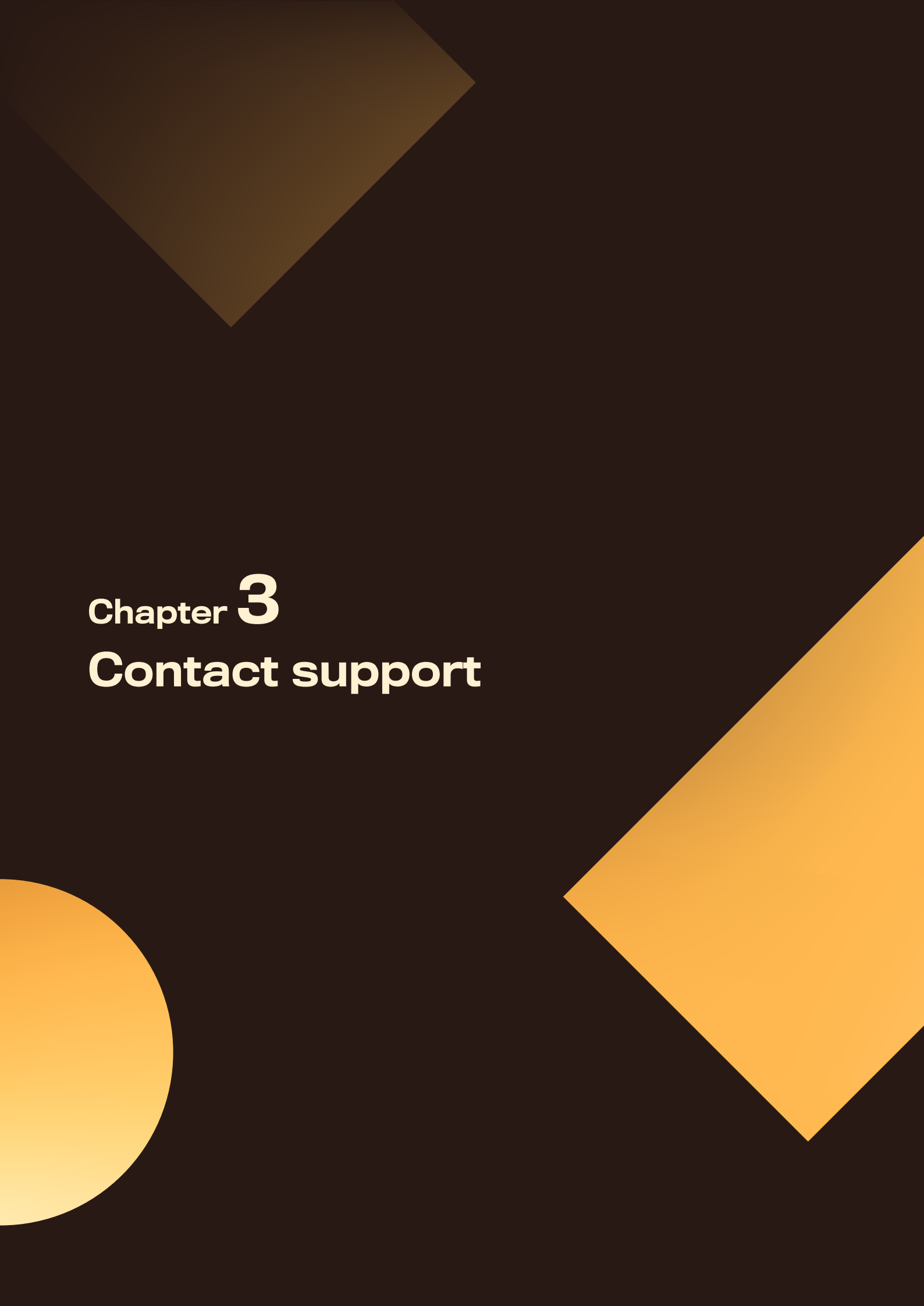
1. On the main view, under **Network Protection**, review the following statistics:

Option	Description
Internet traffic protected	show the amount (MB) of traffic that the app has protected
Overall sites checked	the number of websites that the app has checked
Harmful sites blocked	the number of harmful websites that the app has blocked
Tracking sites blocked	the number of tracking websites that the app has blocked

2. To view recent activity, do the following:

- a) Tap the **Recent activity** link.
- b) On the **Recent activity** view, tap .
- c) Turn on **Show all recorded URLs**.
- d) Under **URL category**, select the categories that you want to filter, and tap **Save**. You can either select them individually or all at once.

A list opens showing all URLs - allowed and blocked - that the app has recorded.



Chapter **3**

Contact support

Contact support

We welcome comments and feedback on the product's features, usability, and performance.

You can report any technical issues on the WithSecure email support page.



Appendix **A**

Exporting log files

Topics:

- Export log files

Exporting 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.

If technical support asks for log files, you can export them from the WithSecure Elements Mobile Protection app. This section describes how to export log files on Android and on iOS devices, for both activated and non-activated apps.

A.1 Export log files

Exports a log file from an activated or non-activated app on iOS devices for technical support.

If you are reporting a technical issue, export the log file and attach it to your feedback. The procedure depends on whether the app is activated.

Export the log file in one of the following ways:

- In a non-activated app:
 - a. In the **Log in** view, tap the WithSecure logo eight times.
 - b. When the `log.zip` file appears, share it (for example, by email or text message), or select **Save to Files** to send it later.
- In an activated app:
 - a. In the main view, tap .
 - b. In the **Menu** view, tap **About**.
 - c. Tap the WithSecure Elements Mobile Protection profile information eight times.
 - d. Tap **Send log** that appears at the bottom of the screen.
 - e. When the `log.zip` file appears, share it (for example, by email or text message), or select **Save to Files** to send it later.

Appendix **B**

Using MDM

Topics:

- Before you begin
- Web Content Filter payload for Content Filter
- 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 Jamf Pro MDM

Using MDM

Integration options for the WithSecure Elements Mobile Protection app with MDM solutions.

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: VMware Workspace ONE, Microsoft Intune, IBM Security MaaS360, Ivanti Endpoint Management (formerly known as MobileIron Cloud), and Miradore.

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 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.

Before you deploy WithSecure Elements Mobile Protection, decide how to activate the app on your users' devices. You can push and activate the app through a third-party MDM, or invite users from the WithSecure Elements portal so that they install and activate it themselves.

B.2 Web Content Filter payload for Content Filter

The Apple Web Content Filter payload settings that an MDM profile must configure to enable the Content Filter inspection mode.

The MDM profile must create an Apple Web Content Filter configuration for the WithSecure plug-in. Enabling only Apple's built-in allowlist, denylist, or adult-content rules does not enable Content Filter.

Payload identifier

`com.apple.webcontent-filter`, configured with the filter type set to plug-in.

Application association

Set `PluginBundleID` to the bundle identifier supplied for the deployed WithSecure application variant.

MDM labels

The exact profile and field names vary by MDM provider. Consult the provider's current documentation for the exact profile-authoring steps.

Typical workflow: create the iOS Web Content Filter profile, select the WithSecure plug-in, deploy it to a pilot group, and confirm a successful device installation.

For the underlying Apple platform requirements, see NEFilterManager in the Apple Developer documentation.

B.3 Deployment using Google Workspace MDM

Deployment of WithSecure Elements Mobile Protection with Google Workspace MDM to Android devices.

To deploy the WithSecure Elements Mobile Protection app with Google Workspace, add and configure the app for managed Android devices, and enroll and protect Chromebooks.

B.3.1 Add the Android app to Google Workspace Endpoint Management

Adds WithSecure Elements Mobile Protection as an allowed app in Google Workspace MDM for 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

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.

Configure the Android app in Google Workspace

Configures the Android app in Google Workspace using a subscription key and registration key.



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 WithSecure Elements Security Center. 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 **Management > Subscriptions > 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**.

The managed configuration is created.

B.3.2 Chromebook enrollment

Chromebooks enrolled in Google Workspace MDM can run the WithSecure Elements Mobile Protection app and the WithSecure Browsing Protection extension.

To protect Chromebooks, enroll them in Google Workspace, then install the WithSecure Elements Mobile Protection app and the WithSecure Browsing Protection extension on the managed devices.

Chromebook compatibility

Overview of WithSecure product compatibility with Chrome OS.

The following WithSecure products are compatible with Chrome OS:

- Browsing Protection Extension - available via the Chrome Web Store
- Elements Mobile Protection - available as an Android app via the Google Play Store on Chromebooks that support Android apps

Enroll Chromebook in Google Workspace MDM

Enrolls a Chromebook using the Google Admin Console for centralized management.

Before you start, make sure that you have the following:

- A Google Workspace administrator account
- A Chrome Enterprise Upgrade license
- A Chromebook that has been reset to factory settings

To enroll a Chromebook:

1. Log in to the Google Admin Console.
2. Go to **Devices > Chrome > Settings > Device management**.
3. Check that enrollment settings and organizational units are correct.
4. Turn on the Chromebook.
5. Press **Ctrl + Alt + E** to start enrollment.

6. Enter your administrator username and password.
7. Confirm the Chromebook appears in **Devices > Chrome > Devices** in the Admin console.

Install WithSecure Elements Mobile Protection

Installs the app on a managed Chromebook.

Make sure that the following requirements are met:

- The Chromebook is enrolled in Google Mobile Device Management (MDM)
- You have an active WithSecure Elements Mobile Protection subscription
- The Google Play Store is enabled for your organization in the Admin console
- Chromebooks support Android apps (most modern models do)

To install the app:

1. Log in to the Google Admin Console.
2. Go to **Devices > Chrome > Settings > User & browser settings**.
3. Scroll to the **Android application** section, and select the appropriate organizational unit.
4. Set **Android apps on Chrome devices** to **Allow users to install Android apps on Chrome devices**, and select **Save**.
5. Under **Billing > Subscriptions**, activate the Android Enterprise subscription.
6. Accept the Google Play terms of service.

Managed Chromebooks can now install Android apps, including the WithSecure Elements Mobile Protection app.

Install WithSecure Browsing Protection extension

Installs the WithSecure Browsing Protection extension on a managed Chromebook.

Make sure that the following requirements are met:

- The Chromebook is enrolled in Google Mobile Device Management (MDM)
- The Google Play Store is enabled for your organization in the Admin console

To install the extension:

1. Log in to the Google Admin Console.
2. Go to **Devices > Chrome > Apps & extensions > Users & browsers**.
3. Select the target organizational unit where you want to deploy the extension, and select **Add > Add from Chrome Web Store**.
4. Search for **Browsing Protection by WithSecure**, and select it.
5. Under **Installation policy**, select **Force install**, and then select **Save**.

The extension is automatically installed on all enrolled Chromebooks in the target organizational unit.

On a managed Chromebook, log in and open `chrome://extensions` to confirm that the extension is installed and active.

B.4 Deployment using VMware Workspace ONE MDM

Deployment of WithSecure Elements Mobile Protection with VMware Workspace ONE (formerly AirWatch) MDM on Android and iOS.



NOTE: This deployment does not include creating and configuring users and devices.

To deploy the WithSecure Elements Mobile Protection app with VMware Workspace ONE, add and configure the app for the iOS and Android devices that Workspace ONE manages.

B.4.1 Add the iOS app to VMware Workspace ONE MDM

Adds the WithSecure Elements Mobile Protection iOS 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 Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

Adding the app to Workspace ONE lets you deploy and manage it on iOS devices enrolled in the MDM.

1. On the VMware Workspace ONE administration portal, go to **Resources > Apps**.
2. Select the **Public** tab.
3. Select **Add application**.
4. On the Add Application view, do the following:
 - a) In the Managed by field, add you organization.
 - b) From the Platform drop-down menu, select **Apple iOS**.
 - c) In the Name field, enter the application name, for example, **WithSecure Mobile Protection**.
 - d) Select **Next**.
The Search page opens.
 - e) From the Country drop-down menu, you can select your country, and click **Select**.
The Add Application - WithSecure Mobile Protection view opens.
 - f) On the view that opens, under **Name**, enter WithSecure Mobile Protection if its not detected by default and select **Save and assign**.

Next, you need to configure the iOS app.

Configure the iOS app in VMware Workspace ONE

Configures the WithSecure Elements Mobile Protection iOS app in VMware Workspace ONE MDM.

You must have already added the WithSecure Elements Mobile Protection app to VMware Workspace ONE.

Configure its assignment, restrictions, and automatic-activation settings before publishing it to devices.

1. Under **Assignment > Distribution**, enter the following:

Option	Description
Name	the name of the app (WithSecure Mobile Protection)
Description	a description for the assignment (optional)

Option	Description
Assignment groups	select the group to whom you want to assign the app, for example, All devices .
App delivery method	select the app delivery method: Auto or On demand .

2. Select the **Restriction** tab, and turn on the desired options.
3. Next, select the **Tunnel & Other Attributes** tab, and review the options.
4. Select the **Application Configuration** tab.
5. Turn on the **Send Configuration** option, and do the following:
 - a) Next, select **Add** to add the configuration key and device identification details to allow for an automatic activation of the app.
 - b) Under **Configuration Key**, enter values for the following configuration entries:
 - *fate_registration_key* - the subscription key
 - *first_name* (optional) - a name that makes it easier to identify the device in WithSecure Elements Security Center
 - *last_name* (optional) - a name that makes it easier to identify the device in WithSecure Elements Security Center
 - *email* - the user email address
 - *alias* (optional) - an alternate name for the user
 - c) For entering any optional keys, select the icon next to **Insert Lookup Value** and select the respective variables. The fields are automatically filled when the application is deployed to user devices.
6. Select **Create**.
7. On the view that opens, select **Save**.
8. On the Preview Assigned Devices page, when you see your device that you added, select **Publish**.
9. On the main view, select **Devices List View**.

Your device appears in the list.

B.5 Deployment using Microsoft Intune MDM

Deployment of WithSecure Elements Mobile Protection with Microsoft Intune MDM, covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with Microsoft Intune, add and configure the app for the iOS and Android devices that Intune manages.

B.5.1 Deploying the iOS app with Microsoft Intune MDM

Deployment of the WithSecure Elements Mobile Protection iOS app with Microsoft Intune MDM.

To deploy the iOS app with Microsoft Intune, add the WithSecure Elements Mobile Protection app and configure its management settings for your managed iOS devices.

Add the iOS app to Microsoft Intune MDM

Adds the WithSecure Elements Mobile Protection iOS 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 Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

Adding the app to Intune lets you assign and publish it to iOS devices enrolled in the MDM.

1. Log into your Microsoft Intune portal.
2. Select **Apps > iOS/iPadOS > Add**.
*The **Select app type** pane opens.*
3. From the **App type** drop-down menu, select **iOS store app**, and then select **Select**.
4. In the **Add App** view, select **Search the App store**.
*The **Search the App Store** pane opens.*
5. In the Search field, enter WithSecure Mobile Protection.
6. Select **WithSecure Elements Mobile Protection > Select**.
*The **Add App** view opens.*
7. In the **App information** tab, select **Yes** to show WithSecure Mobile Protection as a featured app in the Company Portal, and select **Next**.
8. In the **Assignments** tab, under **Required**, select **Add all users**, and select **Next**.
9. In the **Review + create** tab, select **Create**.
10. When you are done, on the **Add App** blade, choose **OK**.

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

Next, add the app configuration policies.

Add the iOS app configuration policies

Adds WithSecure Elements Mobile Protection app configuration policies for managed iOS devices.

To create an app configuration policy:

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 **iOS/iPadOS**.
 - c) Next to **Targeted app**, select **Select app**.
*The **Associated app** pane opens.*
 - d) Select **WithSecure Elements Mobile Protection**, and select **OK > Next**.
*The **Settings** tab opens.*
5. Do the following:

- a) From the **Configuration settings format** drop-down menu, select **Use configuration designer**.
- b) For the value types, refer to Use the configuration designer on page 30
- c) Select **Next**.
*The **Assignments** tab opens.*
- d) Under **Included groups**, select **Add all users** and select **Next**.
*The **Review + create** tab opens.*
- e) Select **Create**.

The app configuration policy was created and assigned.

You need to install the app on an iOS device.

Use the configuration designer

You can use the configuration designer for apps on devices whether they are enrolled in Intune.



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

The designer lets you configure specific configuration keys and values. You must also specify the data type for each value. For each key and value in the configuration, set:

- Configuration key - The key that uniquely identifies the specific setting configuration.
- Value type - The data type of the configuration value. Types include Integer, Real, String, or Boolean.
- Configuration value - The value for the configuration.

The following key and value is mandatory for WithSecure Elements Mobile Protection license activation.

Table 1: Mandatory configuration key

Key	Type	Description	Value	Notes
<i>fate_registration_key</i>	string	The registration or activation key that is used by the client	ABCD-EFGH-IJKL-MNOP	Example: The actual value is provided by the reseller.

End user is not able to switch VPN off from the WithSecure Elements Mobile Protection app nor disable individual protection features. Read more about the details and limitations with this feature from Keeping VPN switched on automatically.

The following optional keys help to identify devices on WithSecure Elements Security Center. Use Microsoft Intune dynamic variables to get suitable values.

Table 2: Optional device identification keys

Key	Type	Description
<i>email</i>	string	Specifies a user activation email
<i>env</i>	integer	Specifies the environment where the application is activated. For customers using production, set this value to "2"
<i>data_usage_permission</i>	Boolean	Set to true if the administrator allows data collection; otherwise, set to false

Key	Type	Description
<i>diagnostic_usage_permission</i>	Boolean	Set to true if the administrator allows diagnostic collection; otherwise, set to false
<i>create_vpn_profile</i>	Boolean	Set to true to allow creation of the VPN profile; otherwise, set to false

B.6 Deployment using IBM MaaS360 MDM

Deployment of WithSecure Elements Mobile Protection with IBM MaaS360 MDM, covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with IBM MaaS360, add and configure the app for the iOS and Android devices that MaaS360 manages.

B.6.1 Deploying the iOS app with IBM MaaS360 MDM

Adding and deploying the WithSecure Elements Mobile Protection iOS app in IBM MaaS360 MDM.

To deploy the iOS app with IBM MaaS360, add the WithSecure Elements Mobile Protection app and distribute it to your users.

Add the iOS app to IBM MaaS360 MDM

Adds the WithSecure Elements Mobile Protection iOS app to IBM MaaS360 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



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

The integration consists of the following:

- Adding the app to the MDM from Apple Store
 - Assign the app and configure it with the subscription key that WithSecure provides, or
1. Login into the IBM MaaS360 administrator portal as an administrator.
 2. Open the **Apps** view.
 3. Select **Add** and then **iTunes App Store App** from the drop-down list.
 4. In the **App Details** tab, search and select the **WithSecure Mobile Protection** app.
Adjust the app's category if necessary.
 5. Open the **Policies and Distribution** tab and select the distribution methods and groups that you want to use.

6. Open the **Configuration tab.**

The configuration contains the following mandatory attribute:

- `fate_registration_key` - the license key

You can use the `firstName`, `lastName`, `email`, and `alias` keys to add additional user data to the policy configuration.

7. Select **Add.**

The WithSecure Elements Mobile Protection app is in the **App** list.

Distributing the iOS app

The WithSecure Elements Mobile Protection iOS app is delivered to the users in a defined distribution group.

The WithSecure Elements Mobile Protection iOS app is delivered to users through a distribution group that you define in IBM MaaS360. Assign the users who should receive the app to that group.

B.7 Deployment using Ivanti Endpoint Management

Deployment of WithSecure Elements Mobile Protection with Ivanti Endpoint Management (formerly known as MobileIron Cloud MDM), covering Android and iOS devices.

To deploy the WithSecure Elements Mobile Protection app with Ivanti Endpoint Management (formerly MobileIron), add and configure the app for the iOS and Android devices that it manages.

B.7.1 Deploying the iOS app with Ivanti Endpoint Management

Deployment of the iOS app with Ivanti Endpoint Management.

To deploy the iOS app with Ivanti Endpoint Management, add the WithSecure Elements Mobile Protection app, configure app management, and set any additional configuration keys.

Add the WithSecure Elements Mobile Protection iOS app to Ivanti Endpoint Management

Adds the WithSecure Elements Mobile Protection iOS app to Ivanti Endpoint Management.

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 Apple Store
- Assign the app and configure it with the subscription key that WithSecure provides, or

To add the iOS app to Ivanti Endpoint Management:

1. On the Ivanti Endpoint Management administration portal, go to the **Apps** page and select **Add**.
2. Select **App Store**.

3. Search for WithSecure Elements Mobile Protection.
4. Select the app and then select **Next**.
5. Check that the app description is correct, and select **Next**.
6. Configure the app distribution.
7. Select **Next**.

Configure iOS app management

Configures iOS app management.



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

1. On the **Configuration** page, select **iOS Managed App Configuration** and then select +.
2. Under iOS 7+ Managed App Settings, do the following:
 - a) Enter a name for this configuration, for example, WithSecure Elements Mobile Protection license configuration.
 - b) In the **fate_registration_key** field, enter your WithSecure Elements Endpoint Protection license key.
3. Distribute this configuration to the relevant devices or device groups.
4. Configure any other necessary settings.
5. Select **Done**.

The app configuration is created.

Additional configuration keys

The following Ivanti Endpoint Management variables can be used to help identifying devices on WithSecure Elements Security Center.



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.



NOTE: The key names are case sensitive.

Table 3: Additional configuration keys

Key	Value
<i>fate_registration_key</i>	ABCD-EFGH-IJKL-MNOP
<i>email</i>	\$(userEmailAddress)
<i>first_name</i>	\$(userFirstName)
<i>last_name</i>	\$(userLastName)
<i>alias</i>	\$(userDisplayName)

B.8 Deployment using Miradore MDM

Deployment of WithSecure Elements Mobile Protection with Miradore MDM, covering Android and iOS devices.



NOTE: This deployment does not include creating and configuring users and devices.

To deploy the WithSecure Elements Mobile Protection app with Miradore, add and configure the app for the iOS and Android devices that Miradore manages.

B.8.1 Add the iOS app to Miradore MDM

Adds the WithSecure Elements Mobile Protection iOS app to Miradore 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 Apple Store
 - Assign the app and configure it with the subscription key that WithSecure provides, or
1. In the Miradore administration portal, select **Management > Applications** from the left pane menu.
 2. In the Actions menu, select **Add > iOS application**.
The Add application wizard opens.
 3. In the Add application wizard, do the following:
 - a) In step 1, select **App Store** and then **Next**.
 - b) In step 2, enter the following details:
 - Name: WithSecure Elements Mobile Protection
 - App Store ID: 1549210826
 - App Store country: Choose the country that you want to use
 - Package name: com.f-secure.mobileprotection
 - Description: Enter any description that you want to use.
 - Select **Remove application when device is unenrolled**.
 - c) Select **Create**.
 - d) In step 3, make sure the information is correct and select **Close**.

Configure the iOS app in Miradore

Configures the WithSecure Elements Mobile Protection iOS app in Miradore MDM.



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

1. In the Miradore administration portal, double-click the WithSecure Elements Mobile Protection entry on the Application list.
2. Go to the **Configuration** tab and select **Add new**.
The Create configuration setting view opens.
3. Add the following values for the first setting:
 - Setting: `fate_registration_key`
 - Data type: String
 - Value: Enter your subscription key
4. Select **Add** to add the new setting to the configuration.
After you have configured this mandatory setting, you can add optional settings.
5. To add user details, select **Add new** and use the following values:



TIP: User details can help you to identify devices.

Table 4: Configuration keys

Key	Type	Description
<code>email</code>	string	Specifies a user activation email
<code>env</code>	integer	Specifies the environment where the application is activated. For customers using production, set this value to "2".
<code>data_usage_permission</code>	Boolean	Set to true if the administrator allows data collection; otherwise, set to false
<code>diagnostic_usage_permission</code>	Boolean	Set to true if the administrator allows diagnostic collection; otherwise, set to false
<code>create_vpn_profile</code>	Boolean	Set to true to allow creation of the VPN profile; otherwise, set to false

B.9 Deployment using Jamf Pro MDM

Deployment of WithSecure Elements Mobile Protection using Jamf Pro MDM to iOS and iPadOS devices.

To deploy the WithSecure Elements Mobile Protection app with Jamf Pro, buy the app licenses, then configure the app, notifications, and the Safari browsing-protection extension for your managed iOS and iPadOS devices.

B.9.1 Buy licenses for your devices

Buys licenses for your devices.

The WithSecure Mobile Protection app is free from the App Store. To distribute the app via the Jamf Pro MDM, you need to buy Volume Purchase Program (VPP) licenses for the devices on which you want to install the WithSecure Mobile Protection app. This amount must be equal to the amount of the WithSecure Mobile Protection licenses that you have bought from WithSecure.

To buy the required licenses:

1. Log in to the Apple Business Manager portal.
2. Go to **Apps and Books** and search for WithSecure Mobile Protection.
3. Under **Buy Licenses**, enter the amount of WithSecure Mobile Protection licenses that you have bought from WithSecure, and select **Get**.

The purchase is synchronized with your Jamf Pro within 15 minutes.

B.9.2 Configure the app for iOS and iPadOS devices

Configures the With Secure Mobile Protection app for iOS and iPadOS devices in Jamf Pro MDM.



TIP: By default, the installation process requires users to consent to data collection (required by Apple), VPN profile installation and activation, and collection of diagnostics. Configuring the MDM in advance with the configuration keys removes the need for any user approvals.

To configure the app:

1. Log in to Jamf Pro.
2. Select **Devices > Mobile Device Apps > WithSecure Mobile Protection > Edit**.
3. In the General tab, configure the following:
 - a) Under **Distribution Method**, choose your preferred method.
 - b) Select the **Automatically force app updates** option.
 - c) To prevent users from removing WithSecure Mobile Protection, we recommend turning off the **Allow users to remove app (iOS 14 or later)** option.
4. In the **Managed Distribution** tab, select **Assign Content Purchased in Volume**.

To prevent users from removing WithSecure Mobile Protection, we recommend turning off the **Allow users to remove app (iOS 14 or later)** option.



NOTE: "Location" must match the VPP location where you bought the WithSecure Mobile Protection app.

5. In the **App Configuration** tab, do the following:
 - a) Copy the following configuration into the **Preferences** box:

```
<dict>
  <key>fate_registration_key</key>
  <string>ENTER-THE-SUB-KEY-HERE</string>
  <key>email</key>
  <string>$EMAIL</string>
  <key>alias</key>
  <string>$USERNAME</string>
  <key>env</key>
  <string>2</string>
</dict>
```



NOTE: Replace "ENTER-THE-SUB-KEY-HERE" with your WithSecure Mobile Protection subscription key. You can find your subscription key for WithSecure Mobile Protection in WithSecure Elements Security Center.



NOTE: The "alias" key helps you identify devices in the WithSecure Elements Security Center. If you prefer a different value for "alias", Jamf offers other variables to consider. Refer to "Managed App Configuration Variables" in the Jamf Pro User Guide for more details. However, if you prefer to not use an alias, you may remove that key and the associated string from your configuration as this is an optional setting.

- b) Configure the scope to include the devices on which you want to install With Secure Mobile Protection.

B.9.3 Configure notifications for the app

You can configure how notifications are shown via a Configuration Profile.



NOTE: Configuring notifications for the devices is optional.

To configure notifications for WithSecure Mobile Protection:

1. In Jamf Pro, select **Devices > Configuration Profiles > New**.
2. In the Name field, enter WithSecure Mobile Protection Notifications.
3. Select **Notifications payload > Add**, and do the following:
 - **App Name:** WithSecure Mobile Protection
 - **Bundle ID:** com.f-secure.mobileprotection

Configure the alert settings to your organizations preferences, and then scope the policy to match.

B.9.4 Turn on Safari browsing extension via policy configuration

Turns on the WithSecure Browsing Protection extension automatically through policy configuration in Jamf Pro MDM.

Use a Jamf Pro policy to turn on the WithSecure Browsing Protection Safari extension automatically on managed devices.

1. Log in to Jamf Pro.
2. Select **BluePrints > Create BluePrints**.
3. Enter a name for this BluePrint, for example, WithSecure Browsing Protection for iOS/iPadOS.
4. Enter a description and select **Create**.
5. Under **Components Library**, select **Safari extensions**, and do the following:
 - a) Enter the following details:
 - Extension Identifier: com.f-secure.mobileprotection.SafariExtension (V928P8X763)
 - Extension State & Private Browsing State: Always on
 - Allowed Domains: *
 - b) Select **Add**.



NOTE: Extension State & Private Browsing State and Allowed Domains show our recommended settings. You may change these settings as needed to match your environment.

6. Select **Scope**.
7. Select one or more groups to distribute this BluePrint.
8. Select **Save**.

9. When you are ready to apply the configuration, select **Deploy**.

Glossary

Access Control

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

Active Directory (AD)

Active Directory (AD) is a Microsoft directory service that centralizes the management of network resources such as users, computers, and policies, providing authentication and authorization within a Windows domain network.

Agent

An agent is the client software installed on a managed device that enforces protection, reports device status, and communicates with the management service; more broadly, a program that acts on behalf of a user or another system.

Antivirus

Software that prevents, detects, and removes viruses and other malware.

App Configuration

App configuration is the set of settings or values used to preconfigure application behavior, permissions, or features during deployment or management.

Backdoor

An undocumented way of gaining access to a computer system.

Blocklist

A blocklist is a list of entities — such as applications, websites, senders, or file hashes — that are explicitly denied access or execution; the opposite of an allowlist.

Browsing Protection

A feature that evaluates the safety of visited websites and prevents users from unintentionally accessing harmful websites.

Browsing Protection Extension

The Browsing Protection Extension is a browser component that enables web protection features such as reputation-based site analysis and policy-based web content control.

Cloud Security

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

Cloud Service

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

Configuration Keys

Configuration keys are named settings used to preconfigure application behavior and feature values during deployment or device management.

Containment

Response actions that isolate affected hosts or accounts to stop an active attacker from spreading and to prevent the theft, alteration, or destruction of information.

Criticality

The possible impact that a detection would have in the customer environment, based on severity and the importance of affected hosts.

Detection

A detection is an identified suspicious, malicious, or policy-relevant event, activity, or finding recognized by a security control or analysis system.

Discovery Scan

A discovery scan is a scan that identifies assets, systems, or targets present in a network or environment.

Encryption

Encryption is the process of converting data into a secure format using cryptographic algorithms, ensuring confidentiality and protection against unauthorized access.

Endpoint Detection and Response (EDR)

Endpoint Detection and Response (EDR) is a security technology that continuously monitors endpoints to detect, investigate, and respond to suspicious activity and advanced threats.

Endpoint Protection

Endpoint protection is the set of security capabilities used to prevent, detect, and handle threats on endpoint devices such as workstations, servers, and mobile devices.

Entra ID

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

False Positive

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

Group Policy (GPO)

Group Policy (GPO) is a feature in Microsoft Windows that allows administrators to define security policies, user settings, and system configurations across multiple computers within a domain.

Harmful Content

Harmful content is files, applications, or web content that can damage data or compromise a device, such as malware or malicious websites.

Identity and Access Management (IAM)

Identity and Access Management (IAM) is the framework of policies and technologies that ensures the right users have the appropriate access to resources, covering authentication, authorization, and the lifecycle of user identities.

Identity Management

Identity management is the discipline of creating, maintaining, and removing digital identities and their attributes so that users and devices can be reliably recognized across systems.

Incident

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

Lateral Movement

The process of moving through a network to access additional systems after an initial compromise.

License Key

A license key is a unique code that activates a software product or subscription and verifies that its use is authorized.

Lightweight Directory Access Protocol (LDAP)

The Lightweight Directory Access Protocol (LDAP) is an open protocol for accessing and managing directory information, such as users, groups, and devices, over a network.

Linux Authenticated Scanning

Linux authenticated scanning is a scan method that connects to Linux systems by using supplied credentials or keys to collect scan results and system information.

Malware

A program or a file that is developed for the purpose of doing harm. This includes computer viruses, worms and Trojan horses.

Malware Protection

Malware Protection is the feature that detects, blocks, and removes viruses and potentially unwanted applications on a device.

Malware Scan

A malware scan is a scan that checks a device, file set, or workload for malicious software or other harmful content.

Manual Scanning

Manual scanning is a user-started security scan that runs on demand instead of running automatically on a schedule or in real time.

Mobile Device Management (MDM)

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

Network Gateway

Network Gateway is a mobile protection component that routes and inspects device traffic—for example, through a remote proxy—to block unsafe destinations and content.

Network Protection

Network Protection is a security capability that monitors or controls network traffic to help protect users and devices from unsafe connections and content.

Patch Management

Monitoring the patch status of operating systems and third-party software and applying updates to close known vulnerabilities.

Phishing

In a phishing attack, an attacker sends a fraudulent message posing as a trusted sender to trick the recipient into revealing sensitive data such as credentials or financial information.

Privacy

Privacy is the protection of a person's or organization's information from unauthorized collection, access, use, or disclosure.

Ransomware

A malicious program that prevents the user from accessing their data and/or device and demands a ransom to 'restore normal access'. The program may not actually restore normal access even if the ransom is paid.

Reputation Service

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

Role-Based Access Control (RBAC)

A security model that restricts system access based on user roles and permissions to enforce the principle of least privilege.

Scan

A scan is a security check that examines a device, system, application, account, or other target for threats, vulnerabilities, suspicious activity, or policy-relevant findings.

Scan Node

A scan node is a host or service component that runs scans and reports their progress and results back to the management service.

Scan Templates

A scan template is a saved, reusable set of scan options that can be applied across multiple scans.

Scope Selector

A user interface component that can be used to broaden or narrow the scope of information that is displayed in the WithSecure Elements portals.

Security Administrator

A security administrator is a user account that manages security settings, access, or operational tasks according to the roles assigned to it.

Security Cloud

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

Security Events

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

Security Group

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

Service Account

A service account is a special type of account used by applications, scripts, or automated processes to interact with systems and services, often with predefined permissions.

Severity

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

Solution Provider

A Solution Provider is the top-level partner organization tier in the WithSecure Elements management hierarchy, which manages customer companies and delegates access to partner employees.

Subscription Key

A subscription key is a unique code that identifies and validates a subscription and is used to activate WithSecure products for an organization.

Threat Intelligence

Threat intelligence is evidence-based knowledge about existing or emerging threats — such as attacker tactics, indicators, and motivations — used to inform defensive decisions.

Trojan

A Trojan is malicious software that disguises itself as a legitimate program to trick users into running it, then performs harmful actions such as stealing data or opening a backdoor.

Virus

A virus is usually a program that can attach itself to files and replicate itself repeatedly; they can alter and replace the contents of other files in a way that may damage the computer.

Vulnerability

A flaw, loophole or unexpected behavior in a program or operating system that can be exploited by an attacker in order to perform unauthorized actions on the affected system / device.

Vulnerability Management

Vulnerability management is the continuous process of identifying, assessing, prioritizing, and remediating security weaknesses in systems and software.

Web Content Control

A feature that blocks access to web content based on predefined categories and security policies.

Index

A

AirWatch 26
 alert notifications 14
 Android and iOS 28, 31, 34
 Android app 24
 Android app configuration 24
 app activation 7, 23
 app assignment 27
 app configuration 29–30
 app deployment 27–28, 31–32, 34
 app distribution 32
 app installation 26
 app settings 14–16
 App Store 32, 34–35
 Apple Business Manager 35

B

blocked content 14
 blocked threats 16
 browsing protection 5, 14
 Browsing Protection 37
 Browsing Protection extension 25–26

C

Chrome 26
 Chrome Enterprise 25
 Chrome OS 25
 Chromebook 25–26
 Chromebook enrollment 25
 compatibility 25
 configuration designer 30
 configuration keys 30–31, 33–34, 36
 Configuration Profile 37
 Content Filter 11
 counter reset 16

D

device identification 33
 diagnostic file 16
 distribution group 32
 domain name resolution 15

E

email 34
 env 34
 external DNS servers 15

F

F-Secure Business 5
 feedback 19

G

Google Admin Console 25–26
 Google MDM 26

Google Workspace 24–25
 Google Workspace Endpoint Management 23

I

IBM MaaS360 31–32
 IBM Security MaaS360 23
 inspection mode 11
 installation 7
 internet protection 11
 internet traffic 11
 iOS 7, 21, 37
 iOS app 27–28, 31–32, 34–35
 iOS app configuration 27, 34, 36
 iOS app configuration policies 29
 iOS app management 33
 iOS store app 28
 iPadOS 35–36
 Ivanti Endpoint Management 23, 32–33

J

Jamf Pro 35–37

L

log file export 21
 log files 21
 log removal 16

M

malicious websites 14
 malware protection 5
 managed Android app 24
 managed iOS devices 29
 MDM 5, 23–25, 27, 33–34
 MDM deployment 7, 24, 26, 28, 31–32, 34–35
 MDM integration 23
 Messages app 13
 Microsoft Intune 23, 28–30
 Miradore 23, 34
 mobile app 5
 mobile device 11, 13, 15–16
 mobile devices 21, 23
 Mobile Protection 5, 7, 13, 21, 23–32, 34–37
 Mobile Protection app 21
 mobile security 5, 23
 mobile threats 5
 MobileIron Cloud 23, 32

N

Network Extension 11
 Network Gateway 5, 11, 15
 network protection 11, 14–16
 Network Protection 11, 16
 notifications 14, 37

P

- phishing protection 5
- policy configuration 37
- portal 23
- protection log data 16
- protection statistics 16

R

- registration key 24
- remote collection 16
- remote proxy server 15
- reputation-based browsing 14, 16

S

- Safari extension 37
- Samsung Knox 23
- Security Center 5, 7, 24, 27, 30, 36
- Security Cloud 5, 11
- SMS phishing 13
- SMS protection 13
- statistic counters 16
- statistics 16
- subscription key 24

- support website 19
- supported MDMs 7
- system requirements 7

T

- technical support 19, 21
- traffic routing 15
- troubleshooting 15–16

U

- URL reputation 11

V

- VMware Workspace ONE 23, 26–27
- Volume Purchase Program 35
- VPN 11
- VPN configurations 15
- VPP licenses 35

W

- With Secure Mobile Protection 36
- WithSecure 5, 7, 21, 25, 35