

Unified Mobile Security Platform

Directed Activity Beta Testing

Updated February 22, 2023

Table of Contents

| | |
|---|-----------|
| Threat Hunting - Filters (Network) | 4 |
| Threat Hunting - Filters (Malware Discovery) | 7 |
| Create Teams | 10 |
| Search Devices Across Teams | 14 |
| Create Policies for a Team | 16 |
| Clone Policies | 18 |
| Create Groups for a Team | 20 |
| Enroll Devices into each Team - Local Group Activations | 24 |
| Enroll Devices - Group Activation | 27 |
| Enroll Devices - App-Based Inventory Collection Setup (Android Only) | 28 |
| Enroll Devices - App-Based Inventory Collection (Android Only) | 30 |
| MDM Integration - zConsole Setup | 33 |
| MDM Integration - MTD Connector (Microsoft Endpoint Manager) | 38 |
| MDM Integration - Schedule Sync | 40 |
| MDM Integration - Managed App Configuration | 42 |
| App Policies - Out of Compliance Apps | 45 |
| App Policies - Allow Developer Signatures | 50 |
| Partner Setup - Branding | 53 |
| Partner Setup - Create Customer Tenant (UI Based) | 56 |
| Partner Setup - Test Customer Tenant Login | 58 |
| Partner Setup - Create Customer Tenant (API Based) | 60 |

Threat Hunting - Filters (Network)

- Perform a global search for company Wi-Fi network to see all detected threats on that network.

The Threat Intel team was notified by an end user that a strange Wi-Fi name (similar to the office Wi-Fi name that they are familiar connecting into) is available to connect to around the office. The analyst is tasked with finding any suspicious networks or related network attacks.

The analyst can do the following:

1. Select the Threats Tab.
2. Search for the vector type using the keyword “Network.”
 - A large number of Threats that relate to Networks are shown.

Console v5.20.0-SNAPSHOT zIPS

All Teams ▾

Dashboard
Activations
Apps
Devices
Threats
Policies
Integrations
OS Risk

Threats

9 Total Threats
0 Critical
0 Elevated

0 Device Threats

0 Nov 6 '22 Nov 13 '22 Nov 20 '22 Nov 27 '22 Dec 4 '22 Dec 11 '22 Dec 18 '22 Dec 25 '22

network ← Search for Network Related Threats events

Applied Filters

| Severity | Status | Vector ↓ | Threat Name | App Name | Version | OS | Device ID |
|----------|---------|----------|-----------------------|----------|---------|---------|----------------------|
| Low | Fixed | Network | Danger Zone Connected | zIPS | 4.22.8 | iOS | F996C370-E350-4EA9- |
| Low | Pending | Network | Danger Zone Connected | zIPS AFW | 4.22.5 | Android | 89326b5d-fdbc-4f30-b |

To hunt for any patterns and see if any threats are related, the analyst follows these steps:

1. Clicked into one of the first Network Threats, in this case, it was a Rogue Access Point.
2. Scroll down and Identify the Network SSID
 - It is found that attackers used a familiarly crafted Network ID, which is similar to the corporate Wi-Fi name.
 - The analyst can hover over and click the Network SSID value.
 - Network SSID is added to the active search filters.

Console v5.20.0-SNAPSHOT zIPS

All Teams ▾

Threats

Total Threats 3 0 Critical 0 Elevated

Device Threats 0

Activation Name testuser1@z.com

Event ID 35df0ad8-b953-4a86-9dd0-b102a3363bad

App ID 53f4d673-98a8-55b7-a4e6-3ff3b4ee6f7f

Bundle ID com.zimperium.zIPS.appstore

App Name zIPS

App Version 4.22.8

zDefend Version 4.22.8

zEvent Id 0af9d0d1-2108-40a1-9867-819b46f953ed

zDefend Build 463175

OS iOS

General Process List Network Status ARP Tables Nearby

Time Interval N/A

Device IP 192.168.50.85

Network SSID SunnyAir +

Network BSSID fc:34:97:24:fc:54

Action Triggered N/A

External IP N/A

Hover and Click the + button

Add the SSID to the Filters

It is quickly discovered that multiple events are related to the same Network SSID within the same geographic location. This could confirm a targeted network attack on the office location.

Console
v5.20.0-SNAPSHOT

zIPS

10

All Teams

Dashboard

Activations

Apps

Devices

Threats

Policies

Integrations

OS Risk

Docs

Policy

Terms

Jason S.

Threats

3

0 Critical
0 Elevated

Total Threats

0

0 Critical
0 Elevated

Device Threats

3

0 Critical
0 Elevated

Network Threats

network

Network SSID: SunnyAir

| Severity | Status | Vector | Threat Name | App Name | Version | OS | Device ID | Device Owner | MAM ID | Team Name |
|----------|---------|---------|-----------------------|----------|---------|---------|---------------------------|-----------------------|--------|-----------|
| Low | Fixed | Network | Danger Zone Connected | zIPS | 4.22.8 | iOS | F996C370-E350-4EA9-99... | testuser1@z.com | | Default |
| Low | Pending | Network | Danger Zone Connected | zIPS AFW | 4.22.5 | Android | 89326b5d-fdbc-4f30-b4b... | LeeG@M365x79437798... | | Default |
| Low | Pending | Network | Danger Zone Connected | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1-b92... | | | Default |

Threat Name

Danger Zone Connected

Threat Vector

Network

Threat Category

Danger Zone

Threat Severity

Low

Status

Pending

Last Mitigated

N/A

Simulation State

Real Threat

Timestamp

2 Feb 2023 11:35 AM

Device ID

76710385-8f9e-3ef1-b921-63d6b54a4e82

MAM ID

N/A

Map

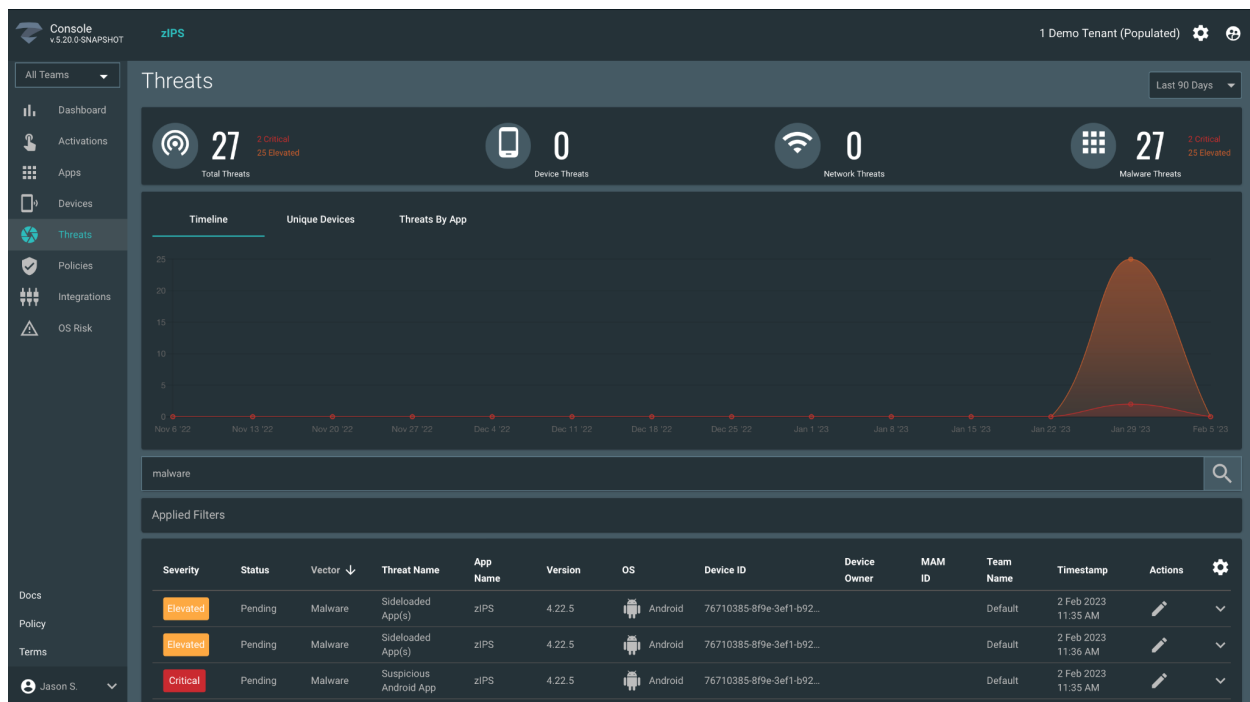
Satellite

Threat Hunting - Filters (Malware Discovery)

- Open a malware threat and click on the name of the malware in the forensics to display all other threats with that same malware name. Find sideloaded app.

The SOC believes there could be a targeted, cross-platform malware campaign. To start hunting on mobile, the analyst can follow these steps:

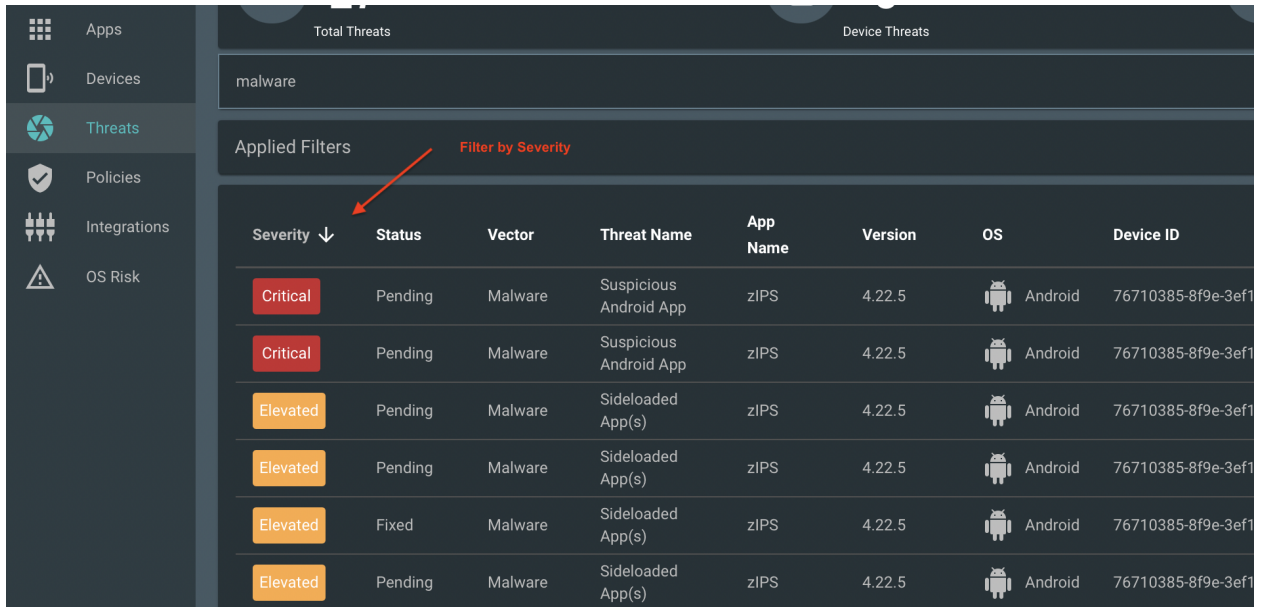
1. Select the Threats Tab.
2. Search for the vector type using the keyword “Malware.”
 - A large total of Threats that relate to Malware or Malicious Apps are shown.
 - Based on the Timeline, most threats occurred on a particular date.



To investigate further, the analyst can do the following:

1. Sort using the Severity column.
 - They discover multiple confirmed cases of Malware and a large amount of Side Loaded Apps.

2. Click into the top Malware Threat (Suspicious Android App).



The screenshot shows a security dashboard with a sidebar on the left containing navigation links: Apps, Devices, Threats (highlighted), Policies, Integrations, and OS Risk. The main content area has a search bar with 'malware' entered. Below the search bar, there's a section for 'Applied Filters' with a red arrow pointing to the 'Severity' header and the text 'Filter by Severity'. The table below lists threats with columns: Severity, Status, Vector, Threat Name, App Name, Version, OS, and Device ID.

| Severity ↓ | Status | Vector | Threat Name | App Name | Version | OS | Device ID |
|------------|---------|---------|------------------------|----------|---------|---------|--------------------|
| Critical | Pending | Malware | Suspicious Android App | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |
| Critical | Pending | Malware | Suspicious Android App | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |
| Elevated | Pending | Malware | Sideloaded App(s) | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |
| Elevated | Pending | Malware | Sideloaded App(s) | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |
| Elevated | Fixed | Malware | Sideloaded App(s) | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |
| Elevated | Pending | Malware | Sideloaded App(s) | zIPS | 4.22.5 | Android | 76710385-8f9e-3ef1 |

To continue their investigation, the analyst wants to check if the device with active malware has any other related threats. They can follow these steps:

1. Inside the Threat event, hover and click on the Device ID value.
 - a. Device ID is added to the active search filters.
 - b. Now only Threats for the selected Device ID will show in the Threat log.

Create Teams

- Then go into the account management settings → users → teams, and add a new team.
- Set up 2 more teams by geography and subsidiary (Division 1, Division 2).

This organization has both BYO and corporate devices, which demands different privacy and security policies - to ensure PII is not collected and security does not over-reach on personal devices. The organization also categorizes its workforce into two divisions, known as “Field Workers” and “Office Workers.”

To meet these grouping and policy requirements, the concept of “Teams” and “Groups” was introduced.

Teams are the overarching mechanism to address the separation of company divisions, geographical regions, or any other organizational separation requirements. For Managed Service Provider (MSP) scenarios, please instead refer to the partner management guides.

Groups can be created within each of these teams to provide a granular separation of administration, end users, and use cases. **Global Groups** can also be created by Global admins and assigned to multiple teams.

Note: *Groups are not the same as Activation Groups, they serve a separate purpose in zConsole.*

Policies are assigned to Groups, allowing admins to meet the unique policy requirements of each Group of users. Policies can be assigned to a single group or multiple groups.

Users & Devices now logically belong to groups and inherit the policies assigned to their given group.

| Teams | Groups | Policies |
|---|---|--|
| Company Division 1 Field Workers | Group 1 MDM - Corporate Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 2 MDM - BYO Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 3 Rugged Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 4 High Security Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| Company Division 2 Office Workers | Group 1 Corporate Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 2 BYO Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 3 Rugged Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |
| | Group 4 High Security Devices | Privacy, Threat, Device Inactivity, App Settings, Network, App |

Currently, the analyst is viewing “All Teams” for an organization-wide view of the environment.

Console

v5.20.0-SNAPSHOT

zIPS

1 Demo Tenant (Populated)

⚙️

🔍

All Teams

Dashboard

Activations

Apps

Devices

Threats

Policies

Integrations

OS Risk

Docs

Policy

Terms

Jason S.

Devices

All Time

10

Total Devices

5

iOS

5

Android

Applied Filters

| Model ↑ | OS | OS Version | App Name | Version | Build | Team Name | Group Name | Device Owner | Created | Actions | ⚙️ |
|---------------------|---------|------------|----------|---------|----------------|-----------------------|----------------|------------------------|---------------------|---------|----|
| Nexus 5 | Android | 6.0.1 | zIPS | 4.22.5 | 10324 | Field Worker Division | Default Group | cory.walker@zFun.com | 7 Feb 2023 10:21 AM | 🗑️ | ⌵ |
| Pixel 2 XL | Android | 10.0 | | | | Default | sg-Engineering | LeeG@M365x79437798... | 3 Feb 2023 10:37 AM | 🗑️ | ⌵ |
| Pixel 2 XL | Android | 10.0 | | | | Default | sg-Engineering | LeeG@M365x79437798... | 4 Feb 2023 2:01 PM | 🗑️ | ⌵ |
| Pixel 2 XL | Android | 10.0 | zIPS AFW | 4.22.5 | 10324 | Default | sg-Engineering | LeeG@M365x79437798... | 3 Feb 2023 4:35 PM | 🗑️ | ⌵ |
| Pixel 4 XL | Android | 12 | zIPS | 4.22.5 | 10324 | Default | Default Group | | 2 Feb 2023 11:35 AM | 🗑️ | ⌵ |
| iPhone 6s | iOS | 15.1 | | | | Default | sg-Engineering | LeeG@M365x79437798... | 3 Feb 2023 10:43 AM | 🗑️ | ⌵ |
| iPhone 8 Plus (GSM) | iOS | 13.2 | zIPS | 4.22.8 | 3114 | Default | Default Group | testuser1@z.com | 2 Feb 2023 10:08 AM | 🗑️ | ⌵ |
| iPhone 11 Pro Max | iOS | 15.0.2 | zIPS | 4.22.6 | 3091 | Field Worker Division | Default Group | Bella.hondura@zFun.com | 7 Feb 2023 10:17 AM | 🗑️ | ⌵ |
| iPhone14,3 | iOS | 16.2 | Zips 5 | 5.0.0 | 20221128182554 | Field Worker Division | Default Group | steven.he@zFun.com | 3 Feb 2023 2:36 PM | 🗑️ | ⌵ |
| iPhone 7 (GSM) | iOS | 14.0.1 | zIPS | 4.22.7 | 3100 | Default | Default Group | | 2 Feb 2023 10:10 AM | 🗑️ | ⌵ |

Rows per page:

25

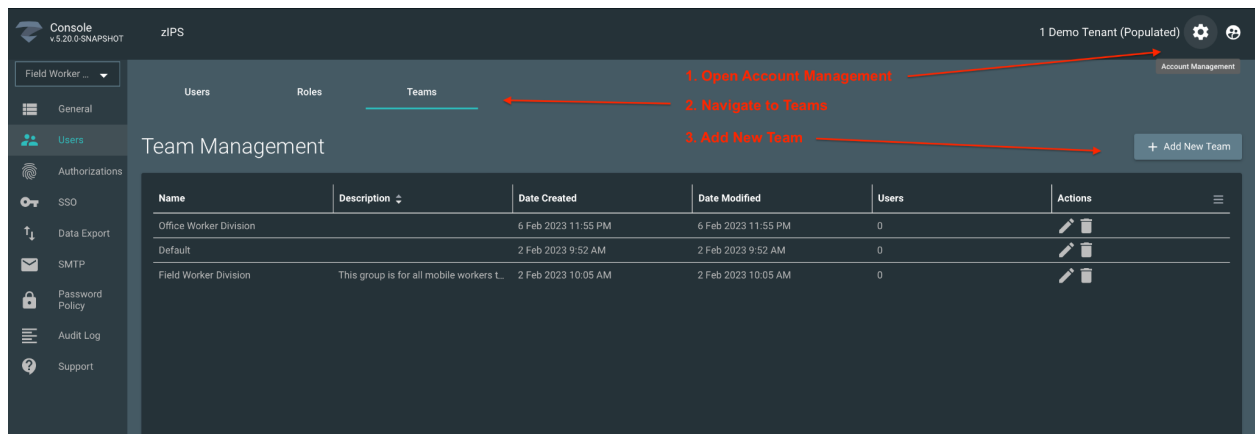
1-10 of 10

⏪

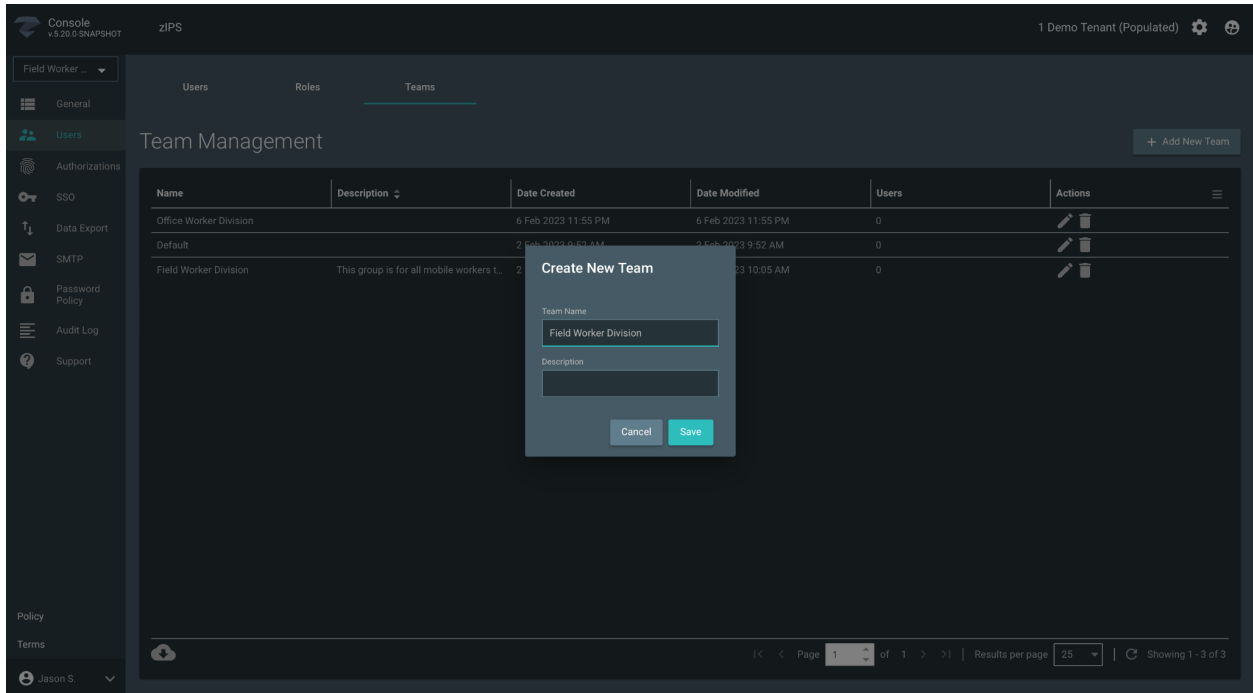
⏩

To create new Teams for the two divisions, the admin proceeds to:

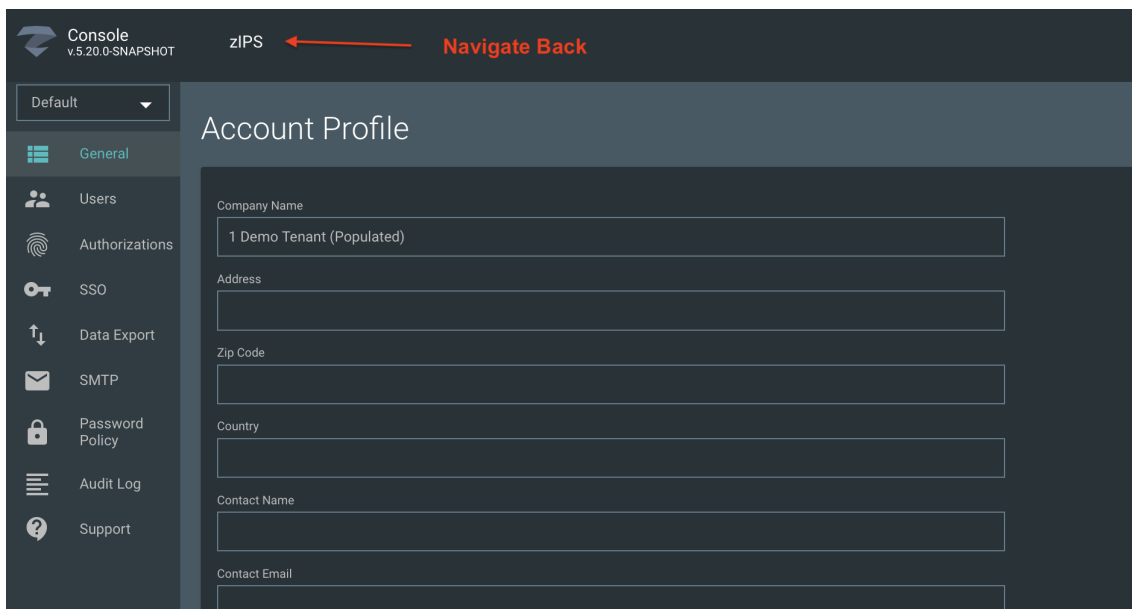
1. Open the top-right account management settings cog.
2. Select the Users tab.
3. Select the Teams option.
4. Select + Add New Team



5. The analyst names the first Team the “Field Worker Division” and then the second called the “Office Worker Division.”



The analyst navigates back to the zIPS main console section by clicking on “zIPS” in the top product bar.

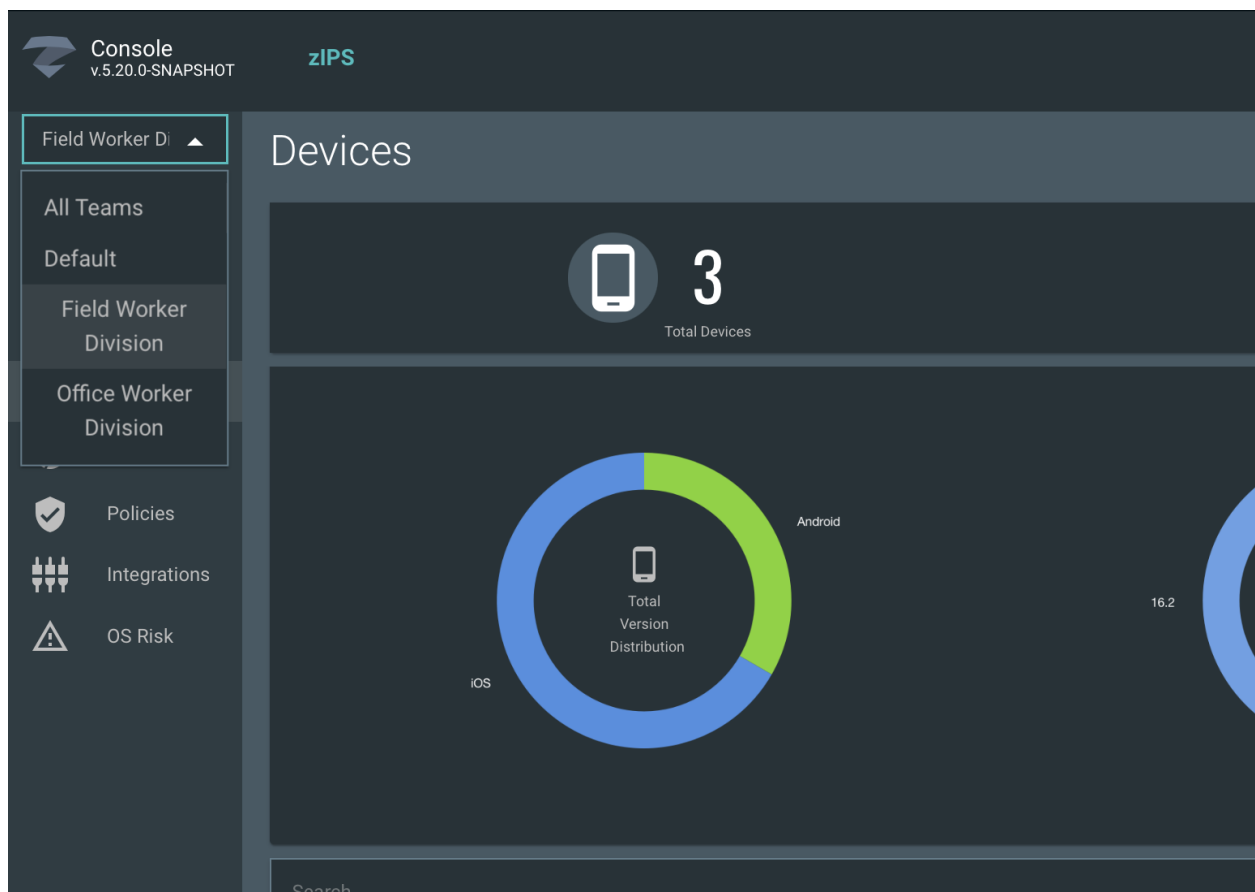


Search Devices Across Teams

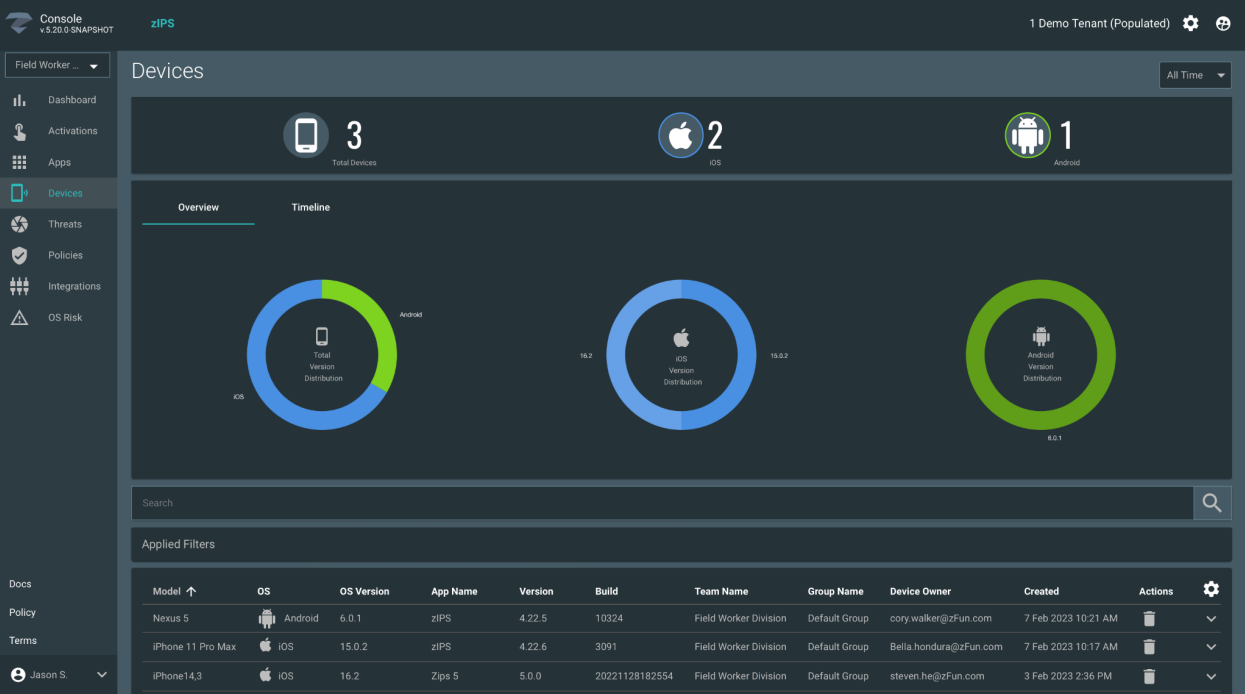
Show multiple devices returned and prove global due to devices being in a different team than lower group level?

- Show that your devices, policies, etc., are segregated by team.

The analysts can now quickly change their console view to see specific Teams using the top-left Teams drop-down option.



Once a team is selected, all views within the console will be specific to that Team. Including Dashboards, Activations, Apps, Devices, Threats, Policies, Integrations, and OS Risk.



Docs

Policy

Terms

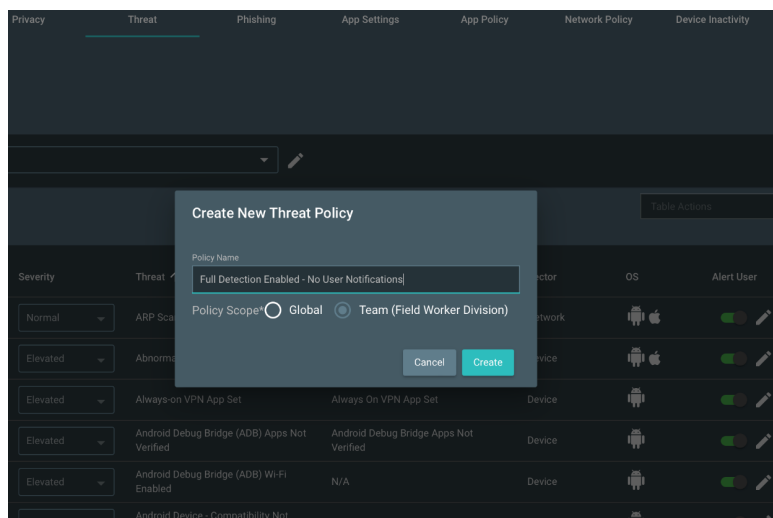
Jason S.

Create Policies for a Team

- Create a new threat policy that is team-bound (Division 1) and assign it to Division 1 Group.
- Show that your devices, policies, etc., are segregated by team.
- Now activate devices per group - the easiest way without MDM is group activation.
- QR code activation link under group activations and use with zIPS.

The organization would like to build custom Threat Policies that meet the detection and user experience requirements of each individual worker division. The analyst does the following:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the Threat option.
4. Select + Add New Threat Policy
 - Names the Group “Full Detection Enabled - No User Notifications”
 - Select the Policy Scope of “Team.”



To customize the policy, the analyst followed these steps:

1. Edit Policy using the Pencil tool.

- Select all Threats or the threats in the scope of detection.
- Select “Enable detection for all selected.”
- Click “Go” to implement the action.

2. Save Policy.

The screenshot shows the zIPS console interface for configuring a Threat Policy. The interface includes a sidebar with navigation options like Dashboard, Activations, Apps, Devices, Threats, Policies, Integrations, and OS Risk. The main content area is titled 'Threat Policy' and shows a table of threats. Red arrows and text annotations indicate the steps to edit the policy:

- 1. Start Editing Policy (points to the pencil icon in the policy header)
- 2. Select all Threats (points to the 'All' checkbox in the table header)
- 3. Select "Enable detection for all selected" (points to the corresponding option in the 'Table Actions' dropdown menu)
- 4. Select "Go" (points to the 'Go' button in the table header)
- 5. Save (points to the 'Save' button in the policy header)

The table of threats is as follows:

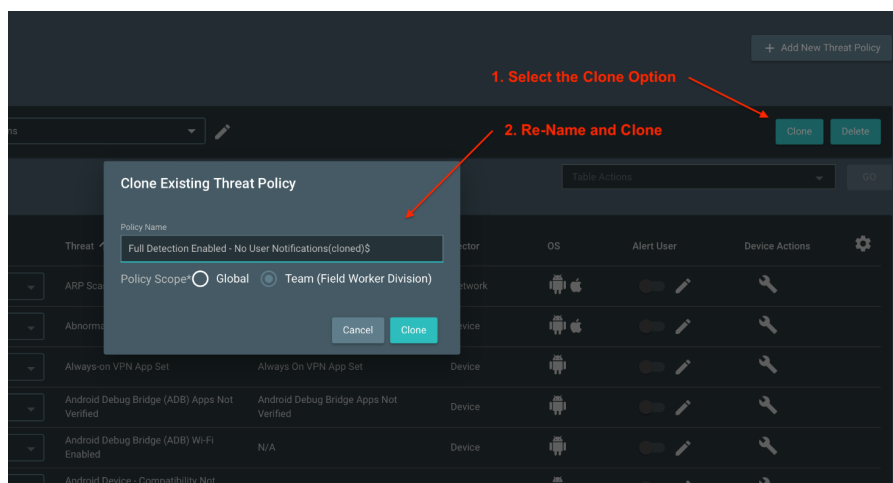
| Enabled | Severity | Threat | Category | Vector | OS | |
|-------------------------------------|----------|---|--|---------|----|--|
| <input checked="" type="checkbox"/> | Normal | ARP Scan | Reconnaissance Scan | Network | | |
| <input checked="" type="checkbox"/> | Elevated | Abnormal Process Activity | Abnormal Process | Device | | |
| <input checked="" type="checkbox"/> | Elevated | Always on VPN App Set | Always On VPN App Set | Device | | |
| <input checked="" type="checkbox"/> | Elevated | Android Debug Bridge (ADB) Apps Not Verified | Android Debug Bridge Apps Not Verified | Device | | |
| <input checked="" type="checkbox"/> | Elevated | Android Debug Bridge (ADB) Wi-Fi Enabled | N/A | Device | | |
| <input checked="" type="checkbox"/> | Low | Android Device - Compatibility Not Tested By Google | SafetyNet Attestation | Device | | |
| <input checked="" type="checkbox"/> | Critical | Android Device - Possible Tampering | SafetyNet Attestation | Device | | |
| <input checked="" type="checkbox"/> | Elevated | App Debug Enabled | App Tampering | Device | | |

Clone Policies

Clone template for a new BYOD threat policy and make incremental updates.

The analyst is tasked with creating multiple threat policies unique to each Team and Group. To quickly achieve this, they can Clone the Threat Policies and make incremental changes.

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the Threat option.
4. Choose the Threat Policy to Clone using the drop-down.
 - Click the Clone button on the right side.
5. Clone the Policy.
 - Rename the Policy for the new group, such as “BYOD Detection Enabled.”
 - Select the “Team” Policy Scope.



Edit the policy to meet the use case, such as BYO devices.

Console
v3.20.0-SNAPSHOT

zIPS

1 Demo Tenant (Populated)

Field Worker ...

GroupsPrivacyThreatPhishingApp SettingsApp PolicyNetwork PolicyDevice Inactivity

Dashboard

Activations

Apps

Devices

Threats

Policies

Integrations

OS Risk

Docs

Policy

Terms

Jason S.

Threat Policy

+ Add New Threat Policy

Global

Full Detection Enabled - No User Notifications(cloned)

SaveCancel

Table Actions

GO

| <input type="checkbox"/> Enabled | Severity | Threat ↑ | Category | Vector | OS | Alert User | Device Actions | |
|-------------------------------------|---------------------------------|---|--|---------|----|------------------------|----------------|--|
| <input checked="" type="checkbox"/> | <div><div></div></div> Normal | ARP Scan | Reconnaissance Scan | Network | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Elevated | Abnormal Process Activity | Abnormal Process | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Elevated | Always-on VPN App Set | Always On VPN App Set | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Elevated | Android Debug Bridge (ADB) Apps Not Verified | Android Debug Bridge Apps Not Verified | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Elevated | Android Debug Bridge (ADB) Wi-Fi Enabled | N/A | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Low | Android Device - Compatibility Not Tested By Google | SafetyNet Attestation | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Critical | Android Device - Possible Tampering | SafetyNet Attestation | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Elevated | App Debug Enabled | App Tampering | Device | | <div><div></div></div> | | |
| <input checked="" type="checkbox"/> | <div><div></div></div> Low | App Pending Activation | iPDS Not Running | Device | | <div><div></div></div> | | |

Create Groups for a Team

- Enter Division 1 team to create a group for that team.
- Assign a previously created threat policy to that group.

The analyst must now create new (or edit existing EMM) Groups within the Team, which can have unique policies assigned. These groups are used to separate use cases within Teams, such as different device ownership models, privacy requirements, threat detection requirements, etc. The analyst created a new group following these steps:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the Groups option.
4. Select + Add New Group.
5. Creates Group based on device ownership named Corporate devices.
 - Use the “Team” Policy Type.
 - Select previously created Threat Policy.
6. Save Group.

Create New Group

Group Name

Corporate Devices (iOS Supervised & Android Device Owner)

Description

Policy Type

☐ Global ☒ Team (Field Worker Division)

Privacy Policy

Default

Threat Policy

Full Detection Enabled - No User Notifications

Phishing Policy

Default

App Settings

Corporate App Settings Policy

App Policy

Default

Device Inactivity

Default

Cancel

Save

Network Policy

Device Inactivity

+ Add New Group

| App Settings | App Policy | Device Inactivity | Actions |
|-------------------------------|------------|-------------------|---------|
| Corporate App Settings Policy | Default | Default | |
| Default | Default | Default | |
| Corporate App Settings Policy | Default | Default | |
| Default | Default | Default | |
| Default | Default | Default | |

Rows per page: 25 1-5 of 5 < >

Select previously created Policies

Assign Cloned Policies

- Assign the BYOD threat policy to the BYOD group.
- Set up tailored policies (threat, privacy, etc.) based on a number of group types, including geography, organizational group, and device types.

To ensure all Teams and Groups have their correct Policies, the analyst can centrally assign all types of policies from the Groups section.

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the Groups option.

The screenshot shows the 'Console v5.20.0-SNAPSHOT' interface. The top navigation bar includes 'zIPS' and '1 Demo Tenant (Populated)'. The left sidebar has a 'Policies' tab selected. The main area is titled 'Groups' and shows a table of groups. A dropdown menu is open for the 'Emm Connection' column, showing options like 'MobileIron Cloud Sandbox (Jason S)', 'Pat-Intune', 'Intune Integration (Jason S)', and 'Integration (Jason S)'. The table has columns for Group Name, Emm Connection, Privacy Policy, Threat Policy, Phishing Policy, App Settings, App Policy, Device Inactivity, and Actions.

| Group Name ↓ | Emm Connection | Privacy Policy | Threat Policy | Phishing Policy | App Settings | App Policy | Device Inactivity | Actions |
|---|------------------------------------|----------------|--|-----------------|-------------------------------|------------|-------------------|---------|
| zIPS Deployment | Intune Integration (Jason S) | Default | Alert All | Default | Corporate App Settings Policy | Default | Default | |
| Default Group | | Default | Alert All Critical | Default | Default | Default | Default | |
| Corporate Devices (IOS Supervised & Android Device Owner) | MobileIron Cloud Sandbox (Jason S) | Default | Full Detection Enabled - No User Notifications | Default | Corporate App Settings Policy | Default | Default | |
| BYOD Policy | | BYOD | Alert All Critical | Default | Default | Default | Default | |
| BYO Devices (User Enrolment & Work Profile) | MobileIron Cloud Sandbox (Jason S) | BYOD | Full Detection Enabled - No User Notifications | Default | Default | Default | Default | |

Edit the new Group, in this case, the BYO Device Group. From the drop-down, select the newly cloned Threat Policy and click Save.

Console
v.5.20.0-SNAPSHOT

zIPS

1 Demo Tenant (Populated)

Field Worker ...

Dashboard

Activations

Apps

Devices

Threats

Policies

Integrations

OS Risk

Docs

Policy

Terms

Jason S.

Groups

Privacy

App Policy

Network Policy

Device Inactivity

Groups

Global

EMM Connection

MobileIron

Cloud

Sandbox (Jason S)

Pat-Intune

Intune

Integration (Jason S)

BYOD

Full Detection Enabled - No User Notifications(cloned)

Default

Default

Default

Default

Default

Group Name

BYOD Devices (User Enrolment & Work Profile)

Description

Policy Type

Global

Team (Field Worker Division)

Privacy Policy

BYOD

Threat Policy

Full Detection Enabled - No User Notifications(cloned)

Phishing Policy

Default

App Settings

Default

App Policy

Default

Device Inactivity

Default

Cancel

Save

+ Add New Group

App Settings

App Policy

Device Inactivity

Actions

Corporate App Settings Policy

Default

Default

Default

Default

Default

Corporate App Settings Policy

Default

Default

Default

Default

Default

Default

Default

Default

Rows per page: 25 1-5 of 5 < >

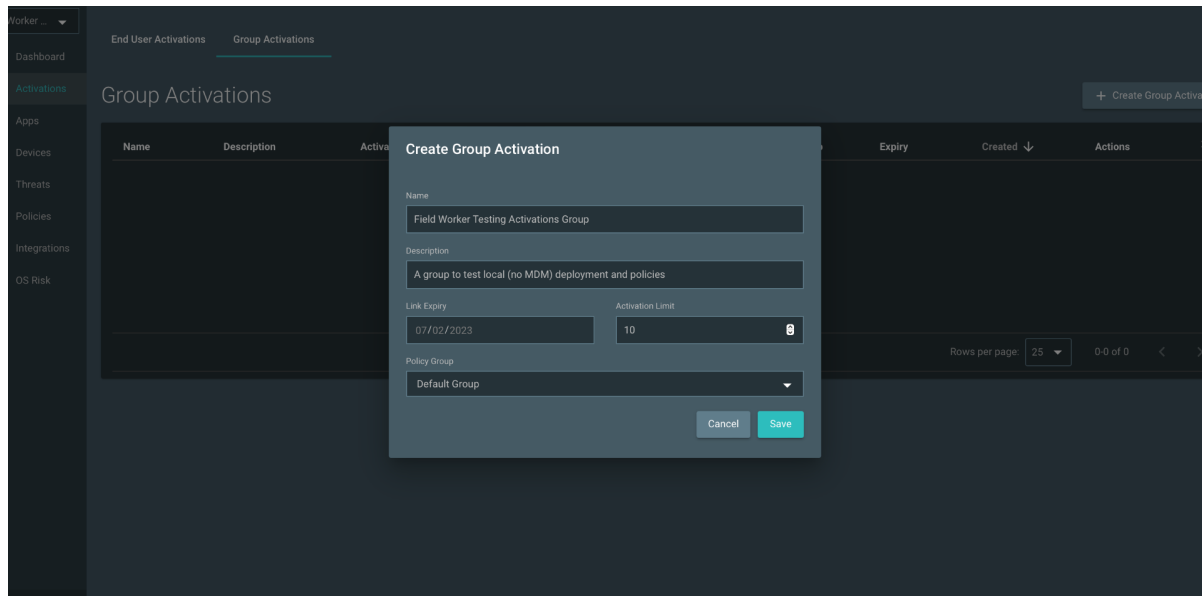
Enroll Devices into each Team - Local Group Activations

- Now activate devices per group - the easiest way without MDM is group activation.

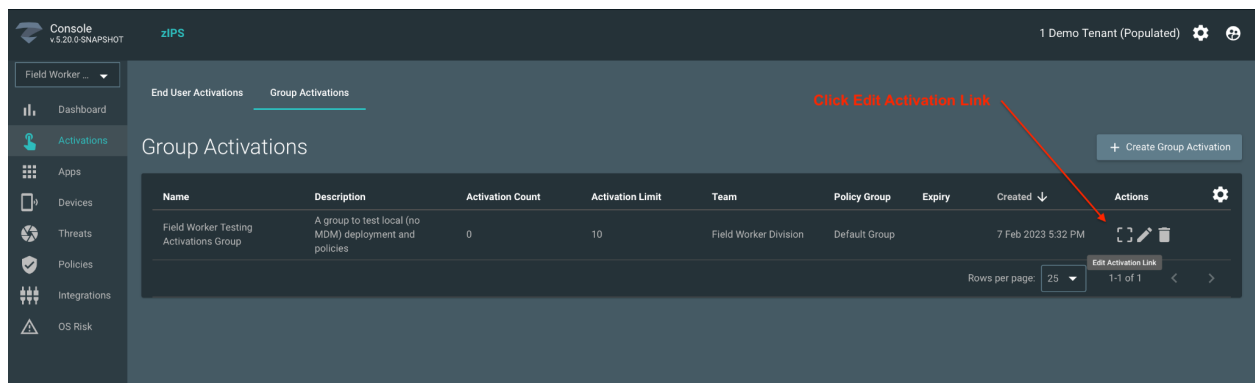
BUG: Confirmed working as per design.

For the analyst to test these groups and policies, they must create Group Activations. These allow the analyst to generate QR codes and URLs, which are generally used by testing (or non-MDM) end users to enroll. To start enrolling, the analyst can follow these steps:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Activations Tab.
3. Select the Groups Activations option.
4. Select + Create Group Activation
 - a. Name Group Activation
 - b. Set expiry.
 - c. Select previously created Team Group.



The Analyst then clicks “Edit Activation Link” to access the enrollment QR code and URL.





The QR code and URL are then distributed to testing users.

Console
v3.20.0-SNAPSHOT

ZIP5

1 Demo Tenant (Populated)



Field Worker ...

Dashboard

Activations

Apps

Devices

Threats

Policies

Integrations

OS Risk

Docs

Policy




Terms

Jason S.

End User Activations

Group Activations


+ Create Group Activation

| Name | Description | Activation Count | Activation Limit | Team | Policy Group | Expiry | Created | Actions |
|--|--|------------------|------------------|-----------------------|---------------|--------|--------------------|---|
| Field Worker Testing Activations Group | A group to test local (no MDM) deployment and policies | 0 | | Field Worker Division | Default Group | | 7 Feb 2023 5:32 PM |    |

Rows per page: 25 1-1 of 1

Manage Activation Link

Share the link or QR code with users to enable them to activate their devices.



Activation Link

<https://mtdparity.zippanum.com/a/>

Or click [here](#) to activate.

Regenerate Link

Close

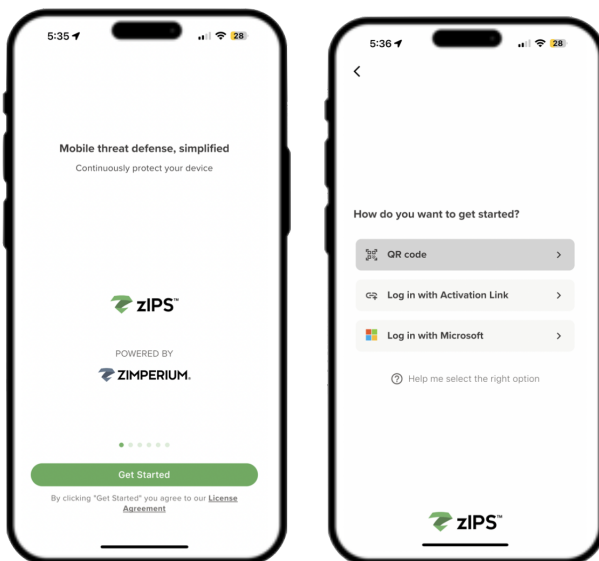
Enrol Devices - Group Activation

- QR code activation link under group activations and use with zIPS

****This activity must be completed in your own testing tenant, not the shared testing environment.***

For the analyst to help these end users enroll, they can follow these steps:

1. Instruct the end users to install zIPS from the public Google Play Store or Apple App Store.
2. Provide the end users with the QR code and URL via any sharing platform (E.g. Email, Slack, SMS).
 - a. The end users can use the QR code option in zIPS to scan the QR code.
 - b. The end user can use the login with the Activation Link option in zIPS to Paste the activation URL.

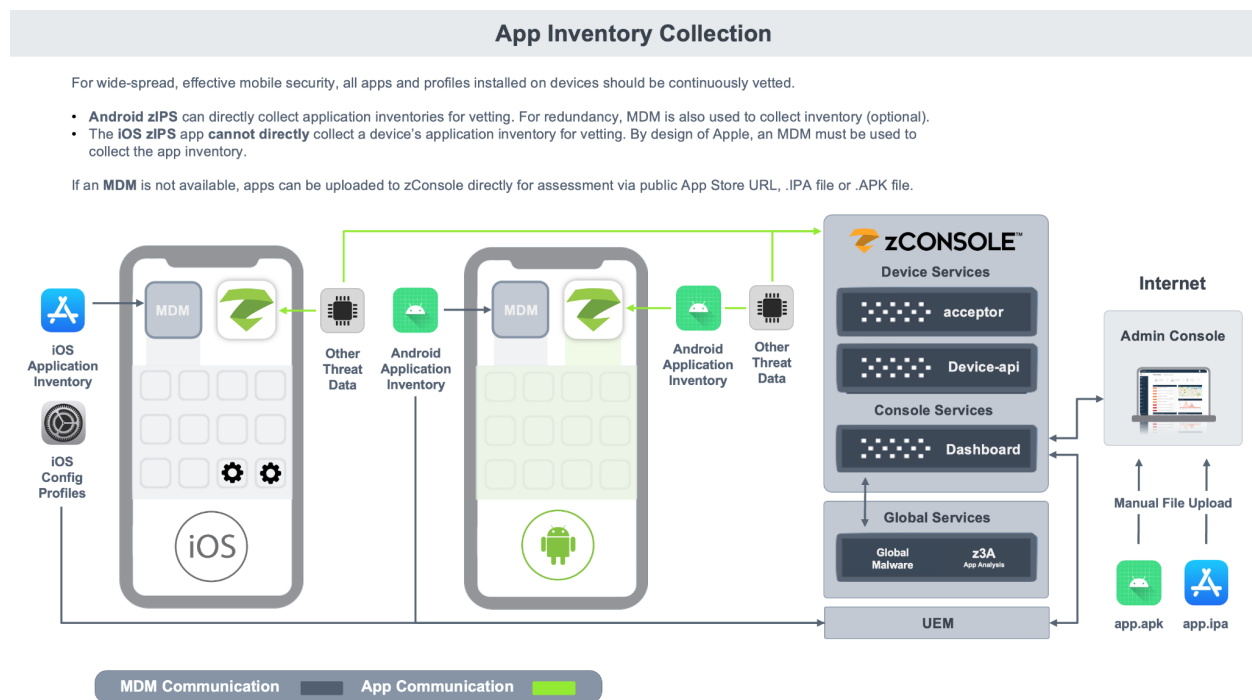


Enroll Devices - App-Based Inventory Collection Setup (Android Only)

- Verify Privacy Policy is configured to enable the collection of app inventory from Android devices

Once the end users have successfully enrolled, the analyst should soon see their device records. They will also see any detected Threats, OS Risks, and Android App Inventories.

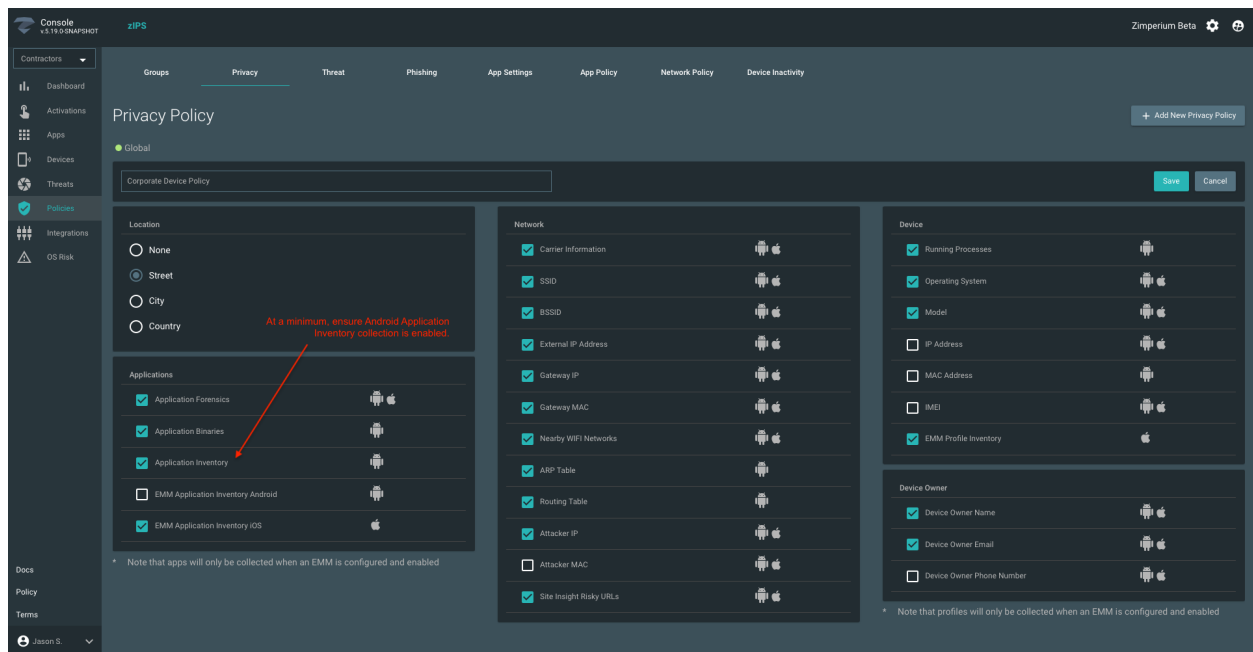
Due to by-design limitations in Apple iOS, an MDM is required to collect any iOS Device App inventories.



Additionally, the respective Privacy Policies must be correctly set. To first check within the zConsole, the analyst can follow these steps:

1. Select the "Field Worker Division" Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the Privacy Option

4. Select the Privacy Policy your test devices have assigned to their group.
 - a. Edit Policy, using the pencil tool.
 - b. Enable the Android “Application Inventory” option.
 - c. Save.



To also ensure applications are also collected by any future MDM, the analyst selects all other application collection options.

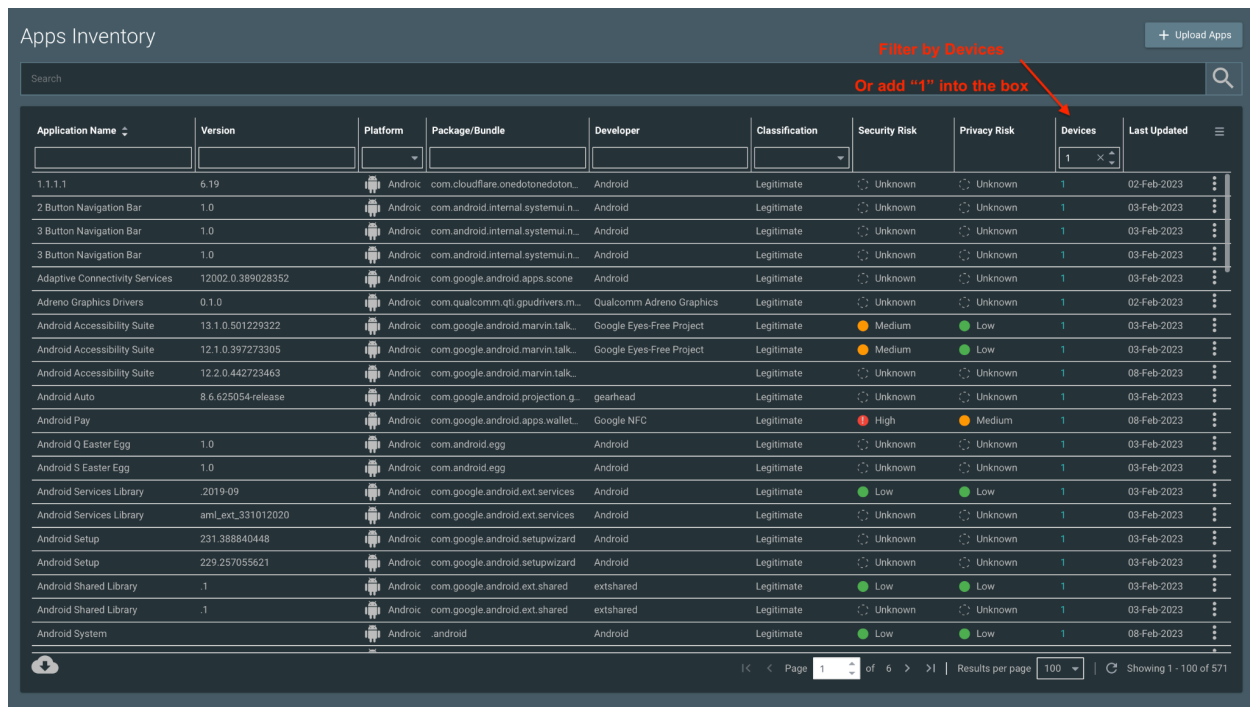
Enroll Devices - App-Based Inventory Collection (Android Only)

- Verify Android apps are shown on the App Inventory page.

Bug: Sorting by most columns will break app results, making them not visible.
(Update, bug fixed.)

The analyst can now ensure test users have enrolled their devices, and the Privacy Policy allows zIPS to directly collect Android Apps for vetting purposes. To check these reported apps, the analyst can follow these steps:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Apps Tab.
3. Filter by the Devices column to see apps that exist on at least 1 currently enrolled device.
 - a. The analyst can see dozens of applications from the enrolled device(s).



Apps Inventory

Filter by Devices
Or add "1" into the box

+ Upload Apps

Search

| Application Name | Version | Platform | Package/Bundle | Developer | Classification | Security Risk | Privacy Risk | Devices | Last Updated |
|--------------------------------|--------------------|----------|------------------------------------|--------------------------|----------------|---------------|--------------|---------|--------------|
| 1.1.1.1 | 6.19 | Android | com.cloudflare.onedotonedotone | Android | Legitimate | Unknown | Unknown | 1 | 02-Feb-2023 |
| 2 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| 3 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| 3 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Adaptive Connectivity Services | 12002.0.389028352 | Android | com.google.android.apps.scone | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Adreno Graphics Drivers | 0.1.0 | Android | com.qualcomm.qti.gpudrivers.m... | Qualcomm Adreno Graphics | Legitimate | Unknown | Unknown | 1 | 02-Feb-2023 |
| Android Accessibility Suite | 13.1.0.501229322 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Medium | Low | 1 | 03-Feb-2023 |
| Android Accessibility Suite | 12.1.0.397273305 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Medium | Low | 1 | 03-Feb-2023 |
| Android Accessibility Suite | 12.2.0.442723463 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Unknown | Unknown | 1 | 08-Feb-2023 |
| Android Auto | 8.6.625054-release | Android | com.google.android.projection.g... | gearhead | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android Pay | | Android | com.google.android.apps.wallet... | Google NFC | Legitimate | High | Medium | 1 | 08-Feb-2023 |
| Android Q Easter Egg | 1.0 | Android | com.android.egg | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android S Easter Egg | 1.0 | Android | com.android.egg | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android Services Library | 2019-09 | Android | com.google.android.ext.services | Android | Legitimate | Low | Low | 1 | 03-Feb-2023 |
| Android Services Library | amLExt_331012020 | Android | com.google.android.ext.services | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android Setup | 231.388840448 | Android | com.google.android.setupwizard | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android Setup | 229.257055621 | Android | com.google.android.setupwizard | Android | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android Shared Library | 1 | Android | com.google.android.ext.shared | extshared | Legitimate | Low | Low | 1 | 03-Feb-2023 |
| Android Shared Library | 1 | Android | com.google.android.ext.shared | extshared | Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 |
| Android System | | Android | .android | Android | Legitimate | Low | Low | 1 | 08-Feb-2023 |

Page 1 of 6 | Results per page 100 | Showing 1 - 100 of 571

The analyst would like to know more about a specific app, they can click anywhere along an app's record to expand the details.

The screenshot displays the zIPS App Inventory interface. The main table lists various applications with columns for Application Name, Version, Platform, Package/Bundle, Developer, Classification, and Security Risk. The 'Android Services Library' app is highlighted, and its details are shown in a side panel.

| Application Name | Version | Platform | Package/Bundle | Developer | Classification | Security Risk |
|--------------------------------|--------------------|----------|------------------------------------|--------------------------|----------------|---------------|
| 1.1.1.1 | 6.19 | Android | com.cloudflare.onedotonedotn... | Android | Legitimate | Unkn |
| 2 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unkn |
| 3 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unkn |
| 3 Button Navigation Bar | 1.0 | Android | com.android.internal.systemui.n... | Android | Legitimate | Unkn |
| Adaptive Connectivity Services | 12002.0.389028352 | Android | com.google.android.apps.scone | Android | Legitimate | Unkn |
| Adreno Graphics Drivers | 0.1.0 | Android | com.qualcomm.qti.gpudrivers.m... | Qualcomm Adreno Graphics | Legitimate | Unkn |
| Android Accessibility Suite | 13.1.0.501229322 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Medi |
| Android Accessibility Suite | 12.1.0.397273305 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Medi |
| Android Accessibility Suite | 12.2.0.442723463 | Android | com.google.android.marvin.talk... | Google Eyes-Free Project | Legitimate | Unkn |
| Android Auto | 8.6.625054-release | Android | com.google.android.projection.g... | gearhead | Legitimate | Unkn |
| Android Pay | | Android | com.google.android.apps.wallet... | Google NFC | Legitimate | High |
| Android Q Easter Egg | 1.0 | Android | com.android.egg | Android | Legitimate | Unkn |
| Android S Easter Egg | 1.0 | Android | com.android.egg | Android | Legitimate | Unkn |
| Android Services Library | 2019-09 | Android | com.google.android.ext.services | Android | Legitimate | Low |
| Android Services Library | aml_ext_331012020 | Android | com.google.android.ext.services | Android | Legitimate | Unkn |
| Android Setup | 231.388840448 | Android | com.google.android.setupwizard | Android | Legitimate | Unkn |
| Android Setup | 229.257055621 | Android | com.google.android.setupwizard | Android | Legitimate | Unkn |
| Android Shared Library | .1 | Android | com.google.android.ext.shared | extshared | Legitimate | Low |
| Android Shared Library | .1 | Android | com.google.android.ext.shared | extshared | Legitimate | Unkn |
| Android System | | Android | .android | Android | Legitimate | Low |

Android Services Library Details:

- Classification: LEGIT
- Privacy Risk: Low
- Security Risk: Low
- Developer Name: Android
- Developer Signature: 1cf8b8fa9ea575057acbe3b958560be5
- Package/Bundle: com.google.android.ext.services
- Version: 2019-09
- Original File Name: GoogleExtServices.apk
- Creation Date: 03-Feb-2023
- Device Count: 1

Risk Details:

- Security Risk: Low
- Privacy Risk: Low

Permissions:

- android.permission.ACCESS_NETWORK_STATE
- android.permission.MONITOR_DEFAULT_SMS_PACKAGE
- android.permission.PROVIDE_RESOLVER_BANNER_SERVICE
- android.permission.READ_DEVICE_CONFIG
- android.permission.REQUEST_NOTIFICATION_ASSISTANT_SERVICE

File Hashes:

| Type | CRC16 | Size | Hash | Data |
|------|--------|--------|----------------------------------|------|
| 0 | 6-4709 | 8-2334 | 330d8f728ba156d0d1d5107f10d1c022 | |

Since this app has been flagged by the security team, the analyst needs deeper reporting and forensics. They can do this by:

1. Identifying the app of interest.
2. Hover over the three dots on the far right of the app's record, they can select from:
 - a. **Executive Report:** Cut-down, simplified report for executives or meeting briefings.
 - b. **Technical Report:** An extended technical report of all findings.
 - c. **JSON Report:** An extended technical report of all findings in a standardized raw JSON format. This could be ingested into threat, analytics, or reporting platforms.

+ Upload Apps



| Classification | Security Risk | Privacy Risk | Devices | Last Updated | |
|----------------------|---------------|--------------|--------------------------------|--------------|--|
| <input type="text"/> | | | <input type="text" value="1"/> | | |
| Legitimate | Unknown | Unknown | 1 | 02-Feb-2023 | |
| Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 | |
| Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 | |
| Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 | |
| Legitimate | Unknown | Unknown | 1 | 03-Feb-2023 | |
| Legitimate | Unknown | Unknown | 1 | 02-Feb-2023 | |
| Legitimate | Medium | Low | 1 | 03-Feb-2023 | |

Executive PDF Report
Technical PDF Report
JSON Report

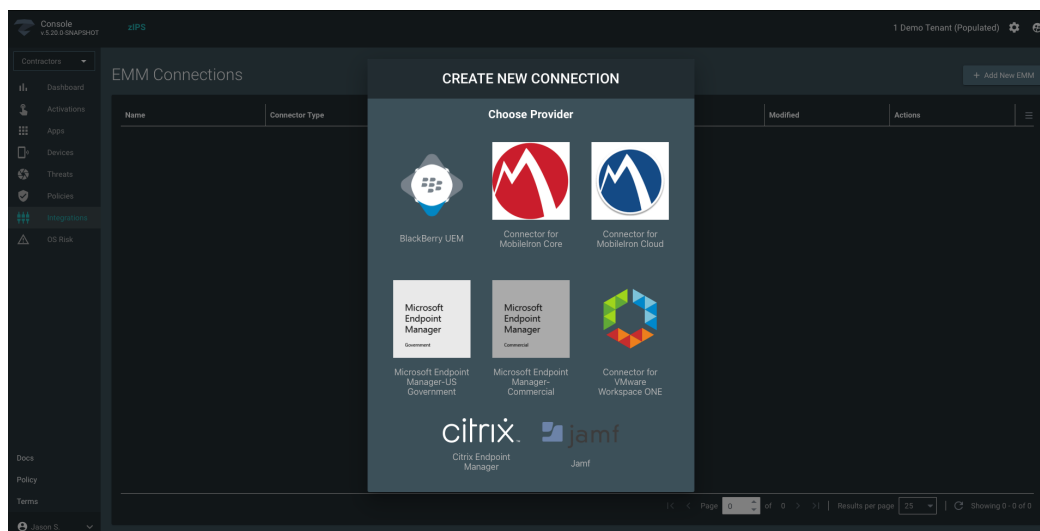
MDM Integration - zConsole Setup

- Choose a Team for the EMM connection or simply select the Default team.
- Go to the Integrations page and Add a New EMM connection.
 - Confirm the Team for the EMM connection and setup the authentication configuration for the EMM
 - Select the EMM Groups to associate with this connection
 - Select the Policies to assign to the selected groups and click Add Groups

****This activity must be completed in your own testing tenant, not the shared testing environment.***

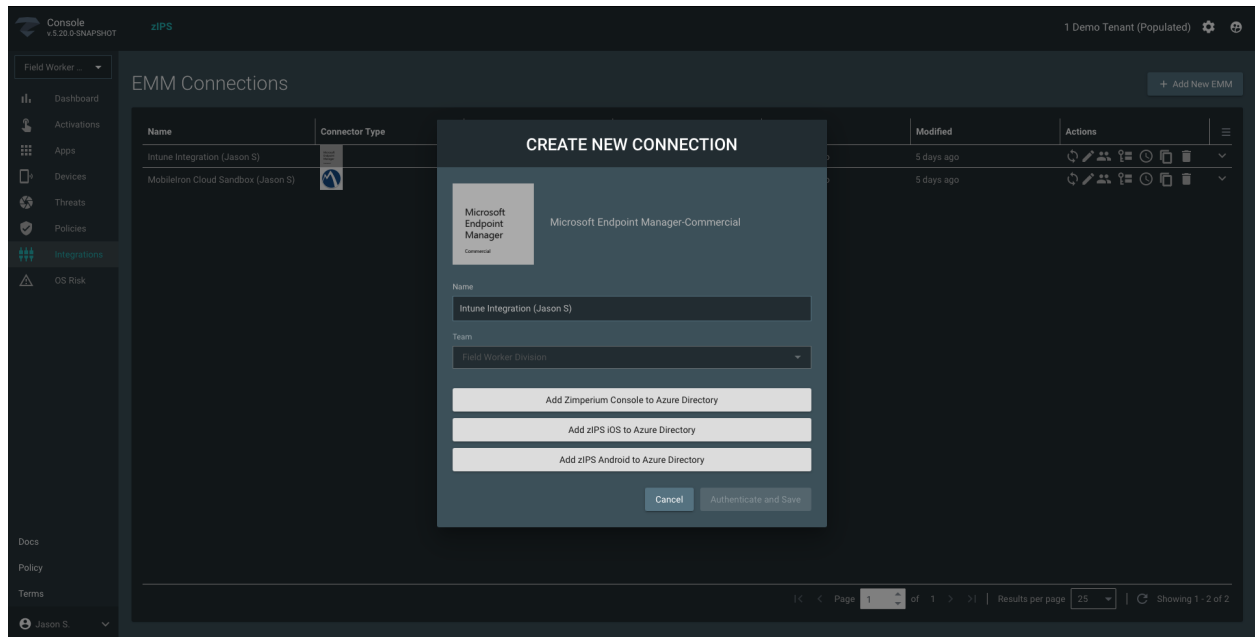
The analyst has now moved past testing individual devices and needs to set up the system for production deployment using their MDM. They can start by following these steps:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Integrations Tab.
3. Select + Add New EMM
 - a. Select the MDM, in this example Microsoft Endpoint Manager (Intune) will be selected.



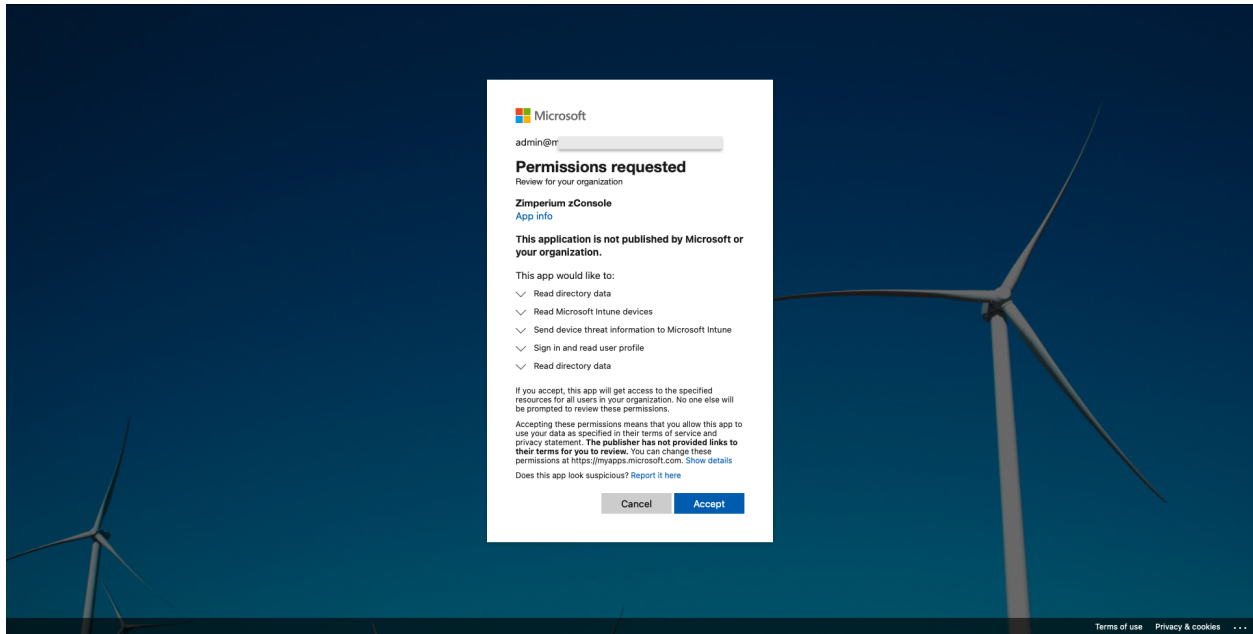
Once selected, the analyst then needs to:

1. Name the EMM Connection.
2. Click “Add” on each of the 3 Azure Integrations.



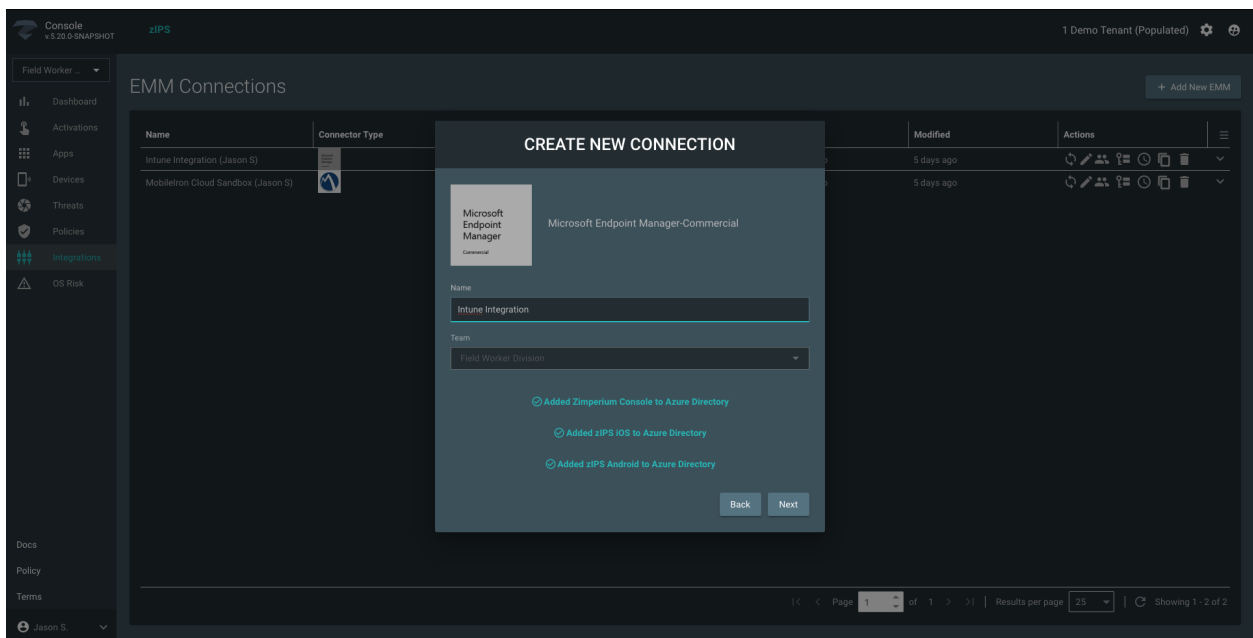
A popup will be displayed to the analyst, requiring them to log in to Microsoft and accept the Integration.

1. Read the permissions.
2. Click Accept.



Once all 3 Microsoft Integrations are accepted, they can:

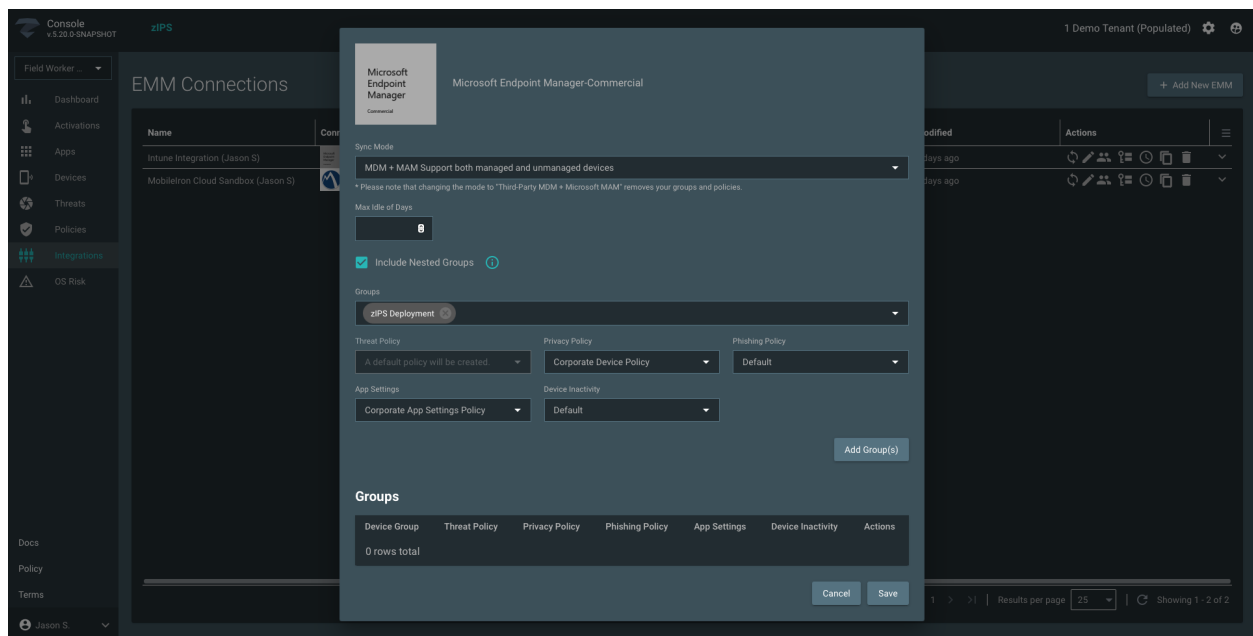
1. Click Next.



Now the analyst must configure the integration, following these steps:

1. Select the Sync Mode.

- In this example, the option: “MDM + MAM Support both managed and unmanaged devices” was selected.
2. Select Include Nested Groups.
 3. Select the Azure Group(s).
 - The Group(s) must have devices assigned to avoid sync errors.
 4. Select the Policies.
 - These will not be applied to the whole integration, only the Group(s) selected.
 5. Click “Add Groups.”
 6. Repeat this process for other Groups that have different policy requirements.



The analyst must confirm they have selected all their groups and associated policies before continuing.

Once confirmed, they can select Save to complete the integration within zConsole. Additional steps are required for full integration, within the Microsoft Endpoint Manager console.

Add Group(s)

Groups

| Device Group | Threat Policy | Privacy Policy | Phishing Policy | App Settings | Device Inactive |
|-----------------|---------------|-------------------------|-----------------|-------------------------------|-----------------|
| zIPS Deployment | To be created | Corporate Device Policy | Default | Corporate App Settings Policy | Default |
| 1 row total | | | | | |

Cancel

Save

MDM Integration - MTD Connector (Microsoft Endpoint Manager)

- Create the MTD Connector, to sync compliance data between zConsole and the Microsoft Endpoint Manager console.

Note: During Step 1 of deploying MTD Connector, ignore the link in step 1.

****This activity must be completed in your own testing tenant, not the shared environment.***

Next, the analyst must finish the console integration by deploying the MTD Connector within Microsoft Endpoint Manager. They do this by following these steps:

1. Navigate to “Tenant Administration | Connectors and Tokens | Mobile Threat Defense.”
2. Click + Add.
 - Select Zimperium from the drop-down.
3. Click Create.
4. Once created and active, enable the required settings.
 - In this example, all settings are turned to “On.”

Microsoft Endpoint Manager admin center

admin@M365x3712526...
CONTOSO (M365X37125268.O...

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Tenant admin | Connectors and tokens > Connectors

Connectors and tokens | Mobile Threat Defense

Search

+ Add

Refresh

Microsoft Store for Business

Windows enterprise certificate

Microsoft Endpoint Configuration Manager

Windows 365 Citrix connector (preview)

Windows data

Apple

Apple VPP Tokens

Android and Chrome OS

Managed Google Play

Chrome Enterprise (preview)

Cross platform

Microsoft Defender for Endpoint

Mobile Threat Defense

Partner device management

Partner compliance management

TeamViewer connector

Certificate connectors

Status

0 active connections

MTD Connectors

No items to display

Add Connector

Mobile Threat Defense

Connection status: Not set up

Last synchronized: --

Select the Mobile Threat Defense connector to setup *

Zimperium

1. Set up your admin settings via the Zimperium admin console. [Learn more about integration with Microsoft Endpoint Manager](#)

[Open the Zimperium admin console](#)

2. Connector settings

Some toggles are disabled and acting as "off" because Zimperium is not actively communicating with Intune for this account. Please check the state of the connection in the Zimperium admin console.

When the connection has returned to a healthy status (Active or Provisioned), the toggles will be re-enabled and any pre-existing setting state will be restored.

Compliance policy evaluation

Connect Android devices version 5.1 and above to Zimperium

Connect iOS/iPadOS devices version 10.0 and above to Zimperium

Enable App Sync (sending application inventory) for iOS/iPadOS devices

Create

MDM Integration - Schedule Sync

- Go to created EMM connection and select the icon to schedule the EMM sync at the desired frequency.

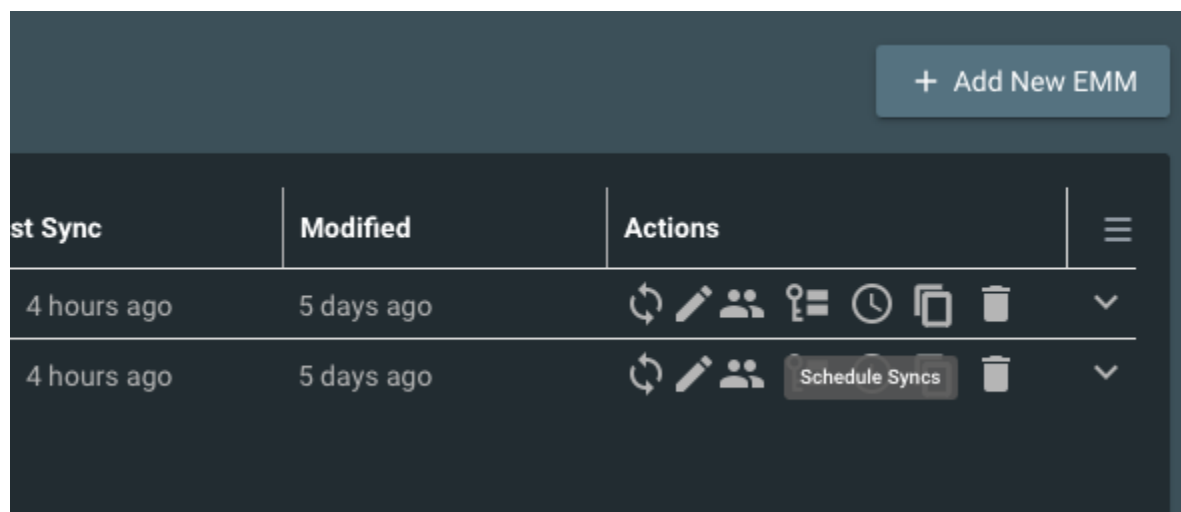
Bug: Confirmed as by design. Can select 1 hour, but the minimum is 4 hours.

****This activity must be completed in your own testing tenant, not the shared environment.***

Previously, the organization had issues where devices could be enrolled in MDM but experienced a sync delay to the zConsole. This was due to the settings previously being unconfigurable at a tenant level.

Using the new Schedule Syncs Action, they can address this:















1. Click on the “Schedule Syncs” action.



The analyst could configure a scheduled sync up to once every 4 hours.

EMM Connections

+ Add New EMM

| Name | Connect | Modified | Actions | |
|------------------------------------|---|----------------|---|---|
| Intune Integration (Jason S) |  | ago 5 days ago |       | ✓ |
| MobileIron Cloud Sandbox (Jason S) |  | ago 5 days ago |       | ✓ |

EMM SYNC SCHEDULING

How you wish to handle console sync?

☒ Scheduled ☐ Manual sync only

Hourly

Daily

Sync every hours starting at

Cancel

Save

MDM Integration - Managed App Configuration

- Go to created EMM connection and select icon to view EMM app configuration parameters to use in the zIPS app configuration in your EMM

Bug: *Mandatory Value for Intune deployment is missing in UI. The MDMDeviceID value is missing for Intune Integrations, it is there for others integrations such as MobileIron.*

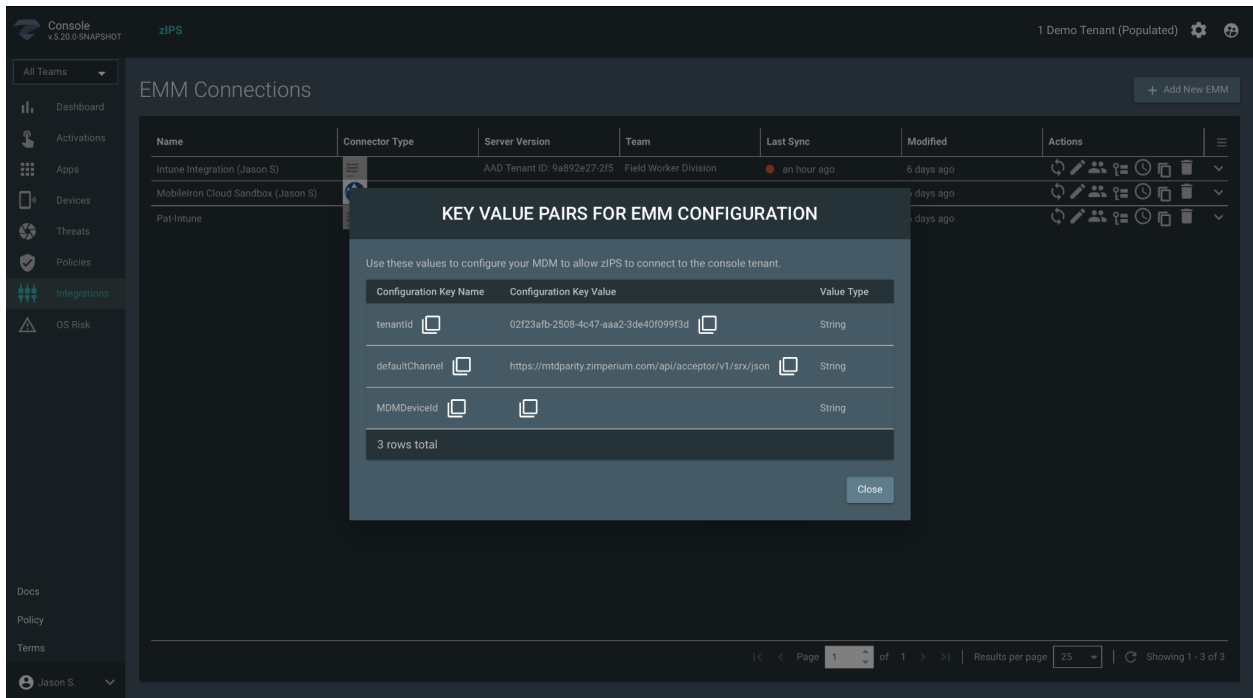
Design Floor: *Other Missing Values when you view the EMM App Configuration parameters, we do not provide all the required parameters. We only provide 3 of 14 for Android and 3 of 6 for iOS.*

Recommendation: *We should also generate a . PLIST file to download for iOS: which can be uploaded to any MDM for auto-configuration. It removes all chances of misconfiguration or mistakes.*

****This activity must be completed in your own testing tenant, not the shared environment.***

Finally, to start rollout, the admin must use their MDM to deploy the zIPS app with Managed App Configuration. They can get the values by following these steps:

1. Click the “Key Value Pairs for EMM Configuration” Action.
2. Copy Keys & values.
 - a. These Key/Values will be pasted into the Managed App Configuration Section of the MDM.



Since the organization uses Microsoft Endpoint Manager, the analyst does the following:

1. Deploys the zIPS Application using Apple Business Managed (Previously VPP).
2. Navigates to the “Apps | App configuration policies” section.
3. Creates a Policy for zIPS.
 - Pastes the Key/Value pairs into the settings field.
 - **Note:** Key/Value pairs are case-sensitive.

Microsoft Endpoint Manager admin center

Home

Dashboard

All services

Devices

Apps

Endpoint security

Reports

Users

Groups

Tenant administration

Troubleshooting + support

Home > Apps > App configuration policies > zIPS iOS Config

zIPS iOS Config | Properties

Search

Overview

Manage

Properties

Monitor

Device install status

User install status

Basics

Name

Description

Device enrollment type

Platform

Targeted app

zIPS iOS Config

--

Managed devices

iOS/iPadOS

Zimperium zIPS

Settings

| Configuration key | Value type | Configuration value |
|-------------------------------|------------|--|
| tenantid | String | jason-demo |
| defaultchannel | String | https://mtddemo-acceptor.zimperium.com/srx |
| uuid | String | {{AzureADDeviceId}} |
| display_eula | String | no |
| assume_vpn_permission_granted | String | true |

Assignments

Included groups

| Group | Filter | Filter mode |
|-----------------|--------|-------------|
| zIPS Deployment | None | None |

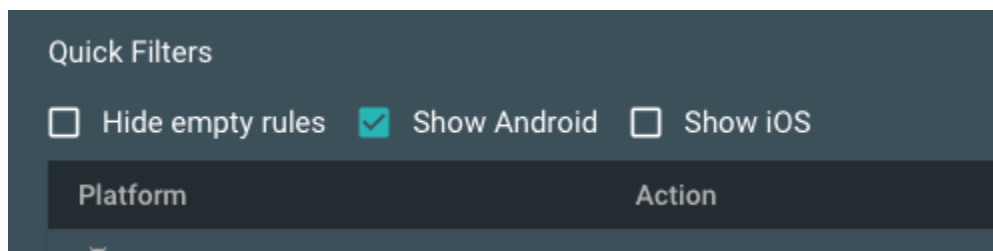
App Policies - Out of Compliance Apps

- Go to Policies and select the App Policies tab.
- Mark Android apps Out of Compliance by Package ID: Edit the Rule for Android, OOC, Package ID
 - Select one or more package IDs to mark OOC
 - Click the eye icon in the selected package ID row to see the list of apps which match this package ID
 - Optionally upload an APK file to mark an additional package ID as OOC
 - Add the selected package ID to the rule and choose to save changes

Now the platform has its fundamental components setup the analyst needs to start actioning app-related security requests. The SOC Team have already identified a set of Android App Package IDs that must be added to the Out of Compliance (OOC) rules to automatically trigger a Threat event when any of the apps are detected on devices going forward.

To add these devices to the OOC rule, the analyst can follow these steps:

1. Select the “Field Worker Division” Team using the top-left drop-down.
2. Select the Policy Tab.
3. Select the App Policy option.
 - Since the request is for Android Package IDs, untick the “Hide empty rules” and “Show iOS”



The request was to mark the Android App Package IDs as Out of Compliance:

1. The analyst will select the second rule, based on the OOC and Package ID requirement.
2. Click the Actions button.

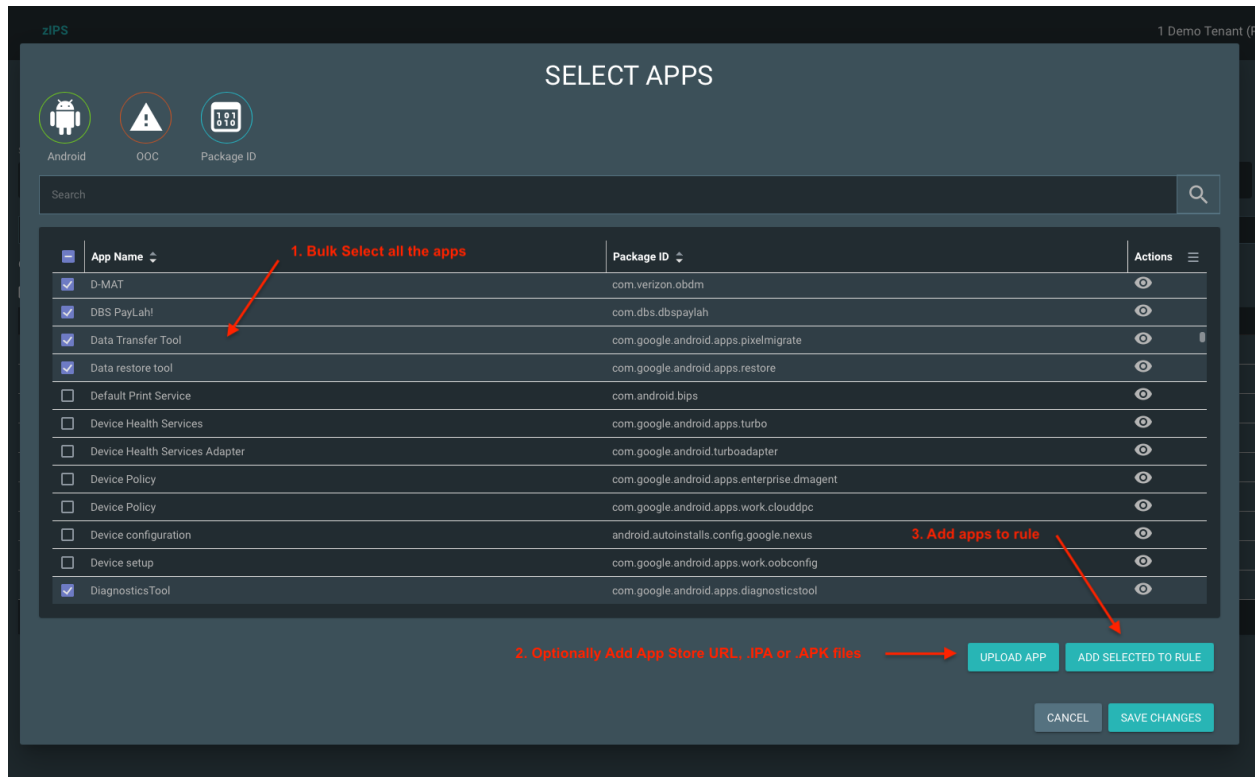
The screenshot shows the 'App Policy' configuration page. At the top, there are tabs for Groups, Privacy, Threat, Phishing, App Settings, App Policy (selected), Network Policy, and Device Inactivity. Below the tabs is a 'Select Policy' dropdown menu set to 'Data Leaking'. A 'RULES IN THIS POLICY' section contains a table of rules. The table has columns for Platform, Action, Criteria, # Rows, and Actions. The second rule is highlighted with a red box. Red arrows point to the 'Package ID' criteria and the 'Actions' button of this rule.

| Platform | Action | Criteria | # Rows | Actions |
|----------|-------------------------|--|--------|---------|
| Android | Out of Compliance (OOC) | Package ID + Version | 1 | |
| Android | Out of Compliance (OOC) | Package ID | 0 | |
| Android | Out of Compliance (OOC) | Developer Signature | 0 | |
| Android | Mark as Suspicious | Package ID + Version | 0 | |
| Android | Mark as Suspicious | Package ID | 0 | |
| Android | Mark as Suspicious | Developer Signature | 0 | |
| Android | Mark as Safe | Developer Signature + Package ID + Version | 0 | |
| Android | Mark as Safe | Developer Signature + Package ID | 0 | |
| Android | Mark as Safe | Developer Signature | 0 | |

9 rows total

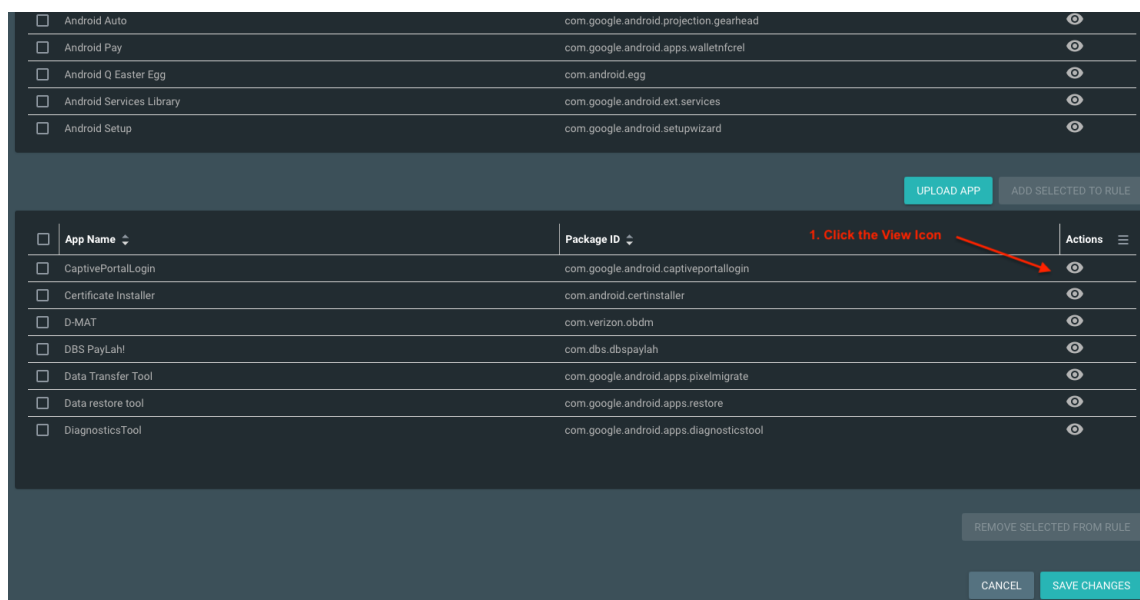
The Select Apps pane will be displayed:

1. The analyst will bulk select all the apps communicated by the SOC Team.
2. The analyst can manually add any additional App Store URLs, Apple .IPA or Android .APK files to the rule.
3. Click Add Selected To Rule.



The pane will reconfigure for the analyst to confirm the selected apps are correct. However, before saving the rule, the analyst wants to confirm how many versions of each app Package ID will be added.

1. Click the View Icon.



Another Pane will overlay, showing all app versions of the selected Package ID. These versions, as well as any future versions, will be added to the rule.

1. Confirm all versions of the app are added to the rule.
2. Click Return to Previous View.

SHOW AFFECTED APPS

Android OOC Package ID

Package ID: com.google.android.captiveportallogin

| Application Name | Version | Platform | Package/Bundle | Developer | Classification | Security Risk | Privacy Risk | Devices | Last Updated |
|--------------------|------------------|----------|----------------------------------|-----------|----------------|---------------|--------------|---------|--------------|
| CaptivePortalLogin | amLnet_331110020 | Android | com.google.android.captivepor... | Android | Legitimate | Low | Low | 0 | 02-Feb-2023 |
| CaptivePortalLogin | amLnet_330811010 | Android | com.google.android.captivepor... | Android | Legitimate | Unknown | Unknown | 2 | 03-Feb-2023 |

1. Confirm all versions are added to rule

2. Return to previous view

GO BACK TO PREVIOUS VIEW

Now the analyst is confident they added the correct Package IDs, and all versions are included, they can continue to save the rule.

1. Click Save Changes.

| | | | |
|--------------------------|------------------------------|--|--|
| <input type="checkbox"/> | CaptivePortalLoginOverlay | com.android.captiveportallogin.overlay | |
| <input type="checkbox"/> | Carrier App Logging | com.google.android.apps.carrier.log | |
| <input type="checkbox"/> | Carrier OMADM | com.android.adm.plugins.dcmo | |
| <input type="checkbox"/> | Carrier Provisioning Service | com.android.omadm.service | |
| <input type="checkbox"/> | Carrier Services | com.google.android.gms | |
| <input type="checkbox"/> | Carrier Settings | com.google.android.carrier | |
| <input type="checkbox"/> | Carrier Setup | com.google.android.wificactivation | |
| <input type="checkbox"/> | | | |

UPLOAD APP

ADD SELECTED TO RULE

| | | | |
|--------------------------|-----------------------|---|---------|
| <input type="checkbox"/> | App Name | Package ID | Actions |
| <input type="checkbox"/> | CaptivePortalLogin | com.google.android.captiveportallogin | |
| <input type="checkbox"/> | Certificate Installer | com.android.certinstaller | |
| <input type="checkbox"/> | D-MAT | com.verizon.obdm | |
| <input type="checkbox"/> | DBS PayLah! | com.dbs.dbspaylah | |
| <input type="checkbox"/> | Data Transfer Tool | com.google.android.apps.pixelmigrate | |
| <input type="checkbox"/> | Data restore tool | com.google.android.apps.restore | |
| <input type="checkbox"/> | DiagnosticsTool | com.google.android.apps.diagnosticstool | |

REMOVE SELECTED FROM RULE

CANCEL

SAVE CHANGES

App Policies - Allow Developer Signatures

- Edit the rule for Android, Mark as Safe by Developer Signature.
 - Select a developer signature and then choose which threats will be suppressed for apps with this developer signature (suspicious, sideloaded and/or OOC threats).
 - Click the eye icon in the selected developer signature row to see the list of apps that match this developer.
 - Add the selected developers and save changes.
 - Deploy all of your app policy changes in bulk by selecting the Deploy Policy Changes green button at the top of the page.

Bug: Cannot add developer signatures to the “Mark as Safe” “Developer Signature” rule.

The analyst was also requested to “Mark as Safe” a specific Developer, which will automate any future approvals for the selected developer's apps.

1. Select the “Mark as Safe” “Developer Signature” rule.
2. Click the Actions Button.

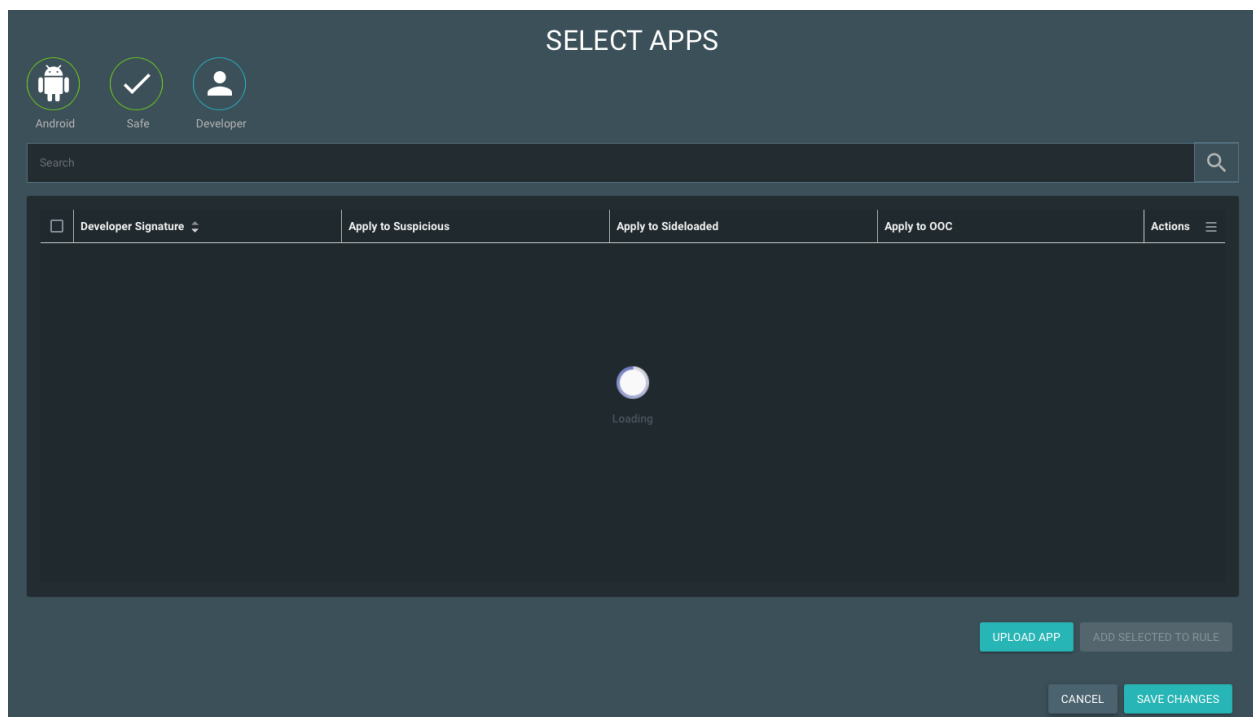
The screenshot shows the 'App Policy' tab in a management console. At the top, there's a 'Select Policy' dropdown set to 'Data Leaking'. Below it, a section titled 'RULES IN THIS POLICY' contains a table of rules. The table has columns for Platform, Action, Criteria, # Rows, and Actions. The rule 'Mark as Safe' with criteria 'Developer Signature' is highlighted in red. Two red arrows point to this rule: one from the text '1. Select the correct rule' and another from '2. Click Actions'.

| Platform | Action | Criteria | # Rows | Actions |
|----------|-------------------------|--|--------|---------|
| Android | Out of Compliance (OOC) | Package ID + Version | 1 | |
| Android | Out of Compliance (OOC) | Package ID | 7 | |
| Android | Out of Compliance (OOC) | Developer Signature | 0 | |
| Android | Mark as Suspicious | Package ID + Version | 0 | |
| Android | Mark as Suspicious | Package ID | 0 | |
| Android | Mark as Suspicious | Developer Signature | 0 | |
| Android | Mark as Safe | Developer Signature + Package ID + Version | 0 | |
| Android | Mark as Safe | Developer Signature + Package ID | 0 | |
| Android | Mark as Safe | Developer Signature | 0 | |

9 rows total

The analyst is given the choice to choose what categories of flagged apps will be Marked as Safe, such as Suspicious, Sideloaded, or OOC. These must be used cautiously, as auto-marking potentially malicious apps as safe could create a future security hole.

1. Select a developer signature.
2. Select relevant categories.
 - In this example, only “Apply to sideloaded” is selected.
3. Click Add Selected to rule.
4. Save Changes.



Now all rule changes have been confirmed, the analyst can deploy changes.

1. The analyst can confirm all changes.
2. Click Deploy Policy Changes.

2. Deploy Policy Changes

DEPLOY POLICY CHANGES

1 Demo Tenant (Populated)

App Settings










App Policy

Network Policy

Device Inactivity

RULES IN THIS POLICY

1. Confirm the apps are added

| Criteria | # Rows | Actions |
|--|--------|---|
| Package ID + Version | 1 |  |
| Package ID | 7 |  |
| Developer Signature | 0 |  |
| Package ID + Version | 0 |  |
| Package ID | 0 |  |
| Developer Signature | 0 |  |
| Developer Signature + Package ID + Version | 0 |  |
| Developer Signature + Package ID | 0 |  |
| Developer Signature | 0 |  |

Partner Setup - Branding

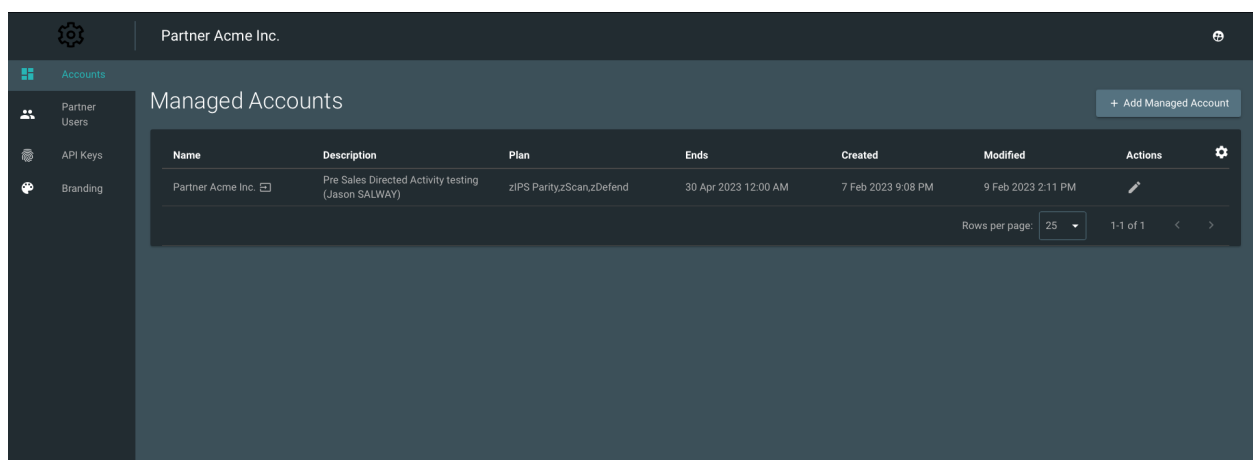
- Set up Partner Branding.
- Design Floor: Cannot easily upload icons in partner branding.

**This activity must be completed in your own testing tenant, not the shared environment.*

Security engineers at a Managed Service Provider have been tasked with onboarding a dedicated Zimperium environment. Since the environment is dedicated and hosted by the partner, they receive additional controls over infrastructure. Contact Zimperium sales for more information.

To start this onboarding process, they start with branding. The engineers follow these steps:

1. Log in to the Partner console
 - *This new view is for partners only which allows them to independently create “Managed Accounts.”*
2. *Select the Branding Tab on the left side.*



The engineers can update the Branding, which will be reflected in all Managed Accounts (customer tenants).

1. Upload Branding

- The engineer must use the .SVG format.
 - Login Page Logo.
 - **Note:** This option is only available to partners that host a dedicated tenant. Please contact Zimperium sales for more info.
- Login Page background.
 - **Note:** This option is only available to partners that host a dedicated tenant. Please contact Zimperium sales for more info.
- Favicon
- Partner Logo After Login
- Theme
 - In this example, the partner selected light.
- Console Name
- Module Naming
 - In this example, the partner rebranded the products to match their own naming conventions.
- Console Logo

2. Click Update down on the bottom right.

zIAP
In-app Protection

Accounts

Partner Users

API Keys

Branding

Partner Acme Inc.

Partner Level

zCONSOLE
Management

Upload Page Logo

Upload File

Upload Page Background

Upload File

Favicon

Upload File

Reset

Partner Logo After Login

Upload File

Reset

Theme

Light

Dark

Account Level

Console Name (document title)

MXDR

Module Naming

zDefend

to

App XDR

zIPS

to

Mobile XDR

Jason Salway

Partner Setup - Create Customer Tenant (UI Based)

- Log in as a partner user and create a managed tenant in UI that will use Partner Branded setup in the previous step

****This activity must be completed in your own testing tenant, not the shared environment.***

Now the engineers have set up branding for all customer tenants (Managed Accounts), they need to create their first managed account. They follow these steps:

1. Log in to the Partner console.
2. Navigate to the Accounts Tab.
3. Click “+ Add Managed Account.”
 - Name the Managed Account.
 - In this example, it is the name of the customer company.
 - Input relevant account details.
 - In this example, it is a Customer ID from the MSP's account management software.
 - Select products purchased.
 - Set subscription end date.
 - Enable MFA
 - This is optional.
 - Insert customer domain(s)
 - Only accounts with this specified email domain will be allowed to register into the tenant.
4. Click Save Managed Account.

Create Managed Account

Account Name

PayWarriors Pty Ltd.

Description

Customer ID: 001291

ACCOUNT SETTINGS

Subscribed Plans

☐ Consumer zIPS

☐ zDefend

☐ zIPS

☐ zIPS Branding

☒ zIPS Parity

☒ zScan

Subscription End Date

10/04/2023

Settings

☐ Two-Factor Authentication

Email Domain(s) - Hit "Enter" to input multiple domains

PayWarriors.com.au

Cancel

Save Managed Account

1. Select + Add Managed Account

+ Add Managed Account

Created

Modified

Actions

7 Feb 2023 9:08 PM

9 Feb 2023 2:11 PM

2. Name Managed Account

Rows per page: 25 1-1 of 1 < >

3. Input relevant customer details

4. Select products purchased by customer

5. Subscription End Date

6. Enable MFA (Optional)

7. Insert customer domain(s)

Partner Setup - Test Customer Tenant Login

Log in to the customer tenant create previously and start configuring....account settings for what products customers purchased (enabled subscribed plans for customer account).

****This activity must be completed in your own testing tenant, not the shared environment.***

Now the first tenant is set up, they can test the login using the partner console.

1. Log in to the Partner console.
2. Select the Accounts Tab.
3. Click the Login Icon on the Managed Account record.

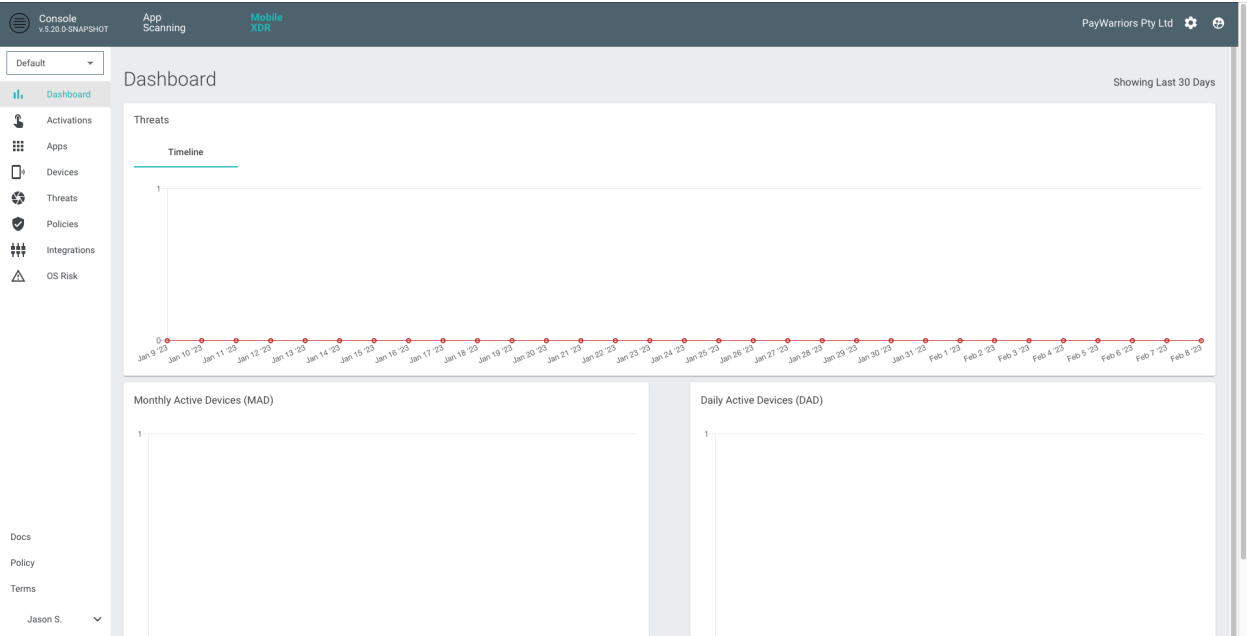
The screenshot displays the 'Managed Accounts' section of a partner console. The interface includes a sidebar with navigation options: Accounts, Partner Users, API Keys, and Branding. The main content area shows a table of managed accounts. The table has columns for Name, Description, Plan, Ends, Created, Modified, and Actions. Two accounts are listed: 'Partner Acme Inc.' and 'PayWarriors Pty Ltd'. An arrow points to the 'PayWarriors Pty Ltd' row, specifically to the 'Login' icon in the 'Actions' column. A red text label '1. Login to Managed Account' is positioned below the arrow.

| Name | Description | Plan | Ends | Created | Modified | Actions |
|----------------------------|--|-------------------------|----------------------|--------------------|--------------------|------------------------|
| Partner Acme Inc. [icon] | Pre Sales Directed Activity testing (Jason SALWAY) | zIPS ParityzScanzDefend | 30 Apr 2023 12:00 AM | 7 Feb 2023 9:08 PM | 9 Feb 2023 2:11 PM | [edit] [trash] |
| PayWarriors Pty Ltd [icon] | Customer ID: 001291 | zIPS ParityzScan | 10 Apr 2023 12:00 AM | 9 Feb 2023 4:10 PM | 9 Feb 2023 4:10 PM | [edit] [trash] [login] |

Rows per page: 25 1-2 of 2 < >

1. Login to Managed Account

The engineers can now validate the tenant was created and partner branding was successful. They have the ability to finish tenant configuration, add end-customer accounts and monitor the environment.



Partner Setup - Create Customer Tenant (API Based)

- For API testing, create a partner API key in UI.
- Create a managed account using APIs.
- Create a 2nd managed account using the same APIs but with different configuration values as needed to show this is a way to configure multiple customer tenants

****This activity must be completed in your own testing tenant, not the shared environment.***

Now the engineers have branded the environment and understand basic partner navigation, they must start developing automation and integration via API. Using the new v5 zConsole APIs, engineers can automate and orchestrate almost every action or task that is available in the UI.

This is notably different from the v4 zConsole API framework, where only certain APIs were exposed for customer consumption. With the v5 zConsole API framework, all APIs are available to customers and their partners via a tenant-based API key.

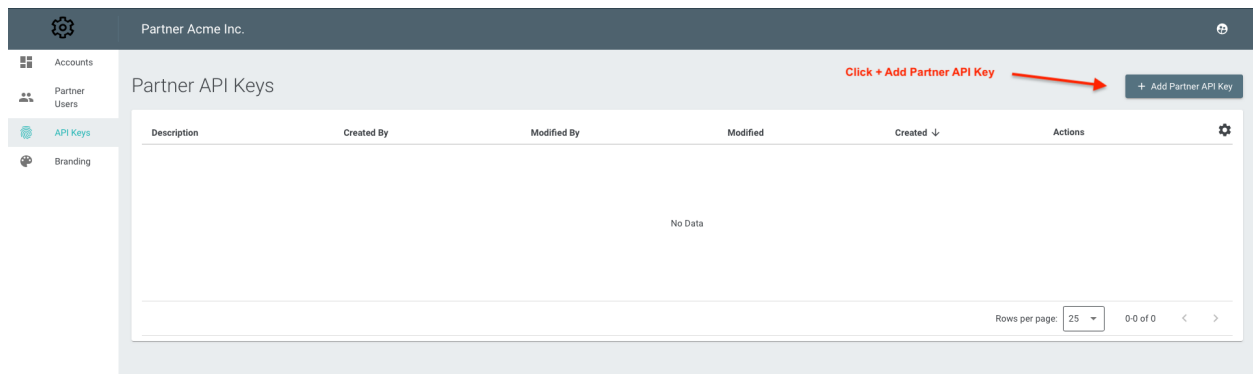
Some example tasks that can be achieved are:

- Integrate with internal MSP billing platforms.
- Integration with CRM for license management.
- Automated Managed Account creation.
- Automated creation of Managed Account users.
- Automated Managed Account Configuration.
- Automated Teams & Group Management.
- Automated Group Activation Creation with QR code and URL retrieval.
- Automate bulk configuration of customer environments.

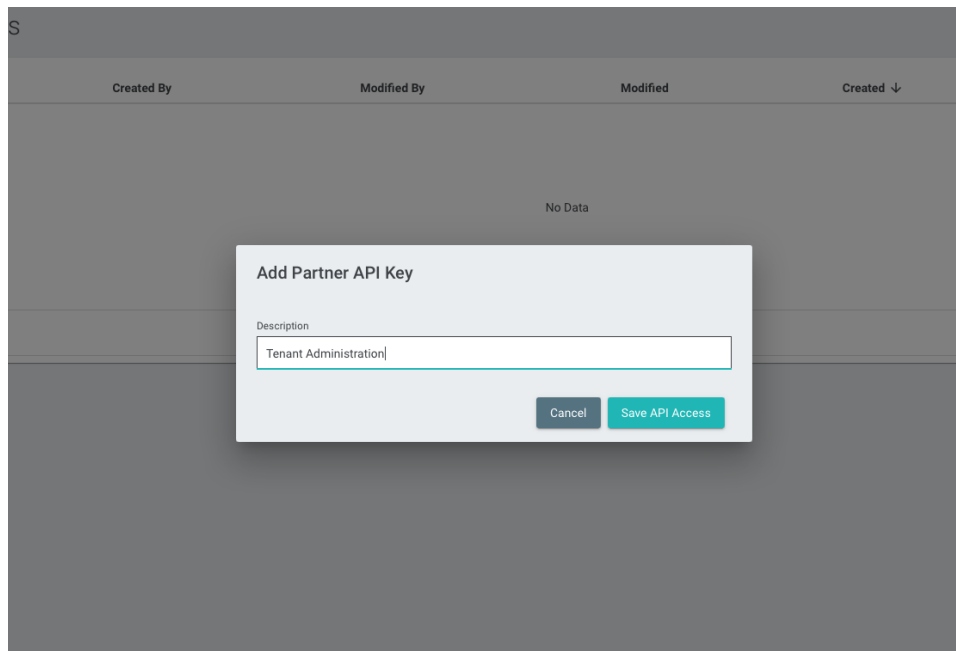
- Centrally retrieve events and threat data.

To start this process, engineers must first generate a customer API key for each Managed Account using these steps:

1. Log in to the Partner console.
2. Select the API Keys Tab.
3. Click + Add Partner API Key.

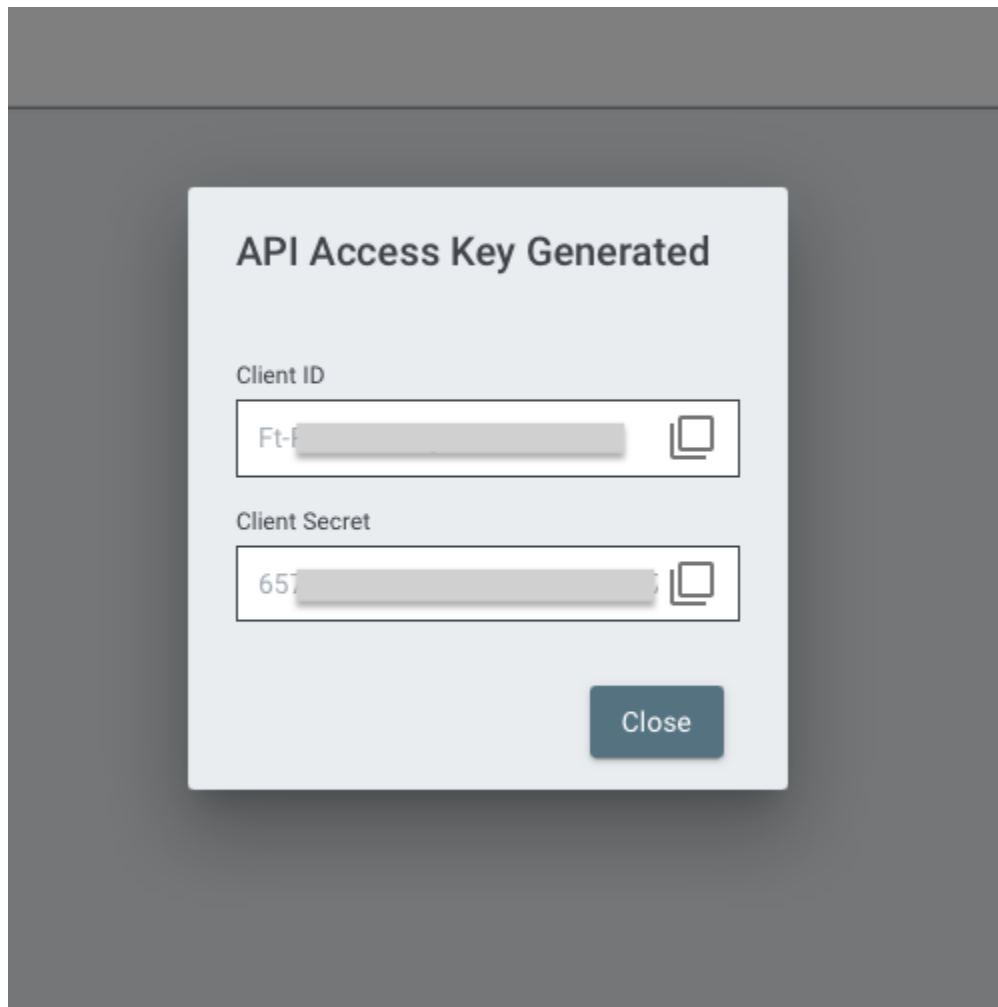


The engineers Name the key, then Save.



Once created, securely save the API Access Key Client ID and Client Secret.

Note: If an API key is not saved at this point, it will need to be re-generated.



Once the key was generated, the engineers referred to the [Partner API Documentation](#) to start testing scripts and automation. All Product and API Documentation is available inside the zConsole Docs tab.



Console
v.5.20.0-SNAPSHOT

App
Scanning

Mobile
XDR



Dashboard



Findings



Apps



Integrations



Policies



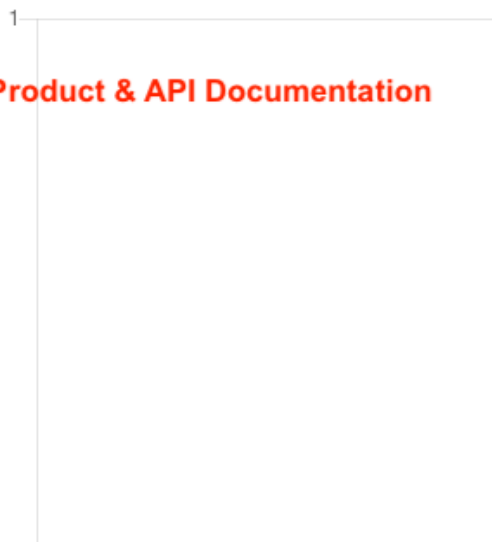
Downloads

Dashboard

Findings Trend



Closed vs. New Findings



All Product & API Documentation

Docs


Policy


Terms

Jason S.



Note: To access documentation, you must be logged into the v5 zConsole for authentication.

 Partner API Keys

 Search

Overview >

User Guide >

Account Management Guide >

REST API Developer Guide ▾

Introduction

Getting Started

Conventions

API Use Cases

zScan Account APIs >

Partner APIs ▾


Partner API Keys

Partner API Authentication

Partner API Details

Requirements

This section covers the Partner API keys for authentication and the authentication process. You must call the partner authentication APIs and get a partner access token to call any other partner API. The partner API flow is a little different than the typical account API flow, and the partner API flow is described in this section. See [Getting Started](#) for an overview of authentication in general.


 **Important**

This section assumes that you have a partner account. If not, contact Zimperium Customer Support team and request a partner account.

From a partner account you can:

- Follow the link in the email and set up a log in access to the zConsole.
- Logging into zConsole takes you to the partner user interface.
- In the partner user interface, you create a partner API key and save off the partner client ID and secret.

To call any API endpoint, you must have an API access token in the request header. The access tokens are temporary and must be generated using API keys. You must obtain the partner client ID and client secret keys. You use this partner client ID and secret to request an access token that has partner account privileges.

 **Note**

All API access tokens are in the format of a JWT and have a limited lifetime of 60 minutes. You must refresh the token before the 60-minute expiration to maintain API access. Regenerate the token after 50 minutes to make sure that requests do not time out.

Table of contents

- Requirements
- Authentication Process
- Generating Partner Access Keys
- Using Access Keys to Generate a Token

Authentication Process