techstep

Techstep Essentials

Mobile Threat Defense

Date: 19/11/2025



Contents

1. Mobile Threat Defense integration 3
2. How to enable integration 4
2.1 Enter the access key 4
2.2 Activate licence on the devices 7
3. Mobile Threat Defense tab in policies 9
3.1 Network & System Threat Rules 10
4. Global application rules 15
5. Per-application threat rule list 22
6. Malware & Virus scanning for applications 24
7. Categorized URLs monitoring 25
8. Administrator console 26
8.1 Mobile threat defense tab 26
8.2 Logs tab 27
8.3 Notifications tab 28
9. On the devices 30
9.1 iOS & iPadOS devices 30
9.2 Android devices 34

1. Mobile Threat Defense integration

Mobile Threat Defense (MTD) is a security solution designed to protect mobile devices from various cyber threats such as malware, phishing, unsafe network connections, and risky device configurations like jailbreaking or rooting. MTD continuously monitors device behavior, app activities, and network traffic to detect and block these threats in real time, ensuring that sensitive data on mobile devices remains secure.

Integrating MTD into our **Mobile Device Management** (MDM) system enables centralized security management and enforcement. This integration offers administrators a simplified way to monitor threats, automate responses such as performing remediations impacting the user experience. Users benefit from seamless, background protection that requires no additional interaction.

In summary, MTD solutions provide:

- Real-time threat detection and automatic mitigation on mobile devices,
- Enhanced visibility and control for administrators via unified dashboards,
- Protection against malware, phishing, network attacks, and risky device states,
- Compliance support and data loss prevention,
- A frictionless experience for users with security running transparently.

The integration of the Pradeo Mobile Threat Defense solution with the Essentials MDM platform is designed to provide robust protection while keeping administration and end-user interaction simple and seamless. This ensures corporate mobile environments are secured without complicating management workflows or user productivity.

Integration is supported on Android devices running version 8.0 or higher, and on iOS or iPadOS devices running version 14.0 or higher.

2. How to enable integration

To begin the integration with the *Pradeo Mobile Threat Defense* solution, a license access key is required. Please **contact your reseller** or our sales department to obtain access to this functionality.

Once the license key has been obtained, ensure the following network requirements are configured:

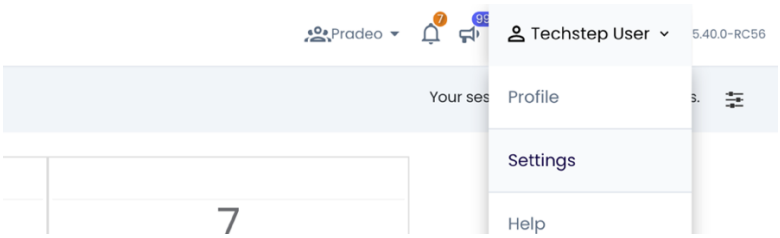
Port 443 must be open to allow communication with the following Pradeo servers:

- Outbound (egress) IP: 145.239.45.193
- Inbound (ingress) IP: 162.19.108.112
- Hostname: https://m201.pradeo-security.com.

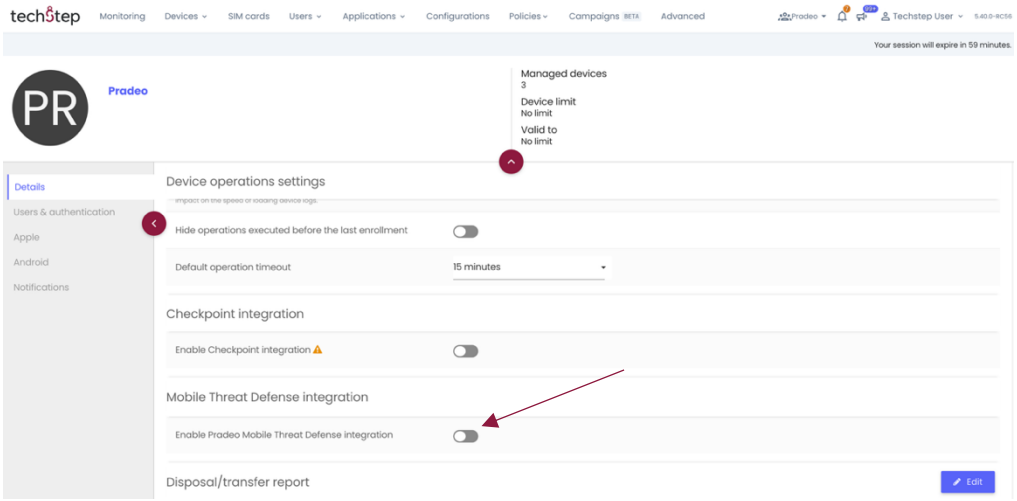
The third step involves adding the key in the organization settings. The fourth and final step is enabling specific threat categories in the policy, which activates licensing on the devices. More details are provided below.

2.1 Enter the access key

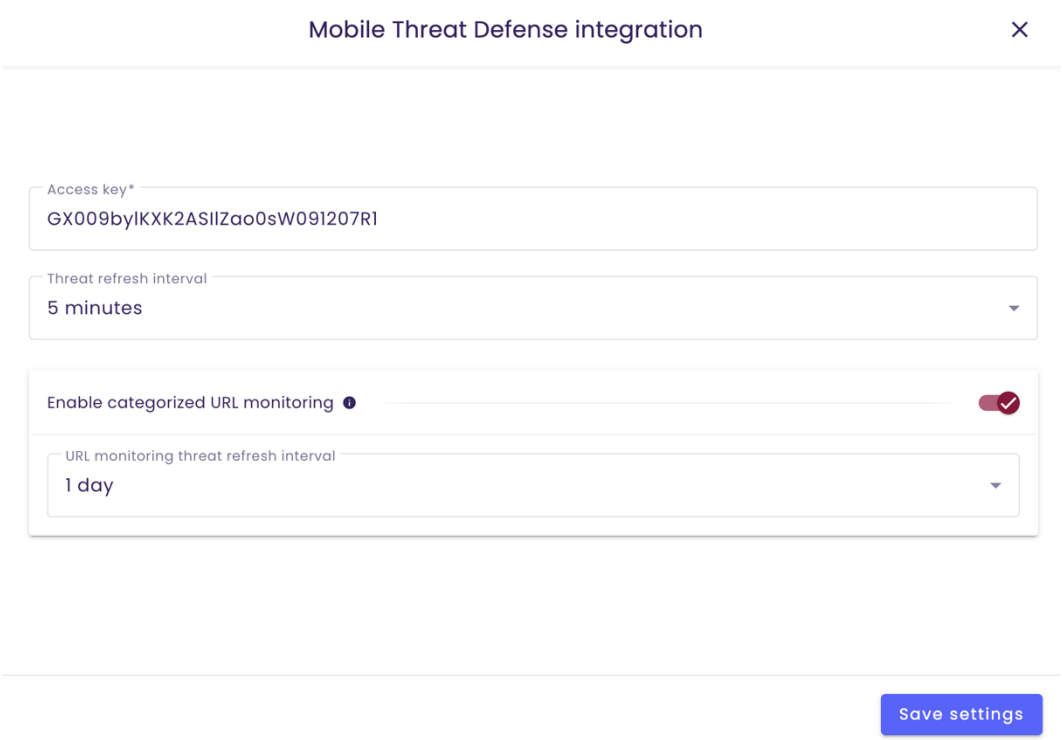
After obtaining the key, log in to the Essentials MDM console and navigate to the organization settings through User profile → **Settings**.



Go to the Details tab and scroll to the bottom to locate the **Mobile Threat Defense integration** section.



To start, enable the toggle. A modal window will appear.



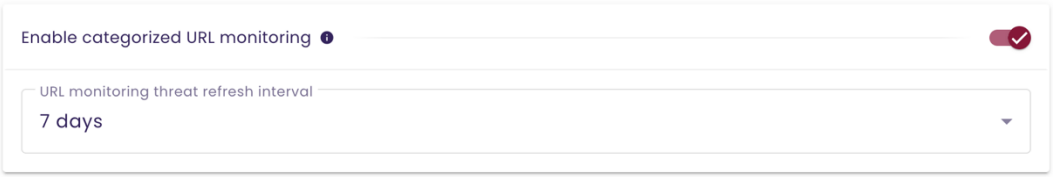
In the modal window, enter the access key obtained from the provider in the **Access key** field. Next, select the **Threat refresh interval**, which defines the frequency of device threat scans.

Possible interval options include 5 minutes, 15 minutes, 30 minutes, 1 hour, 4 hours, 12 hours, once a day, once a week, or once a month.

The selection depends on specific needs and operational scenarios. The recommended value is **once a day**.

On Android devices, the interval is executed with high accuracy and minimal tolerance. On Apple devices (iOS/iPadOS), the behavior depends on system resources allocated to the application, as persistent background execution is not supported by design. Only short background tasks are allowed. Several internal mechanisms are implemented to maintain the most precise execution interval possible.

The last section in the modal is **Enable categorized URL monitoring**.



This functionality enables web content filtering based on a list of risky URLs provided by the MTD solution. In general, it enhances browsing security by automatically filtering web pages through a system-level interceptor that is part of the WebKit framework. It is supported only on supervised devices.

The list of URLs provided by Pradeo is regularly refreshed according to the interval defined in the nested field URL monitoring threat refresh interval. Available intervals include 1 day, 2 days, 3 days, 7 days, 14 days, and 30 days.

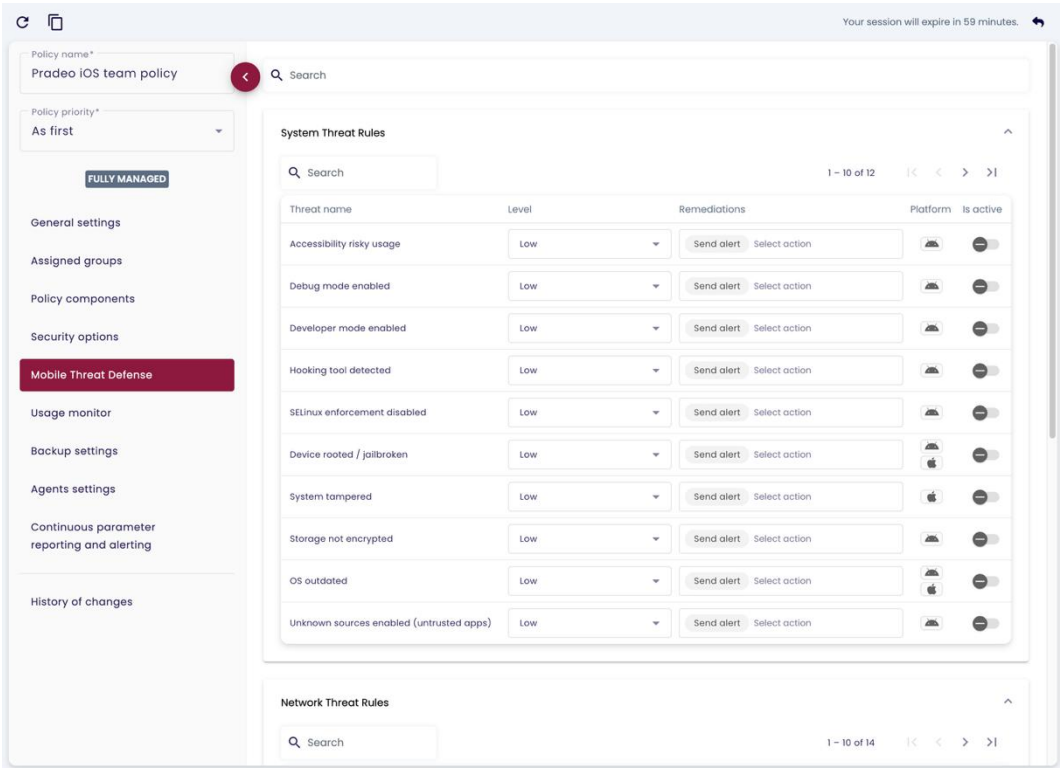
More information about this functionality can be found in the following section concerning categorized URLs.

To complete the first step of the integration, click the **Save settings** button.



2.2 Activate licence on the devices

After configuring the integration settings, full integration also requires activation of the provided access key on the devices to be secured. Entering the access key enables a **new tab in the policies** section named **Mobile Threat Defense**.

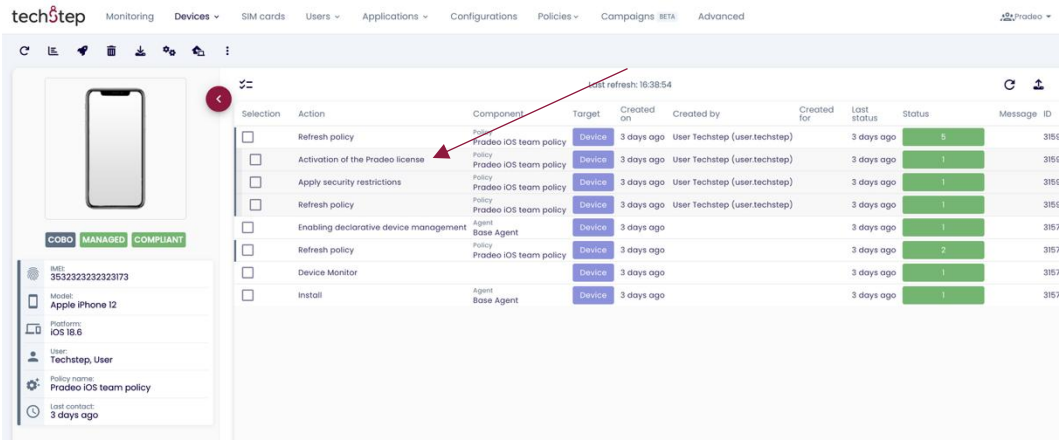


The tab is located directly under Security Options and contains few sections:

- System Threat Rules
- Network Threat Rules
- Global application threats
- Per-application threat rule list
- Enable Malware & Virus scanning for applications

More details about each section are provided in the following parts of this document. At this point, attention should be directed toward completing the integration process by verifying that the license key becomes active on the device.

To do so, any toggle from the policy must be enabled and the policy must be saved. This action will mark the policy as not up to date. During the next policy refresh, an operation named **Activation of the Pradeo license** will be triggered, completing the integration process by registering the device in MTD and initiating threat detection.



As shown in the image above, the operation can be found in the device logs under *Devices* -> *List* -> (select device) -> *Logs*, as well as on the device itself but further details are provided in the following sections.

3. Mobile Threat Defense tab in policies

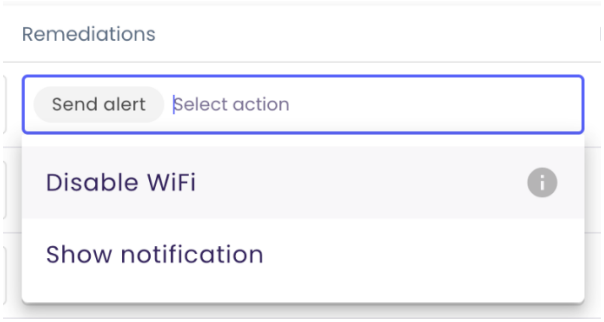
This section provides an overview of the MTD tab, where the user can configure available functionalities and define observed threats. It also includes details on interval operation and the mechanisms behind each component. MTD is supported across all policy types: Fully Managed, BYOD/WPC, and Dedicated.

It should be noted that not all sections are supported on every platform. Compatibility icons are displayed next to the section name or within sections beside specific toggles, as below:



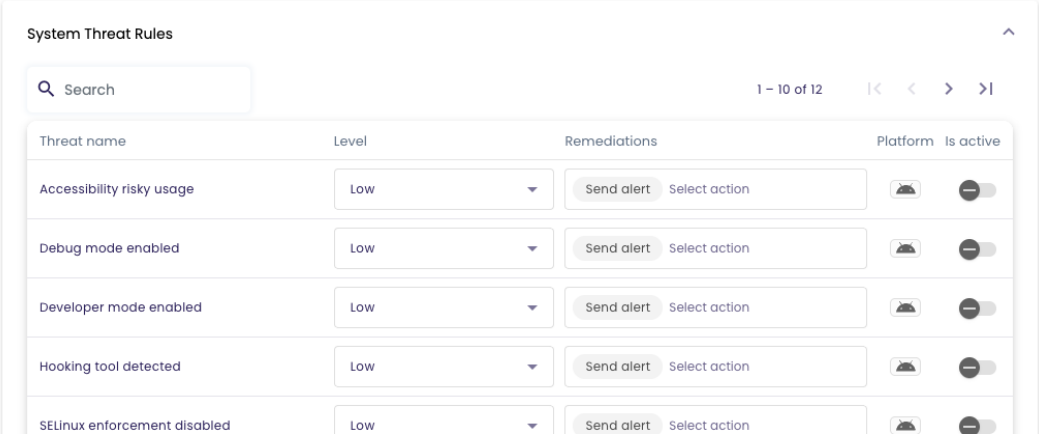
All threats that can appear on the device are defined as **rules**, regardless of the section they belong to. They are referred to as rules because each threat is associated with a corresponding remediation action. This means that when a threat is detected on the device, the appropriate remediation is automatically executed on the mobile side, even without an active internet connection.

Currently, three remediation types are supported: **server alert**, **device notification**, and **Wi-Fi deactivation**. The alert and notification mechanisms inform both the administrator and the user, while the Wi-Fi deactivation option is particularly useful in cases such as man-in-the-middle attacks or rogue access point threats. The list of available remediations is not final and will be expanded in the future.



3.1 Network & System Threat Rules

Network and system threats are scanned on devices according to the interval defined in the organization settings. Scans are performed in batches, covering all enabled threats from the active policy during each scheduled interval. When a threat is detected, the corresponding remediation actions are automatically triggered based on the policy configuration and selected remediation types. Multiple remediations can be applied simultaneously.



As threat types are described below and remediations are already defined, the **Level** column should also be mentioned. This column serves as an informational indicator for administrators and users. It affects messages generated during reporting to the server and while displaying them in device agents. On the iOS agent, three shades of orange and red are used to represent different threat levels.

Next to it, the **Platform** (compatibility) icon indicates which platform supports this type of threat detection. On the right side, a toggle is available to enable or disable threat observation on the device.

3.1.1 Statuses and mechanism

Threats and remediations maintain explicit statuses to reflect detection, execution, and verification stages. When a threat is detected, its status is set to *Remediation started*; after all configured remediations execute successfully, the status changes to *Remediations successfully done*. This does not imply that the threat has been removed - an additional verification step checks whether the threat is still present; if resolved, the status is updated to *Successful*, otherwise it remains *Remediations successfully done*.

If any remediation fails and the threat persists, the overall threat status is set to *Failed*. Each remediation has three possible statuses: In progress (execution underway after detection), Success (execution completed successfully), or Failure (execution did not complete successfully). When a given type of threat (e.g., OS outdated) is resolved, its status is updated automatically and retrospectively across existing operations of that type to reflect the resolution.

Statuses of detected threats are available in the device details on the **Logs** tab, as well as on the **Notifications** tab, which aggregates all alerts generated by the mobile device.

A dedicated **table of detected threats** has also been added to the Device status view, available at *Devices -> List -> (select device) -> Device status* -> click the MTD chart labeled **Mobile Threat Defense**.

Further details are provided in the following sections.

3.1.2 Network & System threats table

Nearly all network and system threat detection features currently available from Pradeo have been implemented; additional features will be included in future releases. The current list is presented in the table below.

Parameter	Description	Compatibility
Network & System Threats		
ARP poisoning	The device is subject to an ARP poisoning attack, meaning its network traffic may be intercepted or diverted without its knowledge. This poses a risk of data leakage or manipulation.	Android
Bluetooth device risk	A Bluetooth connection is active that may expose the device to unauthorized access or data exchange via a nearby device. This can lead to information leakage through the Bluetooth channel.	Android
Connected to open Wi-Fi	The device is connected to a non-secured (open) Wi-Fi network, increasing the risk of network-level attacks such as interception or	Android

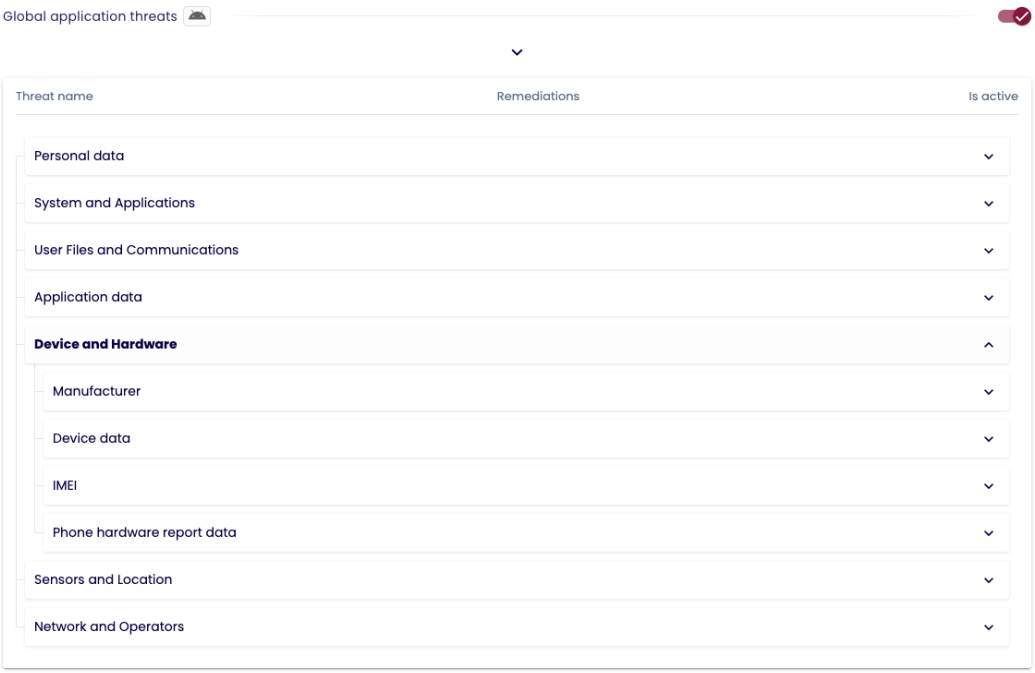
	spoofing. Use of such networks may bypass protections.	
Host file modified	The system hosts file has been modified, which may indicate that network traffic is being redirected to unauthorized servers or that malicious configuration changes exist. This threatens integrity of communication.	Android
Man in the middle attack	The device is under a “man-in-the-middle” (MITM) attack, meaning an attacker is intercepting or altering communications between the device and remote servers. This puts data confidentiality and integrity at risk.	Android, iOS
NFC device risk	The Near-Field Communication (NFC) function is active and may expose the device to local attacks such as data interception, tag manipulation, or unauthorized provisioning. This threatens data exposed via NFC.	Android
Rogue access point	The device is connected to or detecting a Wi-Fi access point that may be malicious (a “rogue” AP). Such access points can intercept or manipulate network traffic.	Android, iOS
Rogue cell tower	The device is exposed to a fake or rogue cell tower, which could intercept voice, SMS or data traffic by masquerading as a legitimate mobile network tower. This risks communications confidentiality.	Android, iOS
Tracking enabled (location)	The device has tracking features enabled (such as location services) which may allow excessive monitoring or data collection. This could impact user privacy or lead to	Android, iOS

	unintended exposure of sensitive data.	
VPN enabled	A Virtual Private Network (VPN) is active on the device, which may mask network traffic but also could interfere with corporate monitoring or control of communications. Administrators must verify policy compliance.	Android, iOS
Accessibility risky usage	Accessibility services are in use in a way that may allow apps to capture screen content or other apps' data. This can be exploited by malicious apps for data leakage or takeover.	Android
Debug mode enabled	The device is running in debug mode, which provides elevated access and could allow malicious actors or apps to manipulate the system or access data they should not. This weakens device security.	Android
Developer mode enabled	Developer mode is active on the device, enabling advanced settings and modifications that bypass standard protections. This may allow installation of risky apps or system changes.	Android
Hooking framework detected	A hooking framework (e.g., for app instrumentation or interception) has been detected, indicating that apps or system functions may be manipulated in non-standard ways. This threatens application and system integrity.	Android
SELinux enforcing disabled	The SELinux enforcement mode is disabled or permissive, reducing the strength of the system's security policy and making it easier for malicious modifications to succeed.	Android
Rooted / Jailbroken device	The device has been rooted (Android) or jailbroken (iOS),	Android, iOS

	meaning system protections have been bypassed. This significantly increases risk of malware, data exfiltration and loss of control.	
System tampered	The operating system integrity on the device has been tampered with (iOS variant), suggesting unauthorized modifications or a compromised state. This may void trust in the device environment.	iOS
Storage not encrypted	The device's data storage is not encrypted, making stored data easily accessible if device is lost or compromised. This increases risk of data breach.	Android
OS outdated	The device's operating system is out of date and missing critical security patches, leaving it vulnerable to known exploits. This reduces the overall security posture of the device.	Android, iOS
Unknown sources enabled (untrusted apps)	The device allows installation of applications from unknown or untrusted sources (Android only), which raises the risk of installing malware or unsafe apps. Administrators should restrict this.	Android
Screen mirroring active	The screen mirroring function is active (iOS), meaning the device's display is being shared externally, which may expose visual sensitive information to unintended viewers.	iOS
Running on simulator	The app or device is running within a simulator (iOS), which may indicate testing or reverse-engineering conditions and reduce trust in the device environment.	iOS

4. Global application rules

After enabling global application threats, Pradeo analyzes the binary files of applications installed on the device; however, **preinstalled applications are excluded**. The section is illustrated by the image below.



For each threat type, three modes are defined for sensitive data usage by applications:

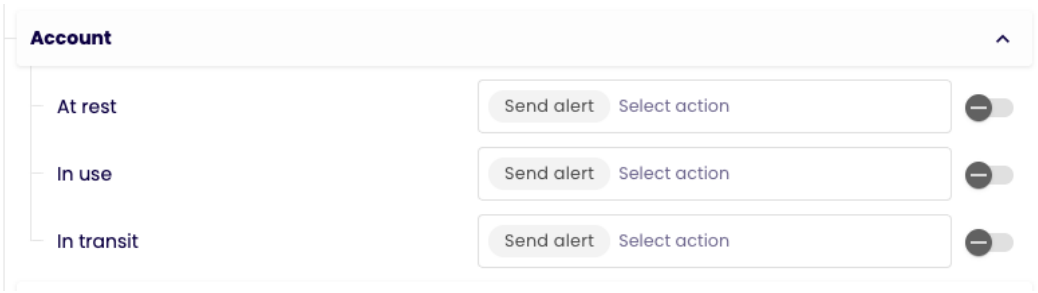
- at rest (read access),
- in use (modify access),
- in transit (data transmission to third parties).

Each mode can be independently enabled and monitored.

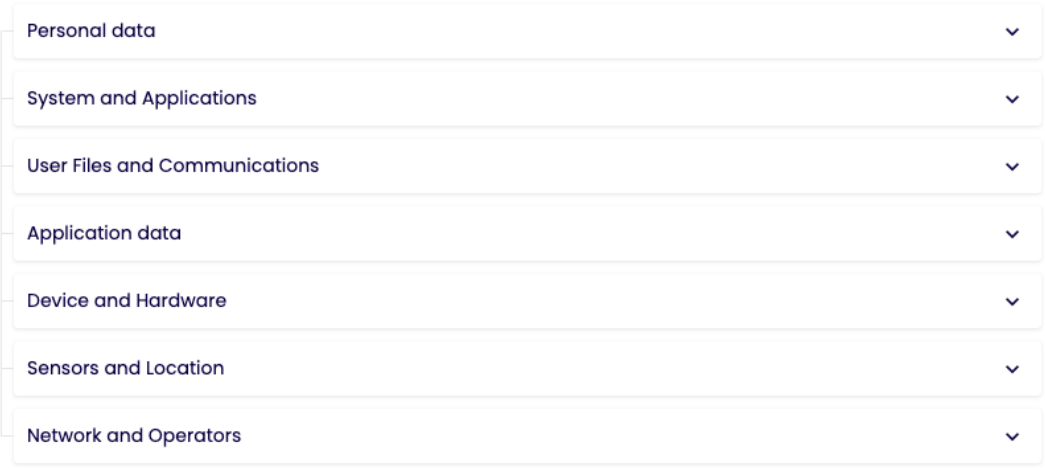
When a threat is detected, its status is set to *Remediation started*; upon successful completion of all configured remediations, the status changes to *Remediations successfully* done. This process is consistent with system and network rule handling. Additionally, the administrator is informed about the specific application (identified by package name) causing the detection. Currently, application threats do not undergo a verification step, so *Remediations successfully done* is the final status.

To **optimize** application report requests, a mechanism dynamically adjusts the reporting interval starting from the configured threat refresh interval. Due to the number of applications and server-side scanning, this interval is efficiently scheduled and may be extended depending on report availability.

Implemented application threats represent cases where an application accesses specific entries, data, or information. For example, detection of a threat based on the “Account” parameter indicates that the application uses a local Android account, which may pose risks in certain scenarios.



The list of implemented application threats is organized into a user-friendly tree structure for easier selection, as shown in the image below.



This hierarchical tree expands into a detailed list of application threats, which is described further in this section.

4.1.1 Application threats table

All enabled application threats in policies are reported to the server, and remediations are executed accordingly. However, the initial version of Essentials MDM with Pradeo integration does not support automatic removal of applications via remediation; this must be handled manually through Device details. Future versions will include automatic remediation to uninstall dangerous applications.

The list below presents **all currently implemented application threats**.

Parameter	Description	Compatibility
Application threats		
User language	The app reads or uses the device's configured language. This may be used for localization but could also be used to fingerprint the user's region or preferences.	Android
Username	The app accesses the device user name. This may reveal a personal identifier that can be used to profile or link activity to a real person.	Android
Device manufacturer	The app reads the device manufacturer information. This helps identify device models but can also be used for device fingerprinting.	Android
Device data	The app collects device details (model, display, product, hardware, serial). Such data can uniquely identify the device and assist targeted attacks or tracking.	Android
Sensor data	The app reads sensor data (e.g., accelerometer, gyroscope). Sensor access can support app features but may also allow inference of user activity or environment.	Android
Device geolocation	The app accesses precise or approximate GPS/location data. Location access reveals user movements and can pose privacy or security risks if shared without consent.	Android

Network information	The app gathers information about the currently connected network. Network info can be used for connectivity handling but also to detect insecure networks or perform fingerprinting.	Android
Operating system information	The app reads the OS version or name. Knowing the OS version helps adjust behavior but may also expose devices with known vulnerabilities.	Android
Mobile network operator	The app reads the GSM operator identifier. This reveals the mobile operator and can be used for profiling or for operator-specific behavior.	Android
Internet service provider	The app reads the ISP / network operator identifier. This is similar to operator info and can be used for profiling or routing decisions.	Android
Camera data	The app accesses the camera or camera data. Camera access can be legitimate for features but risks capturing sensitive visual data if misused.	Android
Contact information	The app accesses contact data (names, phone numbers, thumbnails). Contact access exposes personal connections and carries high privacy risk if transmitted.	Android
Saved address	The app reads stored civic/address information from the device. This reveals precise personal addresses and is sensitive personal data.	Android
Local account	The app uses a local Android account. This indicates the app can read account identifiers stored on the device and may link app data to that account.	Android

Foreground applications	The app detects which application is currently in the foreground. This can be used to infer user activity or to alter behavior depending on which app is visible.	Android
Running applications	The app enumerates currently running apps or services. Listing running apps can be used for fingerprinting, compatibility checks, or to find vulnerabilities.	Android
Installed applications	The app lists installed applications on the device. This is useful for compatibility but can reveal user interests and installed security tools.	Android
Device IMEI	The app reads the device IMEI. IMEI is a persistent hardware identifier and can be used to track or uniquely identify the device.	Android
IP address	The app obtains the device's current IP address. IP addresses reveal network location and can be used for geolocation or network-based profiling.	Android
MAC address	The app reads the device MAC address. MAC is a hardware network identifier that can be used for persistent device tracking if exposed.	Android
Screenshot data	The app accesses data from a screenshot of the current screen. Screenshots may contain sensitive UI content and should be treated as highly sensitive.	Android
SIM phone number	The app reads the SIM card phone number. Phone number access links the device to a contactable identity and raises privacy concerns.	Android
Message content	The app reads message content from SMS/MMS (content, phone number, ...). Message access exposes	Android

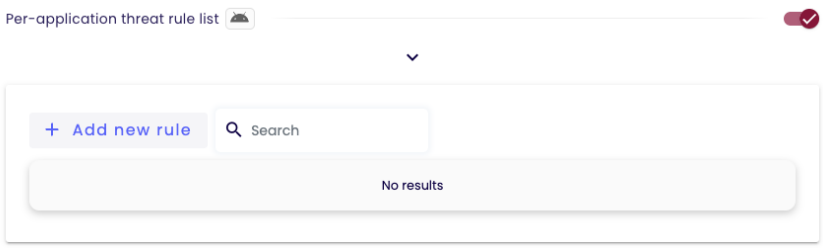
	private communications and is highly sensitive.	
Runtime information	The app accesses current process runtime info (pid, tid, uid). Runtime info can be used for debugging, exploitation or to detect sandbox/analysis environments.	Android
Calendar data	The app reads calendar data (events, attendees). Calendar access reveals schedules and contacts and may expose sensitive personal or business information.	Android
User personal files	The app reads or manipulates user files (Home, Download, SD). Access to personal files can expose documents, photos or other sensitive data.	Android
Unofficial applications	The app detects the presence of unofficial or untrusted apps. This detection can determine whether an application was installed from an official store (such as Google Play Store or Samsung Galaxy Store) or sideloaded onto the device. This may indicate a risky environment where unvetted apps can increase the attack surface.	Android
User call logs	The app reads or modifies call logs. Call log access exposes communication patterns and contact relationships and is privacy-sensitive.	Android
Hardware information	The app reads or modifies phone hardware information. Access to hardware info can allow device fingerprinting or manipulation of hardware features.	Android
Application data	The app accesses files or data handled by the application itself (files, shared preferences...). This	Android

	describes the app's local data handling and any sensitive content it stores.	
Application messages	The app reads or handles messages managed by the application. This can include in-app communications that may contain private content.	Android
Application resources	The app inspects data contained in its resource folder (strings, assets). Resource info can reveal embedded configuration, keys or sensitive text.	Android
Application file content	The app reads files saved in the app's local storage. Local file content may include cached credentials, tokens or personal data that need protection.	Android

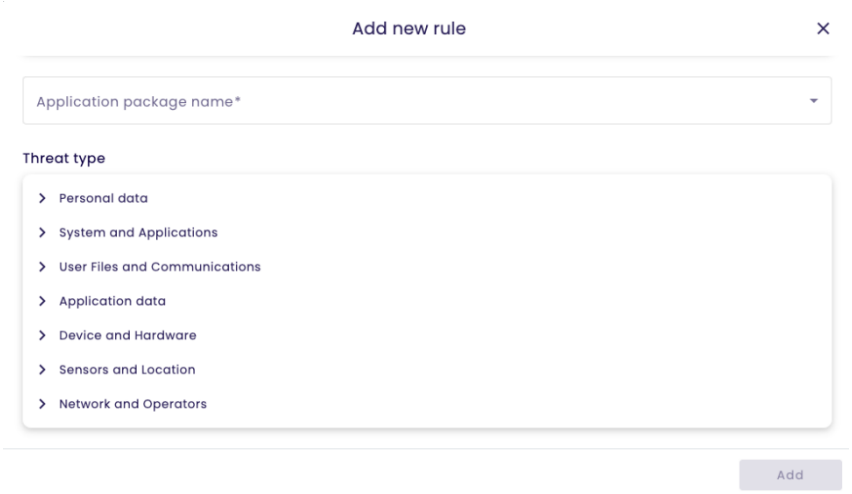
5. Per-application threat rule list

The per-application section allows creating a rule for a specified package name combined with an application threat from the global list. This enables overriding global settings for that specific package. This feature is available only on **Android**, similar to global application rules.

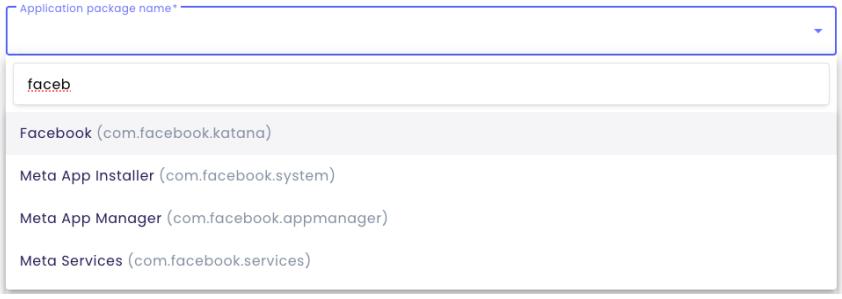
To start adding new rules, the section toggle must be enabled. Then, click the **Add New Rule** button to proceed.



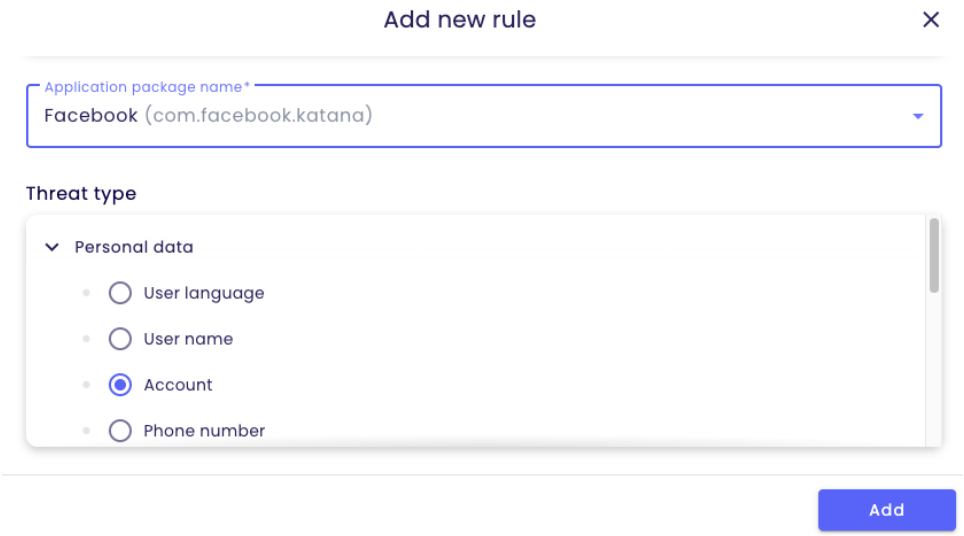
Then, a view with two sections will appear: **Application package name** and **Threat type**.



Firstly, enter the **package name** of the application for which the rule is to be created. A search function is available to facilitate finding the desired package.

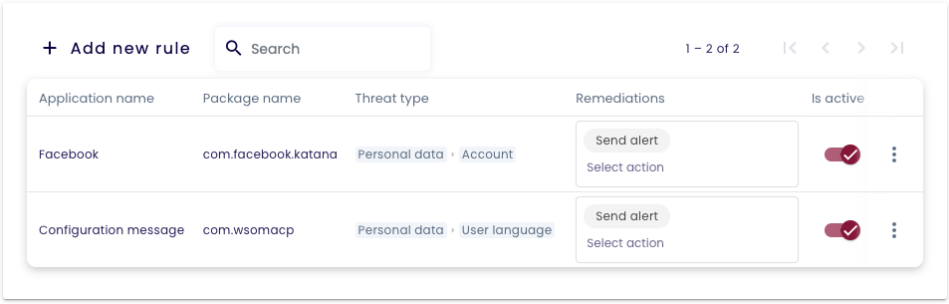


The same hierarchical tree of application threats used in global application rules is also available within the per-application rules section, facilitating consistent threat management. From the category tree, select an application **threat type** to configure in this per-application rule.

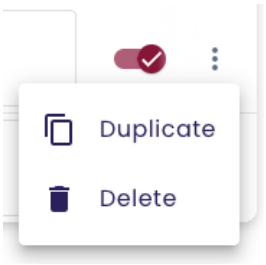


After selecting an application threat from the category tree, all three data usage types-at rest, in use, and in transit-are automatically reported once the rule is created and enabled. Then, click the **Add** button at the bottom of the page.

When two rules are added, the list of per-application rules is displayed as shown below.



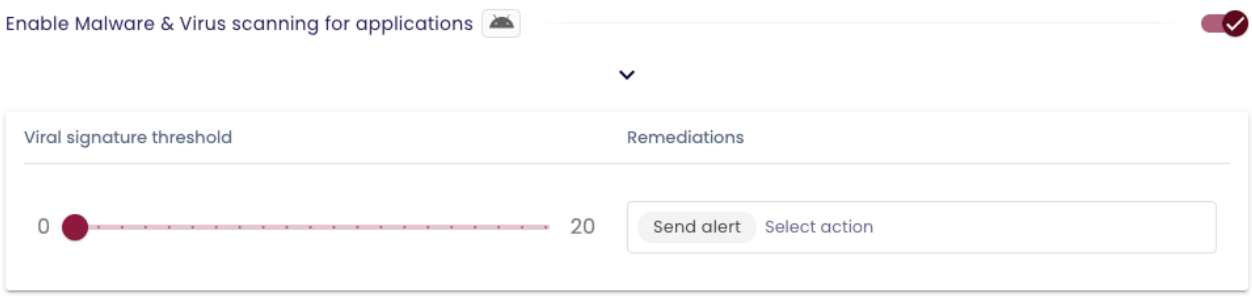
It is possible to set remediation immediately, as well as add, duplicate, or remove rules using the **Actions** button.



Note: This setting overrides the global application rules for the given app.

6. Malware & Virus scanning for applications

This section provides the option to scan applications installed on the device, excluding preinstalled apps. The feature can be enabled using a toggle. When enabled, all installed applications are automatically scanned and reported to the Administrator Console due to the Send Alert remediation setting. Depending on the selected remediations, additional actions may also be triggered.



There are two configuration fields: **Remediation**, which defines the action to perform when a virus is detected, and the **Viral signature threshold**, which specifies how many consecutive vulnerability detections are required for an application to be reported. For example, if the threshold is set to 5, the application will be reported after being flagged for malware or viruses five times in a row. Scans are performed on Pradeo's servers, which use proprietary databases, mechanisms, and algorithms for detection.

The same mechanism as in the Application Threats module is applied here to **optimize** application report requests. It dynamically adjusts the reporting interval, starting from the configured threat refresh interval. Due to the number of scanned applications and server-side processing, this interval is efficiently scheduled and may be extended depending on report availability.

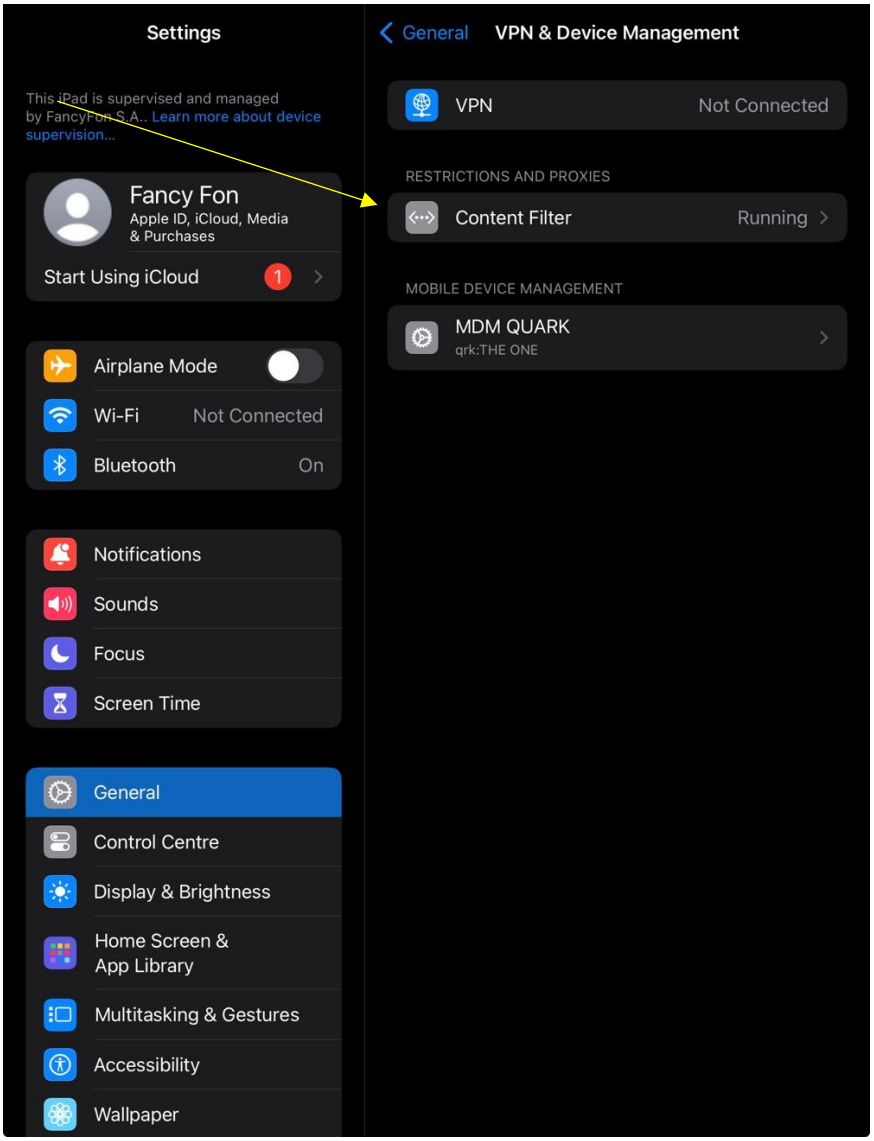
This functionality is only available on **Android** devices.

7. Categorized URLs monitoring

Categorized URL monitoring can be enabled in the organization settings (section 2) and is available only on **supervised iOS** and **iPadOS** devices.

When this functionality is enabled, devices automatically receive an operation that activates the web content filtering feature. This feature securely intercepts browser traffic at the system level and determines which URLs should be allowed or blocked. Apple designed this mechanism to ensure maximum privacy and security - neither Pradeo nor Essentials MDM can view network traffic, but access to URLs identified by Pradeo as risky (for example, phishing sites) can be denied.

The feature works automatically, and no additional configuration is required. To verify that the web content filter is active, go to the device's *Settings*, then navigate to *General → VPN & Device Management*. Confirmation of the filter's status will be visible there, as shown in the image below.



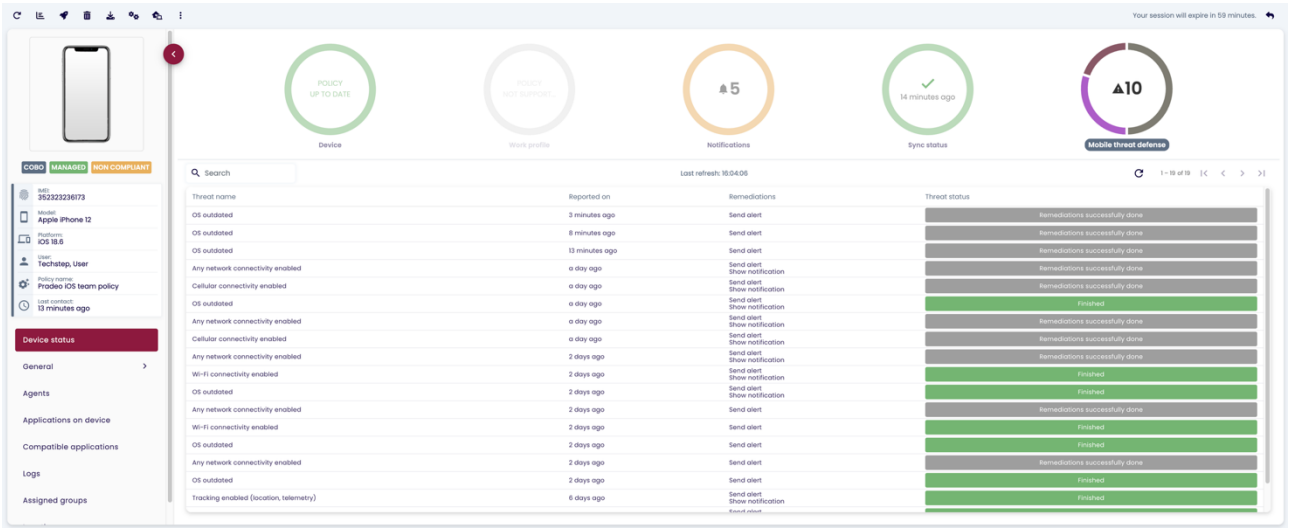
8. Administrator console

Administrators can verify the status of detected threats on devices in three locations: the Device Status section under the **Mobile Threat Defense chart,** the **Notifications tab**, and the **Logs list** available in device details.

8.1 Mobile threat defense tab

The first section, dedicated to threats detected on the device, is a new component added to the console under *Device Details*.

To access it, navigate to Devices -> List -> select a device -> open the Device Status tab on the left, and click the last chart at the top titled **Mobile threat defense**.



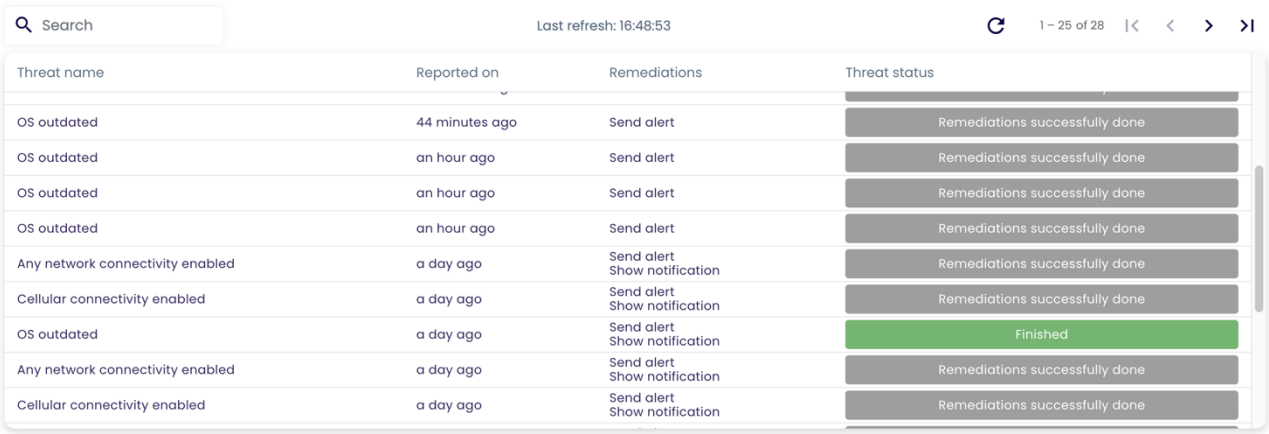
The top of this view includes a chart showing the distribution of detected threat types, providing a quick way to identify them at a high level.



The number displayed before each threat type indicates the exact count of threats detected for that category. The number inside the circle next to the triangle represents the total number of detected threats.

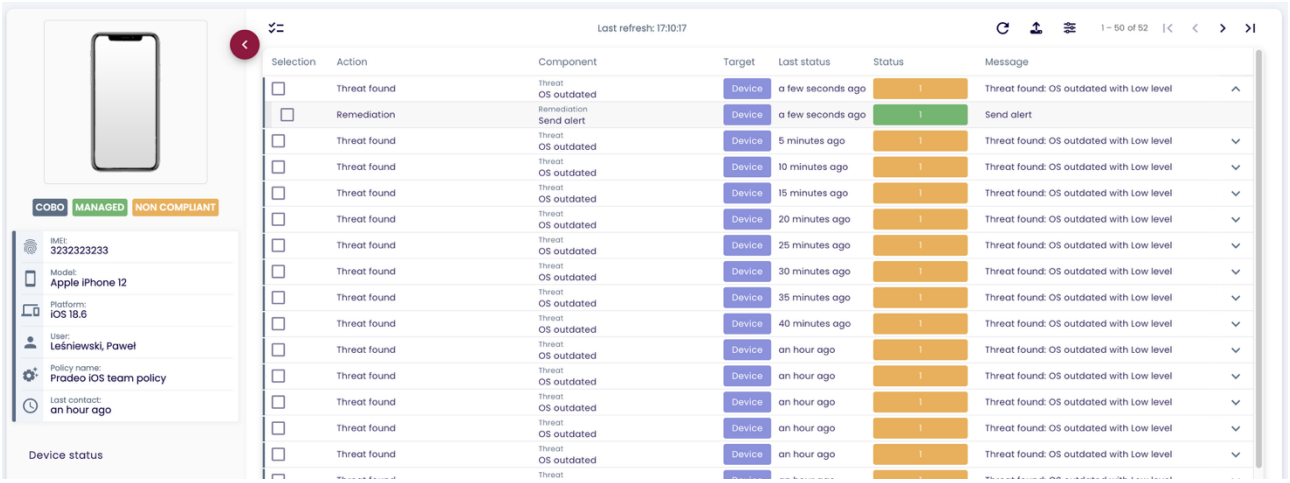
Below the chart, a table lists all threats detected on the device. The table includes the following columns:

- **Threat name**
- **Reported on** – displaying the time when the issue was detected
- **Remediations** – listing all corrective actions assigned to the threat
- **Threat status** – showing the current status as described in section three, where the status mechanism is also explained.



8.2 Logs tab

Each threat detected on the device, in addition to those displayed in the *Mobile Threat Defense* section, is also presented in the **Logs** as operations. The appearance of the table depends on the selected columns, but the most important details are found in the **Action** column, which specifies whether the entry refers to a detected threat or an associated remediation.



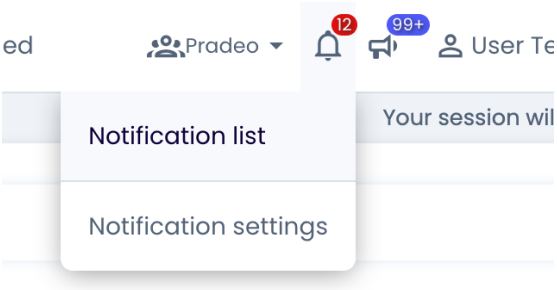
The **Component** column provides information on the threat type, and the statuses correspond to those shown in the *Mobile Threat Defense* tab. The last useful detail is the message generated by the device following the schema: *"Threat found in application: [Threat name] with [Level from Level field]."*

Within the operations view, it is possible to review both remediation statuses and individual threat statuses.

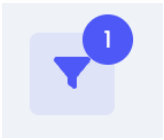
8.3 Notifications tab

The final view showing threats detected and reported to the server is the tab related to the persistent remediation named Send Alert. When a device sends alerts to the server, all of them are displayed in the Notifications tab.

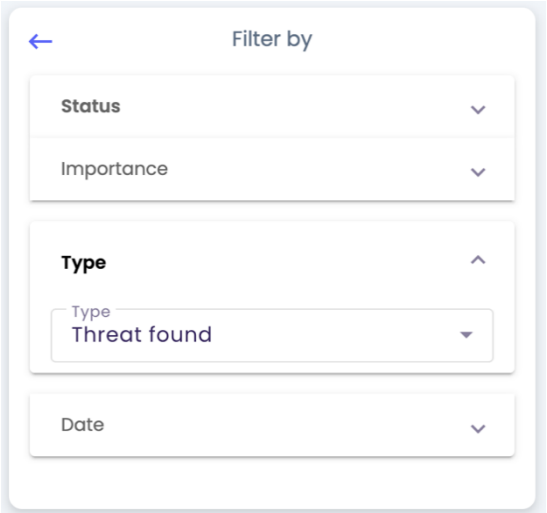
To access the Notifications tab, click the Bell icon at the top of the console, then select Notification List.



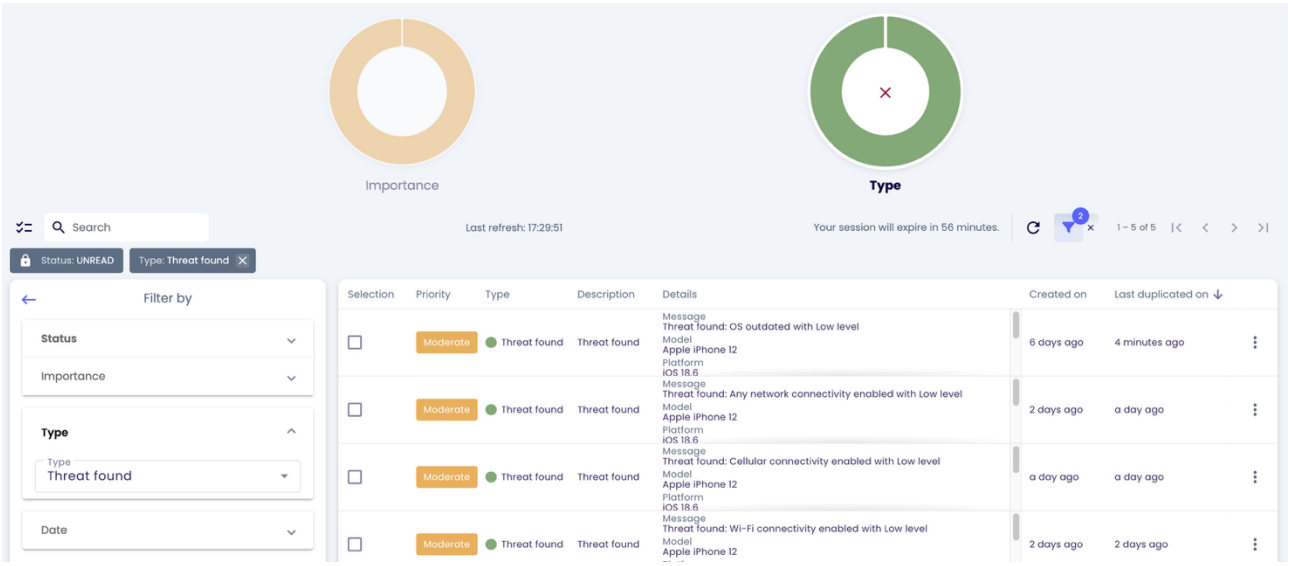
The Notifications tab will then open, displaying all existing alerts. To view only those related to detected threats, click the Filter button.



In the filter list on the left, select *Type* and choose *Threat Found*.



A list of all detected threats across all devices will then appear. In this view, it is possible to filter and group alerts as needed. Alerts can also be marked as read so they no longer appear in the unread counter. To do this, use the action button located at the end of the alert row.



For more details on this tab's functionality, refer to the dedicated *Notifications Tab documentation*.

9. On the devices

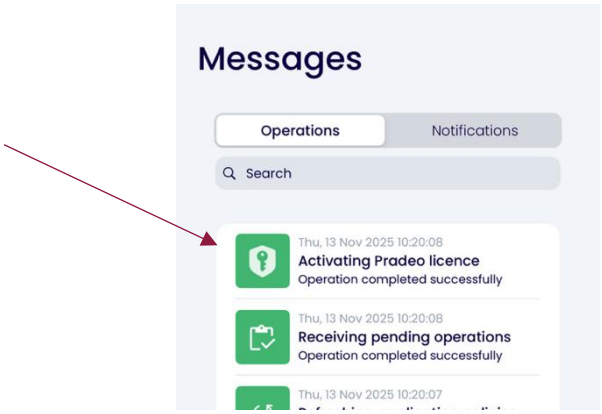
This section provides an overview of the **Mobile Threat Defense status** view available on managed devices. The view is similar across both iOS and Android platforms, and the logic for remediation and threat statuses remains consistent. Further details are described in section 3.1.1.

9.1 iOS & iPadOS devices

Both mobile platforms, **iOS** and **iPadOS**, are supported. The view is adjusted to the platform on both systems and includes two related sections: the *Messages* tab and the *Information* tab with a dedicated chart.

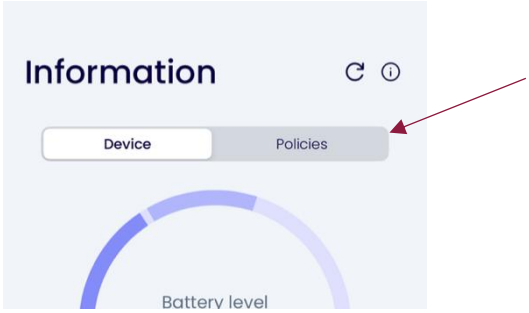
9.1.1 License activation

To start using Pradeo on managed devices, license activation is required. The activation process is described in section 2. When the license is configured in the Administrator Console and any toggle under Mobile Threat Defense in policies is enabled, an operation named "*Activation of License*" is sent to the device. This operation stores the required license locally, enabling access to Pradeo functionality. An analogous operation to **deactivate the Pradeo license** will be sent to the device if all toggles are unchecked in policy or if the integration is disabled.



9.1.2 Chart view on information tab

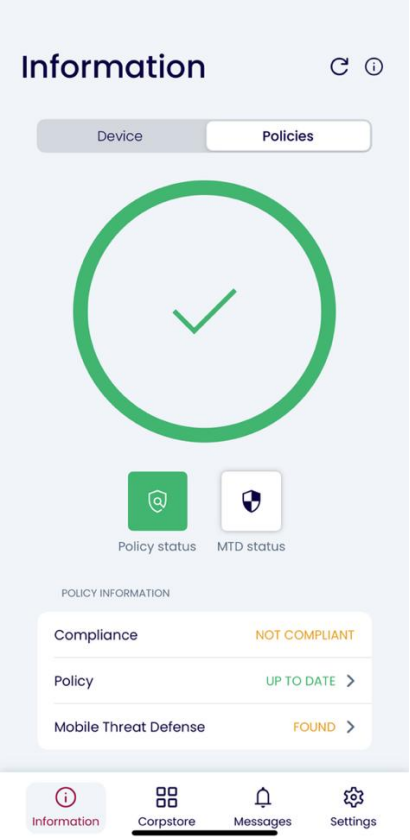
In the Information view, a divider is available that provides access to the *Policies* section. Selecting this option opens a view with a policy chart.



Below the chart, three nodes display policy-related statuses. The first node, **Compliance**, represents the combined result of the **MTD status** and the **policy status**, showing whether the device is compliant or not compliant.

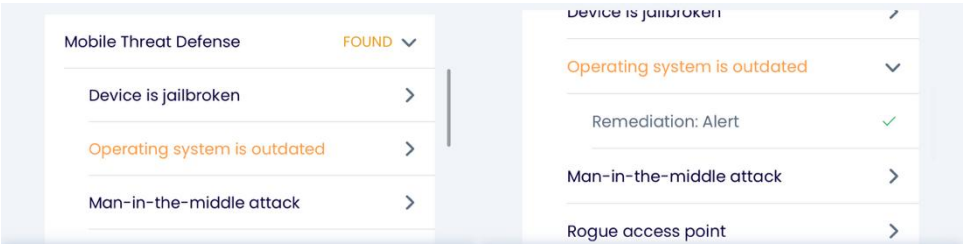
The second node, **Policy Status**, indicates the current policy state and any pending operations.

The third node, **MTD Status**, displays the active Mobile Threat Defense policy and its current state. The same information is also represented below as a circular status indicator. It fills and turns **green** with a checkmark when the policy is applied successfully. If any remediation fails after a threat is detected, the indicator turns **red**. When a threat is still present, it appears **orange** with a pulsing shield icon.

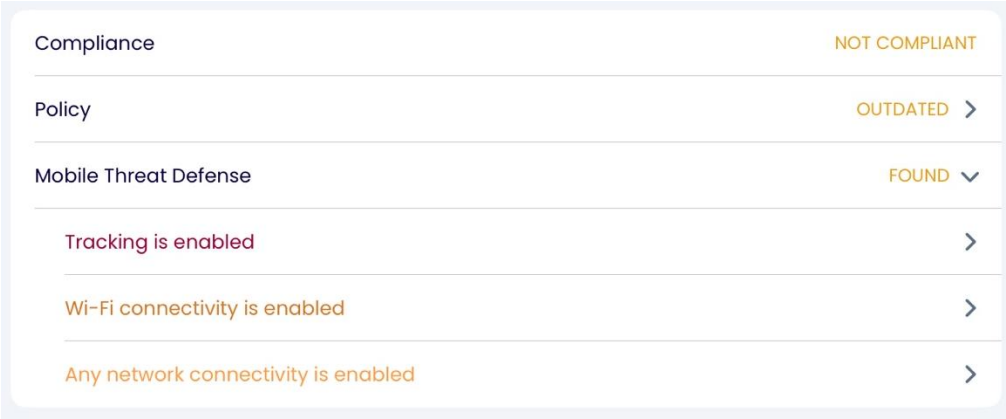


9.1.3 Mobile Threat Defense tab

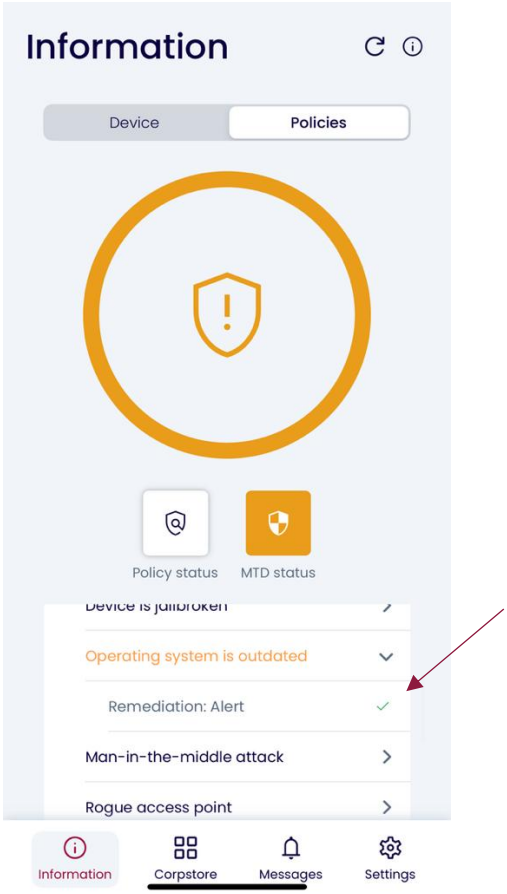
In the **Mobile Threat Defense** tab, all *Network* and *System threats* defined in the policy and compatible with the device platform are displayed. Each listed threat can be expanded to view the remediations assigned to it.



Threats can be displayed in three additional colors depending on the priority level defined in policies by the administrator. A **low-priority** threat is shown in light orange, a **medium-priority** threat in orange, and a **high-priority** threat in red.



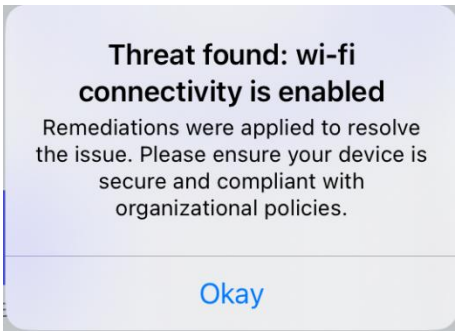
Remediations can display a status icon on the right side if an action was executed in response to a detected threat. A green check icon indicates that the remediation was completed **successfully**, while a red X icon indicates that the remediation **failed**. If no icon is shown, it means that no threat was detected and the entry only provides information about the observed threat type and assigned remediation actions.



9.1.4 Remediations

Apple platforms support only two types of remediations: **Send Alert** and **Show Notification**. The Alert action is triggered on the administrator console, so only the *Show Notification* remediation interacts directly with the user.

The appearance of the notification depends on the app state. When the agent is in the **foreground**, a system **popup** is displayed with information about the detected threat.



When the app is running in the **background**, the information appears as a standard system **notification**.

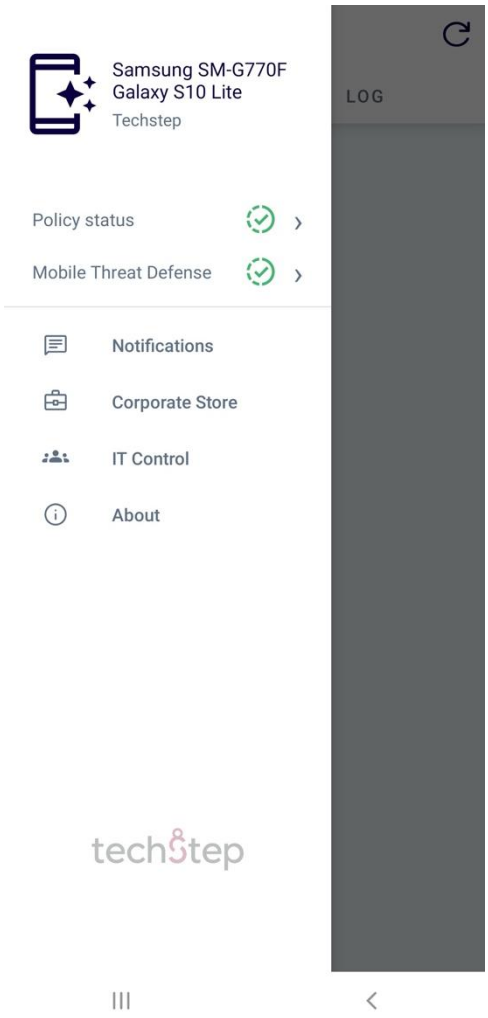


9.1.5 Categorized URLs

Apple platforms natively support web content filtering at the system level. This mechanism securely monitors network traffic to block access to URLs identified by Pradeo as **risky**, such as **phishing** or **spam** sites. The feature is integrated with the operating system to maintain user privacy and operates automatically once enabled in organization settings. For details on how to verify the filter status on the device, see section 7.

9.2 Android devices

On Android devices, a new option is available in the agent's left-side menu that allows users to view the current state of network and system threats, similar to the iOS platform.



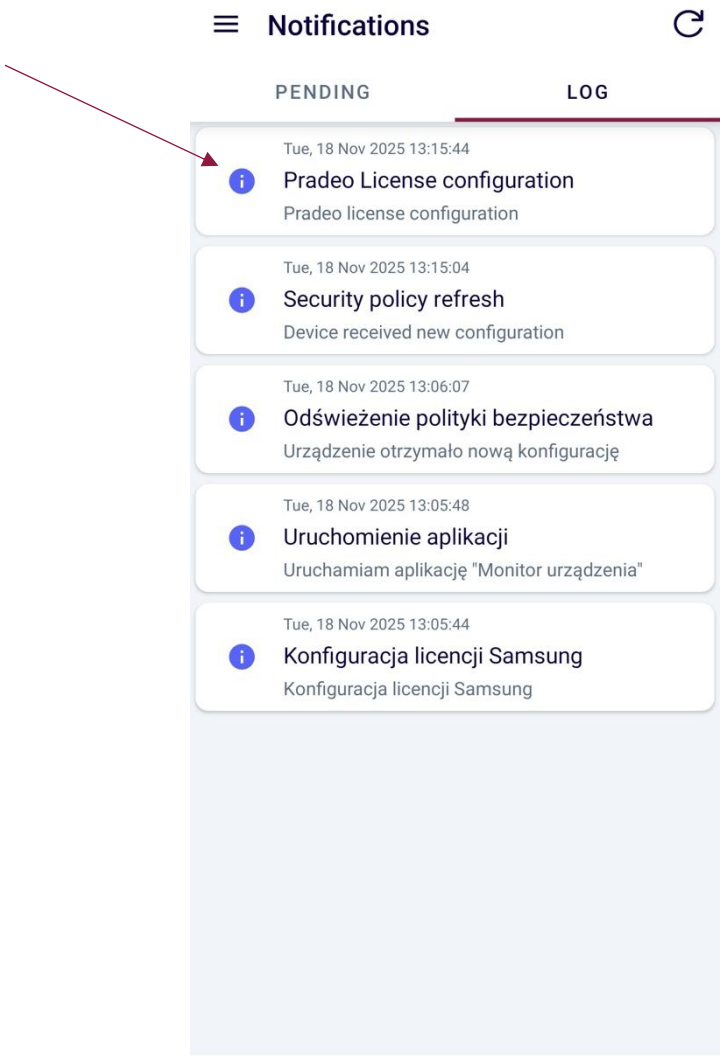
Status indicators are also shown in a circular view, displaying both the active policy status and the new **Mobile Threat Defense** status. However, initially, focus should be on the MTD license, which must be activated on the device before these indicators become available.

9.2.1 License activation

To start using Pradeo on managed devices, license activation is required. The activation process is described in section 2.

When the license is configured in the Administrator Console and any toggle under *Mobile Threat Defense* in the policies is enabled, an operation named "*Pradeo License Configuration*" is sent to the device.

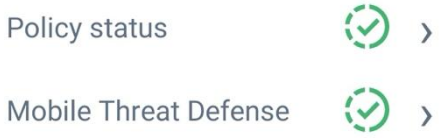
This operation can be found under the **Notifications** tab, in the **Log** subtab. It stores the required license locally, enabling access to Pradeo functionality.



An analogous operation to **deactivate the Pradeo license** will be sent to the device if all toggles are unchecked in policy or if the integration is disabled.

9.2.2 Status tab

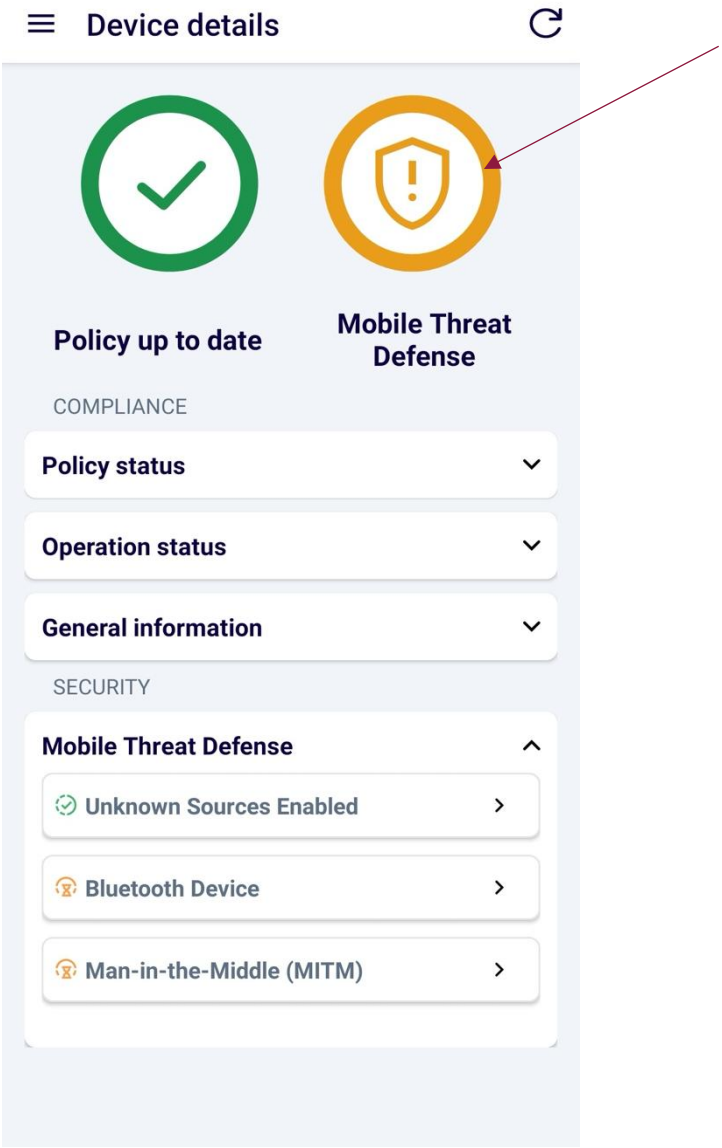
In the **Status tab**, two policy entries are available: *Policy status* and *Mobile Threat Defense* status.



After clicking on them, users are granted access to the *Compliance* and *Security* section. Selecting this option opens a new view that displays two policy views.

These charts provide insights into **policy status** and **MTD status**, helping administrators monitor and manage policies effectively.

Below the chart, the first section, named **Compliance**, represents the policy status and the operations status with all pending operations. It also includes general information about the device and the user.

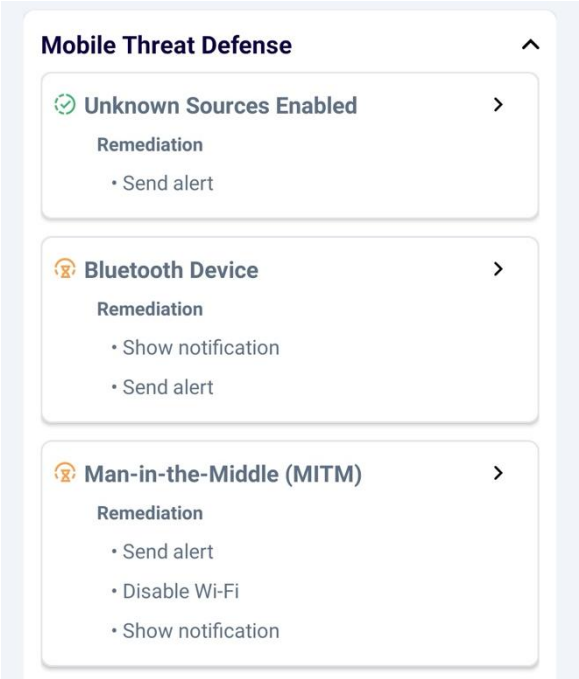


The second section, **Security**, indicates the current Mobile Threat Defense state. It displays the active Mobile Threat Defense policy and its current status. The summary of threat statuses from observed rules is also shown above as a circular status indicator. The indicator turns **green** with a checkmark when the policy is applied successfully and no threats are detected. If any remediation fails after a threat is detected, the indicator turns **red**. When a threat is still present or has not yet been checked, it appears **orange** with a shield icon. To view the observed rules, expand the Mobile Threat Defense field.

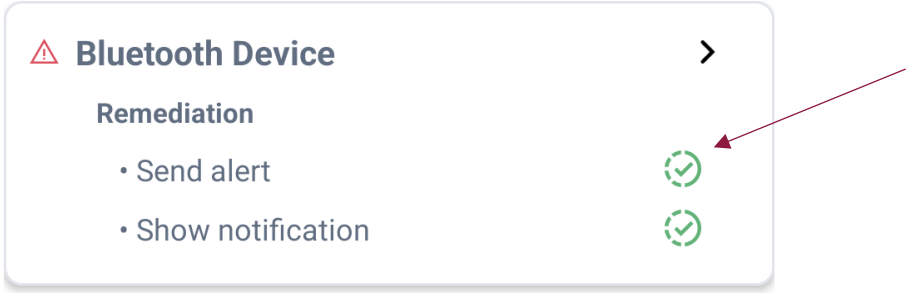
9.2.3 Mobile Threat Defense tab

In the **Mobile Threat Defense** tab, all network and system threats defined in the policy and compatible with the device platform are displayed. Each listed threat can be expanded to view the remediations assigned to it.

When a **threat** is detected, a **red** triangle icon appears before the threat name. If the threat is not present on the device, a **green** checkmark is shown. When a scan has not yet been performed, an **orange** "outdated" icon is displayed.



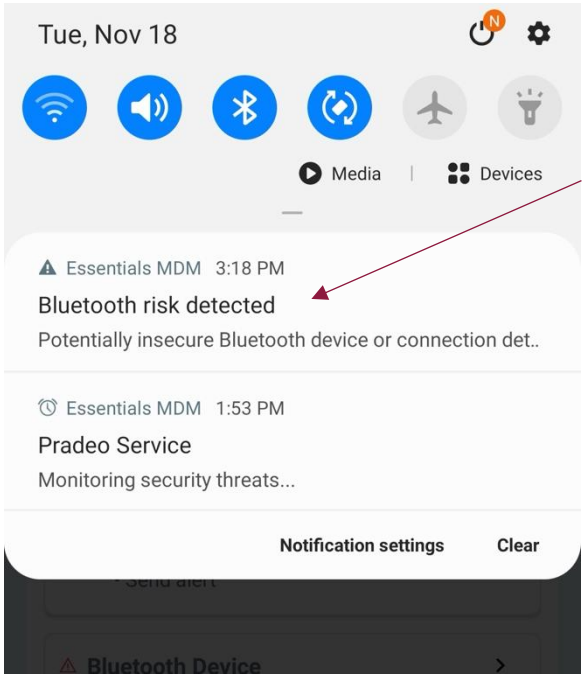
Remediations can display a status icon on the right side if an action was executed in response to a detected threat. A green check icon indicates that the remediation was completed **successfully**, while a red X icon indicates that the remediation **failed**. If no icon is shown, it means that no threat was detected and the entry only provides information about the observed threat type and assigned remediation actions.



9.2.4 Remediations

Android platforms support three types of remediations: **Send Alert**, **Show Notification**, **Disable WiFi**. The Send Alert action is triggered on the administrator console, although the *Show Notification* and *Disable WiFi r*emediations interacts directly with the device.

When the agent detects a threat, it displays information about the detected threat in a notification.



9.2.5 Global & per-application rules

On the device side, applications are scanned in the background **during each policy refresh**. The scan covers all installed apps, **excluding preinstalled ones**. Scanning each app takes up to 12 minutes, and if a threat is detected, remediations are executed automatically.

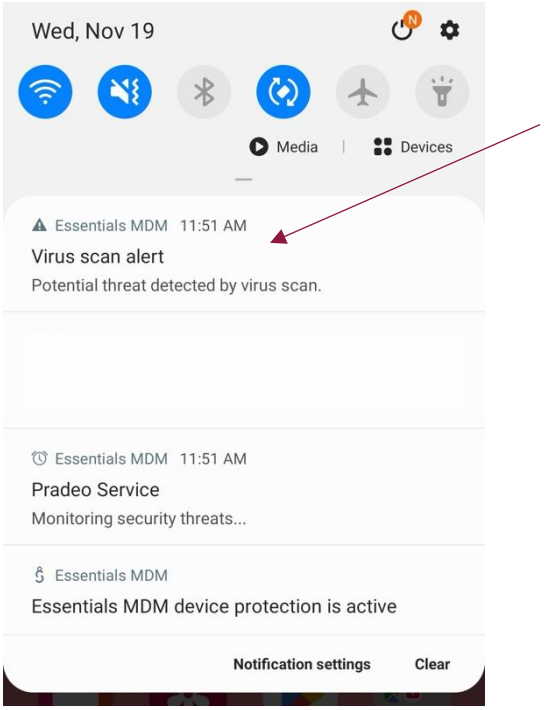
Scanning is performed on behalf of the Mobile Threat Defense provider; when the service provider does not return a report, the process may time out without notifying the user.

In the future, the entire application reports functionality will be moved to a backend-to-backend solution for improved performance and security.

Details about how global application rules work can be found in the Global Application Threats and Per-Application Threat Rule List sections. The only information visible to the user about the scan performed is a remediation notification, similar to those shown for other threats.

9.2.6 Malware & Virus scanning for applications

Similar to the application report, virus scanning also applies to applications. The scanning mechanism operates with a 12-minute timeout during the malware scan performed **on policy refresh**. After the scan, the device attempts to deliver a report containing any detected viruses or malware within the same 12-minute timeout. If the timeout expires, no report is sent to the server. When a virus is detected, **remediation** actions configured by the Administrator in the policies section are **automatically initiated**.



Additional information regarding this section of the policies can be found in section four.