FORESCOUT

Name: _____

The Forescout Test Drive

Experience the Difference of Agentless Device Visibility and Control

Contents

INTRODUCTION

Forescout Test Drive demos let you experience the powerful features of the Forescout platform firsthand. They provide you with a live Forescout instance in a lab environment and easy-to-follow, step-by-step guidance for exploring the product. No Forescout experience necessary.

Following a quick introduction, today's course will take you through six real-world scenarios:

LAP ONE: VISIBILITY. You can't secure what you can't see.™ Learn how to discover every physical and virtual device connected to your network, classify it, and assess its security posture.

LAP TWO: ASSET MANAGEMENT. Agentless device visibility and continuous monitoring fuel every aspect of cybersecurity. Access a real-time hardware and software asset inventory for an annual software audit—without pulling resources from other critical tasks. Query the Asset Inventory to quickly obtain valuable device-related information.

LAP THREE: DEVICE COMPLIANCE. Streamline a security audit as you quickly determine whether networked devices are running up-to-date security software. Next, create and apply a policy that notifies employees that they are of out of compliance and confirms that systems are restored to company standards.

LAP FOUR: INCIDENT RESPONSE. Put the Forescout policy engine through its paces as you respond to a WannaCry outbreak. Use an automated policy to quickly locate vulnerable hosts and determine which need to be patched and which are infected—instead of the complex process most enterprises use today. Create dashboard entries so you can monitor your progress while responding to this incident.

LAP FIVE: NETWORK ACCESS CONTROL. Enforce changes to your company's antivirus policy. Because of the WannaCry outbreak, you must quickly remove devices that aren't running up-to-date antivirus software from your network. Experience a new level of control as you quickly assess devices and restrict, block or quarantine noncompliant systems.

LAP SIX: NETWORK SEGMENTATION. Assess the devices on your network and make sure they can only access the resources they need. Segment access based on device type and security posture to reduce the risks posed by rogue and noncompliant device.

Scenario

You are the Chief Information Security Officer of a small company, ThingCo, that distributes Things. Your growing company recently moved into a larger facility that has a distribution center attached to it. The automated systems in the distribution center can be controlled from the corporate network.

You recently discovered that contractors plugged a consumer wireless access point into the distribution center network to make it easier for them to get their systems on the network, and then left it there. The device is not secured. Luckily, there was no sign of a breach, and its presence did not affect the older industrial control systems running on that network.

However, it highlighted an issue that you have been trying to address. Your company's quarterly e-mail asking about the devices people have on the network, and the manual collection and entry of that information, are clearly not sufficient. Additionally, the agent-based audits of software running on your network are missing many devices in your environment that cannot have agents installed on them. You need a real-time, agentless view into your network.

After hearing about the capabilities of the Forescout platform, you decided to bring it in for a Proof of Concept on your network.

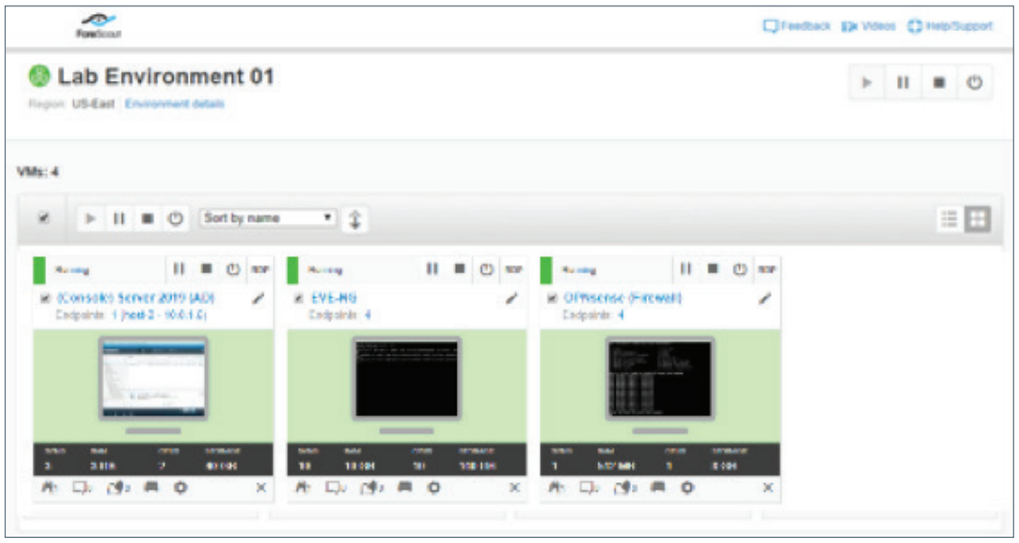
WARM-UP LAP: ACCESSING AND USING THE DEMO ENVIRONMENT

The Test Drive uses virtual devices in a cloud-based environment accessed through your web browser to give you a hands-on experience with the Forescout platform.

Note: Google Chrome is the recommended web browser.

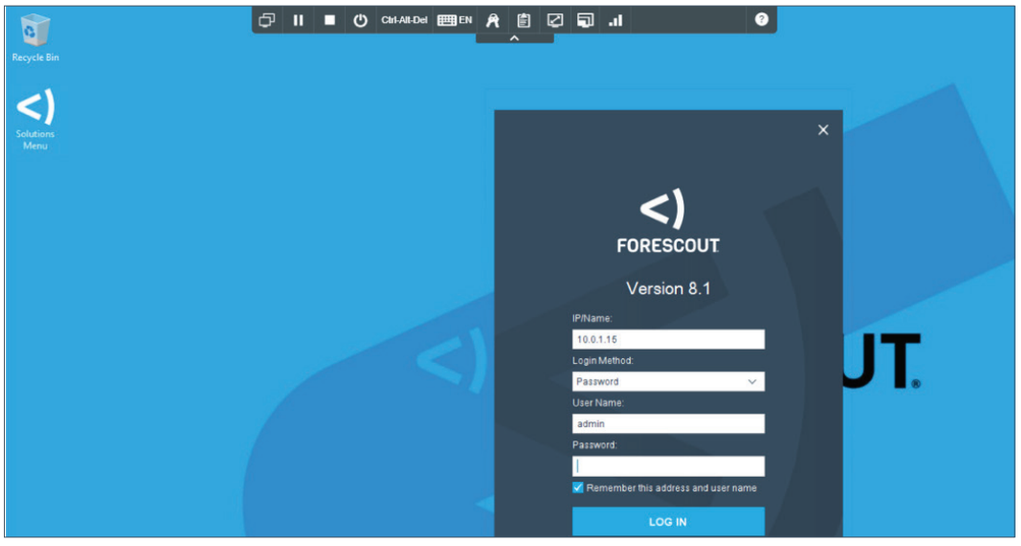
Step 1: Point your browser to the lab link provided in your registration confirmation email message.

Your lab console with three devices appears.



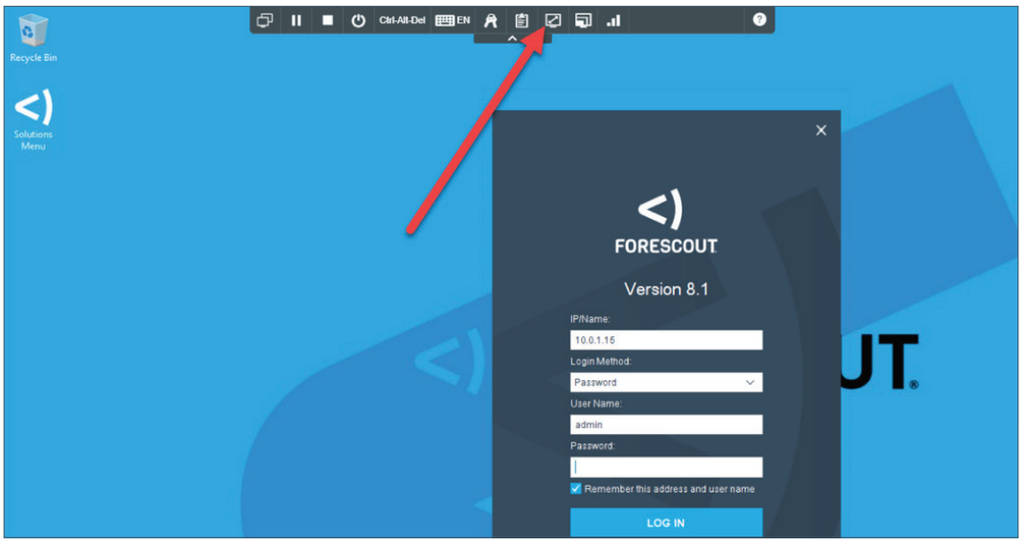
Step 2: Click the **(Console) Server 2019 (AD)** device.

The device interface appears.

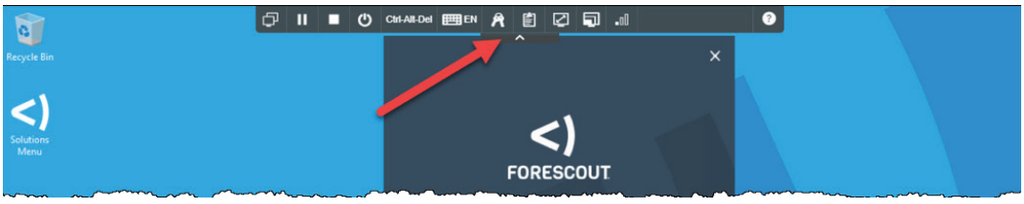


Step 3: Resize your browser to a comfortable size. We recommend making your browser full screen.

Step 4: Click the **Fit to Window** button in the toolbar.



Step 5: Click the **Toggle Toolbar** button to move the toolbar out of the way.



You are now ready to begin.

LAP 1: VISIBILITY

Scenario

You heard that a recent study conducted by IDC found that Forescout customers see 24% more devices than expected on their networks—some seeing as high as 60% more. You had some doubts about the numbers, so you decided to try the Forescout platform on your own network.

After installing the Forescout platform, you discovered that there were many more devices attached to network than you anticipated—lab computers connected to the corporate network, consumer wireless access points that were not part of the planned infrastructure, non-corporate mobile devices, many more network-connected smart speakers than you expected—even a game console and a smart TV.

Forescout has pioneered an agentless approach to security that provides real-time discovery, classification, assessment and monitoring of devices, allowing you to see what's on your network, from campus to cloud, and to securely manage it.

Before you begin

- How do you currently track the devices that connect to your network? How many devices do you currently have on your network? How confident are you that the number is accurate?
- Why types of devices are they? How do you know?

In this lap, you will:

1. Learn about how the Forescout platform discovers, classifies, and assesses the devices on your network.
2. Access the Forescout platform's console.
3. Find your way around the Forescout platform's graphical user interface.

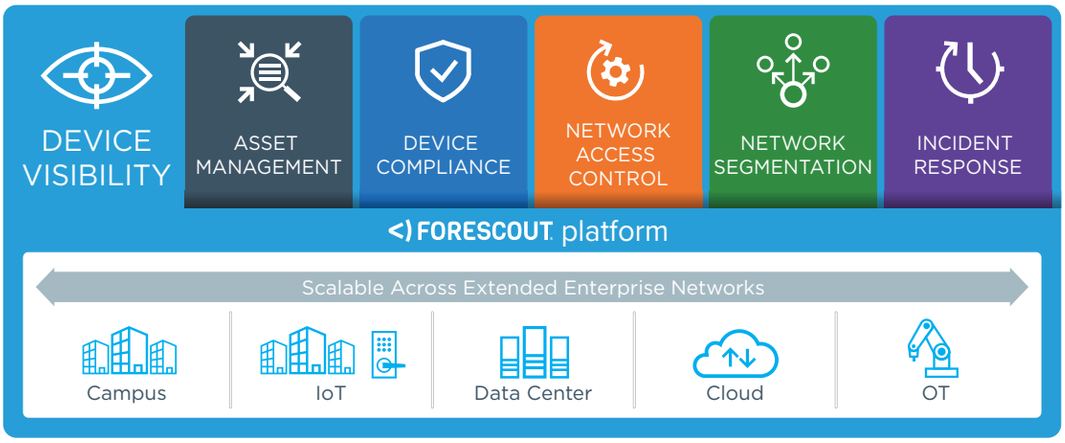
Task 1: How Does Forescout See Devices?

Follow along with the Test Drive leaders as they guide you through how the Forescout platform gives you visibility into the devices on your network.

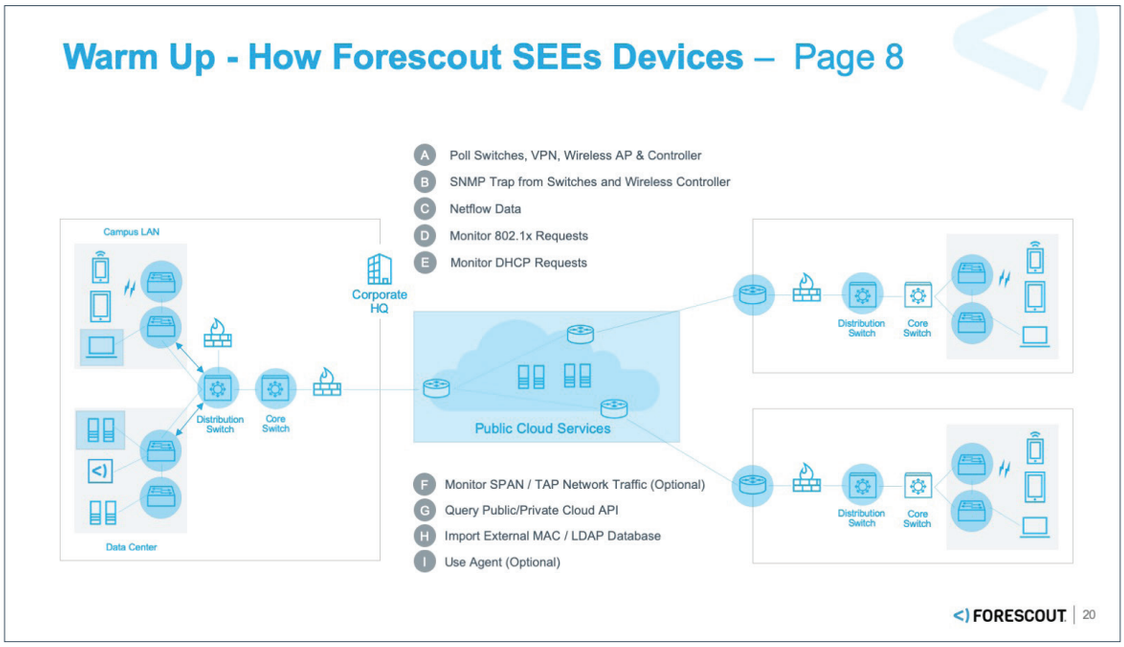
The foundation of the Forescout platform is visibility. This need for visibility goes across the entire enterprise—campus, IoT, data center, cloud and operational technology (OT) environments—and comes together to solve a variety of use cases that address your business needs:

- **Asset Management**
- **Device Compliance**
- **Network Access Control**
- **Network Segmentation**
- **Incident Response**

Forescout's Mission: 100% Device Visibility and Control

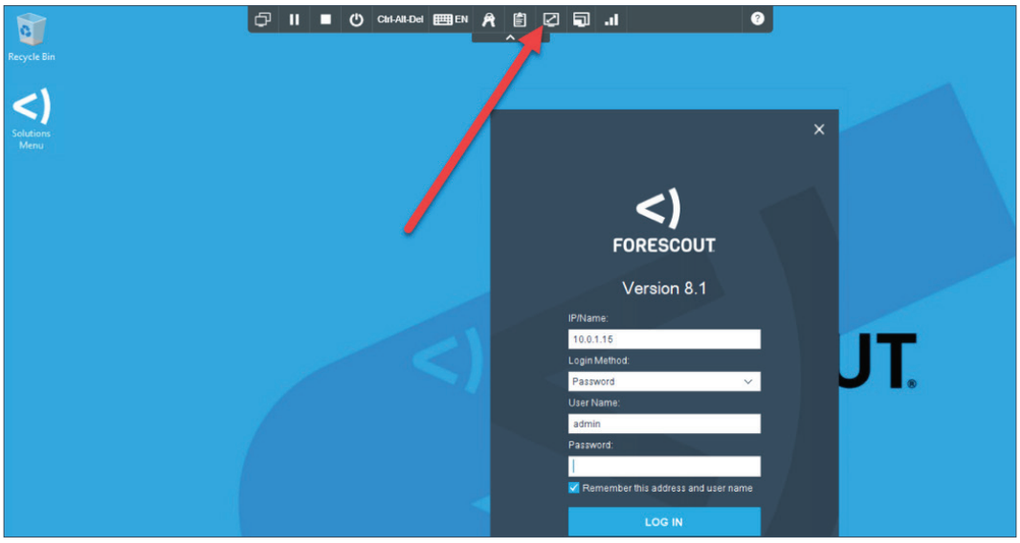


Using a combination of active and passive monitoring techniques, Forescout eyeSight provides in-depth visibility to discover devices the instant they enter the network—without requiring agents. eyeSight classifies and assesses these devices and virtual instances, then continuously monitors them as they come and go from the network.



Task 2: Access the Forescout Console

Step 1: The Console Login dialog box should be running when you first access the console device. If it is not, click the **Forescout Console** icon  in the taskbar.



The Console Login dialog appears.

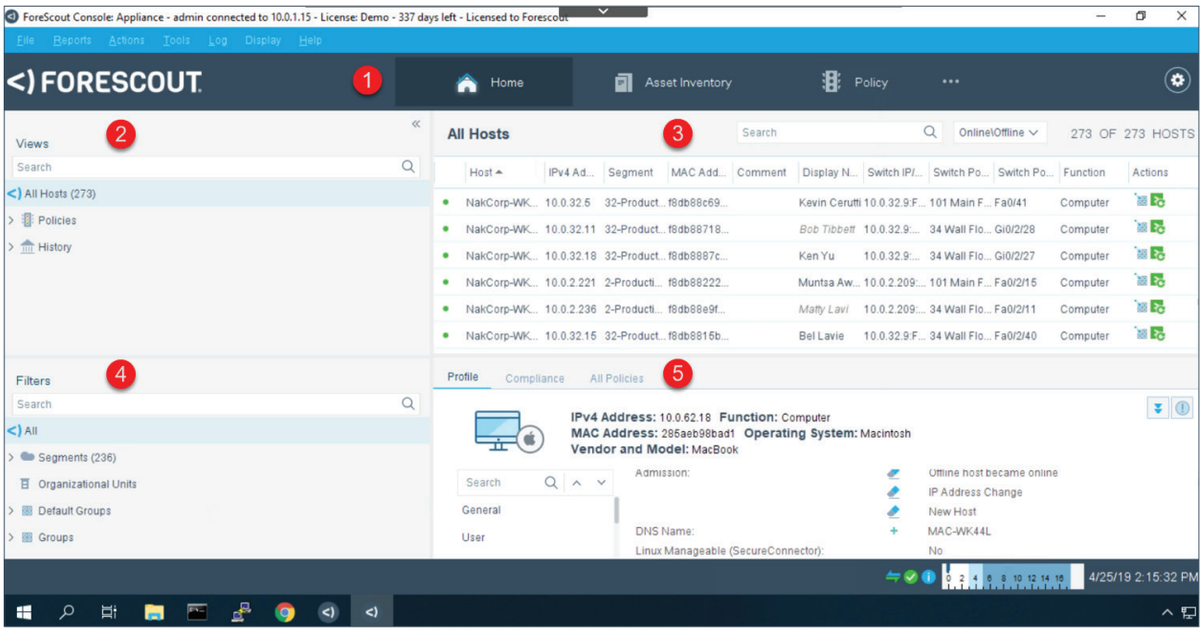
Step 2: Enter **4Scout123** in the password field and press **Enter**. The password is case-sensitive.

The Forescout Console opens.

Task 3: Getting Around the Forescout Platform

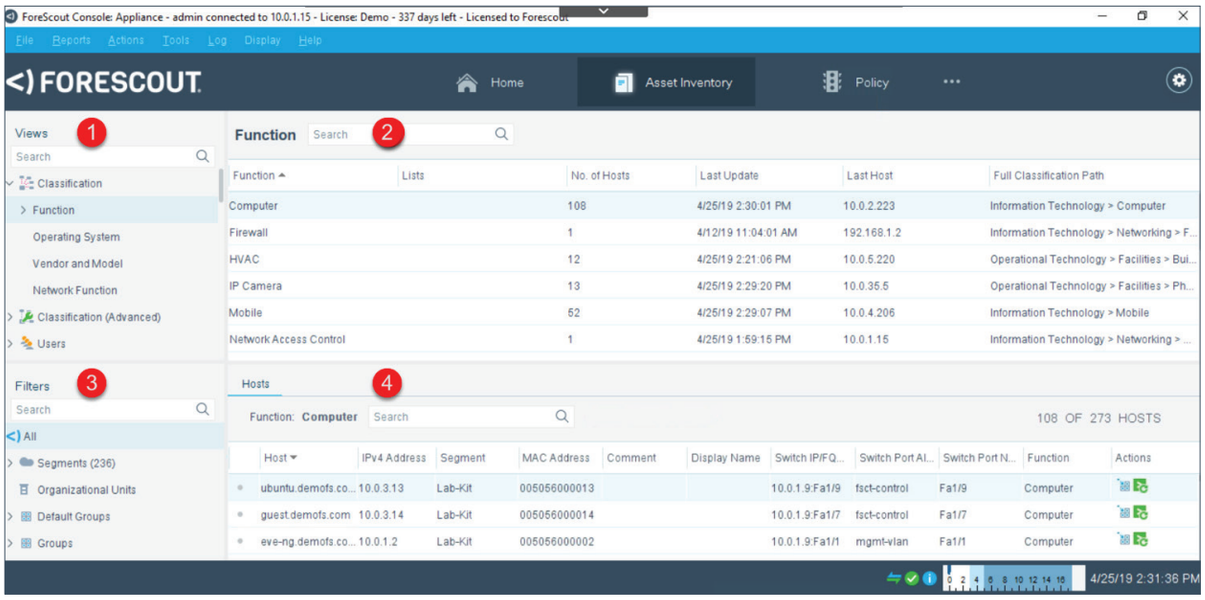
Throughout this guide, you will be directed to look at or interact with various parts of the Forescout platform's interface. Follow along with the Test Drive leaders as they map out the parts of the interface. This will help you navigate your way around the upcoming laps.

Home Screen



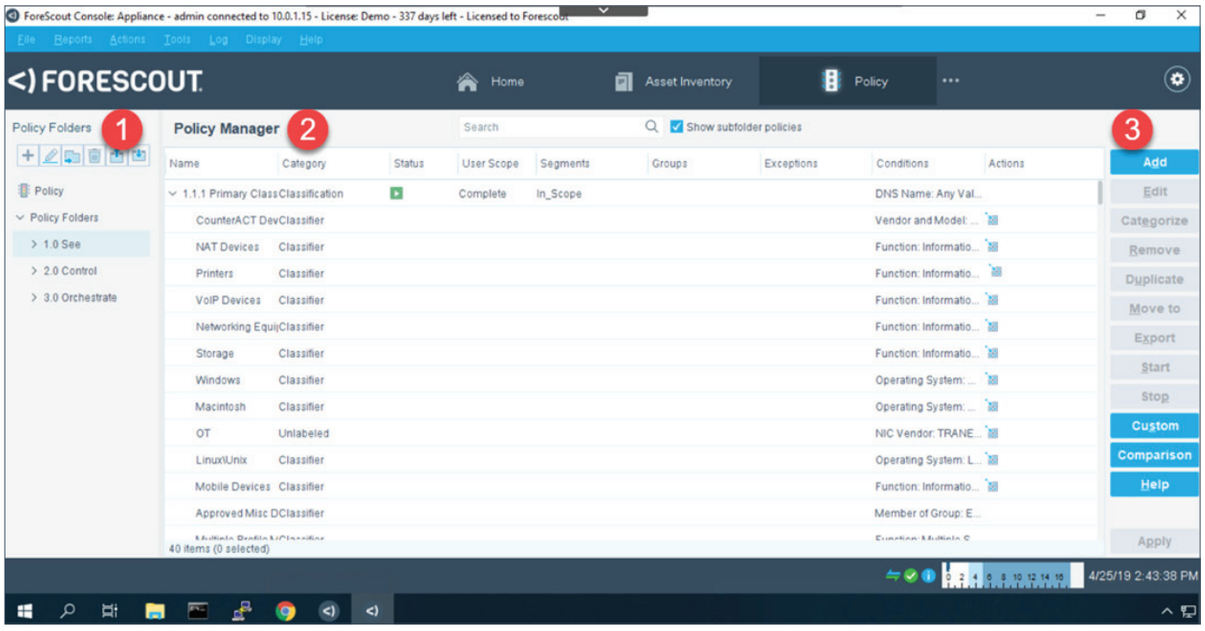
Home Screen	
1	Navigation Tabs (Home selected)
2	Policy Tree
3	Host Table
4	Host Table Filters
5	Host Detail

Asset Inventory Screen



Inventory Screen	
1	Views Tree
2	Sub Groups
3	Host Filter
4	Host Table

Policy Screen



Policy Screen	
1	Policy Folders Tree
2	Policy Manager
3	Policy Actions

Now that we are warmed up, let's get moving. Time to put our visibility in motion with Lap 2: Asset Management.

LAP 2: ASSET MANAGEMENT

Scenario

After the incident with the unsecured wireless access point, your company has decided that it needs to improve their asset management policies and procedures. Management wants tighter control of the hardware and software running on the network.

Because you are already trying the Forescout platform, you have decided to use it to gain visibility to the hardware and software on your network without pulling resources from other critical tasks.

The Forescout platform enables you to discover every Internet Protocol (IP) addressable device that connects to your network, in real time. Using both agentless and agent-based technology, it shows you the software and processes running on the managed endpoints on your network. The Forescout platform can provide detailed visibility into the devices in your operational technology environments.

Once you discover the devices, the Forescout platform classifies them using several criteria: type and function, operating system (OS) and version, manufacturer, model, and network function. Finally, Forescout can assess whether the devices are corporate-managed devices, and if those managed devices comply with corporate policy.

Before you begin

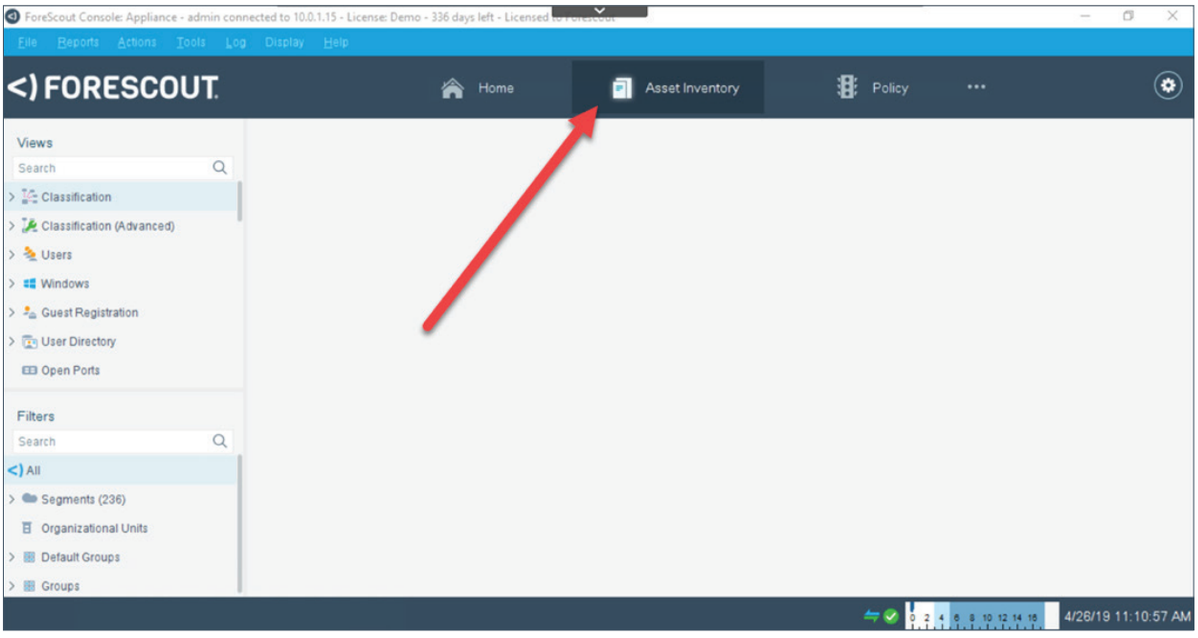
- How do you currently track hardware and software assets in your organization? Spreadsheets? Dedicated applications? Configuration management database (CMDB)?
- How do you keep it current? Surveys? Real-time data collection?
- How confident are you that your asset management tool is up to date with today's information?
- Who are the consumers of this data? How are they using it? What is the impact of inaccurate, out-of-date, or incomplete data to these users?

In this lap, you will:

1. Use the Forescout platform's Asset Inventory functionality to quickly see what types of devices are attached to the network.
2. Use the Asset Inventory to quickly see how many endpoints are running Microsoft Office (and which versions).
3. Use the Asset Inventory to see the operational technology devices running in your distribution center.
4. Use the Forescout Home tab to see all the devices running in your distribution center—both OT and IT devices.
5. Search for some specific devices using the Asset Inventory.

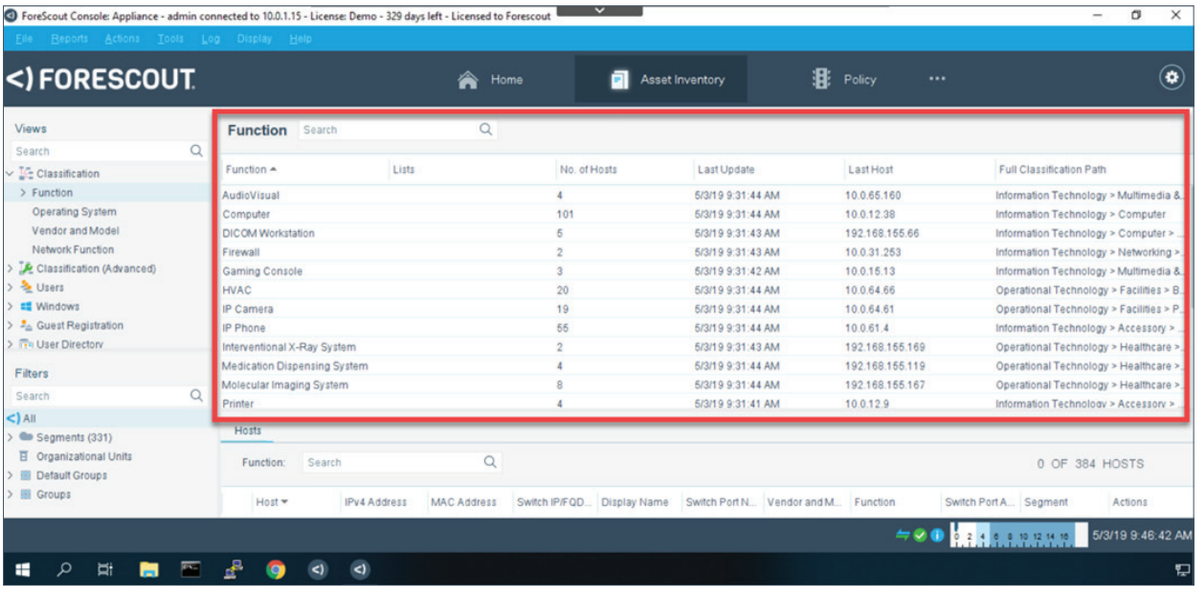
Task 1: Discover the Types of Devices on the Network

Step 1: Click the **Asset Inventory** tab at the top of the screen.



Step 2: In the **Views** tree, expand the **Classification** folder and click **Function**.

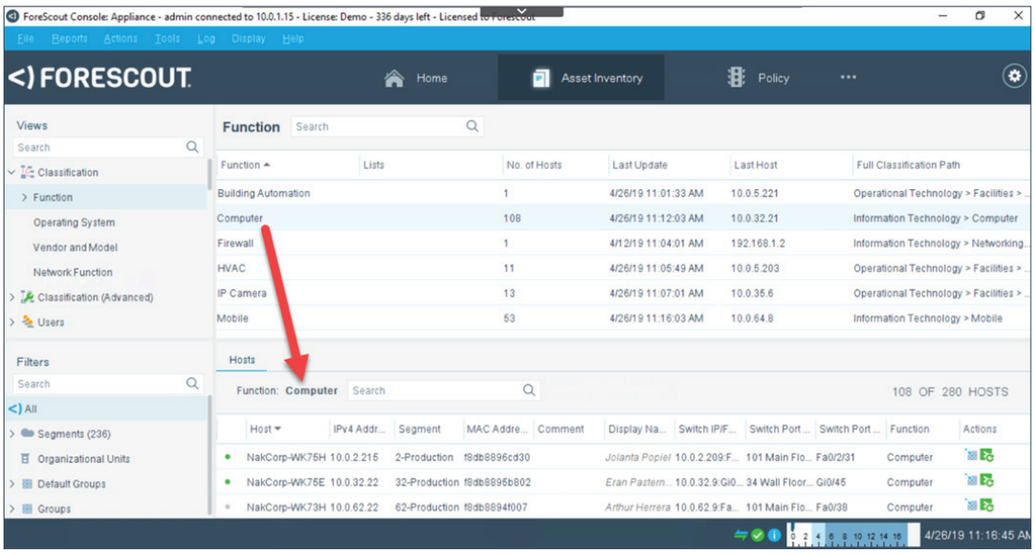
A list of functions with device counts appears.



Step 3: Click a function, such as **Computer**.

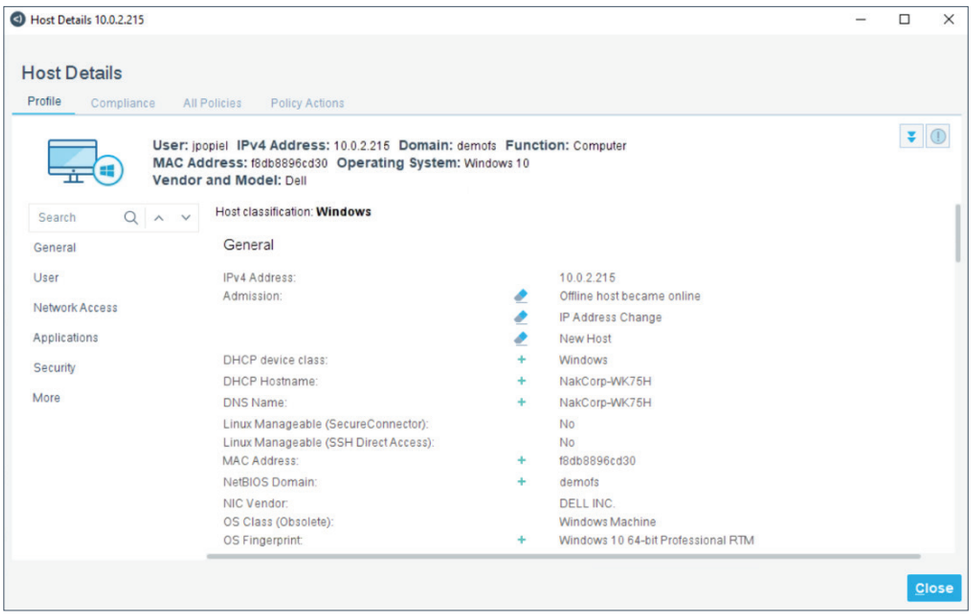
A list of devices that fall into the Computer classification appears at the bottom of the screen. You may need to drag the border between the Function table and the Hosts table up to show the hosts.

Some of their properties are also shown in this table. You can customize the information shown in this table by right-clicking the table headers.



Step 4: Double-click one of the devices that has a name starting with "NakCorp."

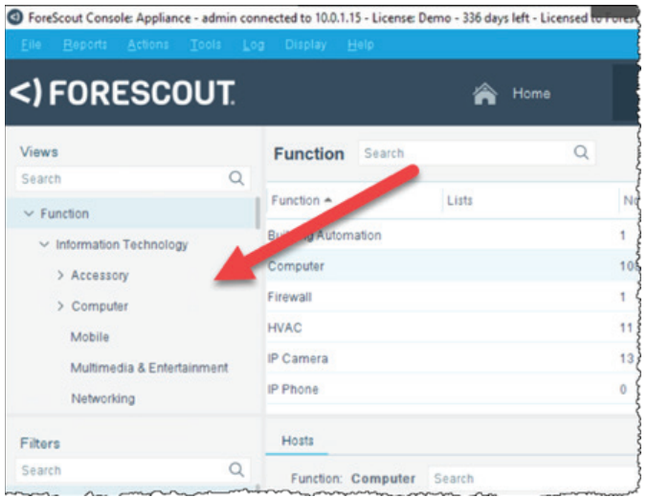
A dialog box shows all the information discovered for the device. You can also see which compliance-specific policies, all policies in general, and policy actions affect the device.



Step 5: Click **Close**.

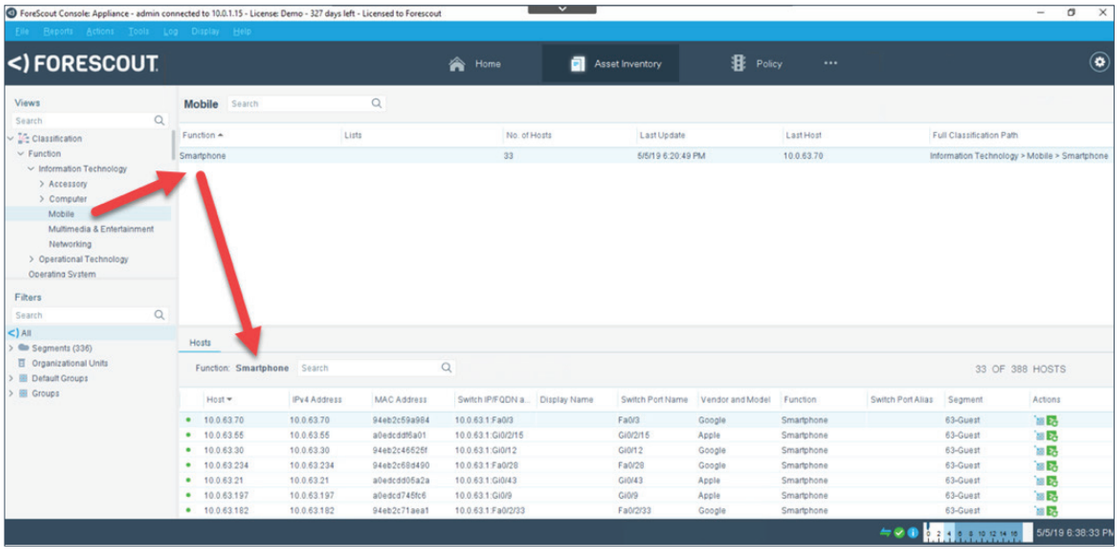
Step 6: Expand the **Function > Information Technology** tree.

You can see other categories of IT devices listed.



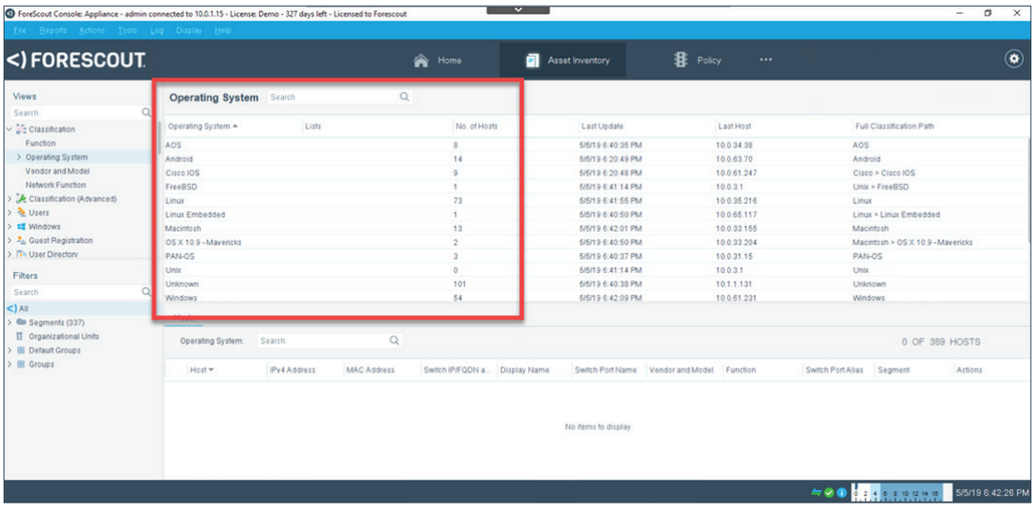
Step 7: Click **Mobile** and select **Smartphone** in the table.

The list of devices is narrowed down to display just the smartphones on your network.



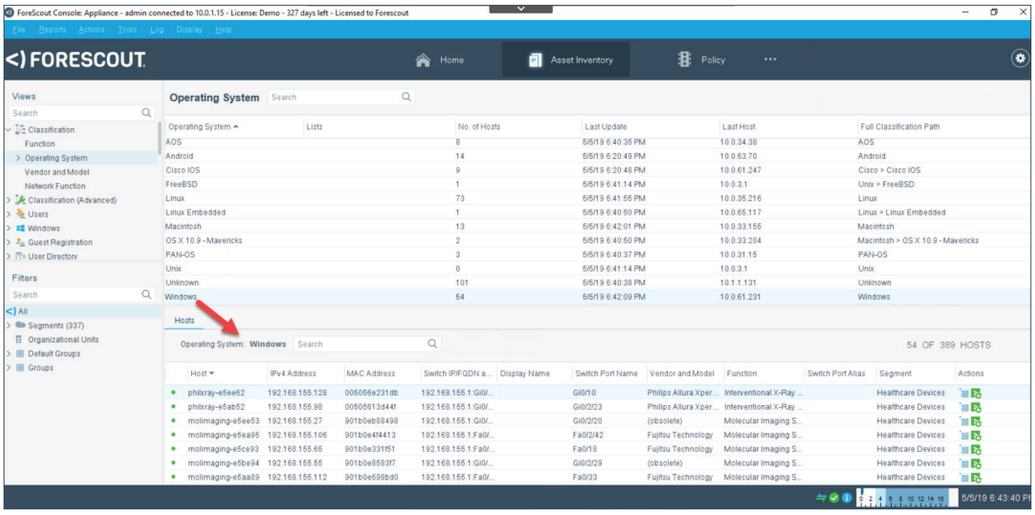
Step 8: Click **Operating System** in the Views tree.

The operating systems of the devices on your network are shown, along with the number of devices that are running those operating systems.



Step 9: In the **Operating System** table, click **Windows**.

You can see all the hosts on your network running a version of the Windows operating system. If you need to, you can even drill down to the specific versions of Windows.

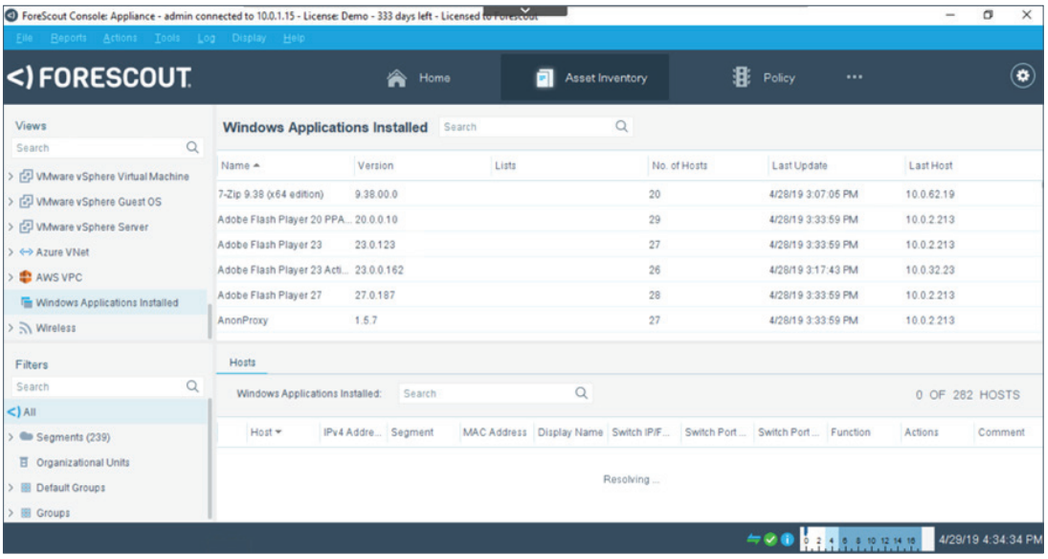


Task 2: See Microsoft Office Installations

Forescout can even tell you about software running on managed endpoints.

Step 1: Scroll down the **Views** tree and select **Windows Applications Installed**.

A list of Windows applications and versions appears in the table on the right. The number of hosts on which each application is installed is also displayed.



Step 2: In the Windows Applications Installed pane's Search field, type **Office**.

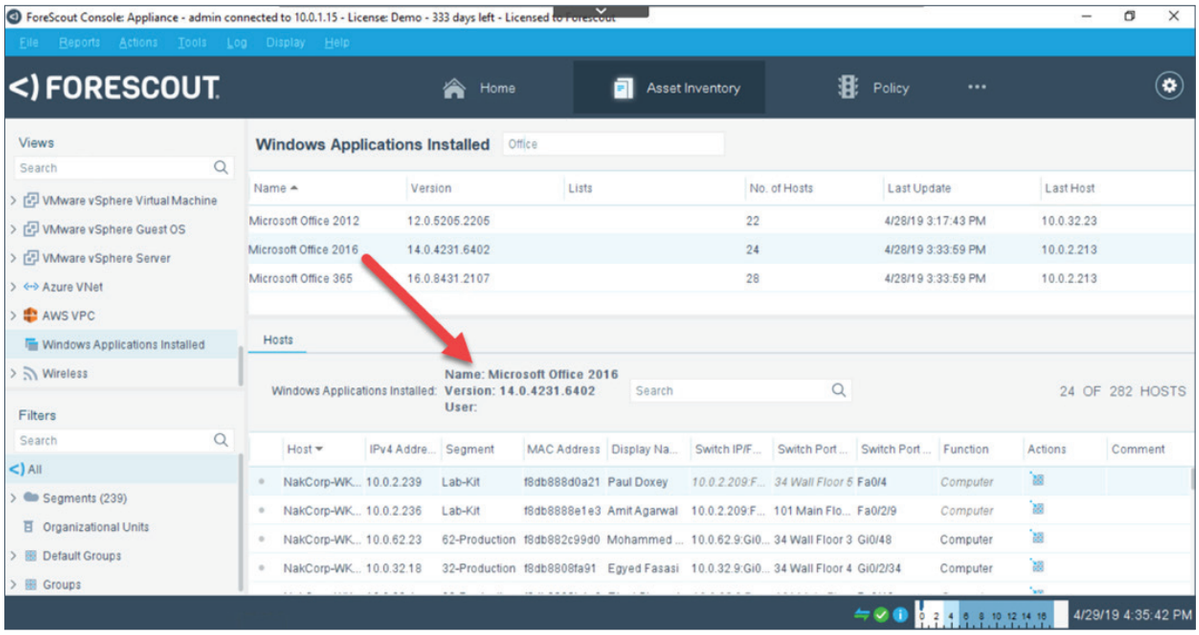
The list is narrowed down to applications with Office in the name.

Name	Version	Lists	No. of Hosts	Last Update	Last Host
Microsoft Office 2012	12.0.5205.2205		22	4/28/19 3:17:43 PM	10.0.32.23
Microsoft Office 2016	14.0.4231.6402		24	4/28/19 3:33:59 PM	10.0.2.213
Microsoft Office 365	16.0.8431.2107		28	4/28/19 3:33:59 PM	10.0.2.213

How many versions of Microsoft Office do you see? Does your company have a standard, licensed version?

Step 3: Click one of the versions of Microsoft Office.

A list of devices running that version of Office and their locations appear in the table below.

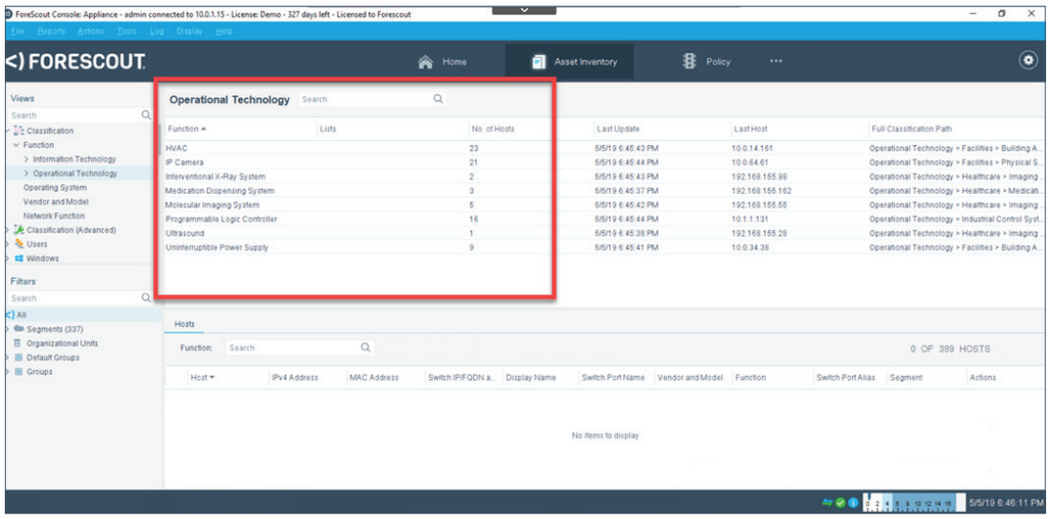


You can create policies for endpoints running specific versions of Microsoft Office. For example, you could notify users of an older version that they need to upgrade to the official, licensed version and where to obtain that version.

Task 3: See Your OT Devices

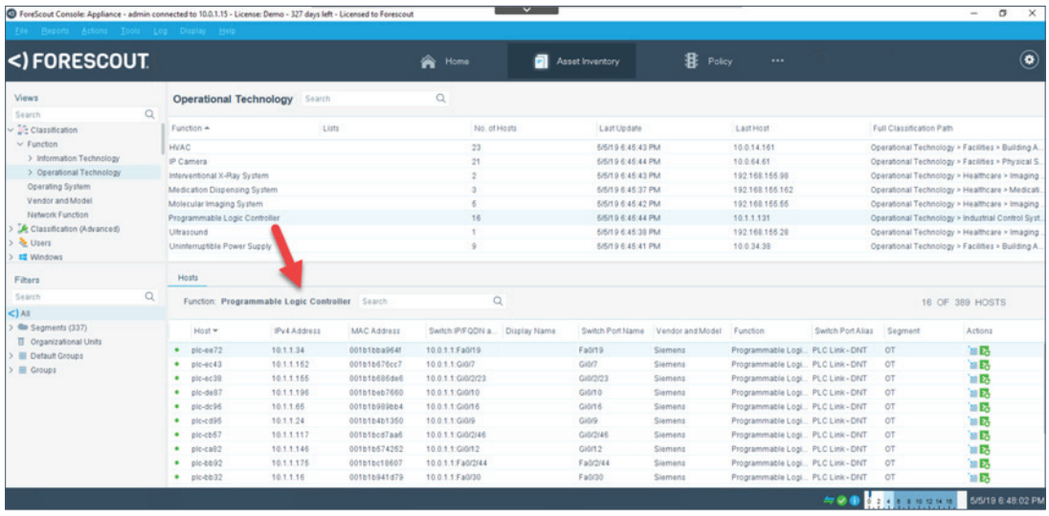
Step 1: In the Views tree, click **Classification > Function > Operational Technology**.

A list of the categories of OT devices appears in Operational Technology table on the right.



Step 2: Click **Programmable Logic Controller** in the Operational Technology table.

A list of the PLCs in your distribution center appears in the Hosts table.

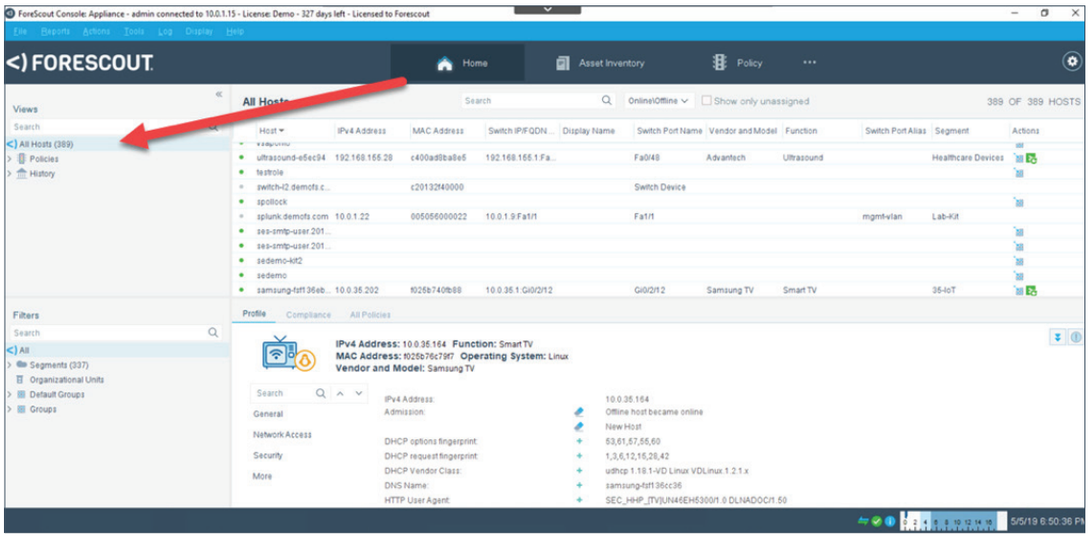


Although this Hosts table shows specific types of OT devices, it does not show every device in your distribution center; it shows only the OT devices. The next task will show you how to see all the devices on your OT network segment.

Task 4: Monitor Your Distribution Center

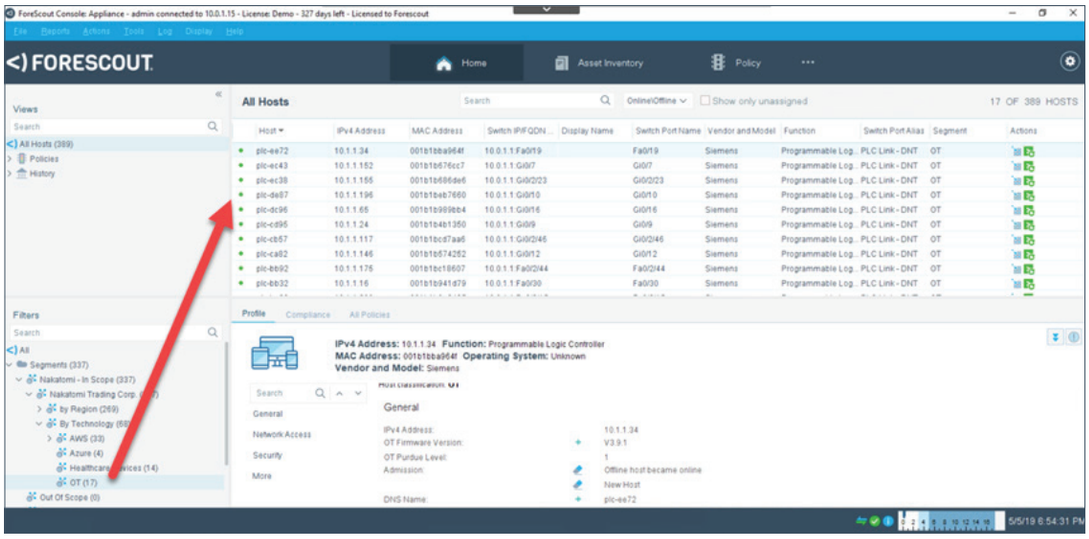
Use the Home tab and segment filter to see the devices attached to your distribution center network. While the Inventory tab can help you see what devices you have on your network by type, the Home tab can help you see all the devices on specific parts of your network. This can help you track down unapproved devices on that network.

Step 1: Click the **Home** tab. If not already selected, click **All Hosts** in the Views tree.



Step 2: In the Filters tree, expand the **Segments > Nakatomi – In Scope > Nakatomi Trading Corp. > By Technology** tree, and then click **OT**.

In the All Hosts table, you will see a list of devices in your Distribution Center's OT network. You will be able to quickly identify devices that do not belong on this network.



Step 3: Scroll through the device list. Are there any devices that you can immediately see that do not belong?

Hint: Look at the function column as you scroll through. Looks like someone is doing some after-hours gaming.

Step 4: Click the **Asset Inventory** tab to return to the Inventory view.

Task 5: Can You Find the…?

Use the **Asset Inventory** tab and the **View** tree to find the following information:

- How many HVAC systems are running a Windows-based OS? Where are they located? What are they connected to?

  Hint: You can right-click the header row of the Function table to select which device properties are shown in the table—including the operating system.

- How many IP cameras are using Telnet?

  Hint: Telnet uses TCP port 23 – you want to locate devices with an Open Port of TCP23.

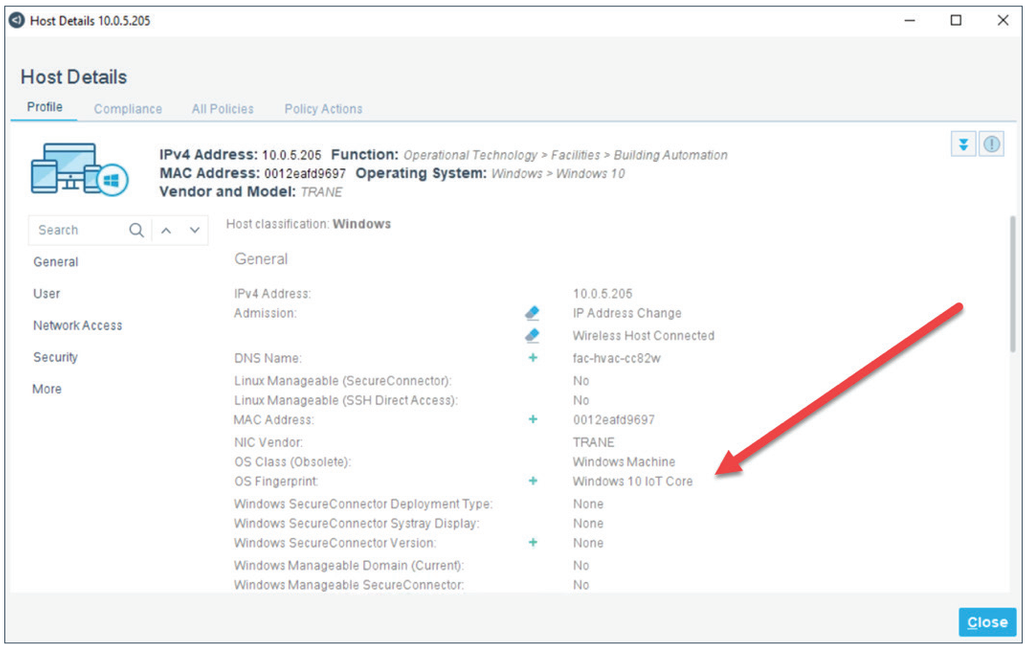
Stuck? See the next page for the solution on where to find the answers.

Solutions for Can You Find the…?

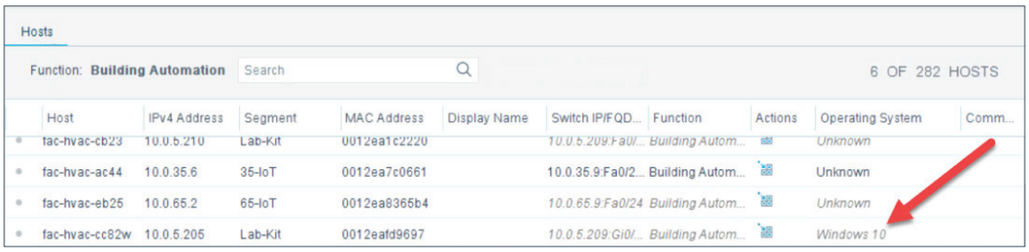
HVAC

You already saw the HVAC entry under **Classification > Function > Operational Technology** in an earlier task. Selecting this entry shows you the HVAC systems. However, it does not show you the operating systems. There are two ways you can find this information.

The first way is to double-click each device to see the OS listed in **Host Details**.



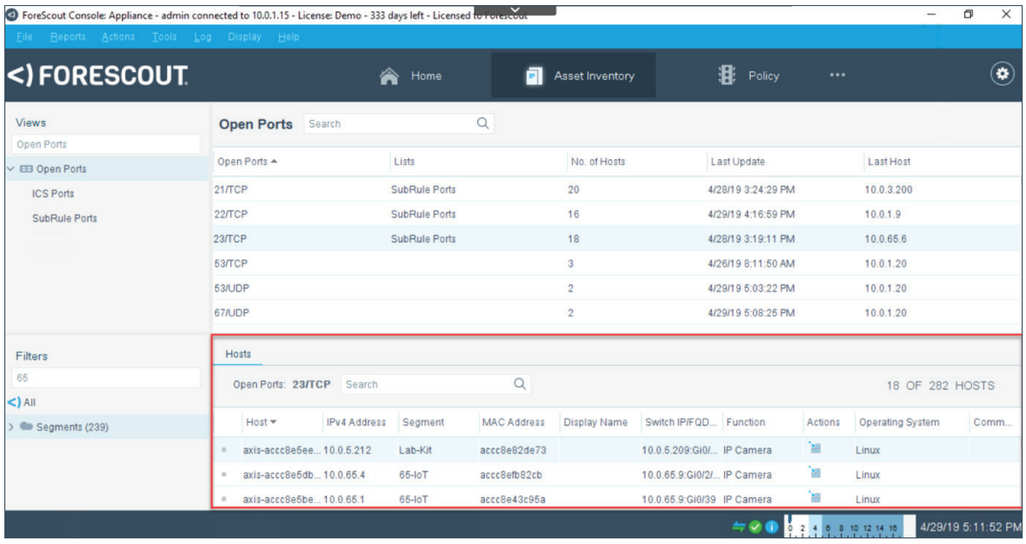
A second way is to right-click the table header in the list of **Hosts** and add **Operating System** as a column. From there, you can quickly sort the table and find the HVAC systems running Windows. Feel free to remove a couple of columns in the same way to make room for your Operating System column.



IP Cameras using Telnet

This one is a little trickier. In the **Views** tree, there is an entry called **Open Ports**. Clicking on that shows you all the open ports on the devices on your network. Click the **23/TCP** entry and you will see all the devices that have an open Telnet port.

From there, you can click the **Function** column head in the **Hosts** table to sort by function and find all your IP cameras with open Telnet ports.



Follow Up

Explore the items in the Inventory tab some more.

- What other types of information did Forescout discover about the devices?
- How could seeing all instances of a specific device type on your network, such as IT, OT, and IoT devices, benefit your business? Open ports?
- What problems does your organization currently face that this type of endpoint visibility could help solve? How much effort and expense currently goes into solving these problems?
- How can Forescout help you keep your asset inventory current?

LAP 3: DEVICE COMPLIANCE – PART 1

Scenario

The software and hardware audit of your network was successful. Now that you have visibility into the devices on your network and the software that those devices are running, you need to see if they comply with your company policies.

You are going to start with antivirus. Your company policy states that each Windows PC attached to the network must be running an up-to-date (updated within the last two weeks) antivirus application.

You are going to use the Forescout platform to check each of the Windows endpoints and verify that they are compliant with this policy.

Compliance with corporate standards can be difficult to manage in large environments. Forescout can help you keep your endpoints in line with corporate policy by continuously evaluating them against those policies.

Before you begin

- How do you currently track your endpoint compliance with corporate policy? Is it automated? What does "noncompliant" mean in your organization? Is it consistent? Based on location? Device type? User? What are some examples in your environment?
- When are your compliance checks currently performed? When systems attach to the network? Weekly or monthly polling intervals? Annually? How automated are these checks?
- How are you notified when an endpoint is no longer compliant? How are end-users notified? What is the impact of noncompliant endpoints on your network?

In this lap, you will:

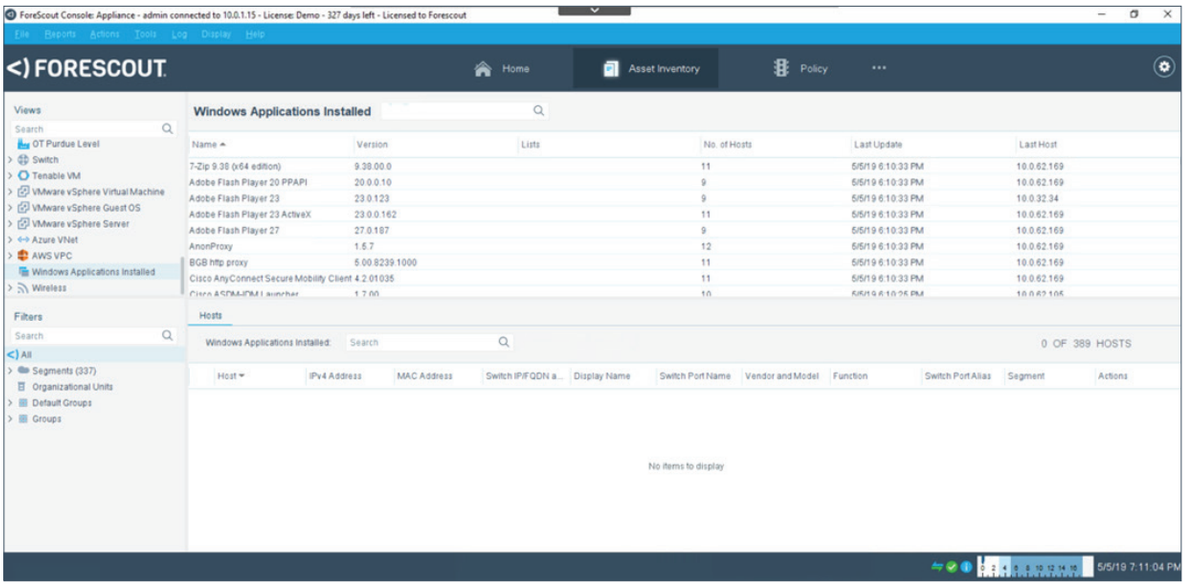
1. Use the Inventory tab to see software programs that typically require some form of compliance, such as regular security updates.
2. Modify an antivirus visibility policy to assign compliance labels to the various states of antivirus software on the endpoint. Is there an antivirus application running on the endpoints? If yes, is it up to date? If not, is one installed but not running? Or is there no antivirus software at all?
3. Test the compliance policy. You will turn off the antivirus on the console device and see how it is reflected in the Forescout console.
4. Create a compliance policy that evaluates the use of default passwords on your IoT devices.
5. View a compliance report for the devices on the network.

Task 1: Survey Endpoint Software for Corporate Compliance Issues

Many software packages have regular updates to address security issues. Java, Adobe Flash and antivirus software are among them. Other software, such as network scanners like NMAP, you want to keep off most endpoints. You can write policies to address both situations: to ensure that required applications are up to date and disallowed applications are not installed on your endpoints.

Step 1: If not still on the Asset Inventory tab, click **Asset Inventory**.

Step 2: Scroll down the Views list and click **Windows Applications** Installed. Delete "Office" from the search field above the Windows Applications Installed table so that you can see all the applications.



One of the first pieces of software you may notice is Adobe Flash Player. There are several versions installed, including older ones that may contain vulnerabilities.

Step 3: Scroll down the list of applications. Look for **Java**, **McAfee** software, and **NMAP**.

See the different versions of Java that are running on the endpoints. How many endpoints have NMAP on them? Are they legitimate users of the software? Is the McAfee software on the endpoints up to date?

Forescout policies let you take a variety of actions on endpoints, including notifying users so they can remediate the issue themselves, quarantining devices to a remediation VLAN, or even initiating a remediation action on the endpoint, based on these properties.

You can also assign compliance categories to endpoints based on specific properties. These categories will help you to see the overall hygiene of the devices on the network. The next few tasks will show you how.

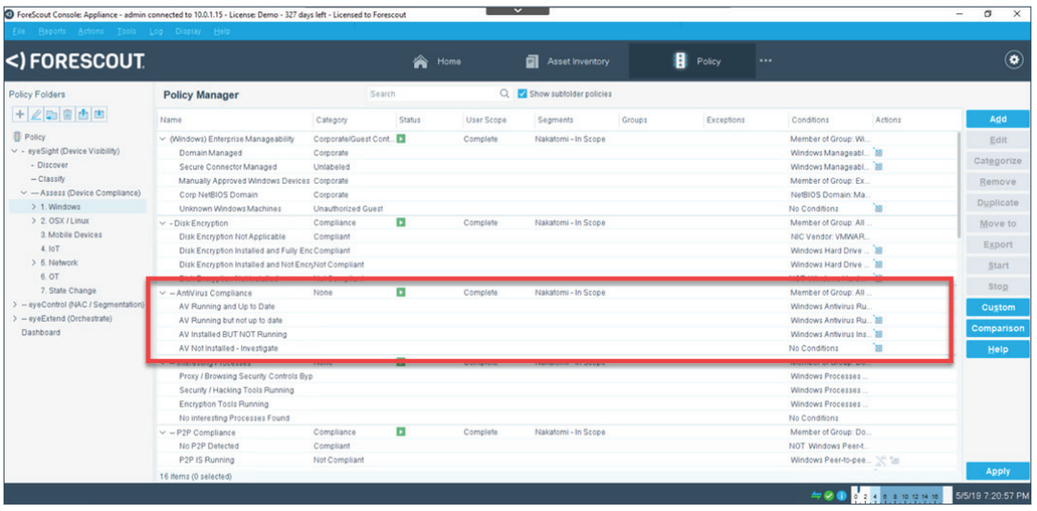
Task 2: Assign Compliance Labels to the Antivirus Policy

Because having up to date antivirus protection on endpoints is an issue that every company faces, we are going to start with that scenario. You will modify an existing policy that evaluates antivirus software status on endpoints and assign compliance labels to each state to match company policy.

Step 1: Click the **Policy** tab.

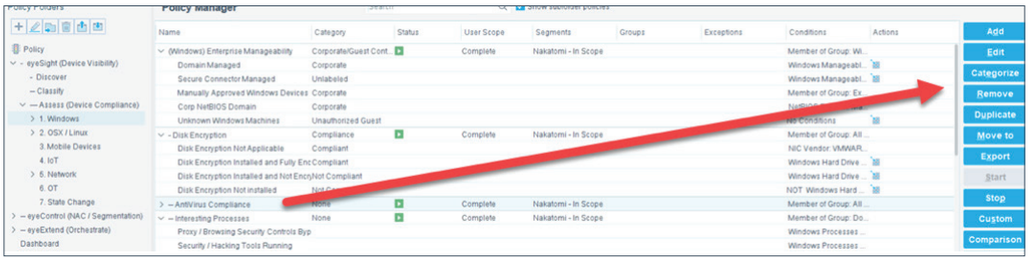
Step 2: In the **Policy Folders** tree, expand **eyeSight > Assess** and click **1. Windows**.

A list of the Windows assessment policies appears in the Policy Manager pane. The third one shown is AntiVirus Compliance. It does not yet have any compliance information assigned to it so the Category listed is None.



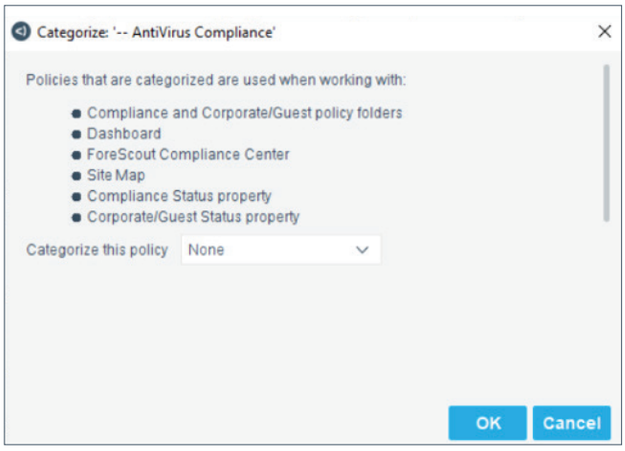
Step 3: Click the **AntiVirus Compliance** policy name to select it.

The name is highlighted and the policy action buttons to the right of the list become active.



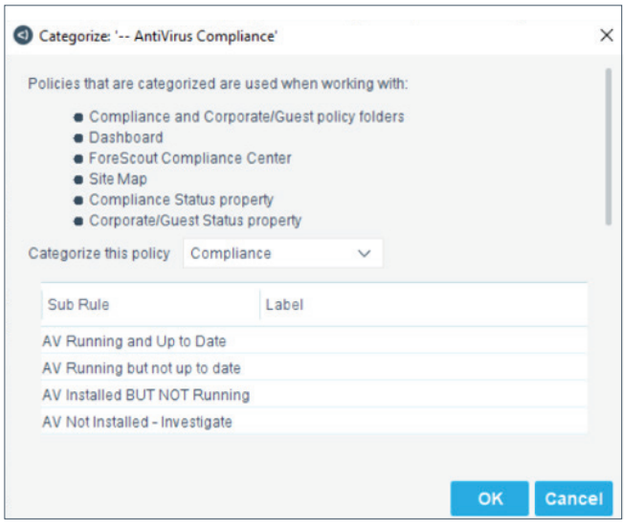
Step 4: Click the **Categorize** button.

The Categorize dialog appears.



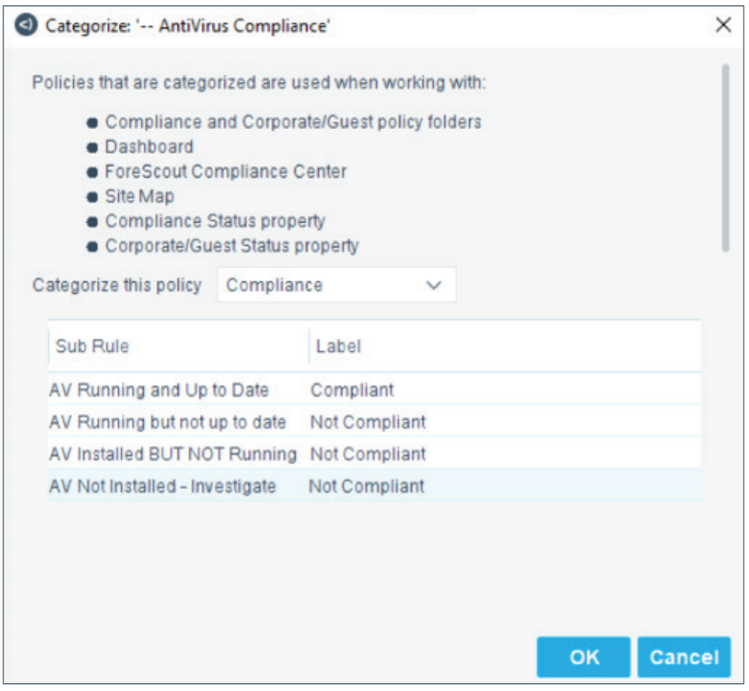
Step 5: In the **Categorize this policy** drop-down list, select **Compliance**.

A list of the policy's sub-rules appears.



Step 6: For each sub-rule, click the **Label** column next to the rule and select the following values:

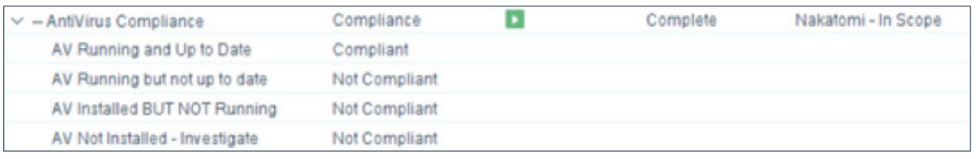
AV Running and Up to Date:	Compliant
AV Running but not up to date:	Not Compliant
AV Installed BUT NOT Running:	Not Compliant
AV Not Installed - Investigate	Not Compliant



Step 7: Click **OK** to save the compliance settings.

Step 8: Click **Apply** to save the changes and start the policy.

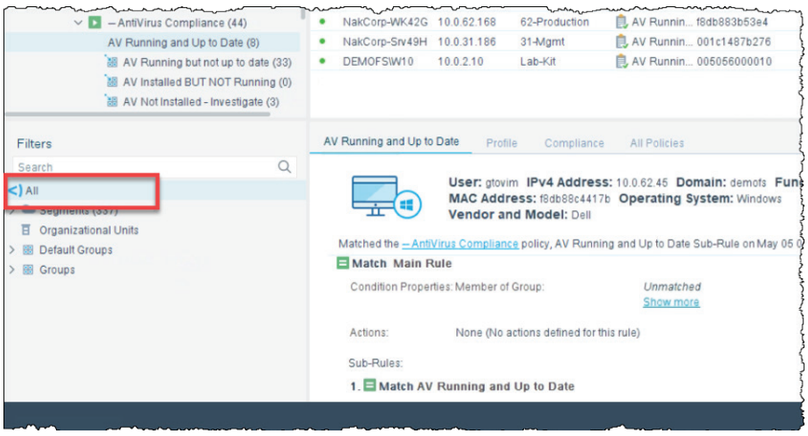
After applying your changes, your AntiVirus Compliance policy should look like the following:



Task 3: Test Your Antivirus Compliance Policy

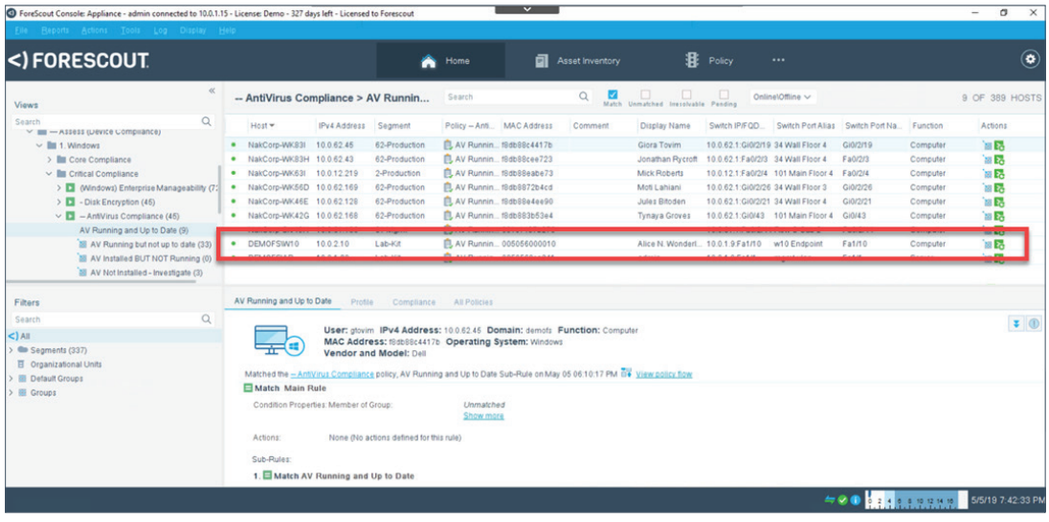
Step 1: Click the **Home** tab in the Forescout console toolbar.

Step 2: In the Filters tree, click **All**.



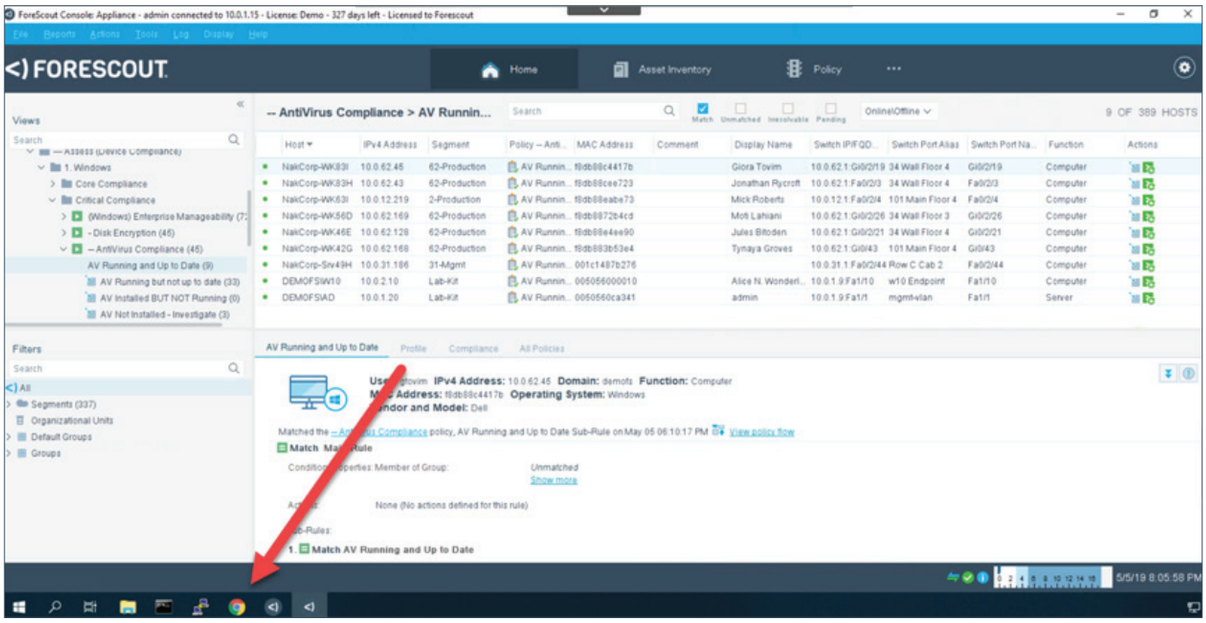
Step 3: Expand the Policies tree. Navigate to **Policies > eyeSight > Assess > Windows > Critical Compliance > AntiVirus Compliance**. Click the **AV Running and Up to Date** sub-rule.

A list of the devices matching that sub-rule displays. Note the DEMOFS\W10 device. To test the policy, we are going to access that device and turn off the antivirus software.



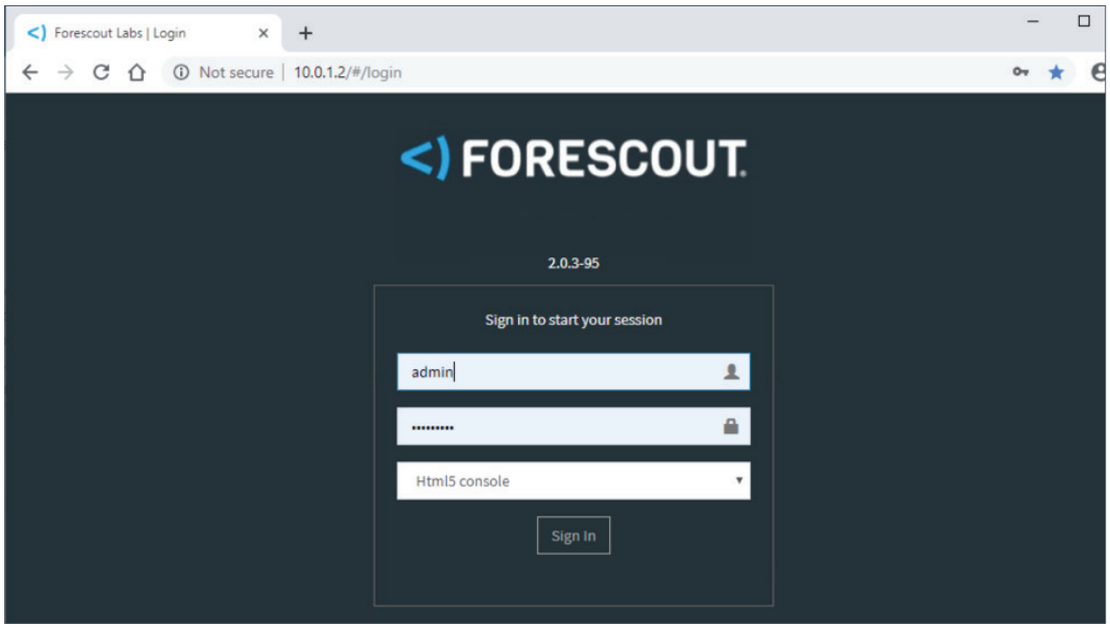
Step 4: Access the DEMOFS\W10 device:

a. Open the Chrome browser from the Windows task bar.



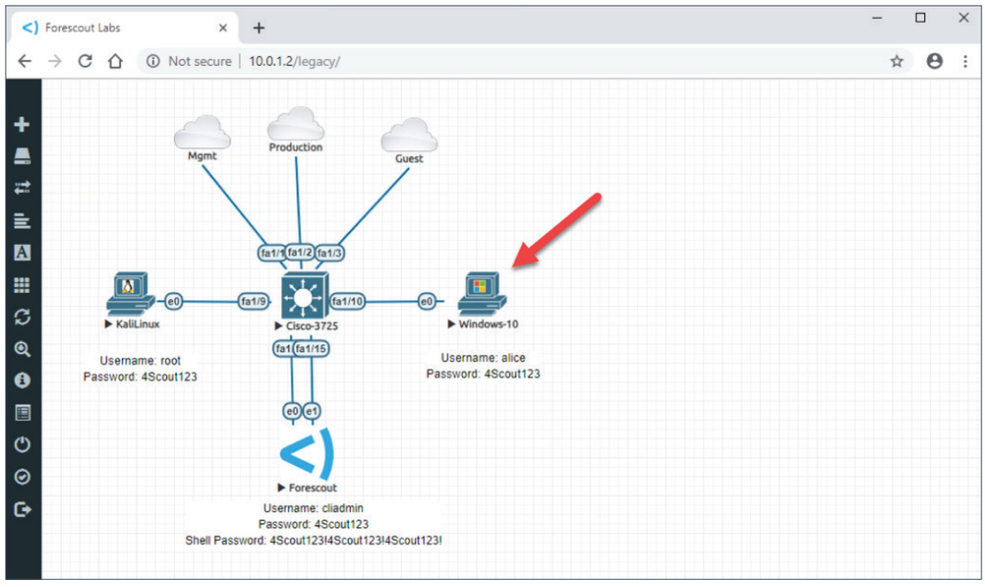
b. Click **Forescout Labs** in the bookmark bar.

The Forescout Labs login screen appears. The Username and Password are pre-populated. Do not change any of the settings.



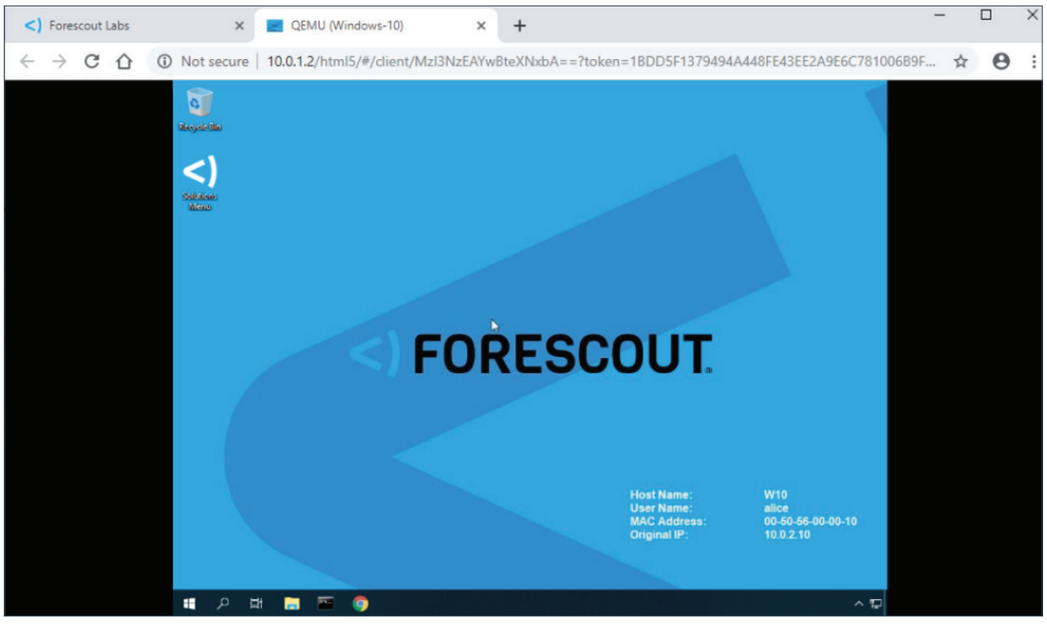
c. Click **Sign In**.

A diagram of the lab devices appears.

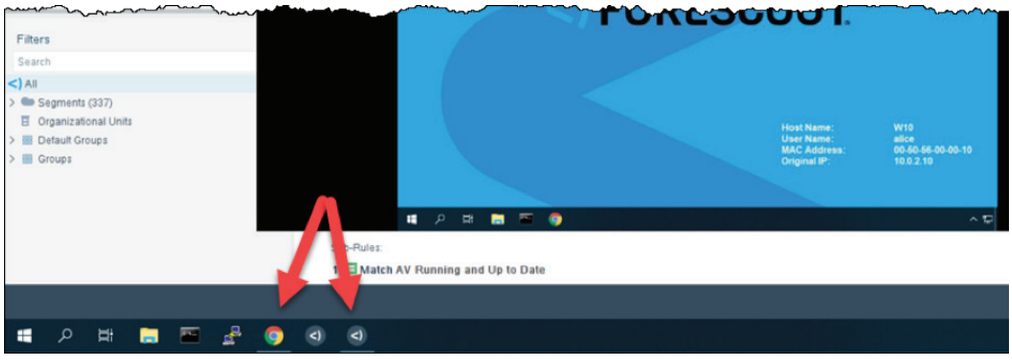


d. Click the **Windows-10** device.

The Windows desktop opens in the browser window.



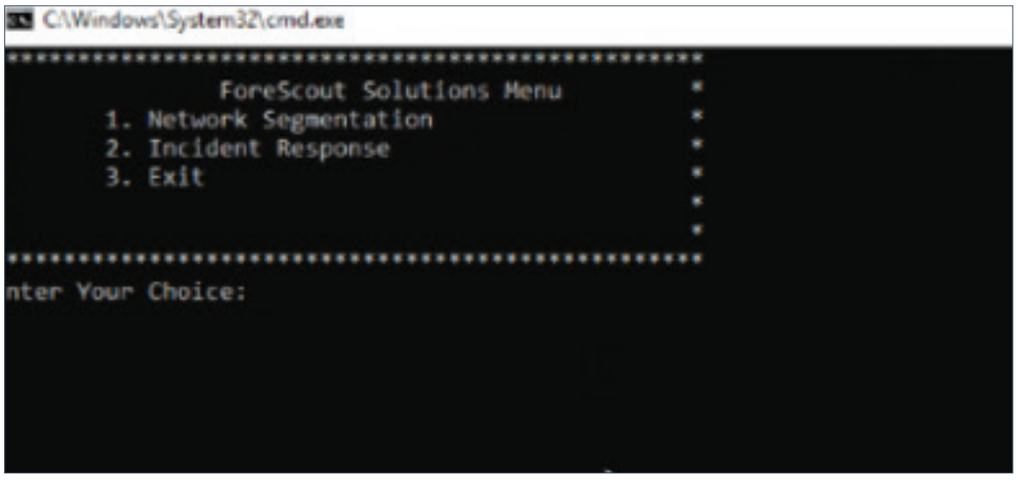
When instructed to switch between the Forescout console and the Windows 10 device, use the icons in the Windows task bar. (This is a browser window within your computer's browser window; pressing ALT-TAB will not switch between those applications.)



Step 5: Disable the antivirus software on the Windows 10 device:

a. Double-click the Solutions Menu Icon on the desktop.

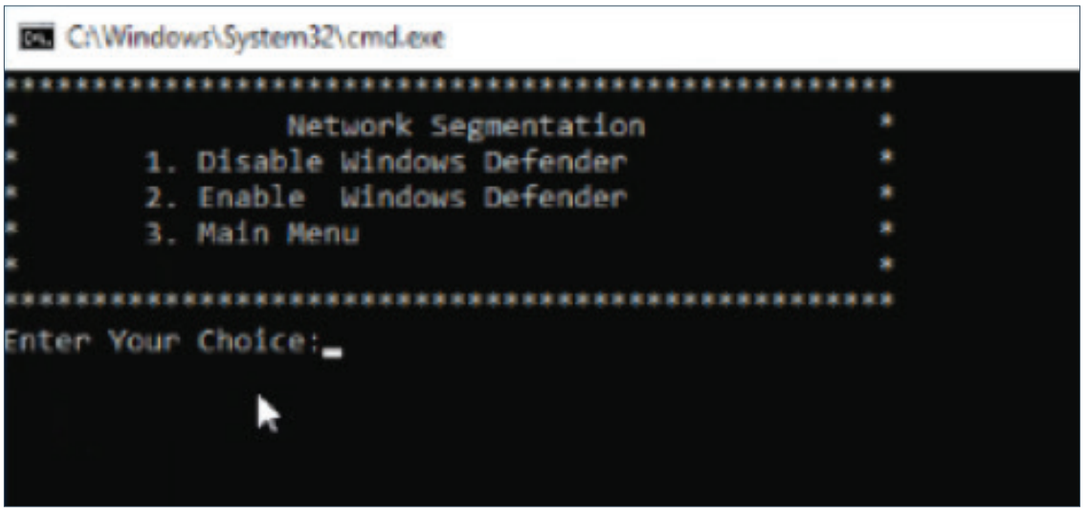
The Forescout Solutions Menu appears.



b. Press **1** and then **Enter**.

The Network Segmentation Menu appears.

c. Press **1** and then **Enter**.



A PowerShell script runs to disable the antivirus. It may take a moment to complete. You will see a pop-up notification that Windows Defender Antivirus is not running.

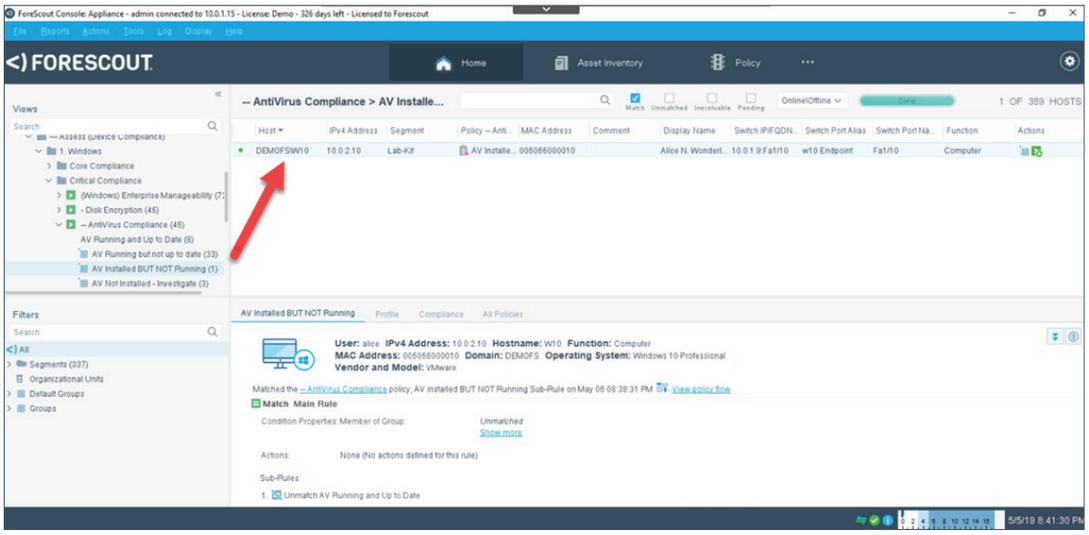
d. Press **Enter**.

Step 6: Return to the Forescout console (click the console icon in the Windows Task Bar).

Notice that the DEMOFS\W10 device is no longer in the AV Running and Up to Date list.

Step 7: Click the **AV Installed BUT NOT Running** sub-rule.

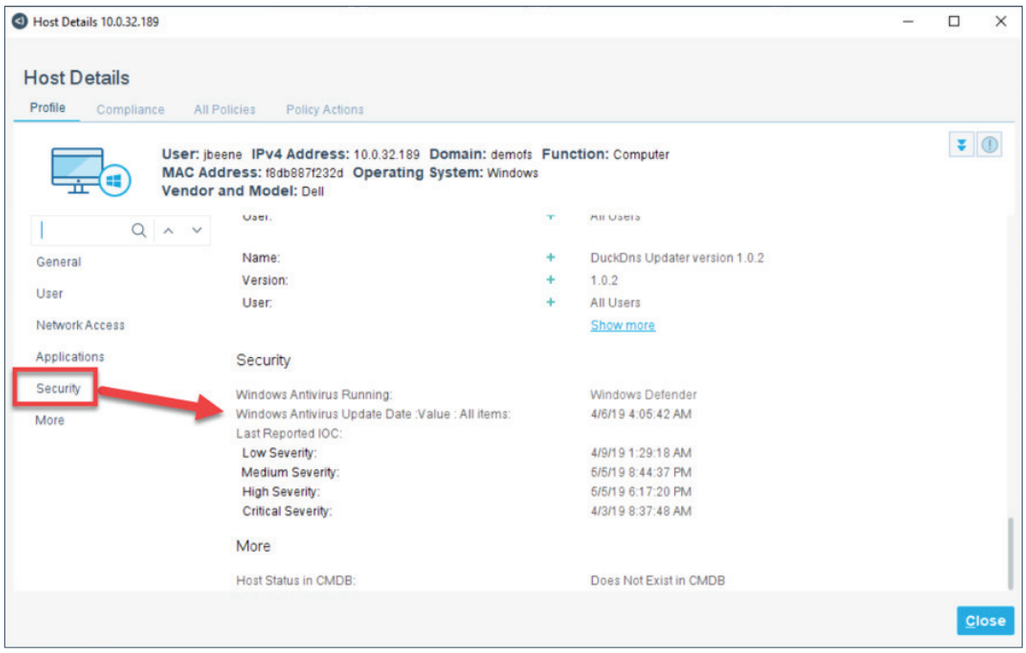
The DEMOFS\W10 device now appears in the device list for this rule.



Step 8: Click the **AV Running but not up to date** sub-rule. Double-click one of the devices to show the device properties details.

Step 9: Click **Security**.

You will see when the last time the antivirus (Windows Defender) was updated.



Step 10: Close the device properties dialog.

Step 11: Return to the DEMOFS\W10 Windows 10 device and use the menu to turn the antivirus software back on.

Step 12: Switch back to the Forescout console and click the AV Running and Up to Date policy. The DEMOFS\W10 device again appears back in this list.

Task 4: Create an IoT Posture Assessment Policy

You have read in the news about several breaches that exploited printers that still used the default administrative login credentials. Your company policy states that the credentials on devices must be changed before they can be deployed on the production network. You are going to create a policy to check the passwords on deployed IoT devices to make sure they are not using the factory defaults.

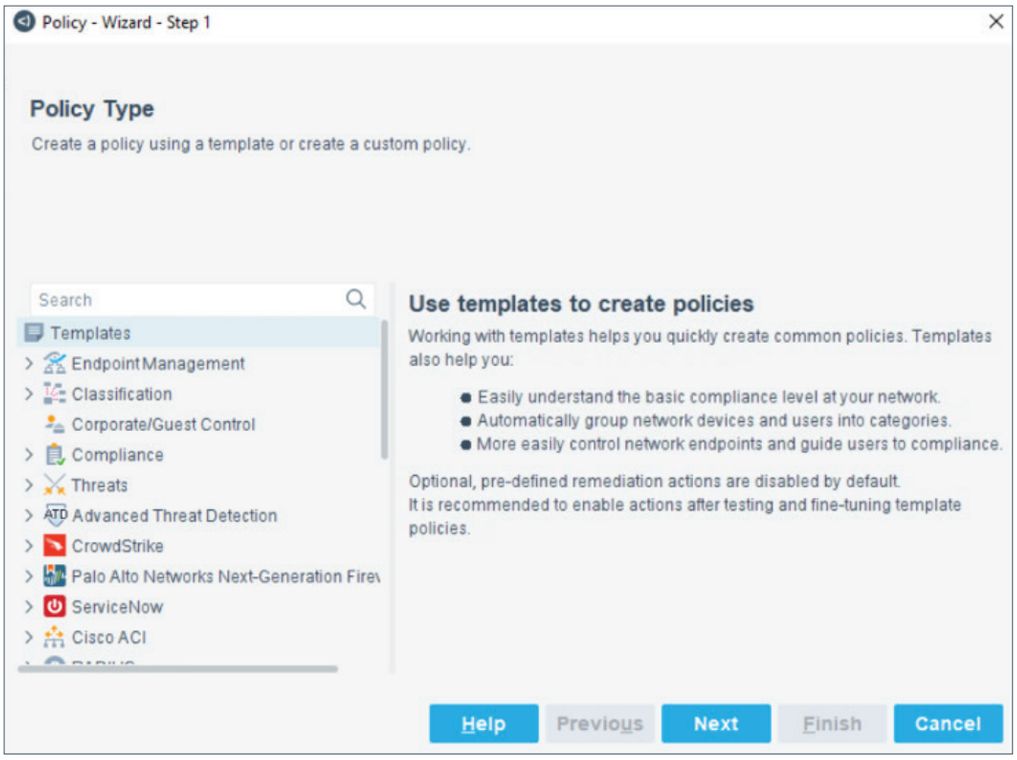
Step 1: Click the **Policy** tab in the Forescout console toolbar.

Step 2: In the Policy Folders tree, expand **eyesight > Assess >** and click the **IoT** folder.

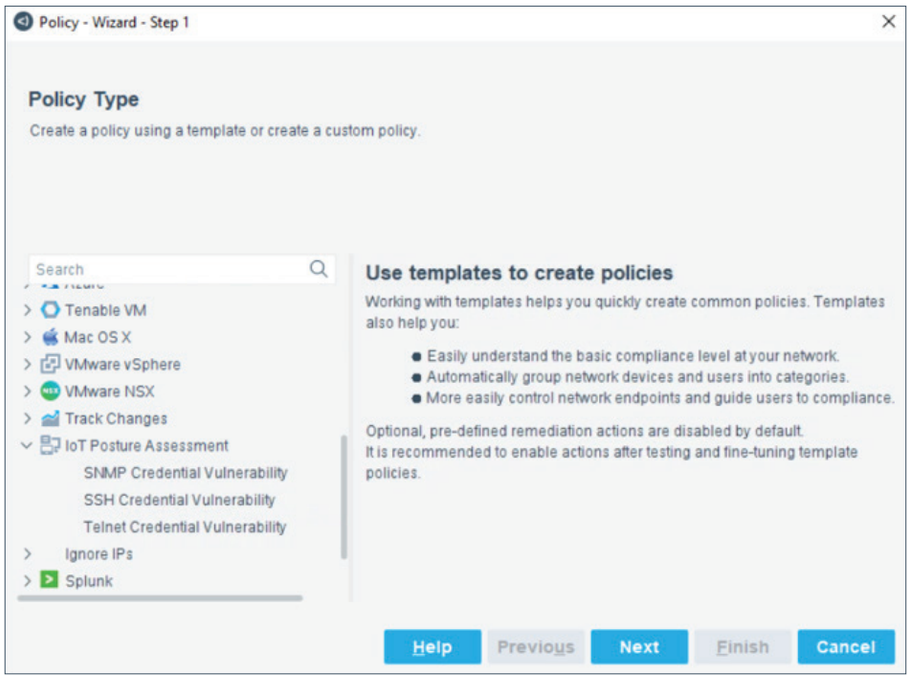
This folder is empty. We will need to put some policies in place.

Step 3: Click **Add**.

The Policy Wizard appears. The Forescout platform contains some policy templates that enable you to quickly create complex policies with just a few clicks.

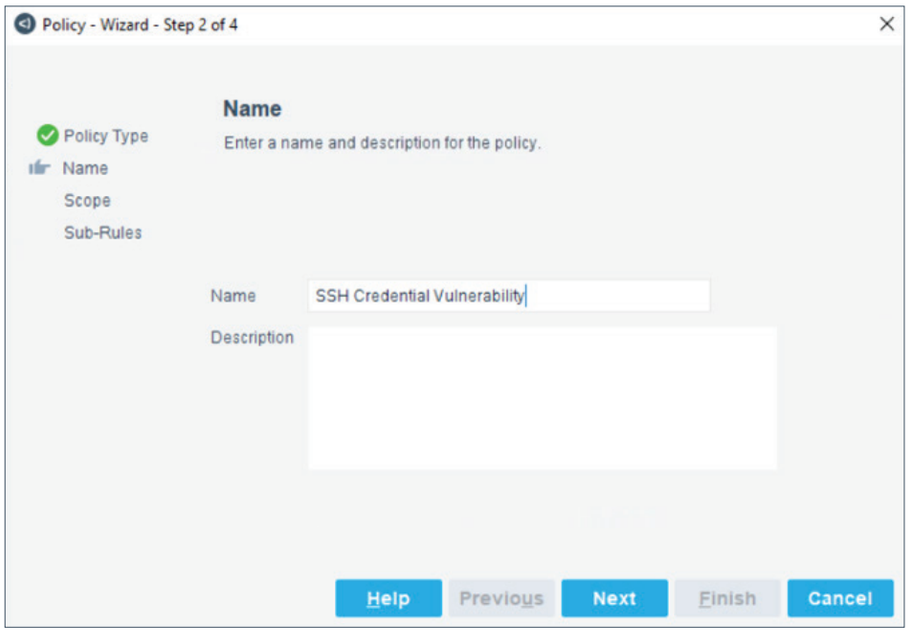


Step 4: Scroll down the list of templates and expand the **IoT Posture Assessment** folder.



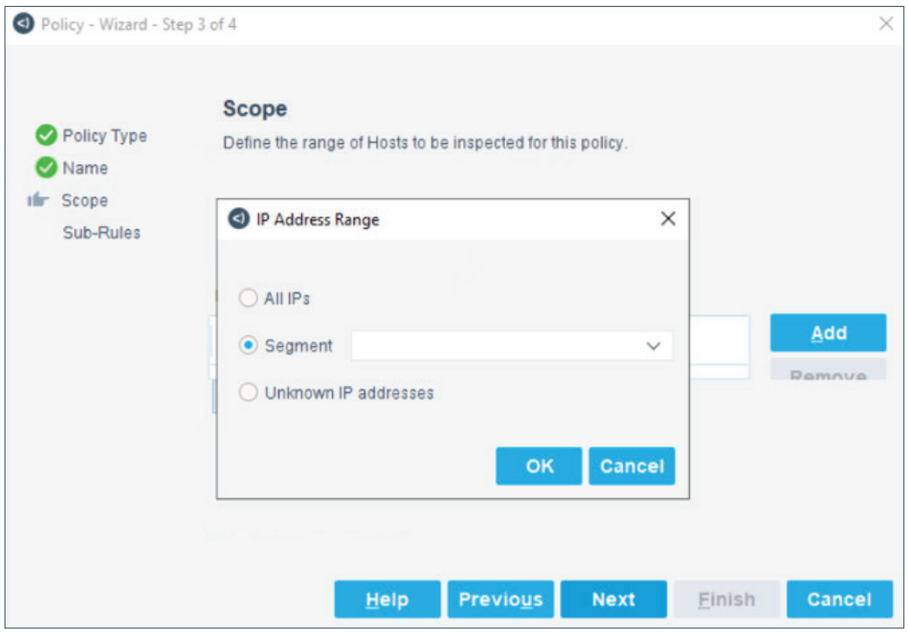
Step 5: Click **SSH Credential Vulnerability** and click **Next**.

The Name window appears.



Step 6: Click **Next** to accept the default name.

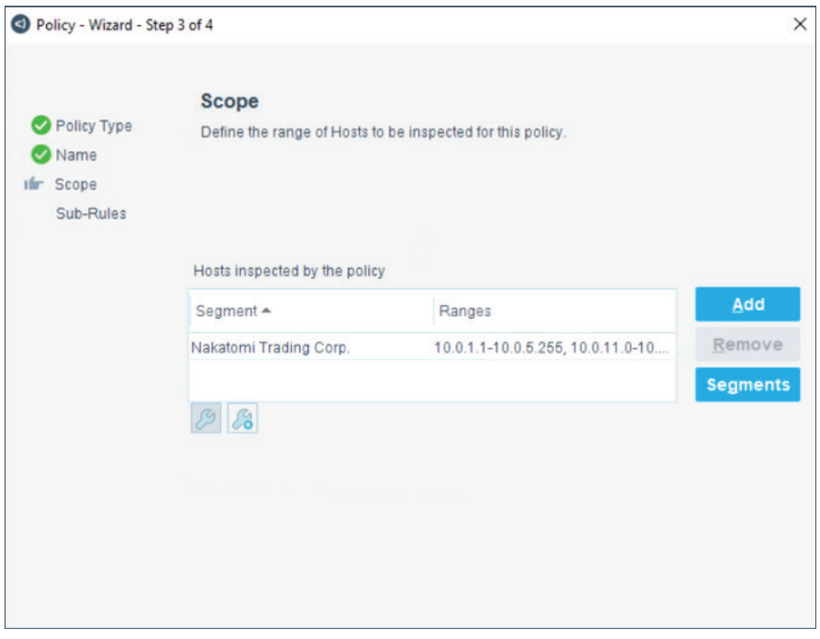
The Scope window appears.



Step 7: From the **Segment** dropdown list, select **Nakatomi Trading Corp** and click **OK**.

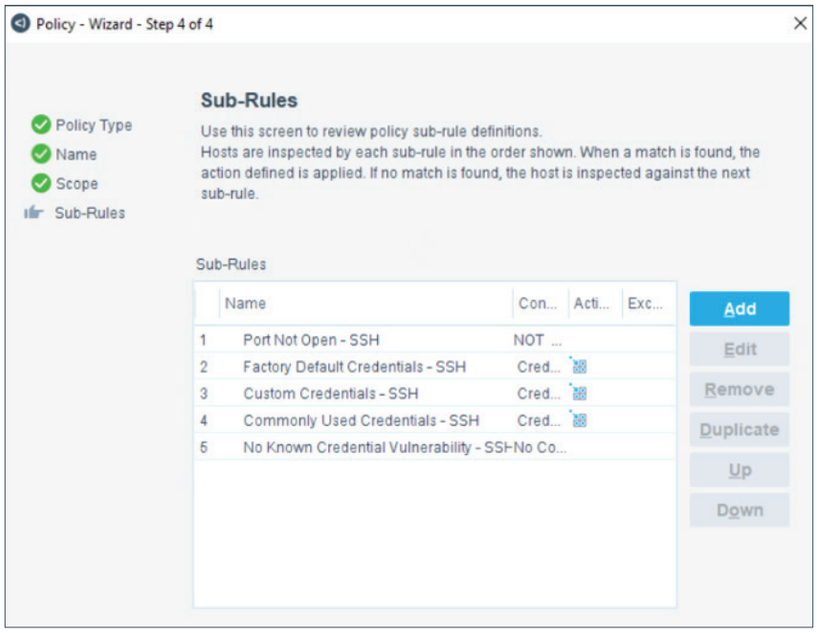
NOTE: Typically, you would narrow the scope to target specific devices and to exclude segments that may contain devices that are sensitive to this type of examination. However, for the sake of this demonstration, we will include all segments and IoT devices.

The segment, which in this environment covers all the devices Forescout has discovered, is added to the Scope table.



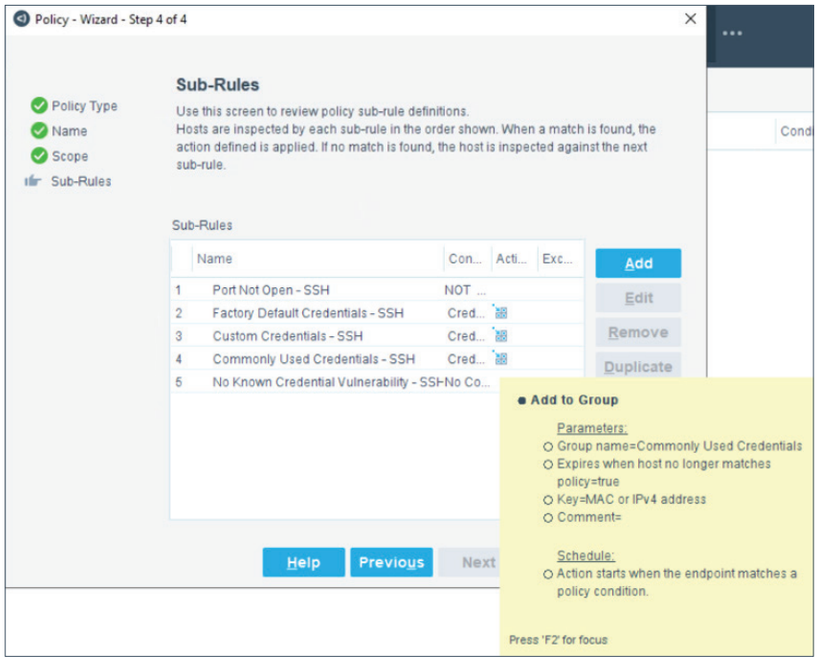
Step 8: Click **Next**.

The Sub-Rules window appears. It shows the default actions taken for each sub-rule. If the port is not open, no action is taken. If the port is open, the Forescout platform looks to see if factory default, commonly used, or specific custom credentials (that you define) are used and the host is put into an appropriate group.



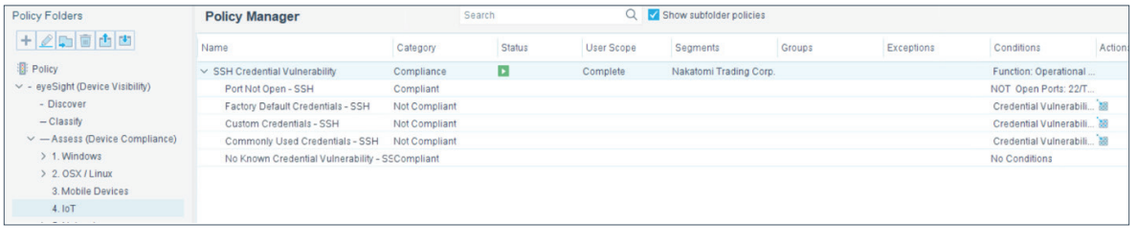
Step 9: Hover your cursor over the icon in the Actions column.

Details about the actions being taken appear in a hover window. We are not going to change any of the actions.



Step 10: Click **Finish**.

The policy is added to the IoT folder and appears in the Policy Manager pane. Note that the template already contains compliance information for each sub-rule.



Step 11: Repeat the above steps to create policies for the other two IoT Posture Assessment Templates:

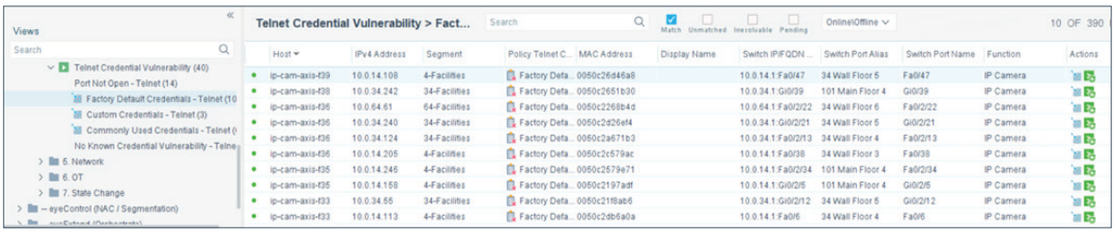
- SNMP Credential Vulnerability
- Telnet Credential Vulnerability

Step 12: Click **Apply**.

The policies are saved and run.

Step 13: Click the Home tab and navigate to **Policies > eyeSight > Assess > 4. IoT > Telnet Credential Vulnerability**. Expand the policy to see the sub-rules.

You will see some devices that match the Factory Default Credentials – Telnet sub-rule. Now that you know which devices on your network still have the default password, you can now take action to remediate the situation by changing the password to one that meets your company policy.



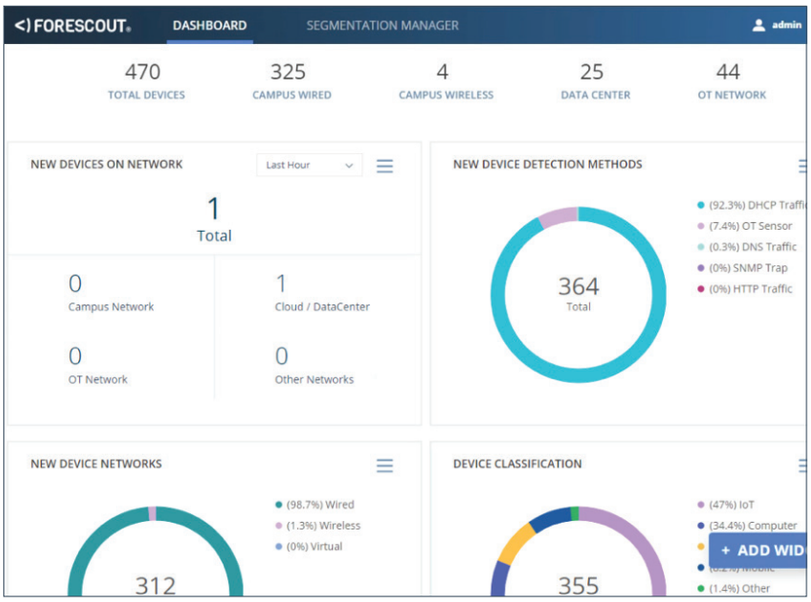
The Forescout platform also looks for devices that use some commonly used credentials, such as admin/admin, and can even look for custom credentials that you define. For instance, if your company uses a common password in labs, such as Nakatomi123, you could enter that password in the IoT Posture Assessment settings to make sure that password is not used on your production network.

Task 5: View Your Compliance Status in the Dashboard

Use the dashboard to monitor the overall status of the Windows devices on your network.

Step 1: Click the **More** icon (…) on the Forescout toolbar and then click **Dashboard**.

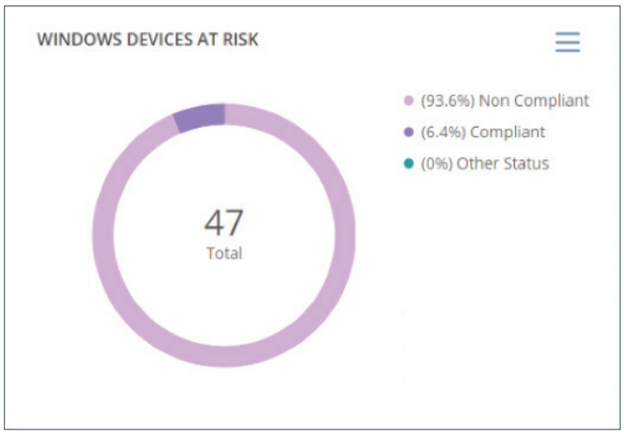
The device dashboard appears. Your dashboard has been populated with various widgets to provide you with useful information about the state of the devices on your network.



Step 2: Scroll down to the Windows Devices At Risk widget.

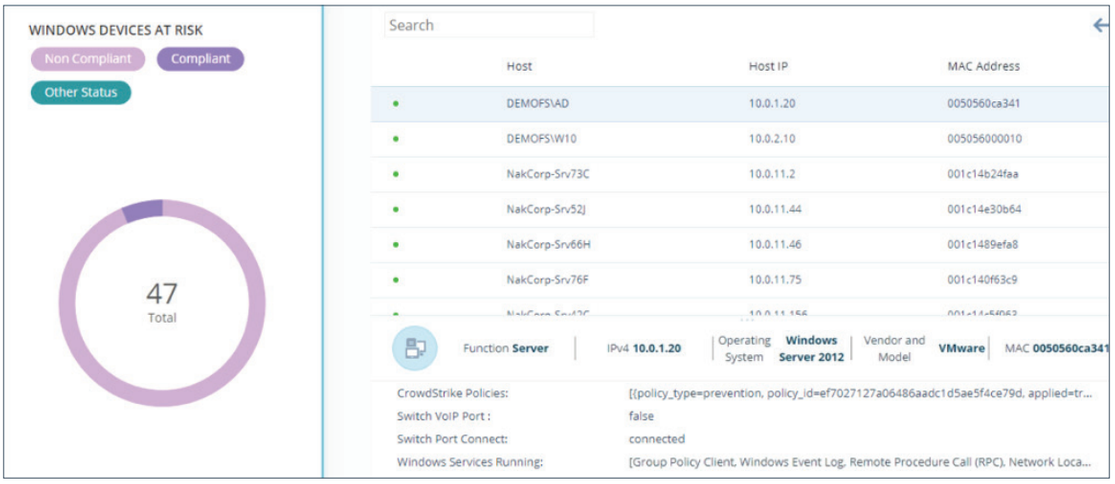
This widget shows the overall compliance status of the Windows devices on your network. There are many different compliance checks in the policy tree. An endpoint just needs to be noncompliant on one of those policies to be noncompliant overall.

Hover your mouse over the colored rings to see the actual number of compliant and non-compliant devices.



Step 3: To see more detailed information about the devices reported, click on the widget.

The widget expands to list details for each of the devices captured by the graphic. This granular detail enables you to drill down and see what is happening on your network.



Step 4: Click the arrow icon in the upper right to close the widget. Take a moment to explore some of the other information presented in the Dashboard.

Step 5: Close the Dashboard browser tab.

Follow Up

Antivirus is just one of many applications you can inspect on your endpoints. Forescout can monitor properties and applications across most endpoint operating systems.

- What other endpoint applications do you have compliance policies for? Drive encryption? Peer-to-peer networking? Removable drives? Cloud storage? Network-scanning utilities?
- How can the Forescout platform help you maintain compliance on your network?

LAP 3: DEVICE COMPLIANCE – PART 2

Scenario

Other products may only check devices for compliance on startup. However, human intervention or malicious software may bring them out of compliance after startup.

You saw in the previous use case that the Forescout platform can continuously monitor endpoints to detect when an endpoint falls out of compliance with policy. However, you do not want to have to manually contact people every time that happens.

So, you are going to create a policy that notifies end users when their device is no longer compliant with company policy and gives them a chance to remedy it.

It is not enough to just know when an endpoint is out of compliance; you need to be able to remediate it. The Forescout platform can do that with Control policies.

Control policies can range from simple notification to redirecting the endpoint to a remediation portal to completely blocking the endpoint from accessing the network.

Before You Begin

- How do your end users find out when their endpoints are no longer compliant with corporate policy?
- How do they know what to do when their device is no longer compliant with corporate policy?
- When previously compliant endpoints fall out of compliance after the initial check, how does this impact your organization? What are some real-life scenarios you face where this is a concern?

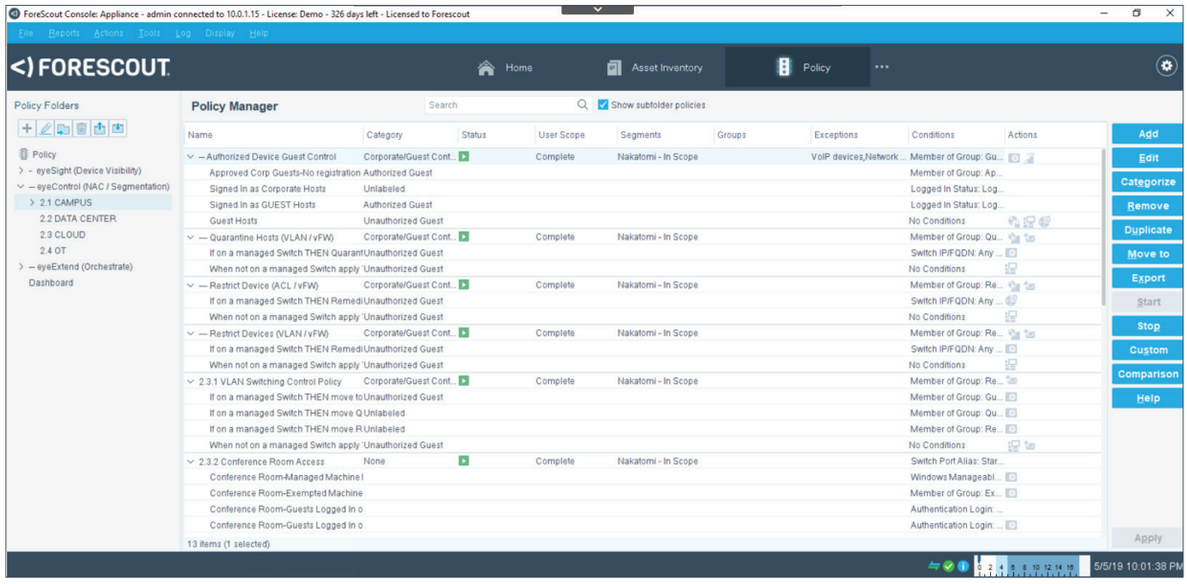
In this lap you will:

1. Create a notification policy to alert end users of Windows endpoints that aren't running antivirus software.
2. Test the notification policy.

Task 1: Create the Notification Policy

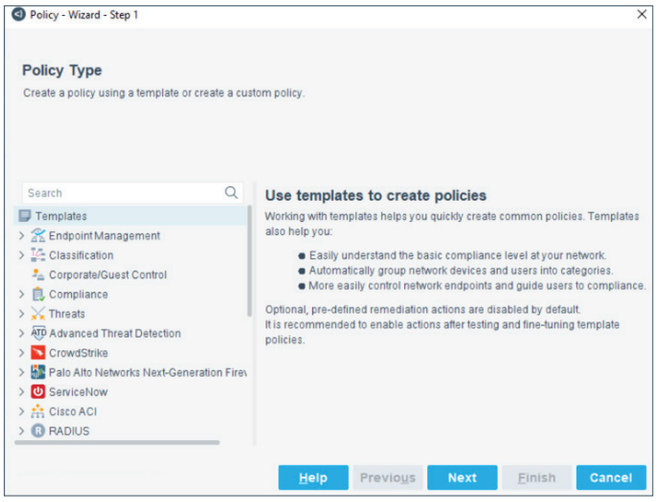
Step 1: Return to the Forescout console and click the **Policy** tab.

Step 2: In the **Policy Folders** tree, expand the eyeControl folder and then click **2.1 CAMPUS** to display the control policies that apply to your office networks.



Step 3: To create a new policy, click **Add** to the right of the policy list.

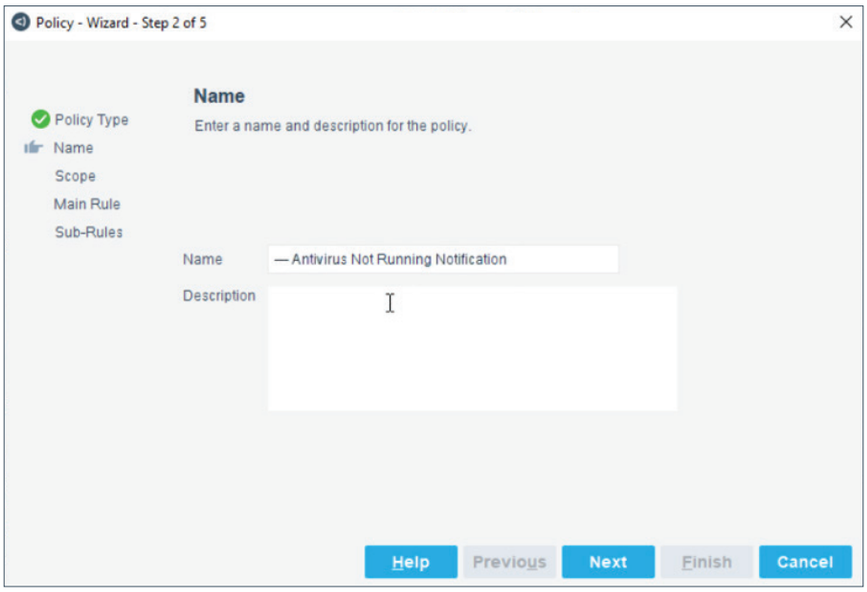
The Policy Wizard appears.



We could use one of the pre-built templates for this task; however, to show how easy it is to create a custom policy, we are going to create our policy from scratch.

Step 4: Scroll to the bottom of the templates list, click **Custom**. Click **Next**.

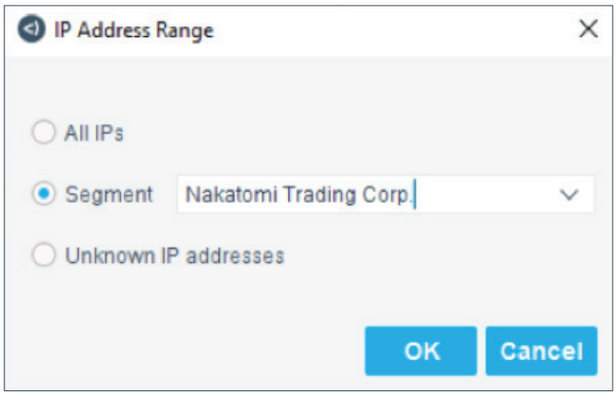
The Policy Wizard Name screen appears.



Step 5: In the **Name** field, type **--- Antivirus Not Running Notification**. Those are three dashes at the beginning of the name to ensure your policy appears at the top of the list.

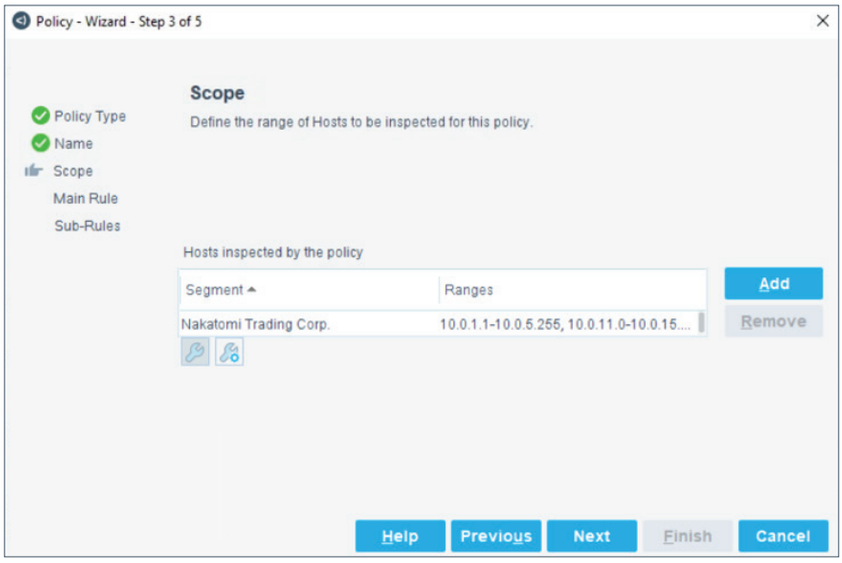
You can leave the **Description** field blank. Click **Next**.

The IP Address Range dialog box appears.



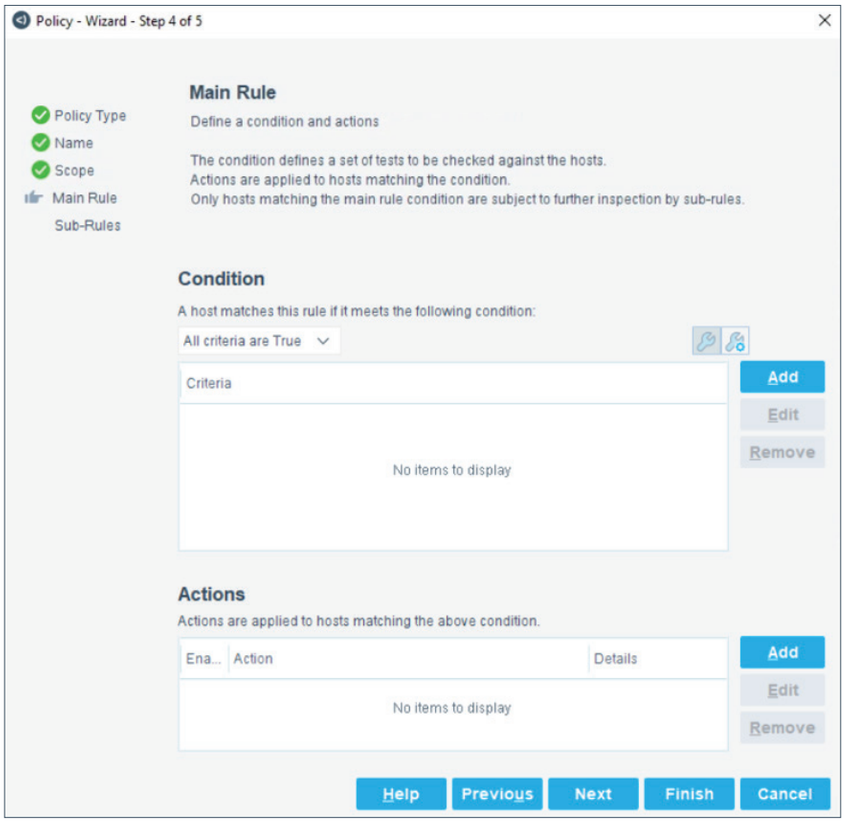
Step 6: Select **Segment** and then select **Nakatomi Trading Corp** from the drop-down list. Click **OK**.

The Nakatomi Trading Corp segment, which contains all the hosts in the lab, is added to the scope of this policy.



Step 7: Click **Next**.

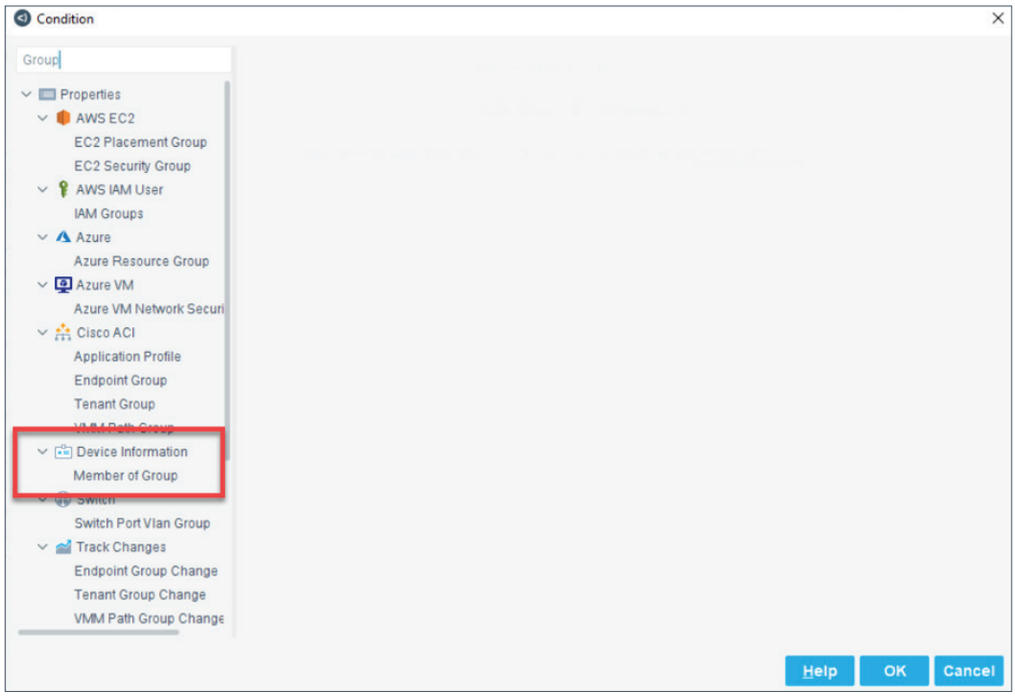
The Main Rule page appears.



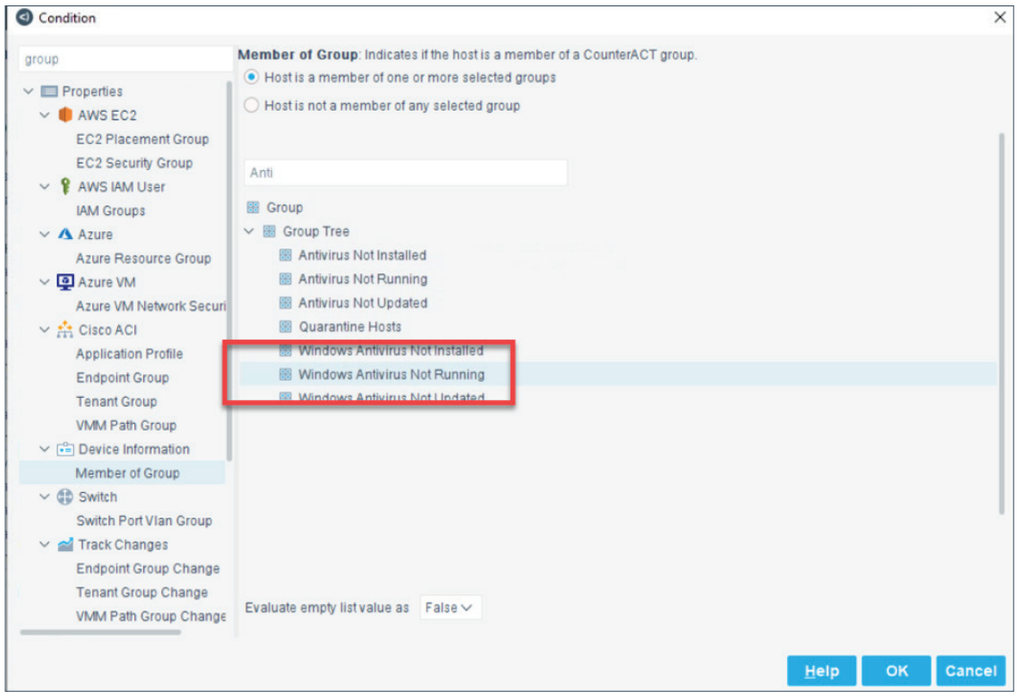
Step 8: In the Condition area, click **Add** next to the right of the **Criteria** table.

The Condition dialog appears.

Step 9: Type **Group** in the **Searc**h field and click **Device Information > Member of Group** in the results.

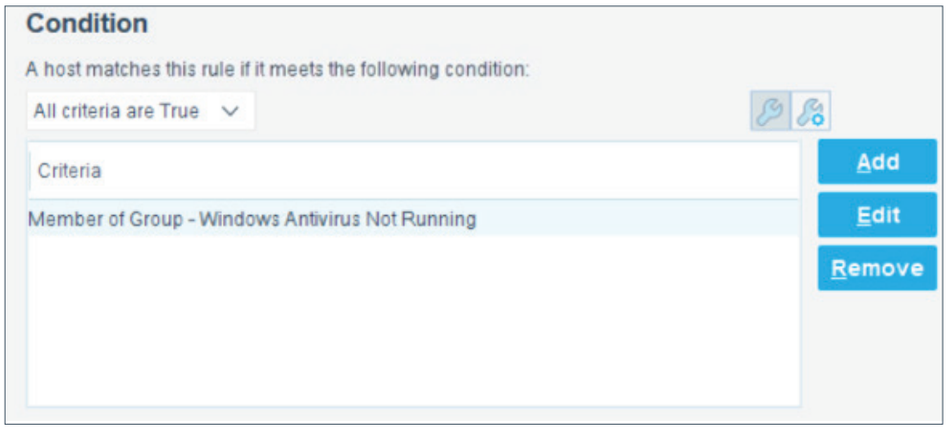


Step 10: Type **Anti** in the Member of Group search box, and click **Windows Antivirus Not Running**.



Step 11: Click **OK**.

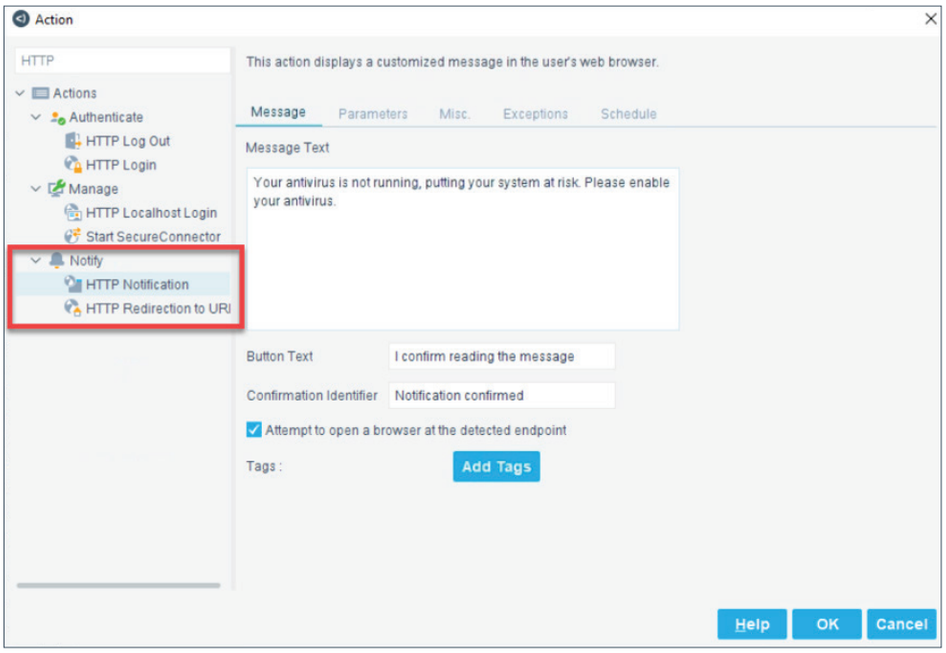
The condition is added to the Criteria table.



Step 12: Click **Add** to the right of the **Actions** table.

The Action dialog appears.

Step 13: Type **HTTP** in the search field and click **HTTP Notification** under the **Notify** heading.

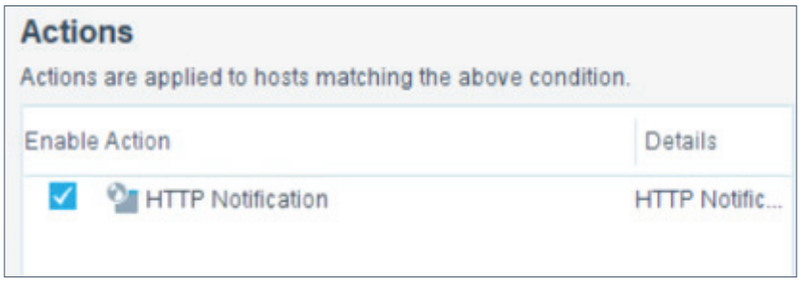


Step 14: In the Message Text field, type:

Your antivirus is not running, putting your system at risk. Please enable your antivirus.

Step 15: Click **OK**.

The action is saved to the policy.



Step 16: Click **Finish** to save the policy.

You do not need to add any sub-rules to this policy.

Step 17: Click **Apply** to save and activate the changes to the policy tree.

Task 2: Test the Control Policy

Step 1: Click the **Home** tab.

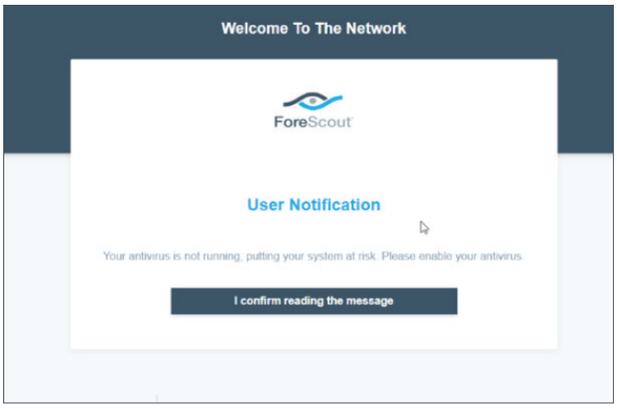
Step 2: Expand the policy tree. Navigate to **Policies > eyeControl > 2.1 CAMPUS**.

Step 3: Select the **--- Antivirus Not Running Notification** policy.

Step 4: Switch to the DEMOFS\W10 device and use the menu to disable Windows Defender.

A PowerShell script runs to disable the antivirus. It may take a moment to complete. When it is finished, a balloon message notifies you that the antivirus is off.

You will see your workstation appear in the policy group. After a moment, a web browser window will pop up with your notification. (You may have to click Advanced and Proceed to… to see the message.)

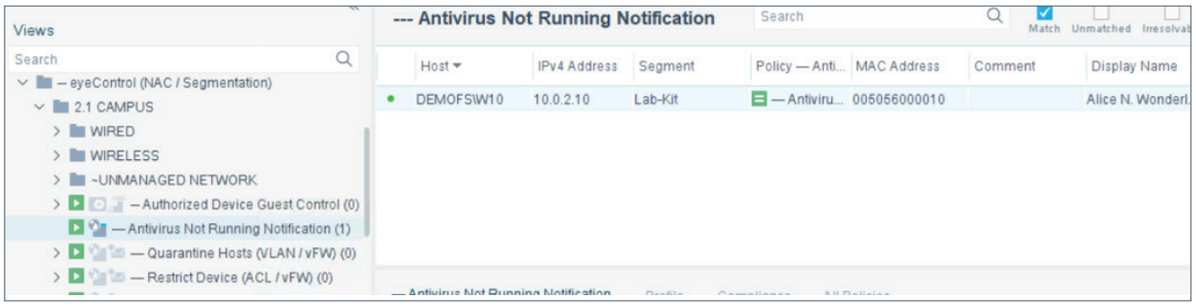


Step 5: Click the **I confirm reading the message** button.

Step 6: Type **forescout.com** into the notification's browser address bar and press **Enter**.

You can continue browsing after confirming this message.

Step 7: Switch to the Forescout console. Notice that the DEMOFS\W10 device now appears in the Antivirus Not Running notification policy hosts table.



Step 8: Switch back to the DEMOFS\W10 device in the Chrome browser. Close the forescout.com page and use the menu to re-enable the antivirus software.

Follow Up

The Forescout platform can act on endpoints based on policy criteria. Some of these actions include notification, redirection to a website, virtual local area network (VLAN) reassignment and network access restriction.

For example, for endpoints with out-of-date antivirus software, you can redirect end users to a site to download the update. For endpoints with antivirus not running, you can restrict network access until it is running. You can even start the antivirus on that endpoint.

- What compliance issues does your organization face?
- What are some of the business and technical consequences of having noncompliant endpoints on your network?
- What is your current process for remediating noncompliant endpoints? Does it involve manual intervention? Helpdesk employees doing face-to-face intervention?
- How can the continuous endpoint monitoring and automatic notifications of the Forescout platform alleviate compliance issues that you are currently experiencing?

LAP 4: INCIDENT RESPONSE

Scenario

Part way through your Forescout proof of concept, a malware outbreak, WannaCry ransomware, goes global.

You need to see if any of your endpoints are infected with or vulnerable to WannaCry and pinpoint exactly where they are. Unfortunately, it is a zero-day outbreak, and your malware software does not yet detect WannaCry.

Luckily, the SE you are working with at Forescout is already aware of this outbreak. The SE sent you a policy you can use to discover vulnerable endpoints and locate where they are within your company.

Because the Forescout platform can identify the switches and switch ports that endpoints are plugged into, you can quickly identify the location of any endpoint.

Couple this capability with a control or orchestration policy, and you can quickly hunt for and isolate compromised or vulnerable locations or have your vulnerability scanners scan the potentially affected endpoints.

Forescout can then use a virtual firewall, VLAN reassignment or orchestration with your other security products to isolate the infected systems.

Before you begin

- How do you hunt for vulnerable systems and possibly compromised locations for zero-day threats?
- What is your process for addressing those systems and locations?
- What is the impact of undiscovered infected or vulnerable endpoints to your organization? How long does it take you to find them now?
- How does the problem/risk to the organization become worse as time elapses?

In this lap, you will:

1. Import a policy to identify endpoints possibly infected by the malware outbreak.
2. Import a policy to identify endpoints vulnerable to it.

Task 1: Import the WannaCry Policy

This policy looks for specific characteristics on endpoints that indicate a WannaCry infection.

Step 1: Click the **Policy** tab in the Forescout console toolbar.

Step 2: Click **eyeSight** in the **Policy Folders** tree.

For this task, we are just going to locate the infected systems.

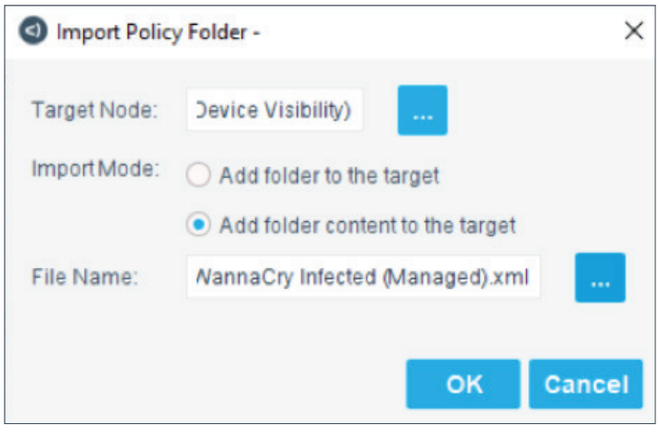
Step 3: Click the **Import Policy** Folder icon .

The Select Policy Folder dialog appears.

Step 4: Keep the Target Node at eyeSight (Device Visibility). Select **Add folder content to the target** under the Import Mode.

Step 5: Click the file browser button next to file name and navigate to the **Documents > Forescout Policies** folder. Select the **WannCry Infected (Managed).xml** file.

Step 6: Click **OK**.

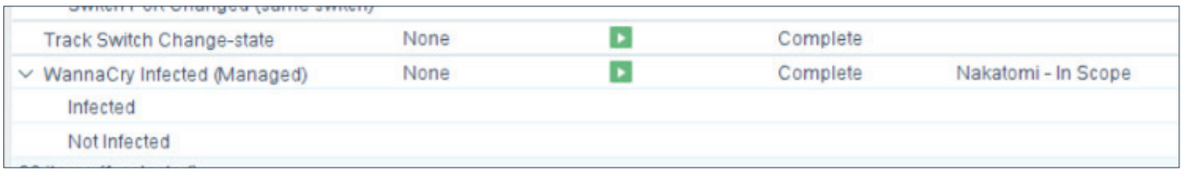


The Policy detail dialog box appears.

Step 7: Click **OK**.

The policy is added to the bottom of the eyeSight policies. You can scroll down to see the policy at the bottom of the list.

Step 8: Click **Apply**.

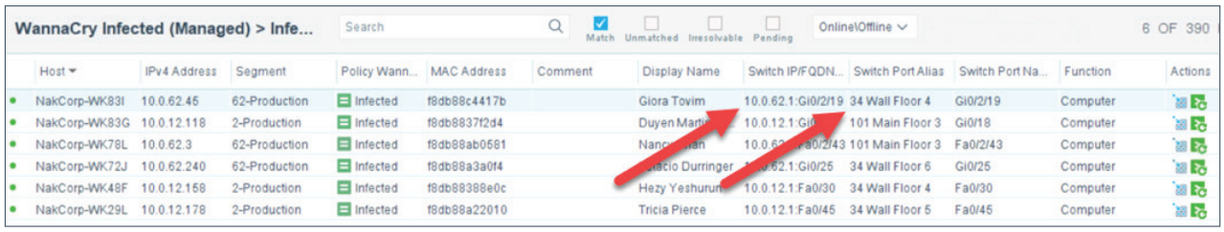


Step 9: Click the **Home** tab at the top of the screen.

Step 10: Expand the Policy tree: **Policies > eyeSight > WannaCry Infected (Managed)**.

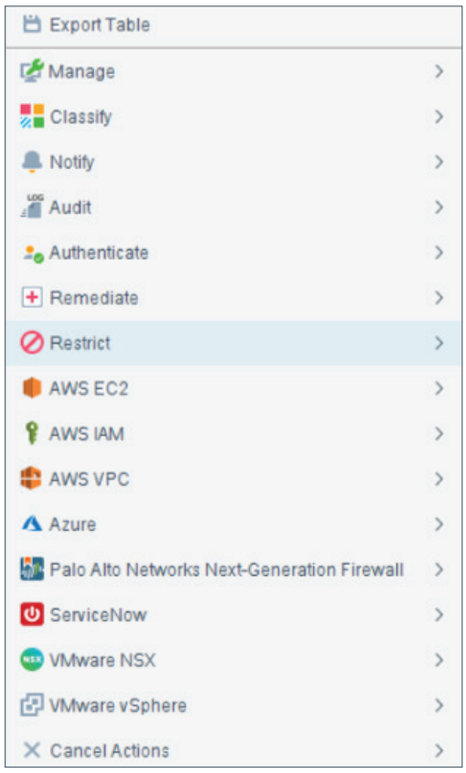
Step 11: Click **Infected**.

Now you will see a list of hosts with properties that indicate a WannaCry infection. Furthermore, you can see which switch and port they are attached to and where they are located.



Now that you have identified the infected hosts, there are several things you can do:

- Take immediate action on each device by right-clicking the device and selecting an action, such as restricting network access either by assigning the endpoint to a quarantine VLAN or by using a virtual firewall to block it.



- Write a policy to act on all of the affected devices.
- Locate the devices and send a support team to remediate them.

We are not going to take any action on these devices in this lap. We will demonstrate a control policy in the next lap.

Task 2: Install the EternalBlue Vulnerability Policy

It is not enough to identify the infected devices. You also want to know which devices are vulnerable to WannaCry. WannaCry takes advantage of the EternalBlue exploit, which is a vulnerability in the Microsoft implementation of the SMB protocol. This vulnerability has been patched. This policy detects endpoints that are still vulnerable to the exploit.

Step 1: Click the **Policy** tab in the Forescout console toolbar.

Step 2: Click **eyeSight** in the **Policy Folders** tree.

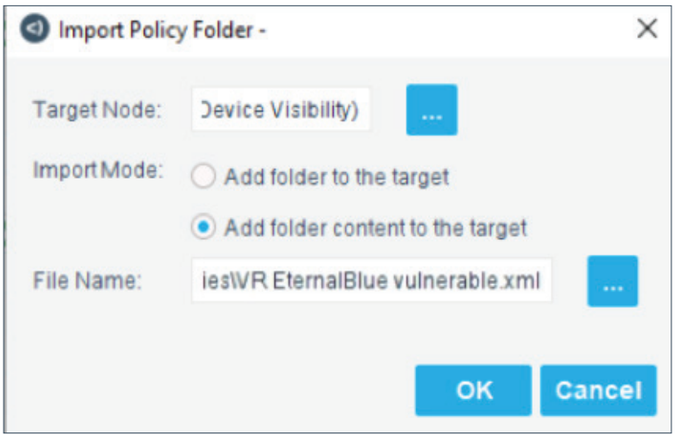
For this task, we are just going to locate the vulnerable systems.

Step 3: Click the **Import Policy Folder** icon .

The Select Policy Folder dialog appears.

Step 4: Keep the Target Node at 1.0 See. Select **Add folder content to the target** under the Import Mode.

Step 5: Click the file browser button next to file name and navigate to the **Documents > Policies** folder. Select the **VR EternalBlue vulnerable.xml** file.

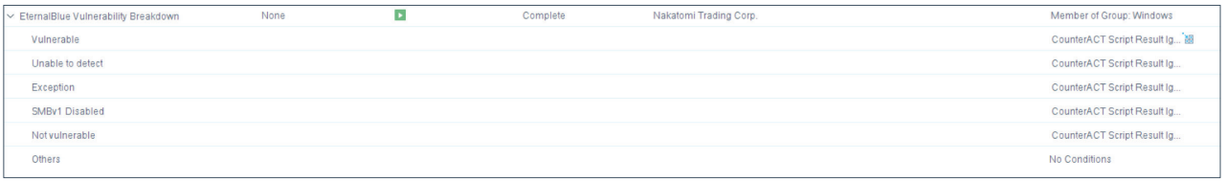


Step 6: Click **OK**.

The Policy detail dialog box appears.

Step 7: Click **OK**.

The policy is added to the eyeSight policies.



Step 8: Click **Apply**.

Step 9: Click the **Home** tab at the top of the screen.

Step 10: Expand the Policy tree: **Policies > eyeSight > VR EternalBlue**.

Step 11: Click **Vulnerable**.

You will see a list of devices that are still vulnerable to this exploit, and therefore to WannaCry.

Like the WannaCry infected devices, you can take several steps to remediate these devices. You could use policy to:

- Quarantine them to a remediation VLAN.
- Start the update process so that they receive the required patches.
- Notify the users of the vulnerabilities.

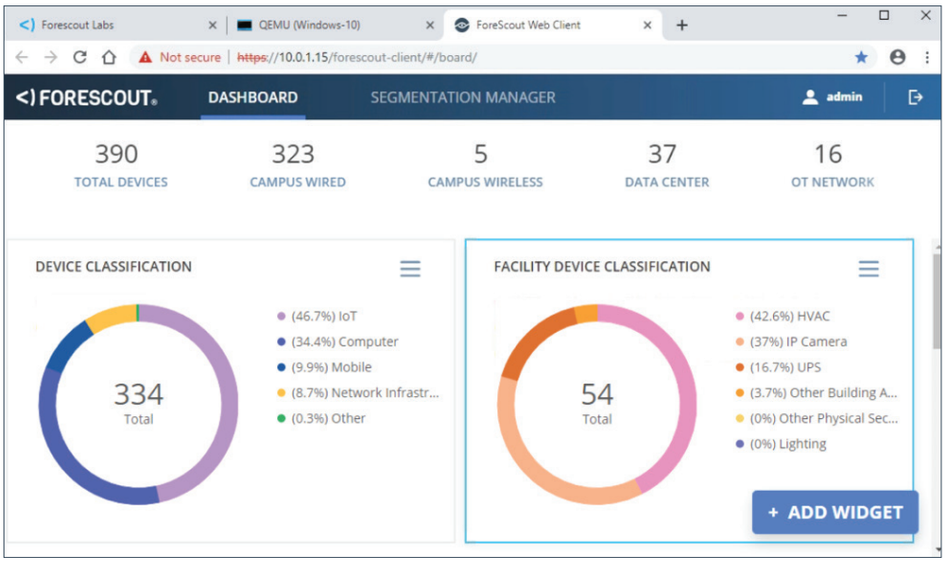
We are not going to take any action on these devices in this task. We will demonstrate a control policy in the next lap.

Task 3: Add WannaCry-Infected and Vulnerable Hosts to the Dashboard

Because of the critical importance of this issue to your company, you are going to create some widgets on the Forescout dashboard to track the progress in identifying and eliminating infected and vulnerable systems.

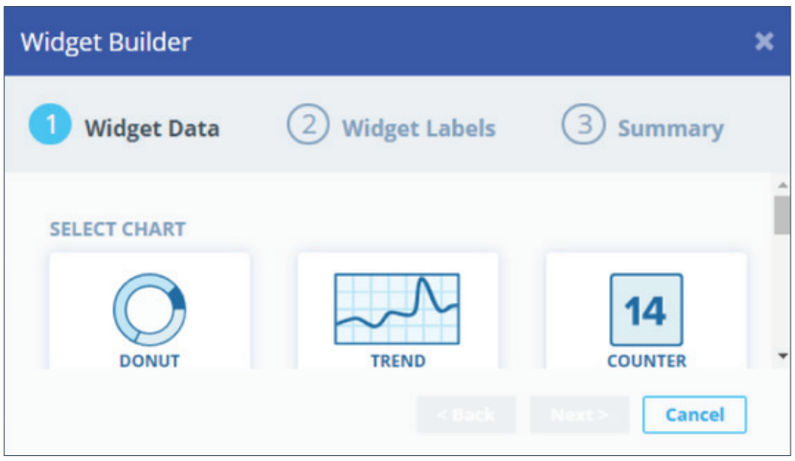
Step 1: Click the **More** (three dots) icon in the Forescout toolbar and then click **Dashboard**.

The device dashboard appears.



Step 2: Click the **Add Widget** button.

The Widget Builder wizard appears.



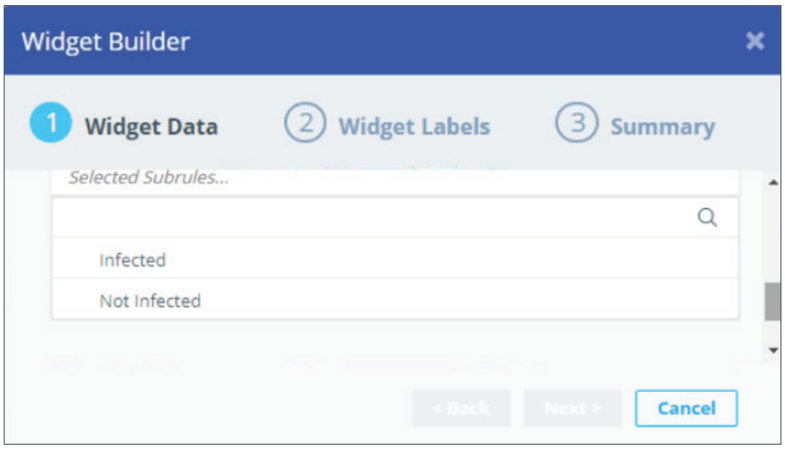
Step 3: Click **Trend** in the Select Chart area.

We want to track our progress in addressing the issue. The Select Policy field appears. You may need to scroll down to see it.

Step 4: Click **Please choose a policy** and enter "wanna" in the search field. Click **WannaCry Infected (Managed)**.

The Select Sub-Rules field appears.

Select **Infected** and the sub-rule and click **Next**.



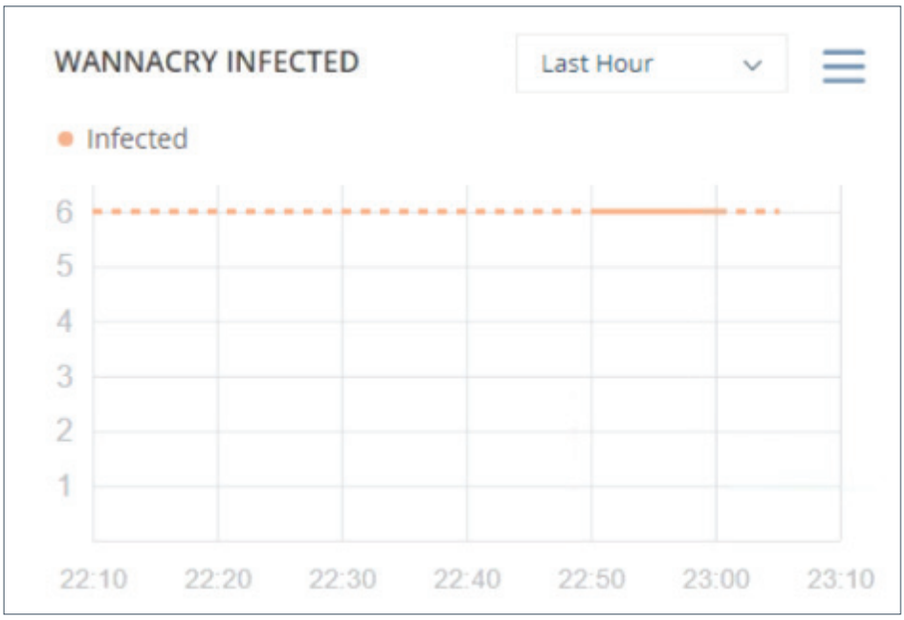
The Widget Labels screen appears.

Step 5: Shorten the widget title to **WannaCry Infected** and click **Next**.

A summary of the options you chose for your widget appears.

Step 6: Click **Finish**.

Your widget is added to the bottom of the Dashboard. It shows the number of WannaCry-infected devices over time, enabling you to track your progress in eliminating the threat. You can change the chart's time frame using the drop-down menu.



Unfortunately, because we have only had the policy for a short time, we only have one value. But over time, as additional hosts become infected, or as infected hosts are remediated, this widget will enable you to track your progress in addressing this incident.

Step 7: Now try adding a widget using the above steps for the **VR EternalBlue** policy. Use the **Vulnerable** sub-rule.

Step 8: Close the web browser when you are done.

Follow Up

- How can the Forescout platform affect your response time for zero-day threats and vulnerabilities? How would a faster response time benefit your business?
- How would the ability to automatically act on compromised or vulnerable endpoints change the way you currently address vulnerabilities?

LAP 5: NETWORK ACCESS CONTROL

Scenario

Because of the recent malware outbreak, your company decided that endpoints without antivirus software actively running on them will not be allowed on the network.

You are going to create a policy to block network access for endpoints without antivirus running on them.

The Forescout platform can do more than just notify users when their endpoints are out of compliance. It can also start processes on managed endpoints, assign endpoints to specific VLANs, and even block network access altogether.

Before you begin

- How do you prevent infected or noncompliant devices from spreading malware?
- How do you currently remediate out-of-compliance endpoints? Is it a manual process?

In this lap you will:

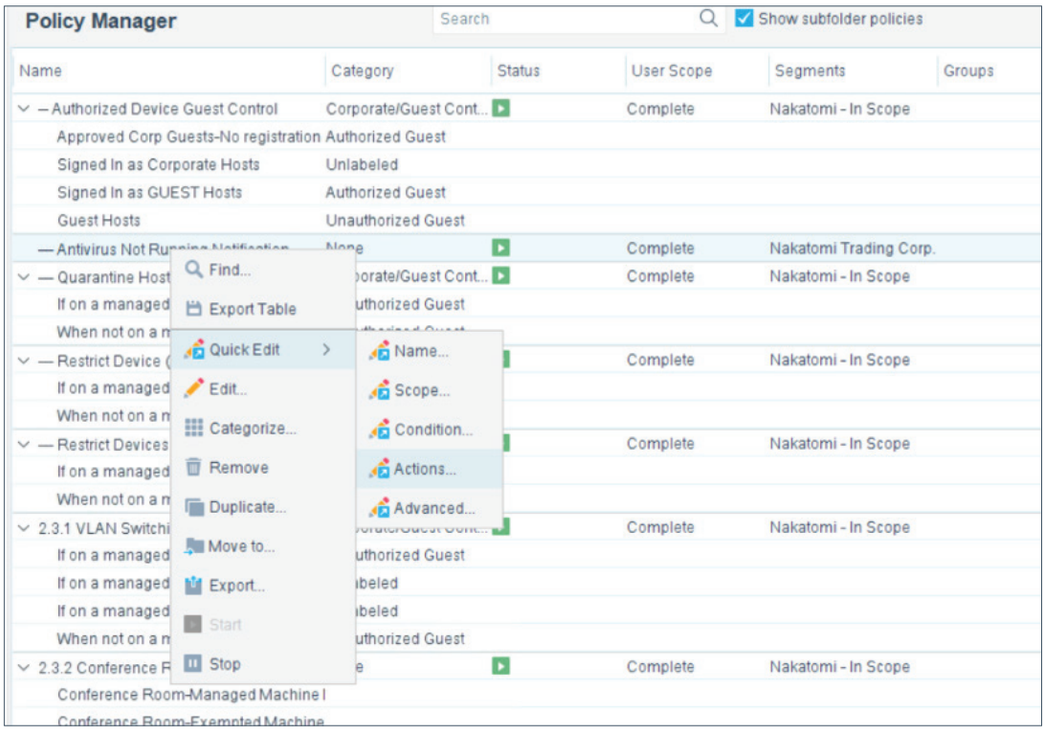
1. Modify your Antivirus Not Running Notification policy to alert the user that the endpoint will be completely blocked from the network until they turn on antivirus protection.
2. Create a control policy to block endpoints that do not have antivirus running from accessing the network.
3. Test your control policy.

Task 1: Modify Your Notification Policy

Step 1: Click the **Policy** tab.

Step 2: Navigate the Policy tree to **eyeControl > 2.1 CAMPUS**.

Step 3: Right-click the **--- Antivirus Not Running Notification** policy and select **Quick Edit > Actions** from the context menu.



Step 4: Click the **HTTP Notification** action in the table and then click **Edit**.

Step 5: In the Message Text field, type: Your antivirus is not running, putting your system at risk. Your system will be blocked from the network until you enable the antivirus.

Step 6: Click **OK** to save the updated message.

Step 7: Click **OK** to save the updated action to the policy.

Step 8: Click **Apply** to apply the policy to the system. Click Yes to confirm the change.

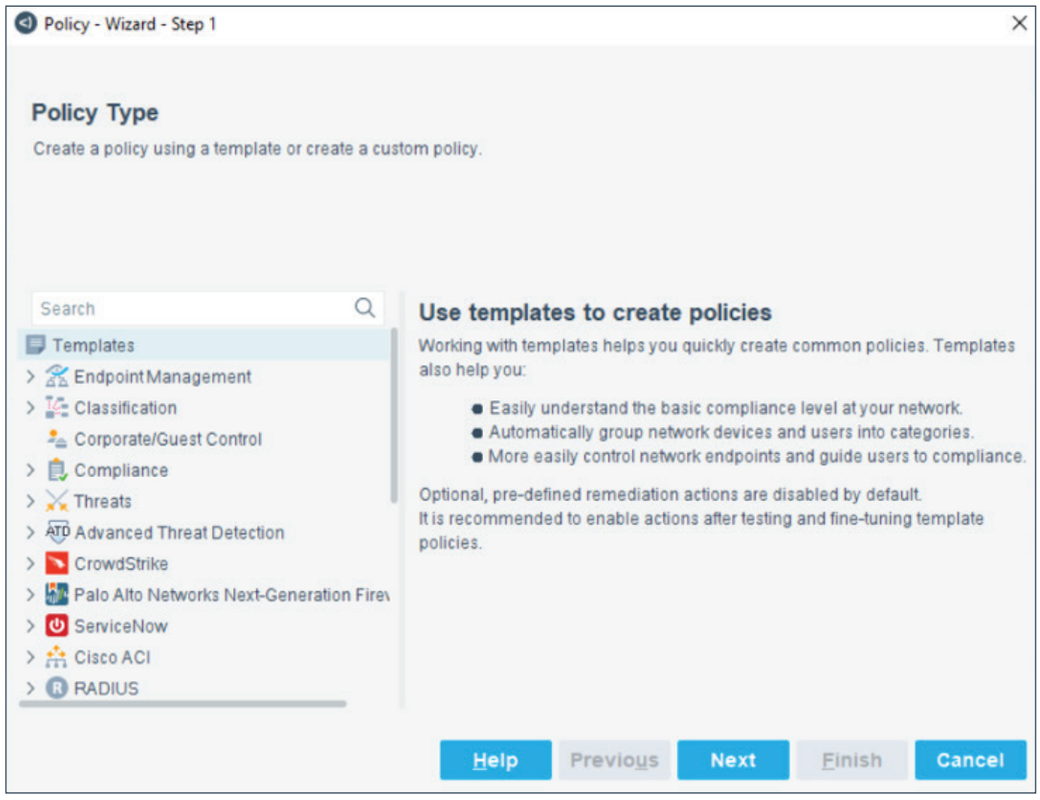
This will alert users to the fact that they will be blocked unless they remediate the issue.

Task 2: Create the Control Policy

Step 1: Navigate the Policy tree to **eyeControl > 2.1 Campus**.

Step 2: Click **Add** to the right of the policy table.

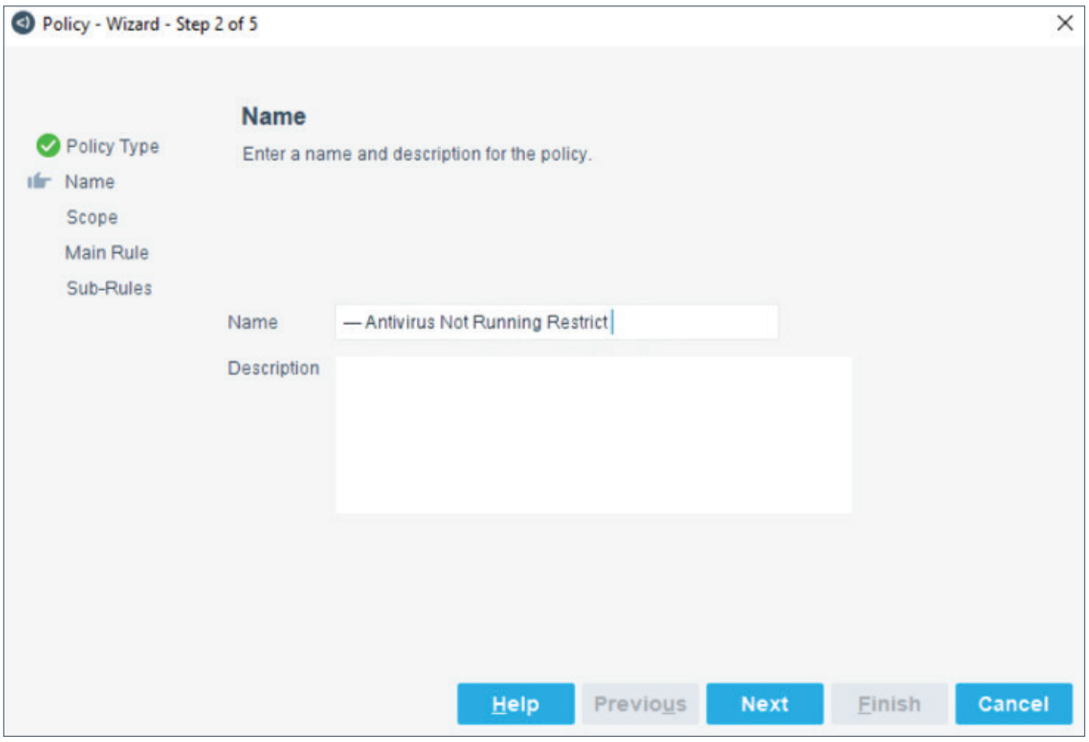
The Policy Wizard appears.



We could use one of the pre-built templates for this task; however, to give you practice, we are going to create our policy from scratch.

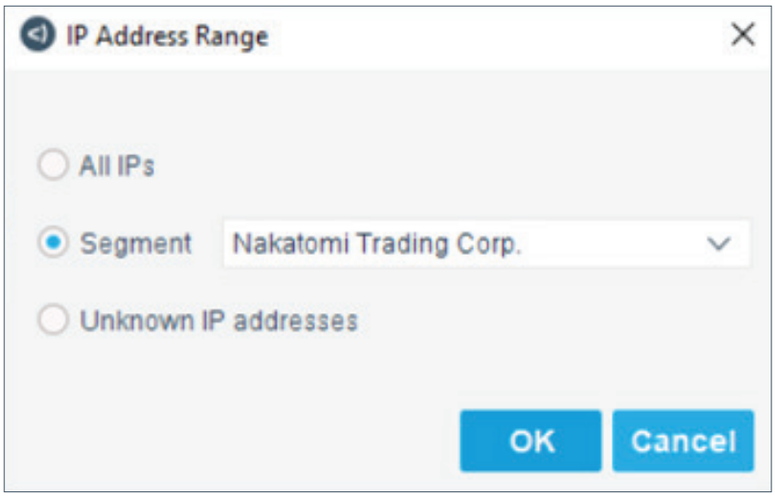
Step 3: Scroll to the bottom of the templates list, click **Custom**. Click **Next**.

The Policy Wizard Name screen appears.



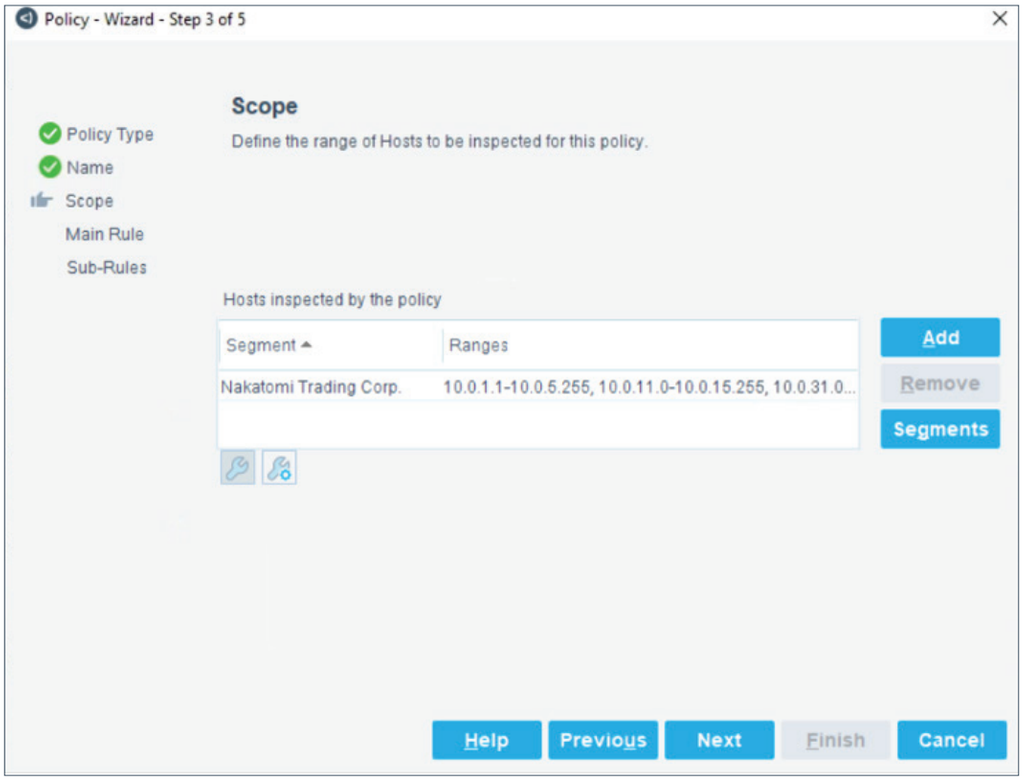
Step 4: Type **--- Antivirus Not Running Restrict** in the Name field and click **Next**.

The IP Address Range dialog box appears.



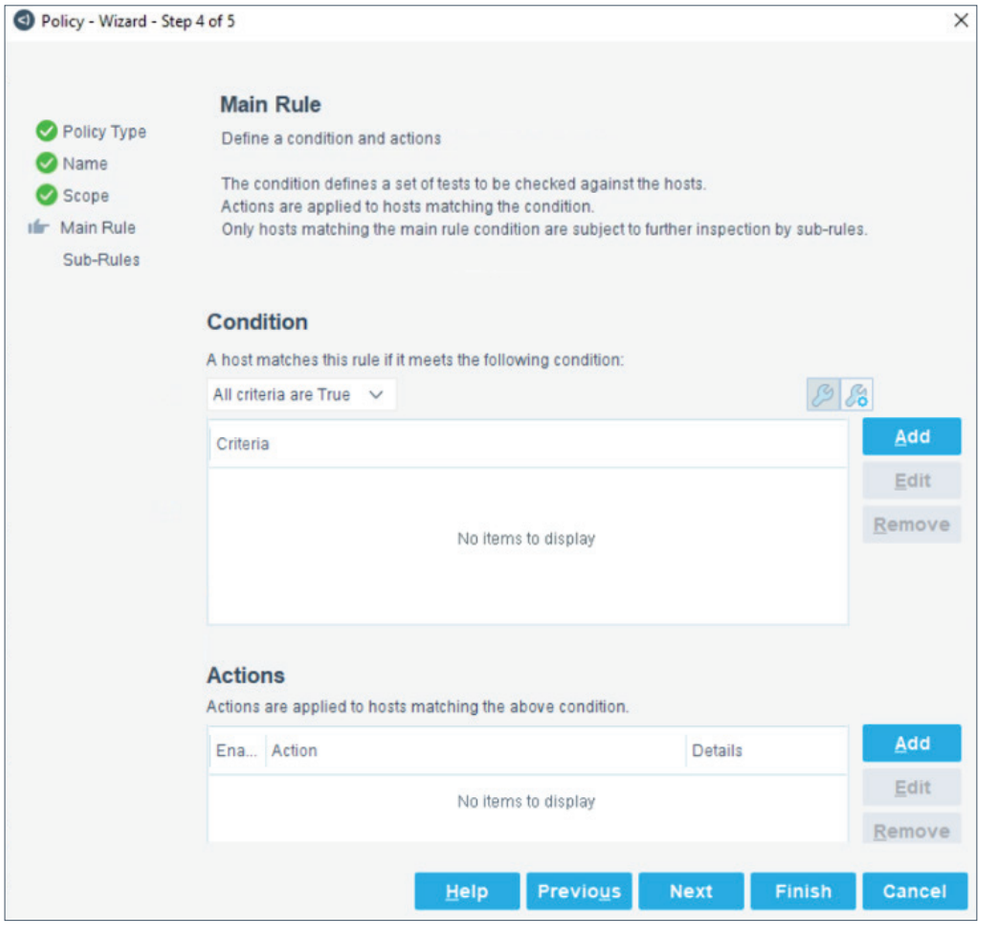
Step 5: Select **Segment** and then select **Nakatomi Trading Corp** from the drop-down list. Click **OK**.

The Nakatomi Trading Corp segment, which contains all the hosts in the lab, is added to the scope of this policy.



Step 6: Click **Next**.

The Main Rule page appears.

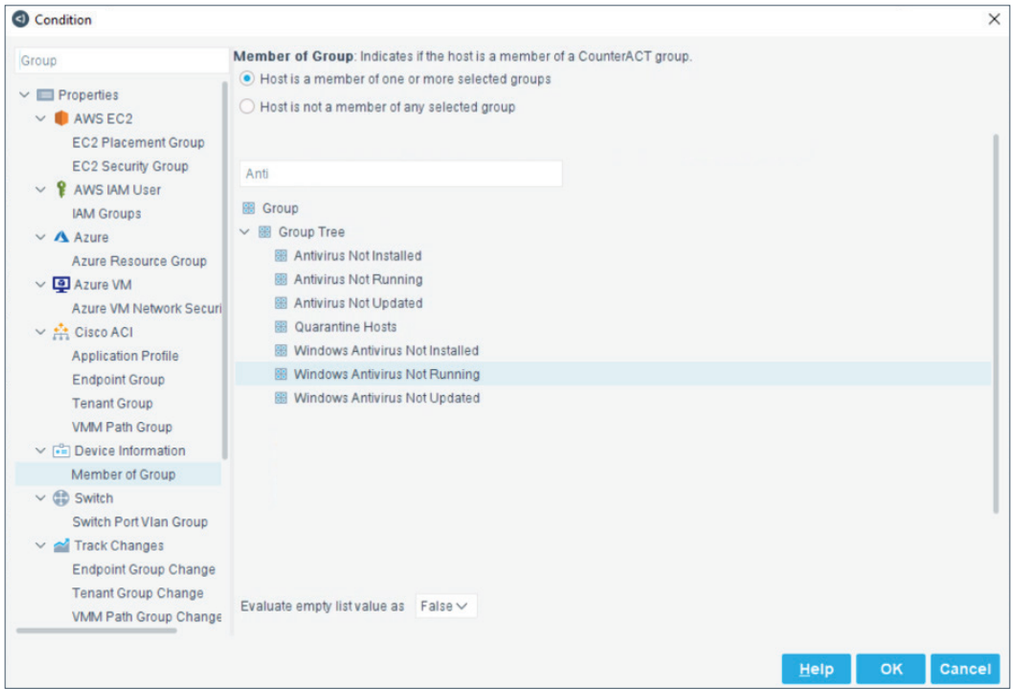


Step 7: In the **Condition** area, click **Add** next to the right of the **Criteria** table.

The Condition dialog appears.

Step 8: Type **Grou**p in the **Search** field and click **Device Information > Member of Group** in the results.

Step 9: Type **Anti** in the Member of Group search box, and click **Windows Antivirus Not Running**.



Step 10: Click **OK**.

The condition is added to the Criteria table.

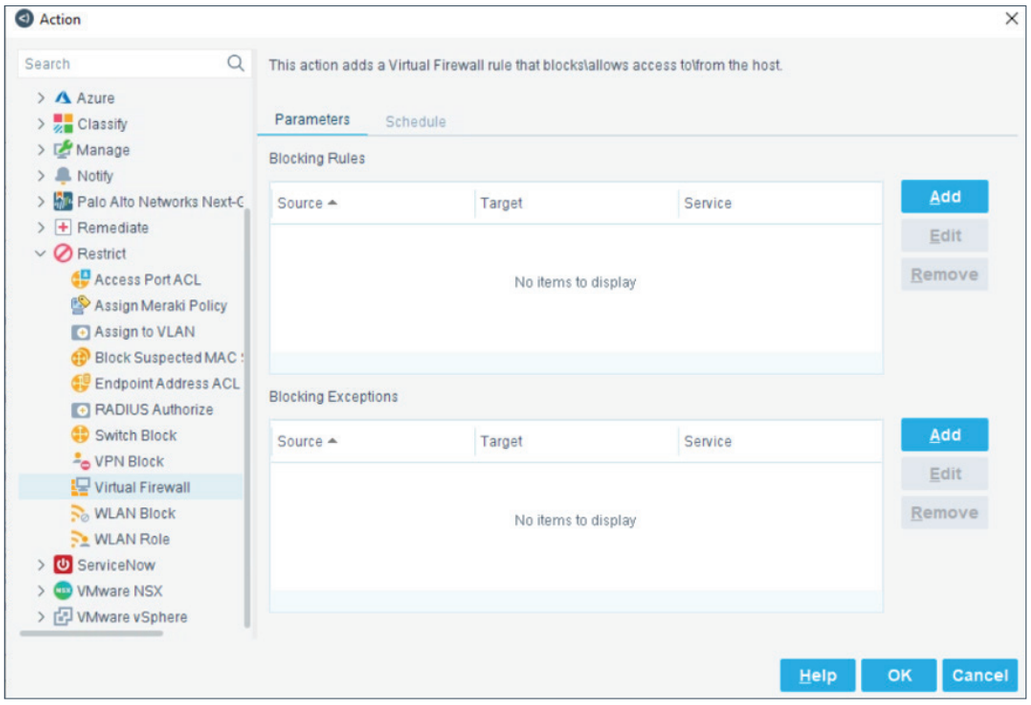
Step 11: Click **Add** to the right of the **Actions** table.

The Action dialog appears.

Step 12: Expand **Restrict** in the Actions tree.

Step 13: Click **Virtual Firewall**.

The Virtual Firewall properties appear.



Step 14: Click **Add** to the right of the **Blocking Rule** table.

The Blocking Rules dialog appears.

Step 15: Select the following values and click **OK**:

Field	Value
Inbound/Outbound	The FW will block traffic from the detected host
Target IP	All IPv4
Target Port	All (TCP and UDP)

Step 16: Click **OK** to save the action.

Step 17: Click **Finish** to save the policy.

Step 18: Click **Apply** to activate the policy.

Task 3: Test Your Network Access Control Policy

Step 1: Click the **Hom**e tab.

Step 2: Expand the Policy tree. Navigate to **eyeControl > 2.1 CAMPUS**.

Step 3: Select the **Antivirus Not Running Restrict** policy.

Step 4: Switch to the DEMOFS\W10 device in the Chrome browser and use the Network Segmentation menu to disable the antivirus software.

After a moment, a web browser window will pop up with your notification.

Step 5: Click **I confirm reading the message**.

Step 6: In the notification's browser address bar, type **forescout.com** and press **Enter**.

You should receive a "This site can't be reached" error. This is because the virtual firewall has blocked the endpoint.

Step 7: Switch to the Forescout console.

You will see the DEMOFS\W10 device in the Antivirus Not Running Restrict policy host list.

Step 8: Switch back to the DEMOFS\W10 device interface. Minimize the browser with the error message and enable Windows Defender.

Step 9: Open the web browser and try to access forescout.com again.

You can now access the website because your device is now in compliance with policy and the tag was removed from it in the firewall.

Follow Up

The Forescout platform has many ways to control endpoints, from simple notification to network access restrictions.

- What types of compliance issues does your company currently experience that a simple notification policy would resolve?
- Do you see any circumstances where blocking a device completely from the network would be beneficial? What about segmenting it to a remediation VLAN?

LAP 6: NETWORK SEGMENTATION

Scenario

Rather than block endpoints from the network, you have decided it would be better to restrict them to a particular VLAN for remediation. This allows your users to address the issues with their endpoints without jeopardizing any additional devices.

The Forescout platform lets you control endpoint access to specific resources using several methods: modifying ACLs, virtual firewalling, and assigning endpoints to specific VLANs based on the endpoint's properties. In this lap, we will show how to initiate a simple VLAN reassignment based on the antivirus status of the endpoint.

Before you begin

- How do you ensure that endpoints only access the systems that they are permitted to access? What data would be important to know when making those decisions?
- What currently manual security practices do you wish you could automate?

In this lap you will:

1. Create a network segmentation policy that will change the device's vLAN based on the state of the antivirus software.
2. Modify your notification policy to alert users that they are being redirected to a specific area of the network.
3. Disable your control policy that blocks the DEMOFS\W10 from the network when the antivirus is disabled.
4. Test your segmentation policy.

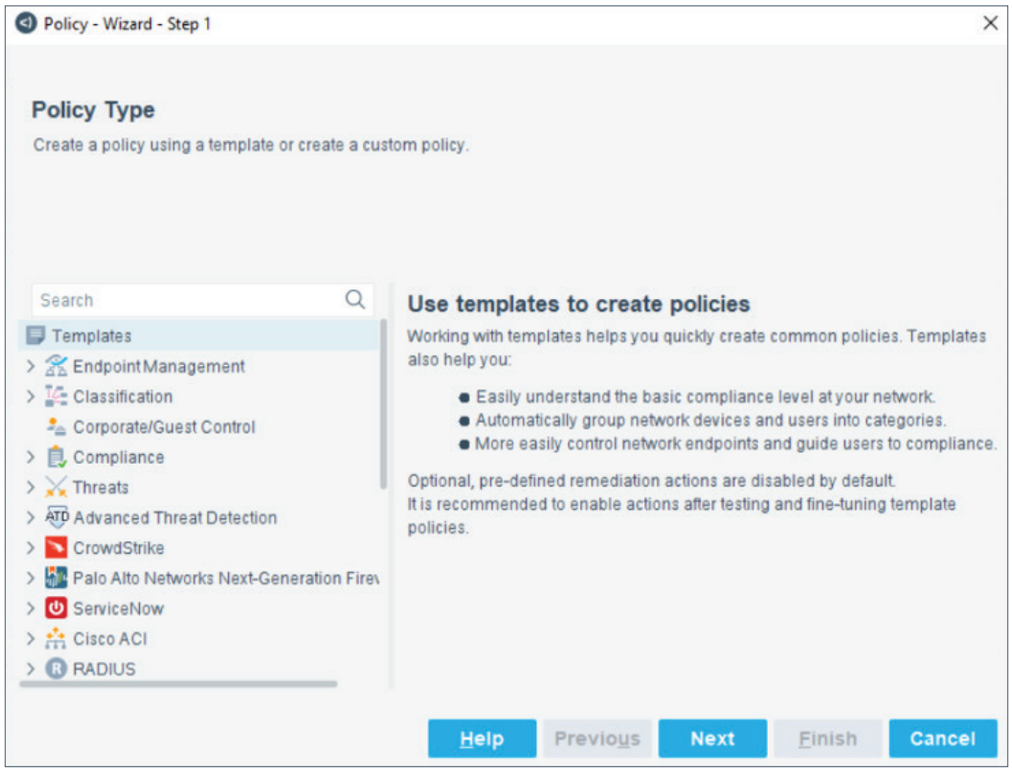
Task 1: Create the Segmentation Policy

You will create your segmentation policy first, and then disable your previous policy, because you still want noncompliant endpoints to be restricted until you are ready to transition to the new policy.

Step 1: Navigate the Policy tree to **eyeControl > 2.1 CAMPUS**.

Step 2: Click **Add** to the right of the policy table.

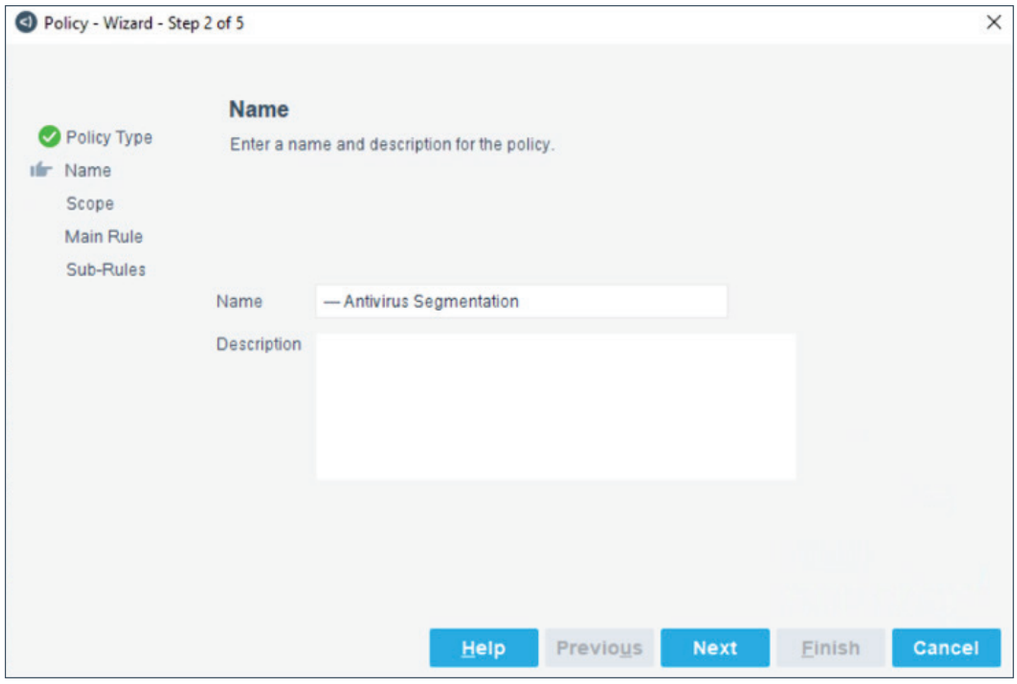
The Policy Wizard appears.



We could use one of the pre-built templates for this task. However, for the sake of practice, we are going to create our policy from scratch.

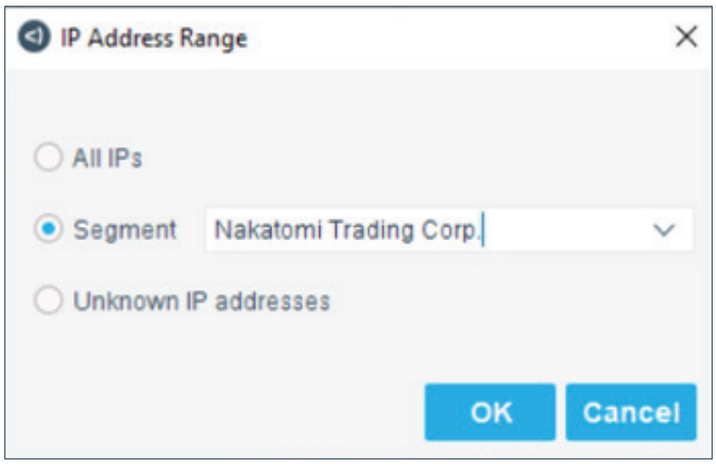
Step 3: Scroll to the bottom of the templates list, click **Custom**. Click **Next**.

The Policy Wizard Name screen appears.



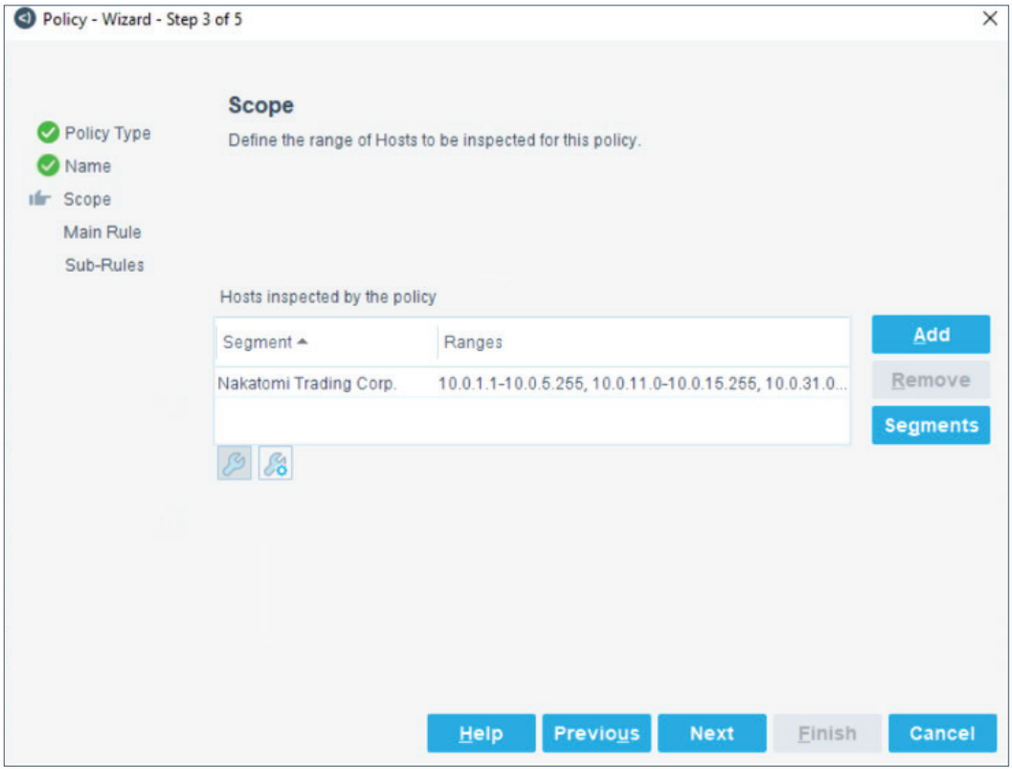
Step 4: Type the name **--- Antivirus Segmentation** and click **Next**.

The IP Address Range dialog appears.



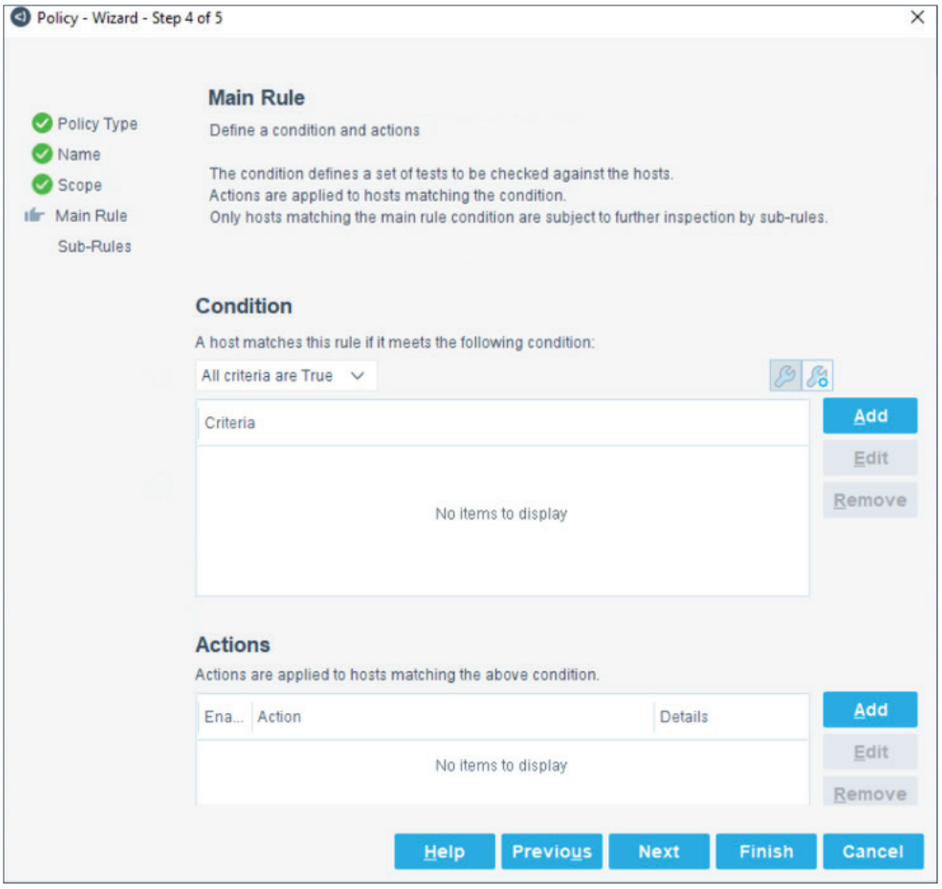
Step 5: Select **Segment** and then select **Nakatomi Trading Corp** from the drop-down list. Click **OK**.

The Nakatomi Trading Corp segment, which contains all the hosts in the lab, is added to the scope of this policy.



Step 6: Click **Next**.

The Main Rule page appears.

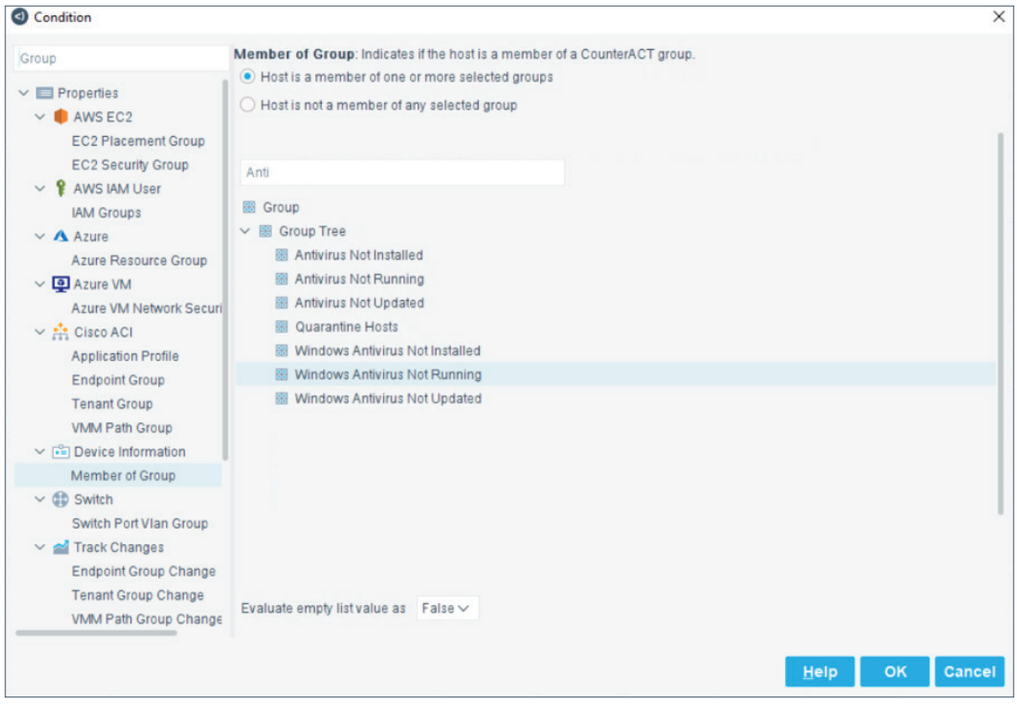


Step 7: In the **Condition** area, click **Add** next to the right of the **Criteria** table.

The Condition dialog appears.

Step 8: Type **Group** in the **Search** field and click **Device Information > Member of Group** in the results.

Step 9: Type **Anti** in the Member of Group search box, and click **Windows Antivirus Not Running**.



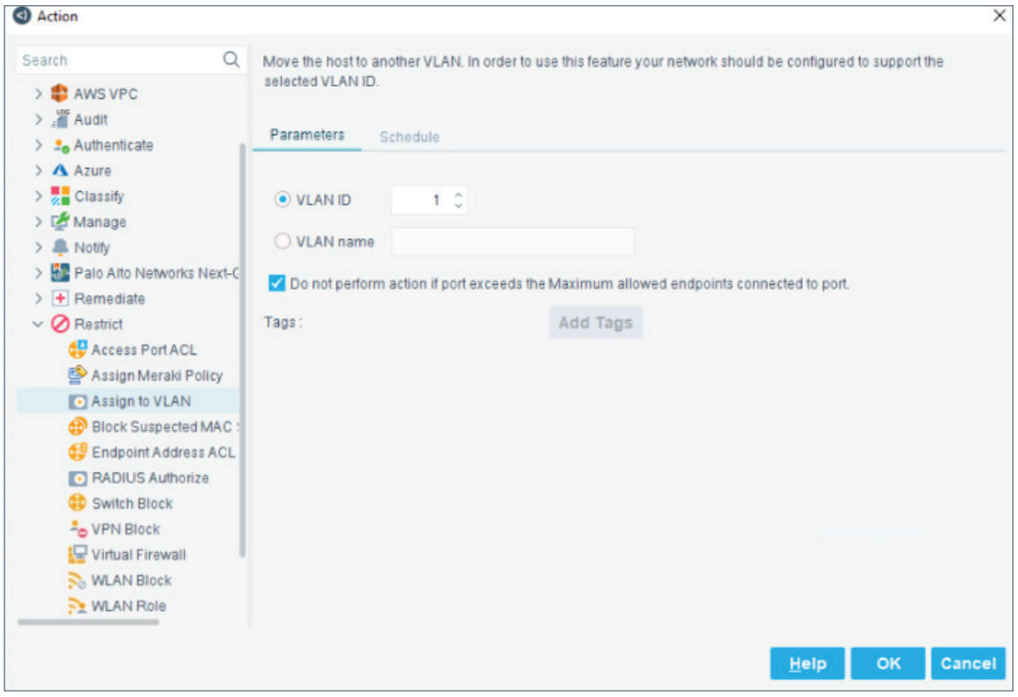
Step 10: Click **OK**.

The condition is added to the Criteria table.

Step 11: Click **Add** to the right of the **Actions** table.

The Action dialog appears.

Step 12: Expand **Restrict** in the Actions tree and click **Assign to VLAN**.



Step 13: Leave the VLAN ID field at **1**. That is the VLAN we want to move the device to.

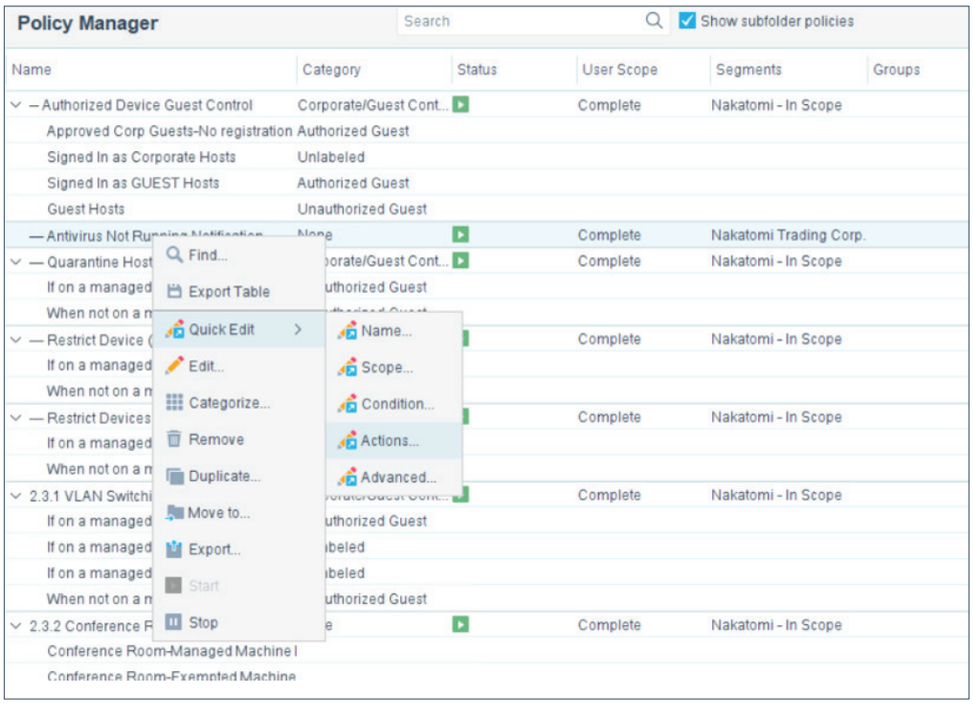
Step 14: Click **OK** to save the action to the Actions Table.

Step 15: Click **Finish** to save the policy. Click **Apply** to activate the policy.

Task 2: Modify Your Notification Policy

Step 1: Navigate the Policy tree to **eyeControl > 2.1 CAMPUS**.

Step 2: Right-click the **--- Antivirus Not Running Notification** policy and select **Quick Edit > Actions** from the context menu.



Step 3: Click the **HTTP Notification** action in the table and then click **Edit**.

Step 4: In the Message Text field, type:

Your antivirus is not running, putting your system at risk. Your system has been moved to a remediation network until the issue has been resolved.

Step 5: Click **OK** to save the updated message.

Step 6: Click **OK** to save the updated action to the policy.

Step 7: Click **Apply** to apply the policy to the system. Click **Yes** to confirm the change.

This will alert users to the fact that they will be moved to a specific network until they remediate the issue. This network could have limited access to resources or access to specific remediation tools.

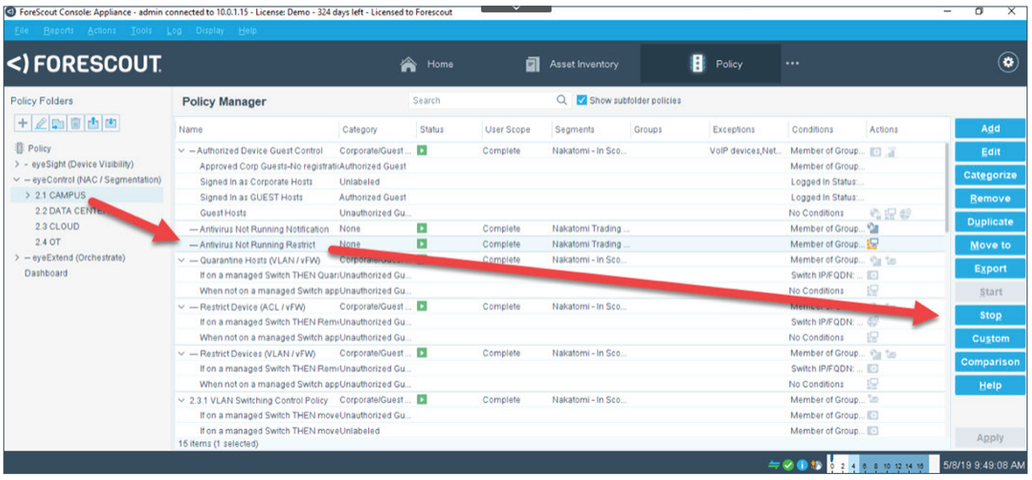
Task 3: Disable Your Antivirus Not Running Restrict Policy

Step 1: Click the **Policy** tab.

Step 2: Navigate the Policy tree to **eye Control > 2.1 CAMPUS**.

Step 3: **Select the --- Antivirus Not Running Restrict Policy** in the policy table.

Step 4: Click **Stop**.



Step 5: Click **Yes** to confirm that you want to stop the policy.

A message box informs you that the policy has been stopped and saved.

Step 6: Click **OK** to close the message box.

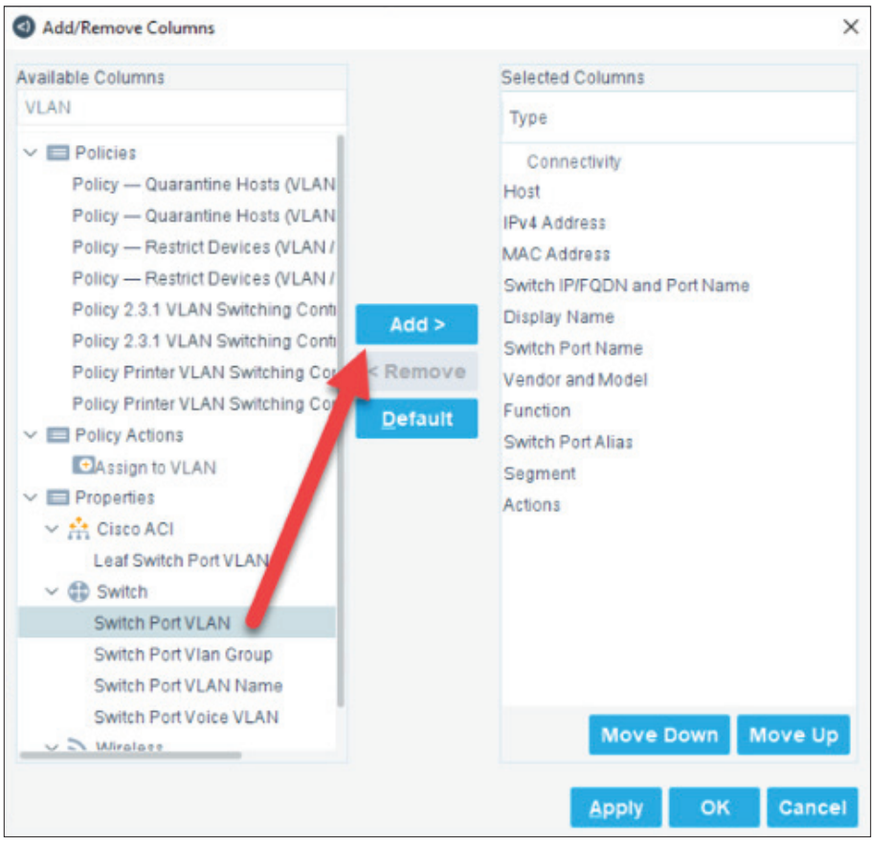
Task 4: Test Your Segmentation Policy on the Endpoint

Step 1: Click the **Home** tab.

Step 2: Under Views, click **All Host**s. Then above the Hosts table, type **DEMOFS/W10** in the search box.

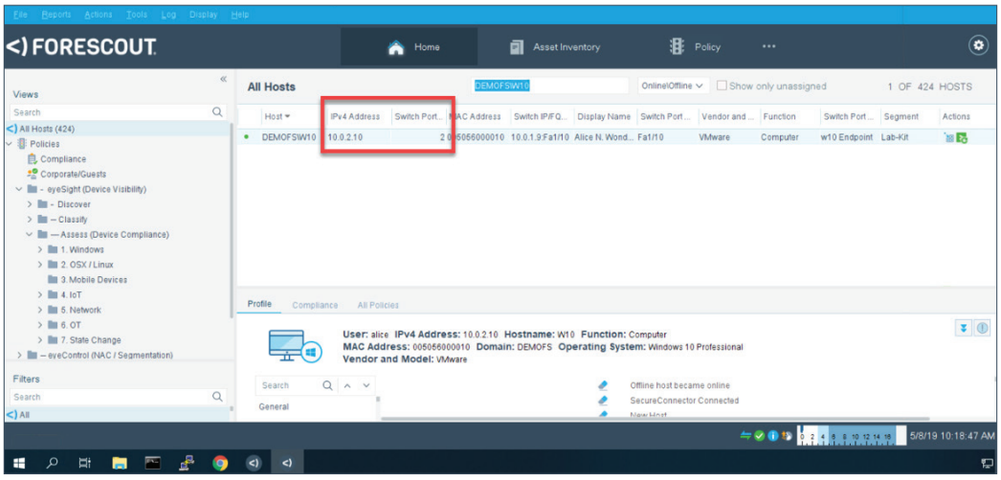
Step 3: Right-click the table headings and select **Add/Remove Columns**.

Step 4: Type **VLAN** in the Available Columns search box. Select **Switch Port VLAN** and click **Add**.



Step 5: Select **Switch Port VLAN** in the Selected Columns list and click **Move Up** until it is just below the IPv4 Address entry. Click **OK** to save your changes.

The Switch Port VLAN is now displayed in the All Hosts table. Note the IP address and Switch Port VLAN of the DEMOFS\W10 device.

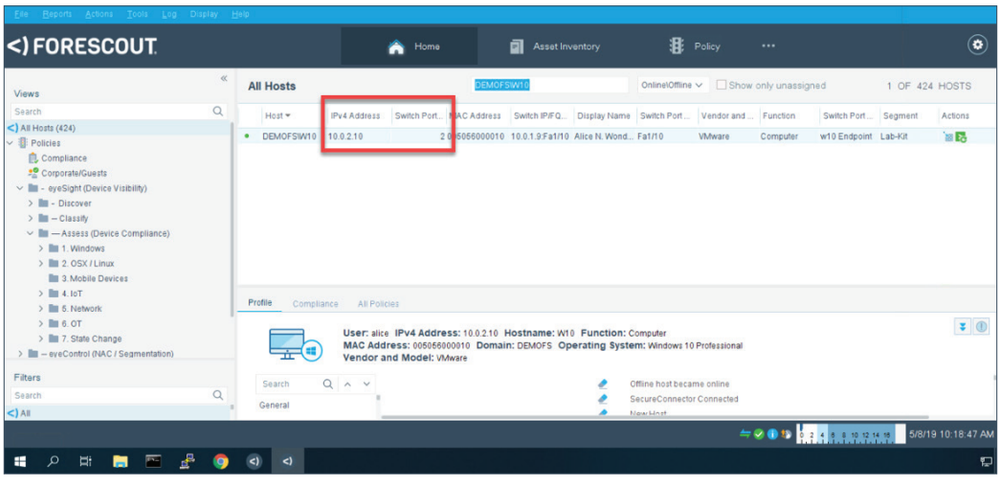


Step 6: Switch to the DEMOFS\W10 device and use the Solutions Menu to disable the antivirus.

The notification that you are being moved to a different network pops up. You can leave the notification there.

Step 7: Switch back to the Forescout console.

The IP Address and Switch Port VLAN of the DEMOFS\W10 device have changed.



NOTE: It may take up to a minute for the console to reflect the VLAN and IP address change.

Follow Up

The Forescout platform has many ways to control an endpoint's access to network resources, from blocking the endpoint to creating ACLs on the switch to reassigning the endpoint to a specific VLAN. And you can base this control on any of the properties that the Forescout platform discovers for the endpoint.

- How would being able to control what an endpoint can access on your network based on that endpoint's properties help you at your company?
- Can you think of a process that this capability could help you automate?

TAKE THE NEXT STEP

Learn more about how you can drive your security initiatives forward using the Forescout platform. We offer several complimentary options to further boost your knowledge, help engage your peers and share the business benefits of agentless visibility, policy-based control and multivendor security orchestration.

- **Spend 10 minutes with the Forescout Business Value ROI Tool**. This tool, based on IDC's methodology, provides statistical analysis of the business impact the Forescout platform can deliver to your organization. It generates a custom ROI report that you can share with co-workers.
- **Visit forescout.com for more information,** including details on our growing list of Forescout products that share device context between the Forescout platform and many of the security and IT management tools you use today. Forescout eyeExtend products can help automate policy enforcement across disparate solutions, accelerate system-wide response to mitigate risks, and increase productivity in multiple ways.
- **Contact Forescout to set up an appointment:**

  salesdev@forescout.com

  Tel: +1-866-329-9352

Forescout Technologies, Inc.
190 W Tasman Dr.
San Jose, CA 95134 USA

Toll-Free (US) 1-866-377-8771
Tel (Intl) +1-408-213-3191
Support +1-708-237-6591