

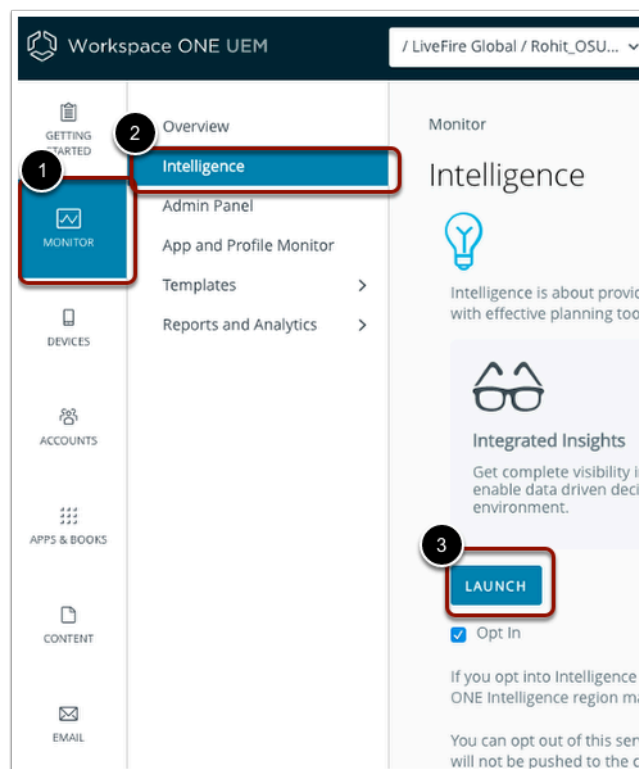
Identify Security Risk using Workspace ONE Intelligence

The Security Risk dashboards in Workspace ONE Intelligence gather reports on numerous device states and quickly identify high-risk devices. In this activity,

1. You will identify the devices that are violating passcode and encryptions policies through the Policy Risks dashboard. Create an automation in Intelligence to mitigate this risk.
2. Experience Intelligence's security capabilities for Windows 10 platform using a Simulation.

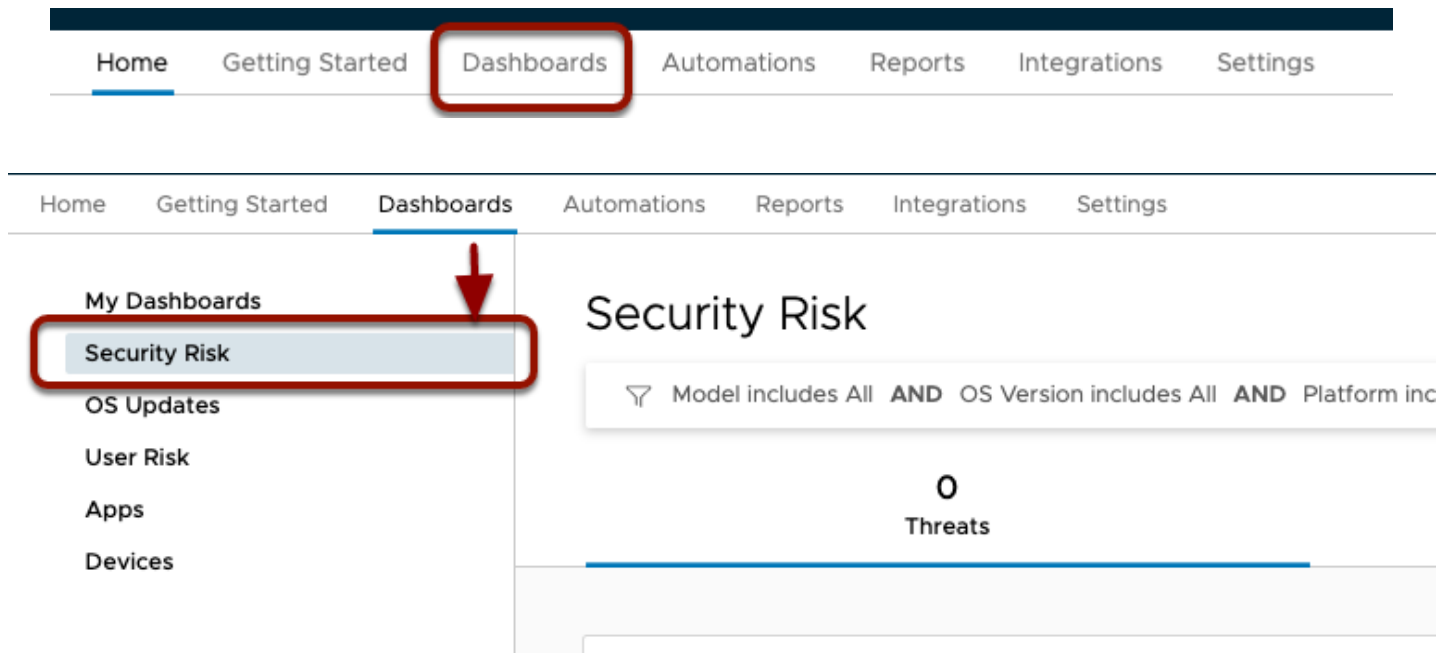
Lets get started.

Part 1: Access the Security Risk Dashboards

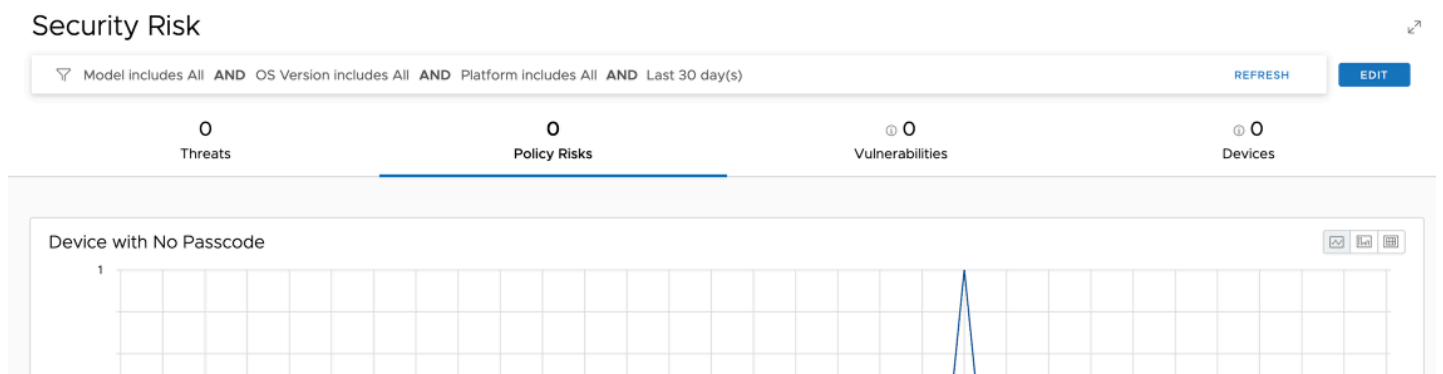


1. From you **ControlCenter** server ,
 - Open a **browser**, navigate to the **Workspace ONE UEM** console, [dw-livefire.awmdm.com](https://livefire.awmdm.com) .
 - Login with your **custom admin** credentials
 - On the left navigation bar, select the **Monitor** Tab
 - Select **Intelligence**.

- Select **LAUNCH**



- On the **Workspace ONE Intelligence** console,
 - From the top options menu, click on **Dashboards > Security Risk**.




- In the **Security Risk** dashboard, you will observe the below modules:

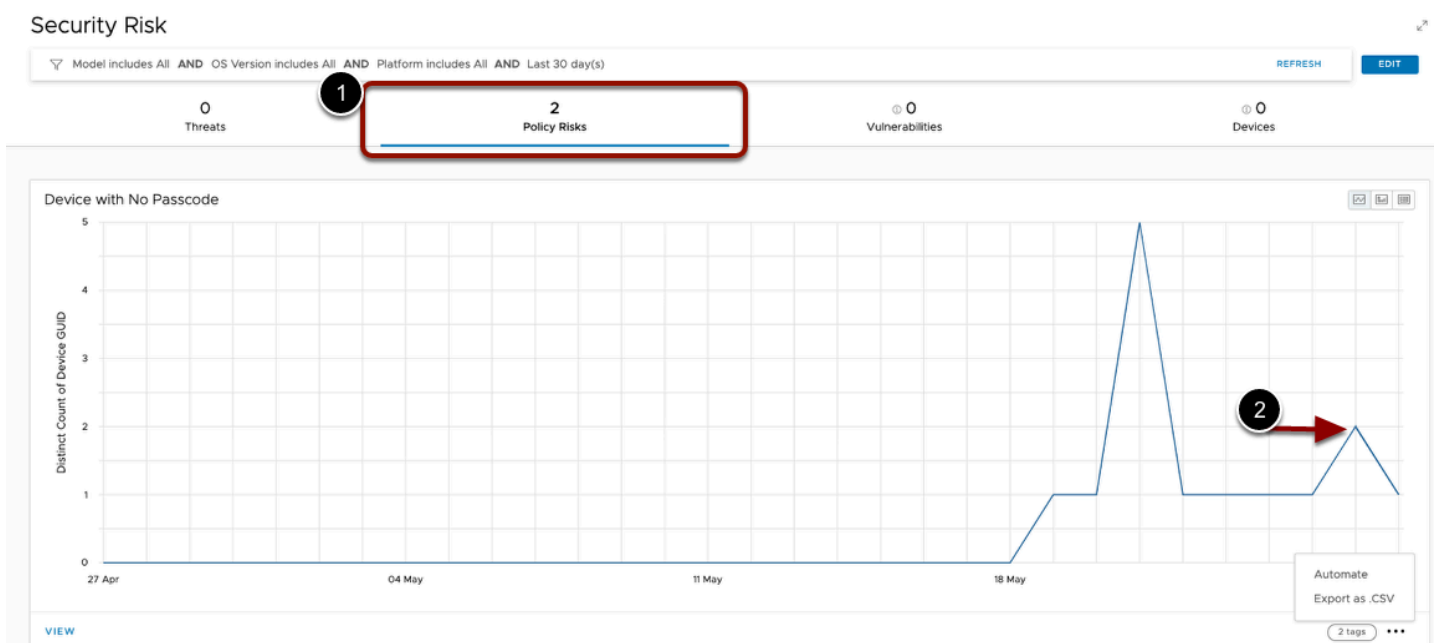
Security Risk Modules

| Groups | Modules |
|-------------|--|
| Threats | The Threats tab displays events identified by your Workspace ONE UEM compliance engine as compromised. It also displays and aggregates events reported by your Trust Network services in the Threats Summary module. |
| Policy Risk | The Policy Risks tab displays events identified by your Workspace ONE UEM compliance engine that do not comply with configured policies. Events include devices with no passcode and devices that are not encrypted. |

| Groups | Modules |
|-----------------|---|
| Vulnerabilities | <p>The Vulnerabilities tab combines and displays information from third-party security reporting services that report security data and Workspace ONE UEM that manages your Windows 10 devices.</p> <p>It displays vulnerabilities reported by the National Institute of Standards and Technology (NIST).</p> <p>It also ties those applicable CVEs to impacted Windows Desktop devices managed by Workspace ONE UEM.</p> <p>Navigate through the CVE explanation cards to find out what devices are impacted, the event's CVSS score, NIST articles, and Microsoft advisories.</p> |
| Devices | <p>The Devices tab displays risk scores for devices managed in your Workspace ONE UEM environment.</p> <p>Select the tab to see device risk scores (reported as a level High, Medium, and Low), risk indicators, and to select single devices for analysis.</p> <p>For details about risk scoring, access User Risk Dashboard.</p> |

 Notice, Risks represented in the Security Risk dashboard are grouped as **Threats, Policy Risks, Vulnerabilities, and Devices**. Next we will identify devices with policy risk and potential vulnerabilities.

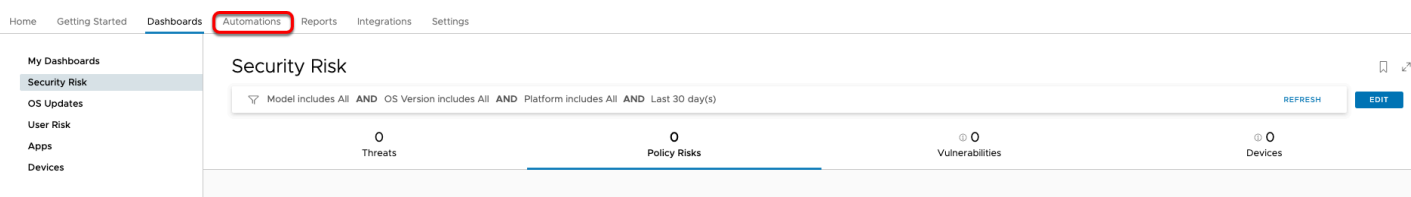
Part 2: Identify Devices without Passcodes



- From the **Security Risk Dashboard**,
 - Under **Security Risk**, next to **Threats**, select **Policy Risk**.

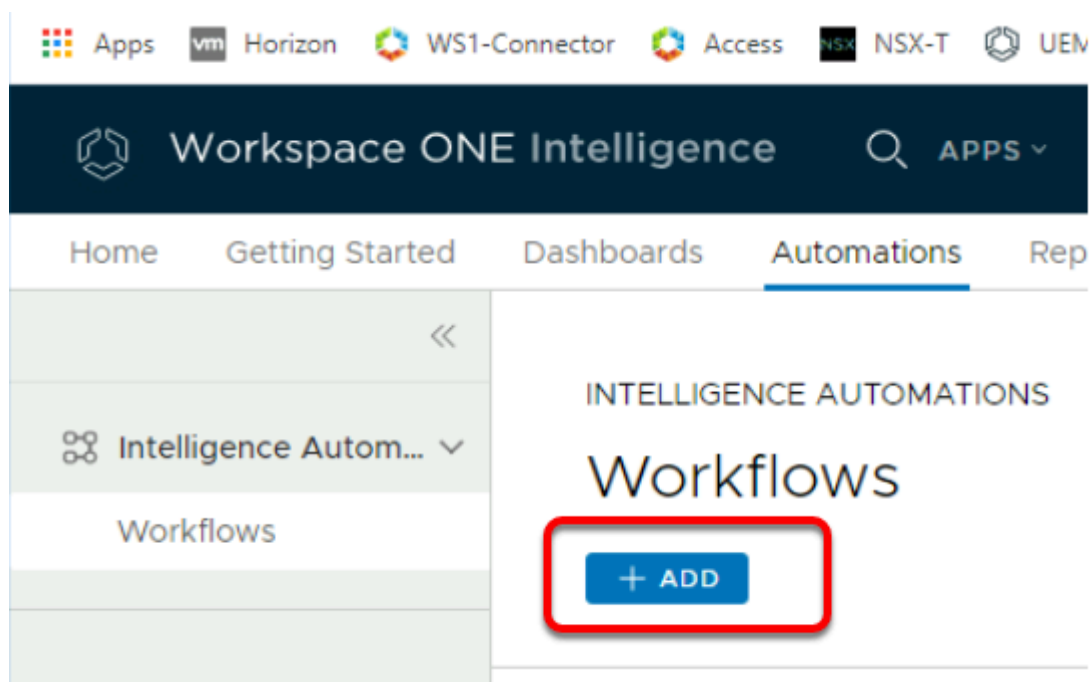
- View the graph to **identify the number of passcode-less devices** detected in the past 30 days. After you understand the scope of the issue, you will build an automation to mitigate this security risk.

NOTE: If you do not see any values listed for the Policy Risks, this is because the device compliance has not been checked yet. Device compliance is queried approximately every 5 minutes, so you may need to click the Refresh button after a few minutes to see the Policy Risks for the newly enrolled Windows 10 device.



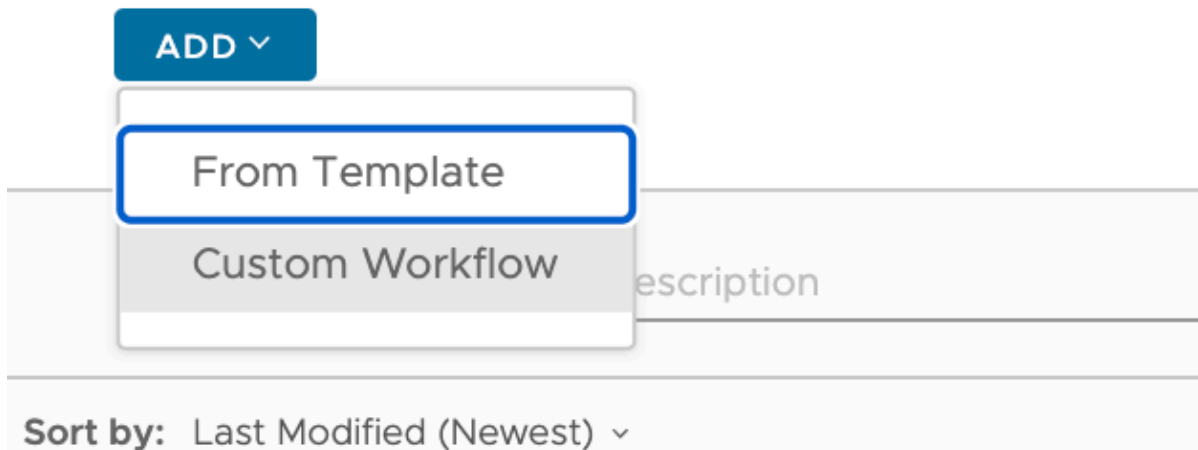
2. In the **Workspace ONE Intelligence** console

- From the top Options Menu, select **Automations**

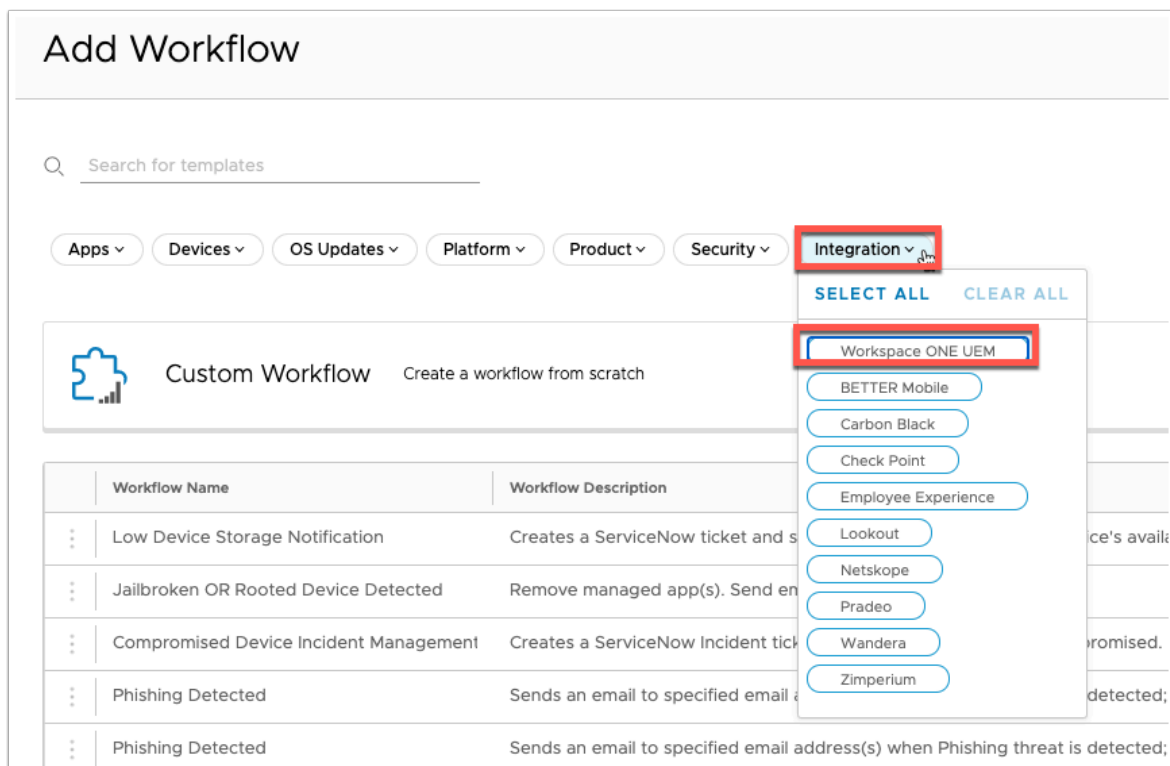


INTELLIGENCE AUTOMATIONS

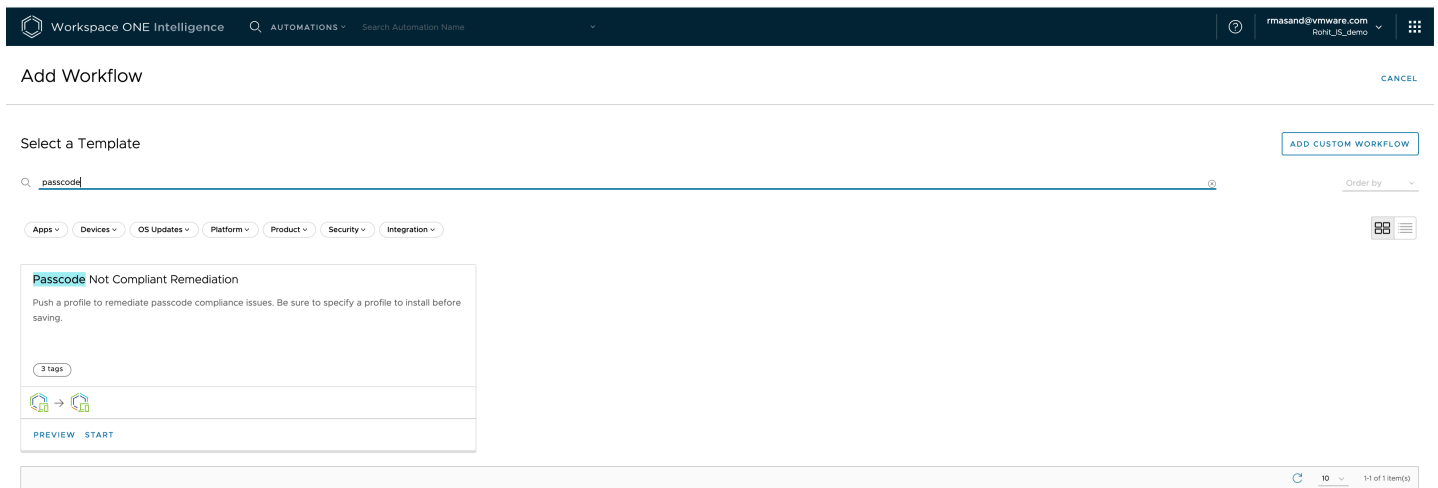
Workflows



3. In the **INTELLIGENCE AUTOMATIONS** area
 - Under **Workflows**, select **+ADD**. Then select **From Template**.

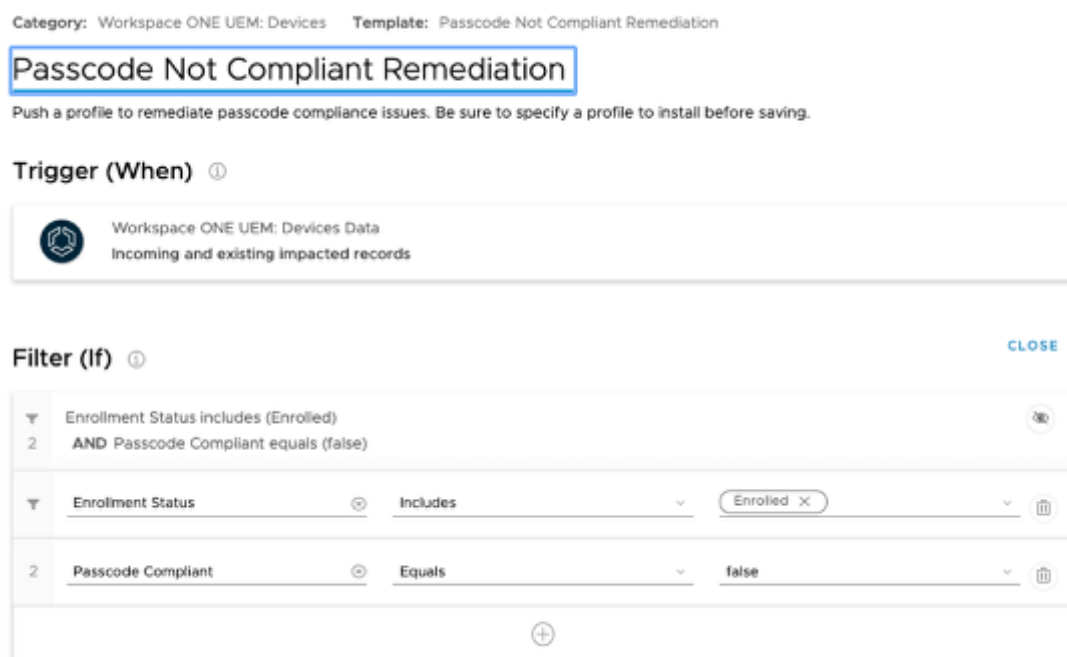


4. In the **Add Workflow** interface
 - Select the dropdown next to **Integration**
 - Select **Workspace ONE UEM**.



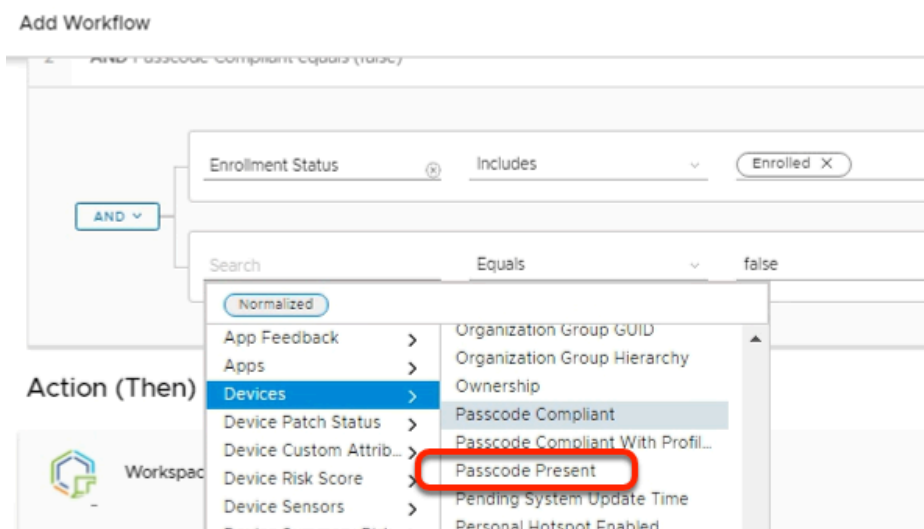
5. In the **ADD Workflow** interface

- find by searching **Passcode Not Compliant Remediation** automation template
- Select **Start** next to the **Passcode Not Compliant Remediation**.



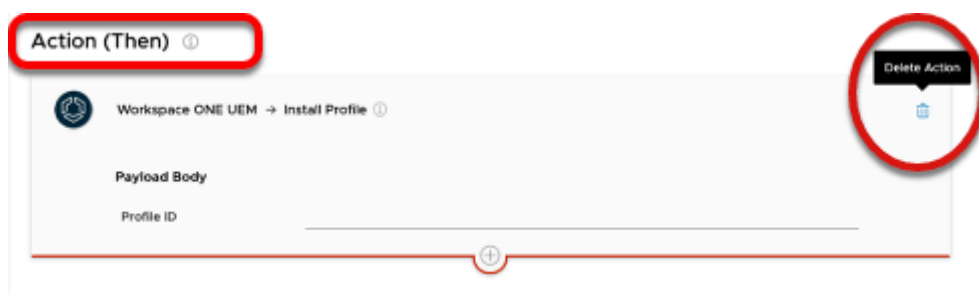
6. Notice the Filter is pre-defined template for devices that are Enrolled and Passcode Compliance status.

- We will be editing the second filter to identify devices that do not have a passcode.
 - If required, Workspace ONE Intelligence gives you the option to add more filters to further target a specific subset of devices



7. In the **Filter Console**

- Select your **cursor** behind **Passcode Compliant**.
 - From the dropdown, select **Device** > **Passcode Present**.

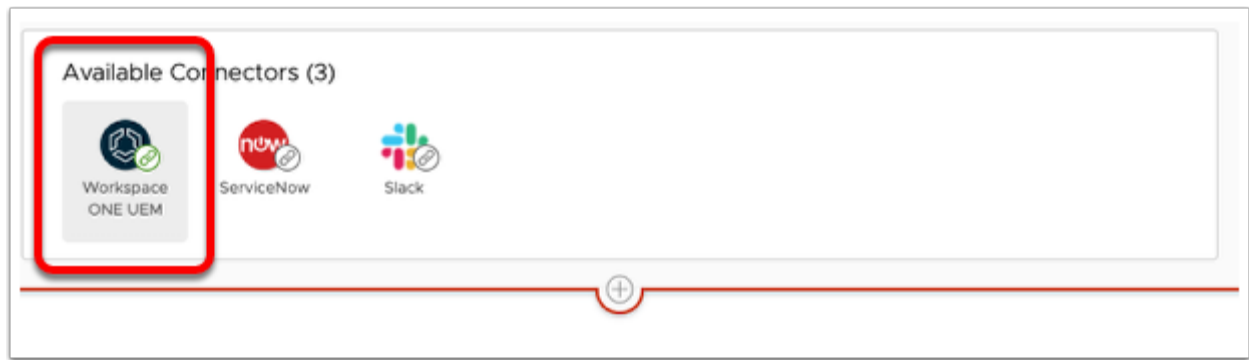


8. In the **Action (Then)** section,

- Notice Install Profile is a default UEM action created. This action will help you to push a passcode profile to all devices that do not have a passcode present.
 - For this test, we will delete this action and rather use a Send Email action.
- To the right of this Action, select the **Delete** icon.

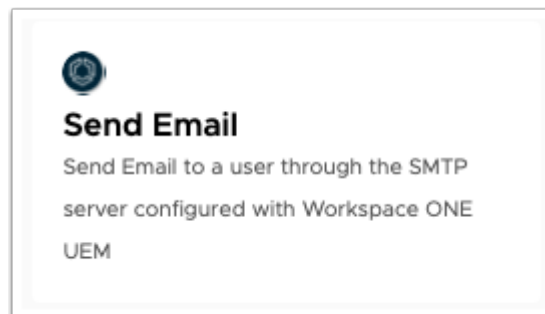


9. Once deleted, In the **Action (Then)** field, click on the **+ icon**.



10. Under **Available Connectors**,
- Select the **Workspace ONE UEM** connector.



💡 Notice you have multiple connectors to choose from. You can either integrate with out of box third party connectors like Slack & ServiceNow or you can add a custom connector. Custom connectors allows you to integrate with any third party portal and create custom actions. For example, Intelligence Automation actions available in UI do not support moving a device to a different Organization group in Workspace ONE UEM. But you can leverage the available APIs to create a custom connector & achieve this use case. In this example, we will select the out of box Workspace ONE UEM connector.



11. Scroll down to find **Send Email** Option.
- Select **Send Email**

💡 Notice there are multiple options and so you can select multiple actions to be taken on the devices that do not have a passcode and are in violation of your Organization's security policies. You can choose to install a profile or revoke a profile until device has met your requirements. In our lab, we will only be using one such possible action.

Action (Then) ⓘ


 Workspace ONE UEM → Send Email ⓘ 

Body


To Address

xeniaforman@gmail.com

Subject

IT notification 

Message

\$(device_enrollment_user_name) 

Wash your hands & set the DEVICE PASSCODE. Then wash your hands again


Path Variables

Device ID

451

TEST

Test successful ⓘ




12. In the **Send Email Action**,

- Enter the following values, next to
 - **To Address.** enter **your registered email address**
 - **Subject box,** enter **IT Notification**
 - **Message:** enter

```
$(device_enrollment_user_name)  
Wash your hands & set the DEVICE PASSCODE. Then wash your hands again
```

- Under **Path Variables**
 - Next to **Device ID**, enter YOUR DEVICEID
- Select **TEST** > **TEST** to verify the Action
 - The Action Test should be successful

 In the example above, we used lookup values to customize our Message to the user under which our device is enrolled.

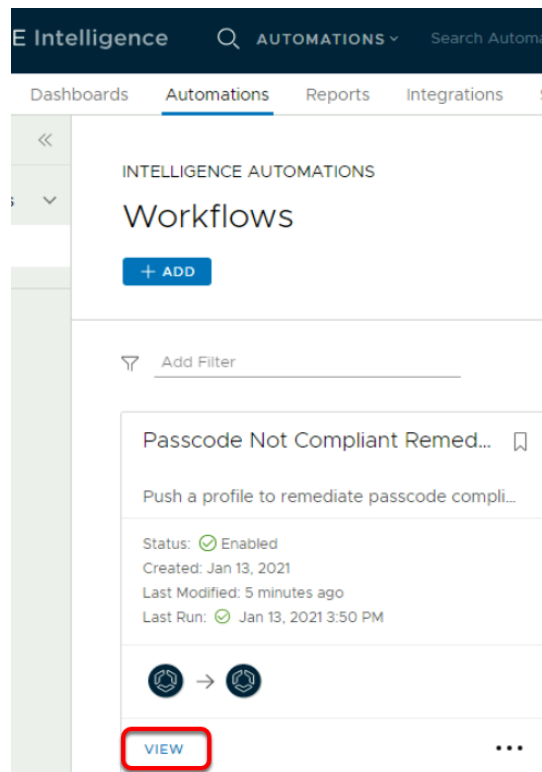
The screenshot shows two identical panels of the 'Add Workflow' window. Each panel contains a toggle switch labeled 'Enable workflow'. In the top panel, the toggle is in the 'off' position (grey). In the bottom panel, the toggle is in the 'on' position (green). Below each toggle are three buttons: 'CANCEL' (light blue), 'BACK' (blue outline), and 'SAVE' (solid blue).

13. In the bottom right-corner of the Add Workflow window
- Change the toggle to Green to **Enable Workflow**
 - Select **SAVE**.

The screenshot shows the 'Save Workflow' window. At the top, it says 'Save Workflow'. Below that is a yellow warning box with a triangle icon and the text 'Actions will execute on 1 filtered results.' Underneath, it says 'Historical data detected' and 'We have detected 1 filtered results based on historical data.' Then, there is a toggle switch labeled 'One-time Manual Run' which is in the 'ON' position (green). Below this, it says 'Workflow will constantly monitor and run on new data that matches your criteria. Do you want to save and enable this workflow?'. At the bottom right, there are two buttons: 'CANCEL' (blue outline) and 'SAVE & RUN' (solid blue).

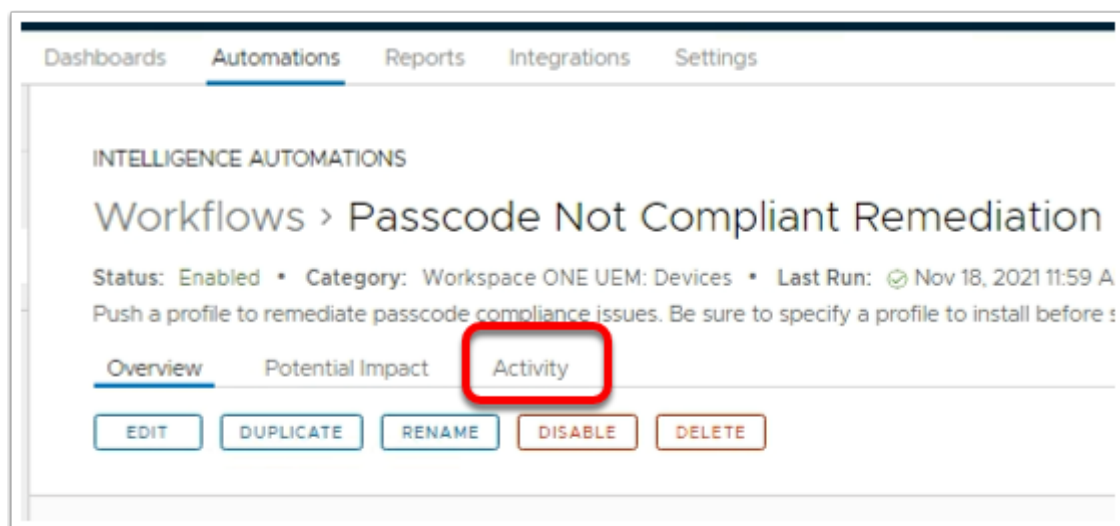
14. In the **Save Workflow** window
- Next to **One-Time Manual Run**, turn the Toggle to **ON**

- Select **SAVE & RUN**



15. In the Workspace ONE Intelligence Console

- Under **Workflows**, under your new **Passcode Not Compliant Remediation Workflow**
- Select **VIEW**.



16. In the **Workflows > Passcode Not Compliant Remediation** window

- Select **Activity**

INTELLIGENCE AUTOMATIONS

Workflows > Passcode Not Compliant Remediation

Status: **Enabled** • Category: Workspace ONE UEM: Devices • Last Run: Jan 13, 2021 3:50 PM • Created: Jan 13, 2021

Overview Activity

Log data of workflow actions taken

| Target Identifier | Target Type | Service Type | Action | Status | Created |
|-------------------------------------|----------------------------|--------------------|------------|------------|---------|
| AB73B00A-5146-4022-B3E5-04C28CCF8BE | Workspace ONE UEM: Devi... | Workspace ONE U... | Send Email | COMPLET... | Jan ' |
| AB73B00A-5146-4022-B3E5-04C28CCF8BE | Workspace ONE UEM: Devi... | Workspace ONE U... | Send Email | ACTIVE | Jan ' |

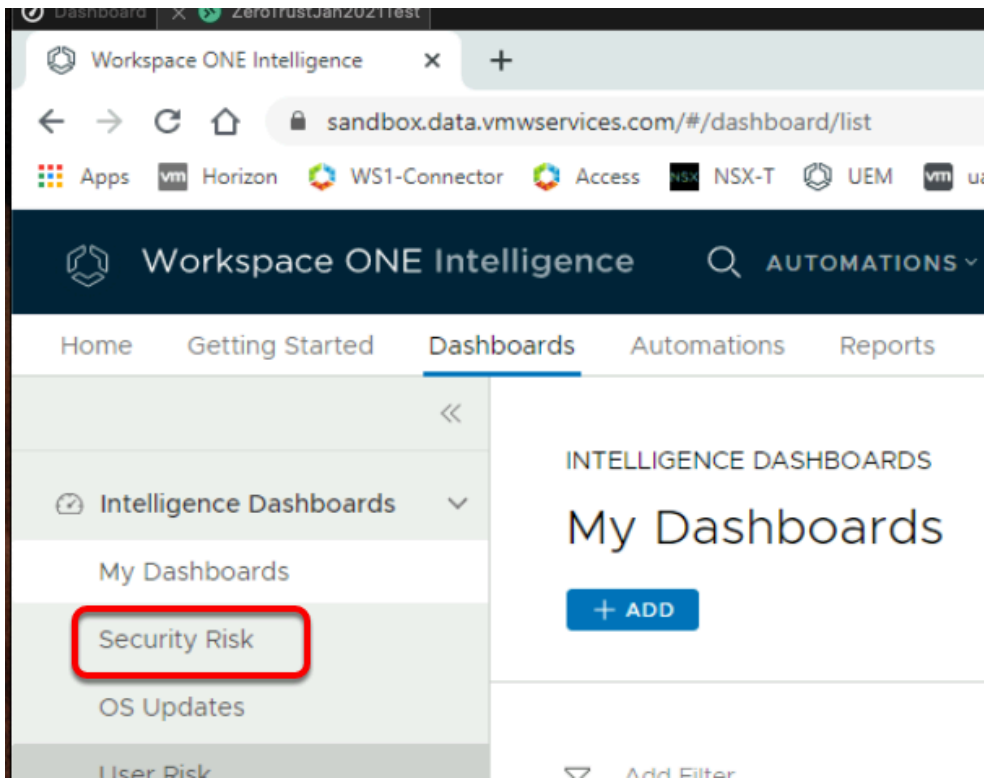


Notice the action SEND EMAIL have been successfully Completed.

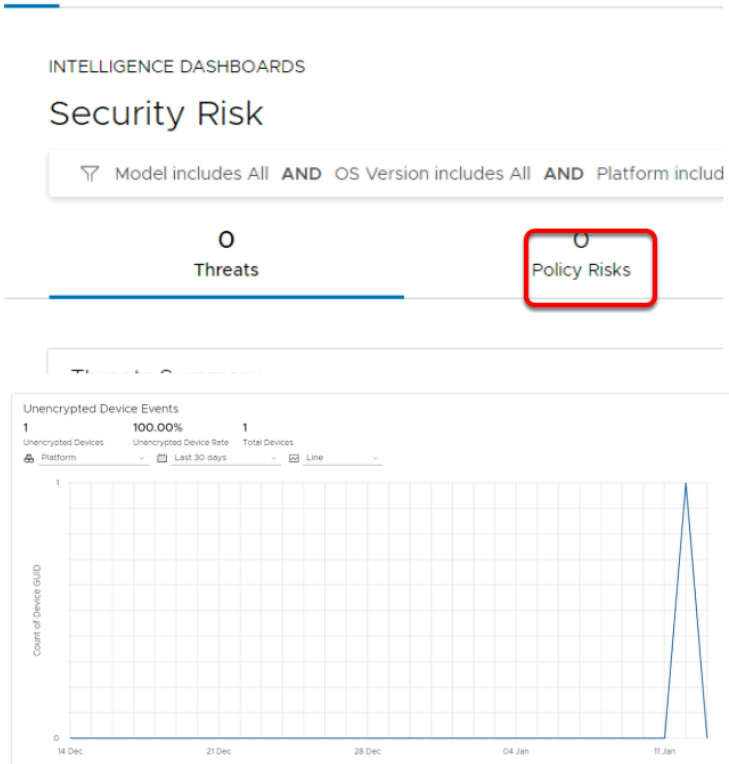


This view allows you to Edit your Automation policy and also check for Activity. Activity tab is useful for admins to monitor the devices and timestamp of the actions successfully taken to mitigate the risk.

Part 3: Identify Unencrypted Devices




1. On the Workspace ONE Intelligence Console,
 - Navigate to **Dashboards** > **Security Risk**.



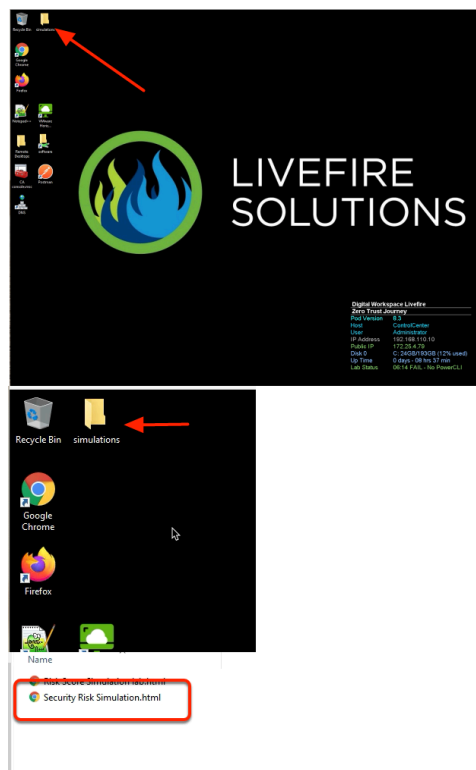
2. In the **INTELLIGENCE DASHBOARDS** window

- Under **Security Risk**, next to **Threats**, select the **Policy Risks** tab.
- **Scroll down** to view the **Unencrypted device Events**
 - This allows administrators to have a quick view of total number of unencrypted devices in their Organization.
- (Optional) You can create an automation by following the same steps as above to experience the automation capabilities in Intelligence. However if you choose to skip, no further action is required.

 **Note:** Typically you would create an automation to enforce device encryption profile on the device to ensure required corporate devices are encrypted.

Part 4: Simulation


This part of the lab is presented as an Interactive Simulation. This will allow you to experience the capabilities that are not feasible to demonstrate in our lab environment due to lack of data and wait time for the CVE data to be updated in Intelligence Console. In this simulation, you can use the software interface as if you are interacting with a live environment.



In order to access the simulation,

1. On your ControlCenter Machine **Desktop**,
 - Find and open the **Simulations folder**
 - Double click **Security Risk Simulation.html** file to start the simulation



NOTE: Use your keyboard left arrow key  to go back in the simulation. The screensteps for this simulation are on the right panel of the simulation screen.

Once completed, simply close the browser and proceed to the next section of the labs.