Use Forescout to discover devices in your network, then use Viakoo to identify vulnerable devices and remediate them through firmware management, certificate management and password management.

Forescout/Viakoo

Integration Guide

Getting Started

To get started, you will need to do a few things in the Forescout console:

- 1. Install the Connect Plugin
- 2. Enable the Web API Connect Module
- 3. Create a Policy to select a set of devices to import.

Detailed Steps:

Installing the Connect Plugin



The Connect Plugin may not automatically start running after installation. From the Modules pane, next to the Connect Plugin, check for the green arrow. If you do not see a green arrow, highlight the Connect Plugin and click the **Start** button.

Enabling the Web API Connect Module

1. From the Options panel on the left, selec Web API.





VIOKOC

Seamless Interoperability of Forescout & Viakoo

2. Select **Add User** and enter credentials (these will be used by Viakoo to fetch device information).

3. In the same pane, click on the **Client IPs** tab, then **Add** and enter the IP of the ViakooCA at the site you wish to import devices to.

4. Once all the changes are added hit **Apply** at the bottom of the window to save the settings and restart the module.

Setting up a Policy for Viakoo

To define the set of devices to remediate through Viakoo, you will need to create a policy.

Define a Segment

Policies in Forescout can be set for All IPs or a Segment of IPs. If you wish for

devices to be imported from only part of your network, a Segment must be defined.

1 From the main Forescout window right click on **Segments** in the lower left pane

Click Segment Manager

- 2. Click the **Plus** button, name your segment, and choose a folder for it. Click **OK**.
- 3. Click **Add** and define the IP range or subnet to add to your segment. You may add as many IP ranges as needed.
- 4. Click OK to finish.

Create a Policy

1. Click on the **Policy** tab at the top of the main window.

2. Click **Add** on the right-side panel.

- 3. You may select a template, but for full control choose **Custom**.
- 4. Click **Next** and enter the name and description for the policy.
- Click Next and enter the Segment this policy should work on. If you want this Policy to collect devices from across your entire network, select All IPs. Click OK.

Manage the list of client ages	that are allowed to access CounterACT Web AP(s.		
IP Address Pange +	Shange Tab	Add CA IP	Ard
			East
	Add IP Range ×		
	All Py4 Well Range		
	Examples: • 10:001-10:00.127		
	 12.561.024 10.001 		
	OK Cancel		
			Apply Unde
	Mangar for the other	And and the off of the off off off off off off off off off of	Add CA IP

Filters Search	Q
<) All	
> 📾 Segments (25)	
Organizational Units	
> 🔢 Default Groups	
> 🔢 Groups	

SegmentManaper					
Ise this option to organize y Ince defined, you can:	ur network into logical cate imation Panel per segmen ing at the Console, e.g. cre id per segment, cific geographic location. U	pories - for example, t. ate a policy that block se this option when w	ales, finance and res s Internet access to er orking with the site ma	earch departments. Idpoints in the finance de Ip.	gartment.
+ 8 2 4 4	Name	Segments		1	
Con Begments C Test C Viakoo Plus button	Q pescription Location No loca Cocation Range Note: Endy the Passiv Search	Son N:	ame sitive to network co before you add the Q	 Add onmettions should be m to a segment. Show sub-set 	placed in agments
	Path	Segment +	Description		Add
			Ad	ld IP Range	Edit





 (Optional) If you wish to define conditions beyond IP range under which devices will be filtered, you may do so here. Next to the Condition table, click Add. Some good places to start are Function, Assigned Label, and Member of Group.

7. Click Finish. Your Policy will automatically take effect. Take a moment to see what devices have been collected under your policy
you may decide to refine your Policy conditions (Right click on your Policy in the left pane and select Edit).

Import Devices to Viakoo

1. Open the ViakooCA console. From the drop-down menu, select **Manage Integrations**.

2. Click on the **Forescout** logo.

3. Enter the URL of your Forescout server (including the

https://), the **name of your Policy**, and the **credentials** you created for Viakoo to use.

4. Click Submit and then Import.

Import From Forescout	× Import From Forescout ×
Forescout URL	perter terme er ce ce ce at
https://10.102.1.77	Modify Configuration
Policy Name	
Viakoo Default	Edit
API User	Load Devices
viakoo-user	Import . In Started Devices will appear in the next collection cycle
API Password	
	Exit
Submit	Exit

5. Devices will become visible in the CA console over the course of the next collection cycle (<2 hours). If you wish to speed up this process, you can click **Trigger Send** on the CA home page (if successful, it will say "New Send Triggered". If a collection was already in progress, try again in a few minutes).

6. Once imported, you may add a name to your devices by clicking the gear icon (it will take another send for these changes to be registered in the cloud).

Condition)
Function	Function: Indicates the most specific endpoint function that was determined. If data sources and inspection methods do not resolve to a single common function, this property has the value Multiple Suggestions?.	
Properties	Meets the following criteria	
	O Does not meet the following criteria	
Active Probe Function	Match from list	
 In Classification 	To detect all sub-classifications of the selected functions, select the 'include sub-classifications' shashing. These bases are selected the superstellar installed Design Bodils Library	
Function		
Network Function	Search	Q,
- 🔆 Classification (Advanced	 Information Technology 	
Suggested Function Clas	> Accessory	
Suggested Function Clas	> Appliance	
Suggested Function Clas	> Computer	
Network Function Resolut	> Healthcare Platform	
Classification Score	> Mobile	
Function Classified By	Abilimania & Entartainmant Include sub-classifications	
DCE Model Decision Sco		
DCE Function Decision S	Match text string Enter a single value (for example: Computer) or use the ' > ' string (space-arrow-space) to	
Device Role	ananonation model with of the Incommutation Bar symmetry Information Technologies, s	
Discovery Score	Evaluate irresolvable criteria as False V	



			E
Viakoo	Commur	nications Actor	N
Home Screen		Start the Collection Cycle	Trigger Send
This screen allows yo monitored by those n before using this pro-	ou to add or remove rec nachines. Each system cedure.	cording servers to your Viakoo site configuration must have a Reader Actor (RA) already install	n, as well as devices to b ed and running on it
Local RA: 10.102	2.1.73	RA: Server: Status	* =
			+ arid a switz
Switches (0)			
Switches (0) IoT Devices (4)			+ add an lot devic
Switches (0) IoT Devices (4) IP: 10.102.200.1	Name: undefined	Add a Device Name	+ add an iot devic
Switches (0) IoT Devices (4) IP: 10.102.200.1 IP: 10.50.100.27	Name: undefined Name: undefined	Add a Device Name	+ add an iot devic
Switches (0) IoT Devices (4) IP: 10.102.200.1 IP: 10.50.100.27 IP: 10.50.100.28	Name: undefined Name: undefined Name: undefined	Add a Device Name	+ add an iot devic
Switches (0) IoT Devices (4) IP: 10.102.200.1 IP: 10.50.100.27 IP: 10.50.100.28 IP: 10.50.100.26	Name: undefined Name: undefined Name: undefined Name: undefined	Add a Device Name	+ add an lot devic
Switches (0) IOT Devices (4) IP: 10.102.200.1 IP: 10.50.100.27 IP: 10.50.100.28 IP: 10.50.100.26 Mobotix Cameras (0)	Name: undefined Name: undefined Name: undefined Name: undefined	Add a Device Name	+ add an lot devic
Switches (0) IoT Davices (4) IP: 10.102.200.1 IP: 10.50.100.27 IP: 10.50.100.28 IP: 10.50.100.28 Mobotic Cameras (0) Aviglion Appliances (Name: undefined Name: undefined Name: undefined Name: undefined	Add a Device Name	add an lot devic add an lot devic add an lot devic add an lot devic add a lot devic add add

10.102.200.1	- Device IP Address
Core Router #2	- Device Name
Router or Switch	- Device Type Name
	- Description
PING	✓ - Probe Type
Http Username	- Http Username
Http password	- Http password

7. (Optional) To take advantage of Viakoo's remediation features like firmware management and certificate management, you will need to add credentials for any imported device through the ViakooCA's **Set Device Credentials** page. Select a Device Type of "IoT Device".

Home Add Multiple RAs	VIAKOO
Add Multiple Devices: Avigilon Appliances Exacq Edge Appliances IoT Devices Mobotix Cameras Switches	Viakoo Device Passwords This screen allows you to add or update device Passwords. Currently Defined Passwords Add Passwords By Device Add Passwords By Manufacturer
Configure Secure Mode Configure SNIMP Trap Connection Settings Manage Integrations Manage IoT Devices OID Entries Set Device Credentials Set VMS Credentials Vulnerable Passwords	* = required field Select Device Type * Username * Password * Device IP Address * * IoT Device V

8. From the web portal, visit your site's details page and expand the IoT Device section. Your Forescout devices are now visible in the cloud and are ready to take advantage of Viakoo's remediation features.

More information

For help with Forescout, including setting up policies, visit the Forescout Support Hub.

If you have any questions, comments, bug reports, or suggestions, please reach out to us through the live-chat feature or contact us at feedback@viakoo.com.



Keep Up-to-Date with Viakoo

Visit viakoo.com for new product information, blogs, webinars, and insights on how to improve security and reduce risks

www.viakoo.com

