

CounterACT[®] Wireless Plugin Integration with Cisco Wireless Management Configuration Guide

Version 1.5.1



Table of Contents

About the Plugin and Cisco Configuration	
Requirements	3
Configuration	4
Cisco Controller Configuration	4
Cisco Aironet Access Point Configuration	7
MIBs Used by the Wireless Plugin	9
Cisco Controller MIBs	
Cisco Aironet Access Point MIBs	
Notification Trap MIBs Received by the Plugin	10
Additional CounterACT Documentation	10
Documentation Downloads	
Documentation Portal	
Counteract Heip Tools	

About the Plugin and Cisco Configuration

This document describes how to configure Cisco wireless controllers and access points (wireless management devices) 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
- Blocking wireless endpoints from the organizational network

Policies	Matched Unmatched Pending Irresolvable Hide (Offline Filtered by 🖧 Wireless Cisco 💌 Hosts: 1
Guest policy_TEST_6.3.1	Host IP Segment Policy Wireles MAC addres Connect	tivity Type Wireless Mireless Ac Wireless Ho Wi Wi
- D C LINUX (0)	10.33.1.103 10.33.1.140 🔳 Wireless 001/31354	res Ciscuairon Ciscuairon
E INUX/MAC Asset Classi	Wireless tests All policies Host info	
— 🔟 Mac - Nmap (0)	IP Address: 10.33.1.103 Domain User: administrator NetBIOS Hostnar	me: IT-LOANER-EN MAC
Mac Update (0)	Policy, Wireless tests. Status: Match. Since: October 06 02:41:33 PM	
- 🖸 📉 MACCC (0)	Match Main Rule	
– 🔟 Policy Mac_Li	B Condition Properties: Wireless Host SSID: CiscoaironetSSIL	
- D SWITCH (C	itch Main Rule	
- D & VPN (0)		214 214 2000
🚽 🗩 🛞 🗰 🖉 🚽 🚽	tion Properties: Wireless Host SSID:	CiscoAironetSSID
VA Scans	Wireless Controller IP:	10.33.1.240
History	Wireless Host Authentication	n: None
Filtore	Wireless Vendor:	aironet
All	MAC address:	00173f354507
🖨 🥶 Segments		
	Wireless Access Point Name	e: CiscoAironet.domain
		energies constraint of space of the second states o

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

Requirements

- Cisco controller with software 5.0.148.0 or higher
- Cisco Aironet access point with software version 12.4(10b) or higher
- Network Module version 1.0 or above with the following components running:
 - Wireless Plugin,
 - Switch Plugin (To work with notification traps).
- CounterACT version 8.0

Configuration

Cisco Controller Configuration

You should perform the following Cisco controller configuration steps in order to work with the Wireless Plugin. SNMP Configuration can be used for both read and write access.

To configure a Cisco controller:

- 1. Log into the Cisco controller.
- 2. Select Management>SNMP>General.

				Sa <u>v</u> e Con	figuration <u>P</u> in	g Logo	ut <u>R</u> efresh
CISCO MONITOR WLAI	Ns <u>C</u> ONTROLLER	W <u>I</u> RELESS	<u>S</u> ECURITY	- M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Management	SNMP System	Summary	,			A	Apply
Summary SNMP General SNMP V3 Users Communities Trap Receivers Trap Controls	Name Location Contact System Descriptio	on Ci	CiscoControlle	r			
Trap Logs HTTP	System Object ID	1.	3.6.1.4.1.9.1.82	28			
Telnet-SSH	SNMP Port Numbe	er	161				
Serial Port	Trap Port Number	r	162				
Local Management Users	SNMP v1 Mode		Disable 💌				
User Sessions	SNMP v2c Mode		Enable 💌				
Logs	SNMP v3 Mode		Disable 💌				
Mgmt Via Wireless							
Tech Support							

- 3. Enable the SNMP version that you want to use and select Apply.
- If you are using notification traps, you must use SNMPv1 or SNMPv2c—the same SNMP parameters are used for the traps and the plugin does not yet support SNMPv3 in this case.
- 4. (SNMPv1 or SNMPv2c) Select Management>SNMP>Communities.

ahaha						Sa <u>v</u> e Cor	nfiguration <u>P</u> in	g Lo <u>q</u> o	ut <u>R</u> efresh
cisco		<u>W</u> LANs	<u>C</u> ONTROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HELP	<u>F</u> EEDBACK
Management	SN	MP v1 / v	2c Communi	ty				N	ew
Summary									
▼ SNMP	Co	nmunity Na	me	IP Addres	is IP M	lask Ac	cess Mode	Status	
General	tes	ter		0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
Communities	tes	<u>:1</u>		0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
Trap Receivers	fore	scout		0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
Trap Logs	a			0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
нттр	net			0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
Telnet-SSH	fibe	<u>r</u>		0.0.0.0	0.0.0	0.0 Re	ad-Write	Enable	
Serial Port	-								

- Select **New**. The SNMP v1 / v2c Community > New pane opens.

SNMP v1 / v2c C	community > New	< Back	Apply
Community Name			
IP Address			
IP Mask			
Access Mode	Read/Write 💌		
Status	Enable 💌		

- Enter Community parameters. Verify that Access Mode is set to Read/Write and that Status is Enabled. The values for IP Address and IP Mask should enable access from the CounterACT device.
- Select Apply.
- 5. (SNMPv3) Select Management>SNMP>SNMP V3 Users.

սիսիս						Sa <u>v</u> e Co	nfiguration <u>P</u> ir	ig Logi	out <u>R</u> efresh
CISCO MONITOR	<u>w</u> L	ANS <u>C</u> ONTE	ROLLER	WIRELESS	<u>S</u> ECURITY	M <u>A</u> NAGEMENT	C <u>O</u> MMANDS	HE <u>L</u> P	<u>F</u> EEDBACK
Management	-	SNMP V3	Users	6					New
Summary									
▼ SNMP		User Name		Access Level	Auth Pro	tocol Privac	y Protocol		
General		Dannymd		Readwrite	HMAC-MD	5 None			
Communities		Dannysha		Readwrite	HMAC-SH	A None			
Trap Receivers Trap Controls		Dannymdae	s	Readwrite	HMAC-MD	5 AES			
Trap Logs		Dannymdde	s	Readwrite	HMAC-MD	5 DES			
нттр		Dannyshaa	es	Readwrite	HMAC-SH	A AES			
Telnet-SSH		Dannyshad	es	Readwrite	HMAC-SH	A DES			
Serial Port	•								

- Select **New**. The SNMP V3 Users > New pane opens.

SNMP V3 Users > N	lew	< Back Apply
User Profile Name		
Access Mode	Read Write 💌	
Authentication Protocol	HMAC-SHA 💌	
Privacy Protocol	Auth Password CFB-AES-128	Confirm Auth Password
	Priv Password	Confirm Priv Password

- Enter SNMPv3 parameters and select Read Write from the Access Mode dropdown list.
- Select Apply.

Cisco Aironet Access Point Configuration

You should perform the following Cisco access point configuration steps in order to work with the plugin.

To configure a Cisco access point:

- **1.** Log into the Cisco Aironet access point.
- 2. Configure read parameters: Select Services>SNMP.
- Select **Enable** from the SNMP Properties section.

ahaha		
CISCO	Cisco Aironet 1	240AG Series Access Point
HOME	Hostname CiscoAironet	CiscoAironet uptime is 11 hours, 39 minutes
EXPRESS SET-UP		
EXPRESS SECURITY	Services: SNMP- Simple Netw	ork Management Protocol
NETWORK MAP +	Services, sharry simple netw	
ASSOCIATION +	SNMP Properties	
NETWORK INTERFACES +		
SECURITY +	Simple Network Managemen	t Protocol (SNMP): Enable Disable
SERVICES		
Telnet/SSH		
Hot Standby	System Description:	Cisco Access Point 12.4
CDP		
DNS		
Filters	System Name (optional):	FTX1233B2TZ
HTTP		
QoS	System Location (optional):	4X6PU
STREAM		
SNMP	System Contact (optional):	4X6PU
SNTP		
VLAN		
ARP Caching		Apply Cancel
WIRELESS SERVICES +		

- Select **Apply**.
- In the **SNMP Request Communities** section, enter a community string and select **Read-Only**.

SNMP Request Communities			
Current Community Strings		New/Edit Community Strings	
< NEW >		SNMD Community	[]
Torescout	Delete	Object Identifier (optional):	
			Read-Only C Read-Write
			Apply Cancel

- Select Apply.
- 6. Configure write parameters: Select Services>Telnet/SSH.
 - Verify that **Telnet** or **SSH** is enabled.

ME	Hostname CiscoAironet	CiscoAironet uptime is 11 hours, 47 r
PRESS SET-UP		
PRESS SECURITY	Services: Telnet/SSH	
TWORK MAP +	Services. Tellieu Soft	
SOCIATION +	Telnet:	Enable O Disable
TWORK INTERFACES +		
CURITY +		
RVICES	Terminal Type:	Teletype C ANSI
ot Standhy		
	Columns:	80 (64-132)
NS		04 (0.510)
ilters	_ Lines:	24 (0-512)
TTP	Secure Shell Configuration	
oS	secure shell configuration	
TREAM	Secure Shell:	Enable Disable
NMP		
NTP		
LAN	System Name:	CiscoAironet
RP Caching	Domain Nama	dense in
RELESS SERVICES +	Domain Name.	domain
STEM SOFTWARE +	RSA Key Size (optional):	•••• (360-2048 bits)
ENFLOG T	Authentication Timeout (option	onal): 120 (1-120 sec)

- Select Apply.
- 7. View blocked host: Select Filters>MAC Addresses Filters.
 - Verify that **Filter Index** is *not* 770. If you define the filter index using this number you will block the CounterACT access list.

cisco	Cisco Aironet 1240AG Series Access Point
HOME	
EXPRESS SET-UP EXPRESS SECURITY	Hostname CiscoAironet uptime is 12 hours, 2 minutes
NETWORK MAP + ASSOCIATION + NETWORK INTERFACES +	Services: Filters - MAC Address Filters
SECURITY + SERVICES	Create/Edit Filter Index: < NEW >
Telnet/SSH Hot Standby CDP	- Filter Index: (700-799)
DNS Filters HTTP QoS	Add MAC Address: Mask: 0000.0000 Action: Forward Add (HIHH, HIHH, HIHH) (HIHH, HIHH, HIHH)
STREAM SNMP SNTP VLAN	Default Action: Block All
ARP Caching WIRELESS SERVICES +	Filters Classes:
EVENT LOG +	1
	Delete Class

MIBs Used by the Wireless Plugin

The following (read-only) MIBs are used by the Wireless Plugin for Cisco controllers and Cisco Aironet access points:

- OID_SYSTEM_UPTIME: 1.3.6.1.2.1.1.3.0 (system.sysUpTime.0)
- CISCO_OID_MOBILE_CLIENT_SSID_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.7 (bsnMobileStationSsid)
- CISCO_OID_MOBILE_CLIENT_IP_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.2 (bsnMobileStationIpAddress)
- CISCO_OID_MOBILE_CLIENT_AP_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.4 (bsnMobileStationAPMacAddr)
- CISCO_OID_MOBILE_CLIENT_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.1 (bsnMobileStationMacAddress)
- CISCO_OID_MOBILE_CLIENT_AUTH_TYPE_ENTRY: 1.3.6.1.4.1.14179.2.1.4.1.30 (bsnMobileStationPolicyType)
- CISCO_OID_MOBILE_RSS_AP_MAC_ENTRY: 1.3.6.1.4.1.14179.2.1.11.1.1 (bsnMobileStationRssiDataEntry)
- CISCO_OID_MOBILE_RSS_AP_NAME_ENTRY: 1.3.6.1.4.1.14179.2.1.11.1.4 (bsnMobileStationRssiDataEntry)

Cisco Controller MIBs

To block endpoints, the Wireless Plugin must have read permissions for the following two MIBs:

- CISCO_OID_BLACKLIST_CLIENT_ROW_STATUS: 1.3.6.1.4.1.14179.2.5.6.1.22.12 (bsnBlackListClientRowStatus)
- CISCO_OID_BLACKLIST_CLIENT_MESSAGE: 1.3.6.1.4.1.14179.2.5.6.1.2.12 (bsnBlackListClient)

Cisco Aironet Access Point MIBs

The Cisco Aironet access point uses another three (read-only) MIBs:

- AIRONET_OID_ARP: 1.3.6.1.2.1.4.22.1.2
- AIRONET_OID_CLIENTS_TABLE: 1.3.6.1.4.1.9.9.273.1.2.1.1
- AIRONET_AP_NAME: 1.3.6.1.2.1.1.5.0

Notification Trap MIBs Received by the Plugin

The following MIBs may be received from a Cisco controller when

- 1.3.6.1.4.1.9.9.599.1.3.1.1.1.0: The endpoint IP address
- 1.3.6.1.4.1.9.9.599.1.3.1.1.10.0: The endpoint MAC address
- 1.3.6.1.4.1.9.9.513.1.1.1.5.0: The AP name
- 1.3.6.1.4.1.14179.2.2.1.1.3.0: The AP name
- 1.3.6.1.4.1.9.9.599.1.2.2.0: The SSID
- 1.3.6.1.4.1.14179.2.6.2.34.0: The endpoint IP address
- 1.3.6.1.4.1.14179.2.6.2.43.0: The endpoint IP address
- 1.3.6.1.4.1.9.9.599.0.4: Indicates that the client is connected
- 1.3.6.1.4.1.14179.2.6.3.2: Indicates that the client is disconnected

Additional CounterACT Documentation

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

- Documentation Downloads
- <u>Documentation Portal</u>
- <u>CounterACT Help Tools</u>

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 <u>Identifying Your</u> <u>Licensing Mode in the Console</u>.

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 <u>www.forescout.com/docportal</u>.
- 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.

Options			
Search	Q	Licenses Activate, update or deactivate your license for CounterACT features and Ext Search Q	ended Module
> 10 NAC		Name A Status	Туре
15 Licenses		ForeScout CounterACT See Valid, Capacity exceed	ed Perpetual
Lists		ForeScout CounterACT Control Valid, Capacity exceed	ed Perpetual
> 🥊 Map		ForeScout CounterACT Resiliency Valid	Perpetual
K Internal Network		ForeScout Extended Module for Check Point Next Valid, Capacity exceed	ed 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 <u>https://www.forescout.com/company/legal/intellectual-property-patents-trademarks</u>. Other brands, products, or service names may be trademarks or service marks of their respective owners.

2018-04-15 13:34