



CounterACT[®] Wireless Plugin

Integration with Xirrus Wireless Controllers

Configuration Guide

Version 1.5.1

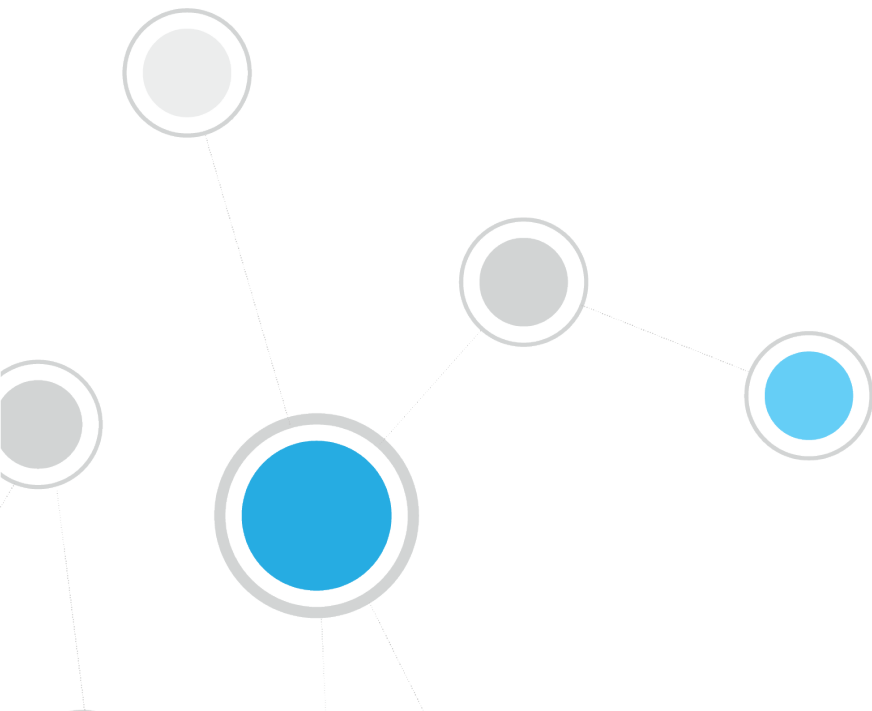


Table of Contents

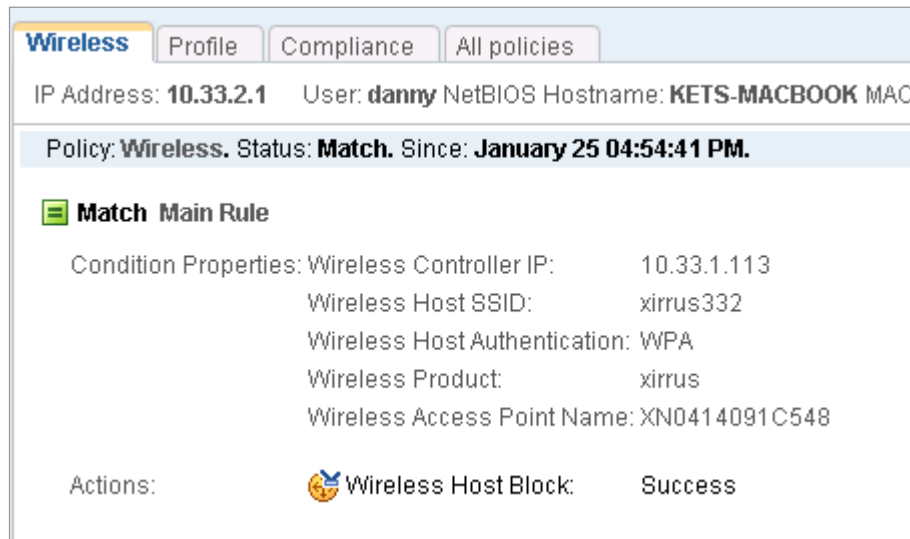
About the Plugin and Xirrus Configuration	3
Requirements	3
Configuration	4
Additional CounterACT Documentation	6
Documentation Downloads	6
Documentation Portal	6
CounterACT Help Tools.....	7

About the Plugin and Xirrus Configuration

This document describes how to configure Xirrus controllers for integration with the CounterACT Wireless Plugin.

The CounterACT Wireless Plugin is designed to provide NAC capabilities to 802.11 wireless network controllers and access points for the purpose of:

- Viewing information about wireless endpoints connected to your network
- Preventing wireless endpoints from connecting to the organizational network



The screenshot displays the 'Wireless' configuration page in CounterACT. It features tabs for 'Profile', 'Compliance', and 'All policies'. The current user is 'danny' with IP address 10.33.2.1. The NetBIOS hostname is 'KETS-MACBOOK' and the MAC address is partially visible. The selected policy is 'Wireless', which is in a 'Match' status since 'January 25 04:54:41 PM'. A 'Match Main Rule' is active, with the following condition properties:

Condition Properties:	Wireless Controller IP:	10.33.1.113
	Wireless Host SSID:	xirrus332
	Wireless Host Authentication:	WPA
	Wireless Product:	xirrus
	Wireless Access Point Name:	XN0414091C548

The actions list includes 'Wireless Host Block' with a success status.

For detailed information about the CounterACT Wireless Plugin refer to <http://updates.forescout.com/support/files/plugins/wireless/1.3.2/1.3.2-142/help.pdf>

Requirements


- Xirrus controller XN4, version 4.0.8 or higher
- Network Module version 1.0 with the Wireless Plugin running.
- CounterACT version 8.0

Configuration

To work with the Wireless Plugin, you must configure SNMP read parameters and SSH or Telnet write parameters on the Xirrus controller.

To configure a Xirrus controller:

1. Log into the controller.
2. Configure SNMP read parameters: select **Configuration > Services > SNMP**.

XN4 Wi-Fi Array			
Status		Name: XN0414091C548 (10.36.1.111)	Location: CUMULUNIMBUS
		Uptime: 0 days, 2 hours, 3 mins	
Array	SNMPv2 Settings		
Network	Enable SNMPv2:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
RF Monitor	Read-Write Community String:	••••••	
Stations	Read-Only Community String:	•	
Statistics	SNMPv3 Settings		
System Log	Enable SNMPv3:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Configuration	Authentication:	<input type="radio"/> SHA <input checked="" type="radio"/> MD5	
Express Setup	Privacy:	<input type="radio"/> AES <input checked="" type="radio"/> DES	
Network	Context Engine ID:	8000521503000f7d077780	
Services	Read-Write Username:	xirrus-rw	
Time	Read-Write Authentication Password:	••••••••	
Netflow	Read-Write Privacy Password:	••••••••	
System Log	Read-Only Username:	xirrus-ro	
SNMP	Read-Only Authentication Password:	••••••••	
DHCP Server	Read-Only Privacy Password:	••••••~•	
VLANs	SNMP Trap Settings		
Security	Trap Host 1 IP Address:	Xirrus-XMS	Port: 162
SSIDs	Trap Host 2 IP Address:		Port: 162
Groups	Trap Host 3 IP Address:		Port: 162
IAPs	Trap Host 4 IP Address:		Port: 162
WDS	Send Auth Failure Traps:	<input checked="" type="radio"/> Yes <input type="radio"/> No	
Filters	Keepalive Trap Interval:	1	
Tools	Apply Save		

3. Configure SSH or Telnet access parameters. Select **Configuration > Security > Management Control**.

Status	Name: XN0414091C548 (10.36.1.111)			Location: CUMULUNIMBUS	Uptime: 0 days, 2 hours, 13 mins
Array	Management Settings				
Network	Failed login retry period (0 - 65535 seconds): <input type="text" value="0"/>				
RF Monitor	Pre-login Banner: <input type="text"/>				
Stations	Post-login Banner: <input type="text"/>				
Statistics	Management Transports				
System Log		Timeout (30-100000 seconds)	Port		
Configuration	SSH:	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="text" value="3000"/>	<input type="text" value="22"/>	
Express Setup	Network:	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="text" value="3000"/>	<input type="text" value="23"/>	
Network	Serial:	<input checked="" type="radio"/> On <input type="radio"/> Off	<input type="text" value="3000"/>		
Services	HTTPS:		<input type="text" value="3000"/>	<input type="text" value="443"/>	
VLANs	HTTPS (X.509) Certificate				
Security	Import Xirrus Authority Into Browser:	xirrus-ca.crt			
Admin Management	Admin RADIUS	Certificate Signed By:	Xirrus		
Management Control	External Certification Authority				
Access Control List	Download Certificate Signing Request	XN0414091C548.csr			
Global Settings	Upload Signed Certificate:	<input type="text"/>	<input type="button" value="Browse..."/>	<input type="button" value="Upload"/>	
External Radius	Common Name:	XN0414091C548			
Internal Radius	Organization Name:	<input type="text"/>			
Rogue Control List	Organizational Unit Name:	<input type="text"/>			
SSIDs	Locality (City):	<input type="text"/>			
Groups	State or Province:	<input type="text"/>			
IAPs	Country Name (2 Letter Code):	<input type="text"/>			
WDS	Email Address:	<input type="text"/>			
Filters	Create New Certificate Signing Request	<input type="button" value="Create"/>			

4. Create a Deny List. Select **Configuration>Security>Access Control List**.

Status	Name: XN0414091C548 (10.36.1.111)			Location: CUMULUNIMBUS	Uptime: 0 days, 2 hours, 19 mins
Array	Access Control List Type: <input type="radio"/> Disabled <input type="radio"/> Allow List <input checked="" type="radio"/> <u>Deny List</u>				
Network	MAC Address				Delete
RF Monitor	<input type="text"/>				
Stations	<input type="button" value="Clear All"/>				
Statistics	<input type="button" value="Apply"/>				
System Log	<input type="button" value="Save"/>				
Configuration					
Express Setup					
Network					
Services					
VLANs					
Security					
Admin Management					
Admin RADIUS					
Management Control					
Access Control List					
Global Settings					
External Radius					
Internal Radius					
Rogue Control List					
SSIDs					
Groups					
IAPs					
WDS					
Filters					

5. Save your changes.

Additional CounterACT Documentation

For information about other CounterACT features and modules, refer to the following resources:

- [Documentation Downloads](#)
- [Documentation Portal](#)
- [CounterACT Help Tools](#)

Documentation Downloads

Documentation downloads can be accessed from one of two ForeScout portals, depending on which licensing mode your deployment is using.

- **Per-Appliance Licensing Mode** - [Product Updates Portal](#)
- **Centralized Licensing Mode** - [Customer Portal](#)

 Software downloads are also available from these portals.

To learn which licensing mode your deployment is using, see [Identifying Your Licensing Mode in the Console](#).

Product Updates Portal

The Product Updates Portal provides links to CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. The portal also provides a variety of additional documentation.

To access the Product Updates Portal:

1. Go to <https://updates.forescout.com/support/index.php?url=counteract>.
2. Select the CounterACT version you want to discover.

Customer Portal


The Downloads page on the ForeScout Customer Portal provides links to purchased CounterACT version releases, Base and Content Modules, and Extended Modules, as well as related documentation. Software and related documentation will only appear on the Downloads page if you have a license entitlement for the software. The Documentation page on the portal provides a variety of additional documentation.

To access documentation on the ForeScout Customer Portal:

1. Go to <https://forescout.force.com/support/>.
2. Select **Downloads** or **Documentation**.

Documentation Portal

The ForeScout Documentation Portal is a searchable, web-based library containing information about CounterACT tools, features, functionality and integrations.

 If your deployment is using Centralized Licensing Mode, you may not have credentials to access this portal.

To access the Documentation Portal:

1. Go to www.forescout.com/docportal.
2. Use your customer support credentials to log in.
3. Select the CounterACT version you want to discover.

CounterACT Help Tools

Access information directly from the CounterACT Console.

Console Help Buttons

Use context sensitive *Help* buttons to quickly access information about the tasks and topics you are working with.

CounterACT Administration Guide

Select **CounterACT Help** from the **Help** menu.

Plugin Help Files

1. After the plugin is installed, select **Options** from the **Tools** menu and then select **Modules**.
2. Select the plugin and then select **Help**.

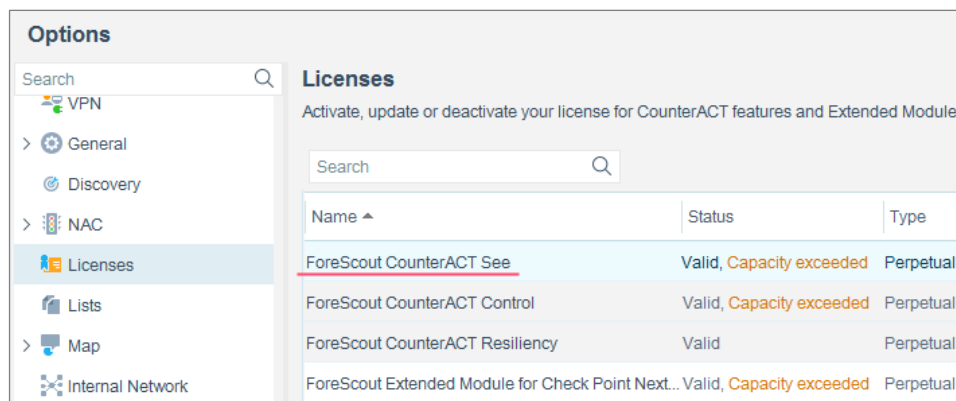
Documentation Portal

Select **Documentation Portal** from the **Help** menu.

Identifying Your Licensing Mode in the Console

If your Enterprise Manager has a *ForeScout CounterACT See* license listed in the Console, your deployment is operating in Centralized Licensing Mode. If not, your deployment is operating in Per-Appliance Licensing Mode.

Select **Options** > **Licenses** to see whether you have a *ForeScout CounterACT See* license listed in the table.



The screenshot shows the 'Options' menu with 'Licenses' selected. The 'Licenses' section displays a table with the following data:

Name	Status	Type
ForeScout CounterACT See	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Control	Valid, Capacity exceeded	Perpetual
ForeScout CounterACT Resiliency	Valid	Perpetual
ForeScout Extended Module for Check Point Next...	Valid, Capacity exceeded	Perpetual

Contact your ForeScout representative if you have any questions about identifying your licensing mode.

Legal Notice

© 2018 ForeScout Technologies, Inc. All rights reserved. ForeScout Technologies, Inc. is a Delaware corporation. A list of our trademarks and patents can be found at <https://www.forescout.com/company/legal/intellectual-property-patents-trademarks>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-15 13:42