DEPLOYMENT GUIDE

Ruckus ICX with Cisco ISE CWA Deployment Guide

Cisco ISE Integration with a Ruckus ICX Switch for Web Authentication Guest Access NAC Solution

Part Number: 53-1005286-02
Publication Date: 20 May 2019

Copyright, Trademark and Proprietary Rights Information

Export Restrictions

These products and associated technical data (in print or electronic form) may be subject to export control laws of the United States of America. It is your responsibility to determine the applicable regulations and to comply with them. The following notice is applicable for all products or technology subject to export control:

These items are controlled by the U.S. Government and authorized for export only to the country of ultimate destination for use by the ultimate consignee or end-user(s) herein identified. They may not be resold, transferred, or otherwise disposed of, to any other country or to any person other than the authorized ultimate consignee or end-user(s), either in their original form or after being incorporated into other items, without first obtaining approval from the U.S. government or as otherwise authorized by U.S. law and regulations.

Disclaimer

THIS CONTENT AND ASSOCIATED PRODUCTS OR SERVICES ("MATERIALS"), ARE PROVIDED "AS IS" AND WITHOUT WARRANTIES OF ANY KIND, WHETHER EXPRESS OR IMPLIED. TO THE FULLEST EXTENT PERMISSIBLE PURSUANT TO APPLICABLE LAW, ARRIS DISCLAIMS ALL WARRANTIES, EXPRESS OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE, TITLE, NON-INFRINGEMENT, FREEDOM FROM COMPUTER VIRUS, AND WARRANTIES ARISING FROM COURSE OF DEALING OR COURSE OF PERFORMANCE. ARRIS does not represent or warrant that the functions described or contained in the Materials will be uninterrupted or error-free, that defects will be corrected, or are free of viruses or other harmful components. ARRIS does not make any warranties or representations regarding the use of the Materials in terms of their completeness, correctness, accuracy, adequacy, usefulness, timeliness, reliability or otherwise. As a condition of your use of the Materials, you warrant to ARRIS that you will not make use thereof for any purpose that is unlawful or prohibited by their associated terms of use.

Limitation of Liability

IN NO EVENT SHALL ARRIS, ARRIS AFFILIATES, OR THEIR OFFICERS, DIRECTORS, EMPLOYEES, AGENTS, SUPPLIERS, LICENSORS AND THIRD PARTY PARTNERS, BE LIABLE FOR ANY DIRECT, INDIRECT, SPECIAL, PUNITIVE, INCIDENTAL, EXEMPLARY OR CONSEQUENTIAL DAMAGES, OR ANY DAMAGES WHATSOEVER, EVEN IF ARRIS HAS BEEN PREVIOUSLY ADVISED OF THE POSSIBILITY OF SUCH DAMAGES, WHETHER IN AN ACTION UNDER CONTRACT, TORT, OR ANY OTHER THEORY ARISING FROM YOUR ACCESS TO, OR USE OF, THE MATERIALS. Because some jurisdictions do not allow limitations on how long an implied warranty lasts, or the exclusion or limitation of liability for consequential or incidental damages, some of the above limitations may not apply to you.

Trademarks

ARRIS, the ARRIS logo, Ruckus, Ruckus Wireless, Ruckus Networks, Ruckus logo, the Big Dog design, BeamFlex, ChannelFly, EdgeIron, FastIron, HyperEdge, ICX, IronPoint, OPENG, SmartCell, Unleashed, Xclaim, ZoneFlex are trademarks of ARRIS International plc and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access (WPA), the Wi-Fi Protected Setup logo, and WMM are registered trademarks of Wi-Fi Alliance. Wi-Fi Protected Setup™, Wi-Fi Multimedia™, and WPA2™ are trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Preface

Introduction

This document describes how to configure central web authentication (CWA) with wired clients connected to a Ruckus ICX switch with the help of the Cisco Identity Services Engine (ISE). The details of a Cisco ISE configuration and the Ruckus ICX switch configuration are shown. Central web authentication offers the possibility of a central device that acts as a web portal (in this case, Cisco ISE). Globally, if the MAC address of the client station is not known by the RADIUS server, the switch authorizes the station (by way of MAC authentication) and then redirects the HTTP traffic to the web portal. Once a user logs in to the guest portal, it is possible by way of Change of Authorization (CoA) to bounce the switch port so that a new Layer 2 MAC authentication occurs. Cisco ISE remembers the user is a web authentication user and applies Layer 2 attributes (such as dynamic VLAN assignment) to the user. The IP address of the client PC is refreshed as well.

This guide offers only the instructions to configure external web authentication using Cisco ISE. For other Ruckus-supported flexible authentication use cases, refer to other Ruckus flexible authentication deployment guides.

Purpose of This Document

The purpose of this deployment guide is to provide an understanding of the Cisco ISE CWA flow and the steps required to configure and deploy it with a Ruckus ICX switch for web guest authentication. This guide describes the following:

- Cisco ISE configuration for CWA
- Ruckus ICX switch configuration
- Sample Ruckus Network Access Device (NAD) profile

The information in this document is based on the following software and hardware versions:

- Cisco Identity Services Engine (ISE), Release 2.1.0
- Ruckus ICX switch running FastIron 08.0.70

Audience

This document can be used by technical marketing engineers, system engineers, technical assistance center engineers, and customers to deploy a Ruckus ICX switch with Cisco ISE.

Related Documents

- *Ruckus FastIron Security Configuration Guide, 08.0.70*

  http://docs.ruckuswireless.com/fastiron/08.0.70/fastiron-08070-securityguide/GUID-15DD872A-E999-4D90-9CB4-C89733A0493B-homepage.html

Document History

Date	Part Number	Description
October 19, 2017	53-1005286-01	Initial release.
May 20, 2019	53-1005286-02	Updated the document with ICX 08.0.70 and with ISE policy configuration change. The updated ISE policy change has been tested with both ISE 2.1 and 2.4.

Overview

Switch Configuration

The Ruckus ICX switch must be configured with MAC authentication, external web authentication, RADIUS, and CoA in order for CWA to work.

1. Configure RADIUS on the ICX switch.

```
aaa authentication dot1x default radius
aaa authorization coa enable
aaa accounting mac-auth default start-stop radius
radius-client coa host <CiscoISE_ip> key <shared_secret>
radius-server host <CiscoISE_ip> auth-port 1645 acct-port 1646 default key <shared_ secret> mac-auth
```

2. Configure global MAC authentication on the ICX switch.

```
authentication
 auth-default-vlan <temporary_auth_vlan>
 mac-authentication enable
 mac-authentication enable ethe 1/1/47
```

3. Configure external web authentication on the ICX switch.

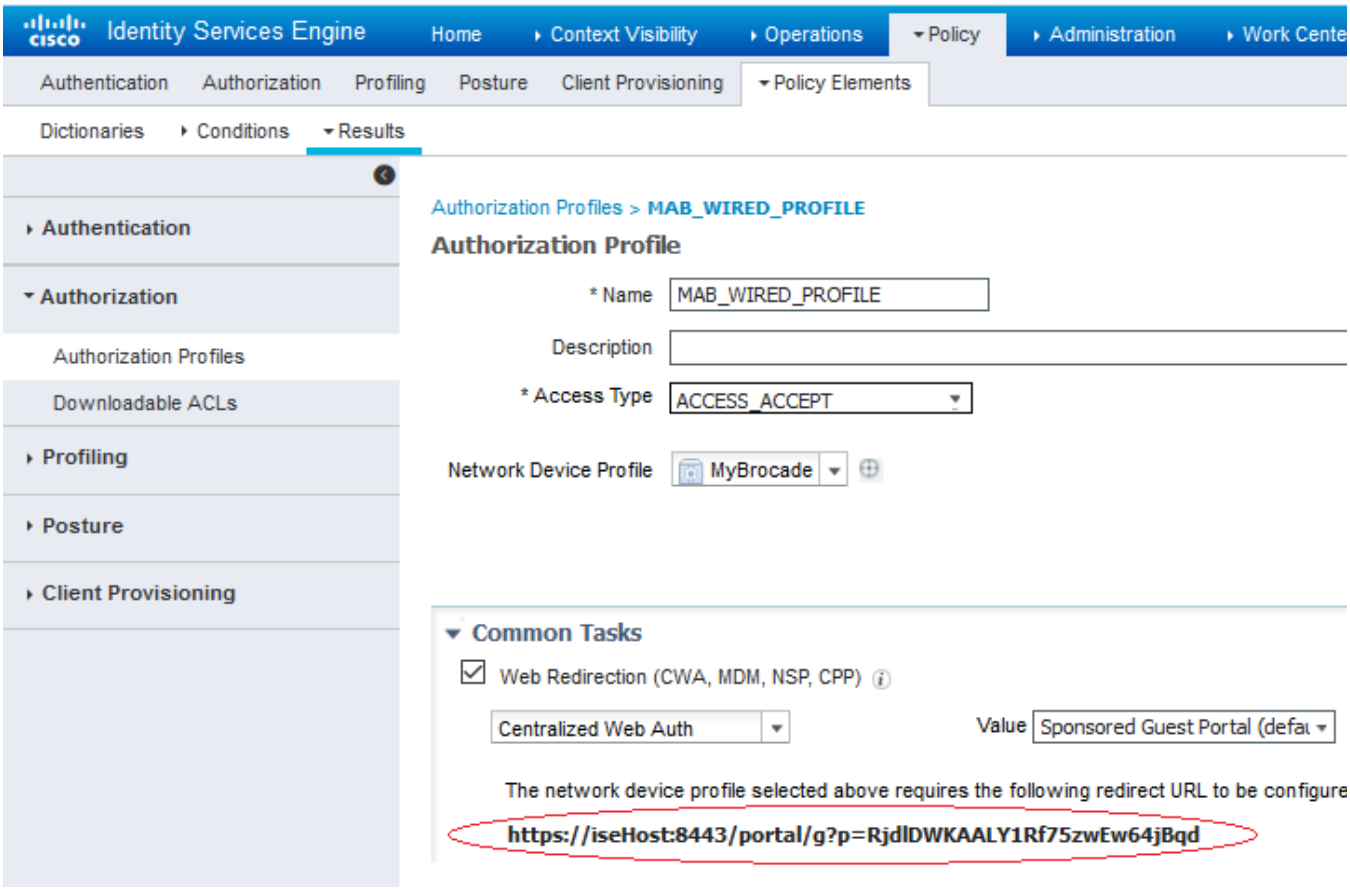
```
captive-portal brocade
  virtual-ip <CiscoISE_domain_name>
  virtual-port 8443
  login-page <CiscoISE_guest_portal>
.............
vlan <temporary_auth_vlan> name <temporary_auth_vlan_name> by port
.............
vlan <temporary_guest_vlan> name <temporary_guest_vlan_name> by port
webauth
  captive-portal profile brocade
  auth-mode captive-portal
  trust-port ethernet 1/1/1 <-- uplink port
  enable
.............
vlan <final_guest_vlan> name <final_guest_vlan_name> by port
...........
web-management https
```

ISE Configuration

Cisco ISE configuration consists of creating an authorization profile, creating an authentication rule, and creating an authorization rule with two policies.

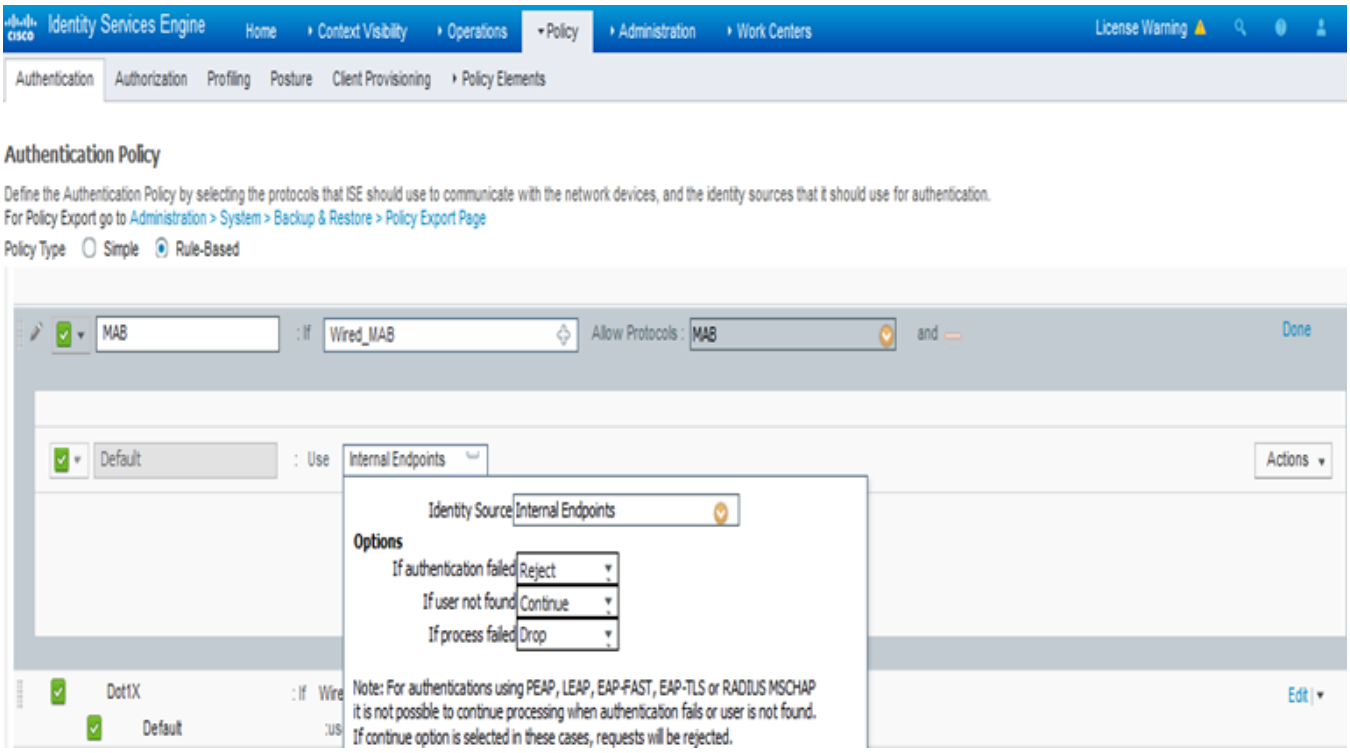
1. Create an authorization profile. Cisco ISE generates a link to access its web portal. The web link must be copied to the login page portion of the captive portal profile on the switch.

FIGURE 1 Cisco ISE Authorization Profile



2. Create an authentication rule to allow the flow with an unknown MAC address to continue rather than being dropped.

FIGURE 2 Cisco ISE Authentication Policy



3. Create an authorization rule with two policies. One policy is applied before web authentication so the user is moved to the temporary guest VLAN to perform web authentication. The other policy is applied after web authentication succeeds so the guest user is moved to the final guest VLAN.

FIGURE 3 Cisco ISE Authorization Rule with Two Policies

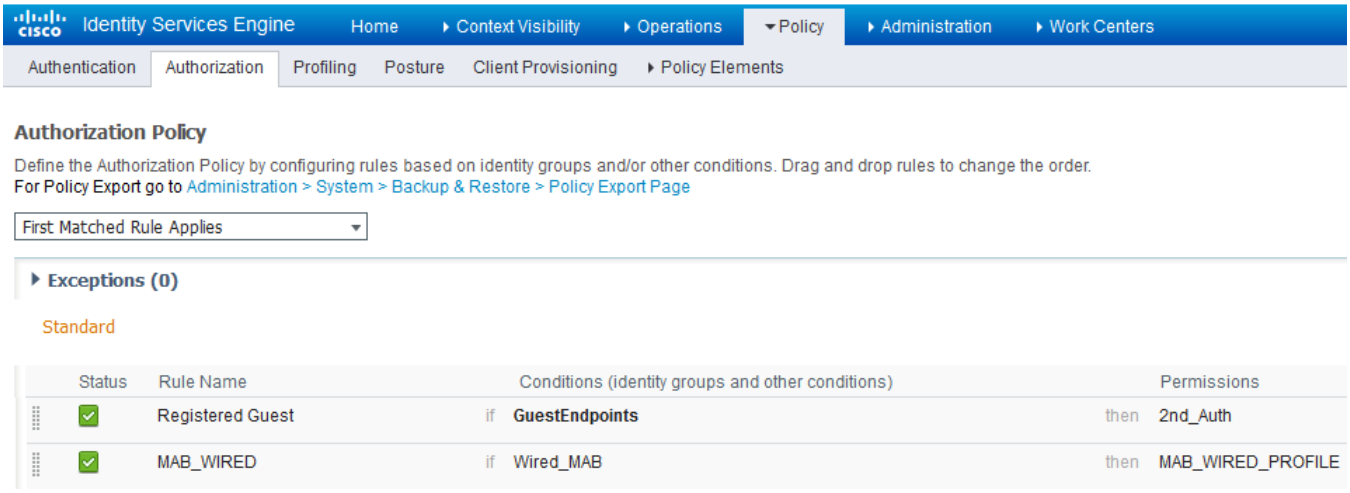


FIGURE 4 Cisco ISE Policy Before Web Authentication

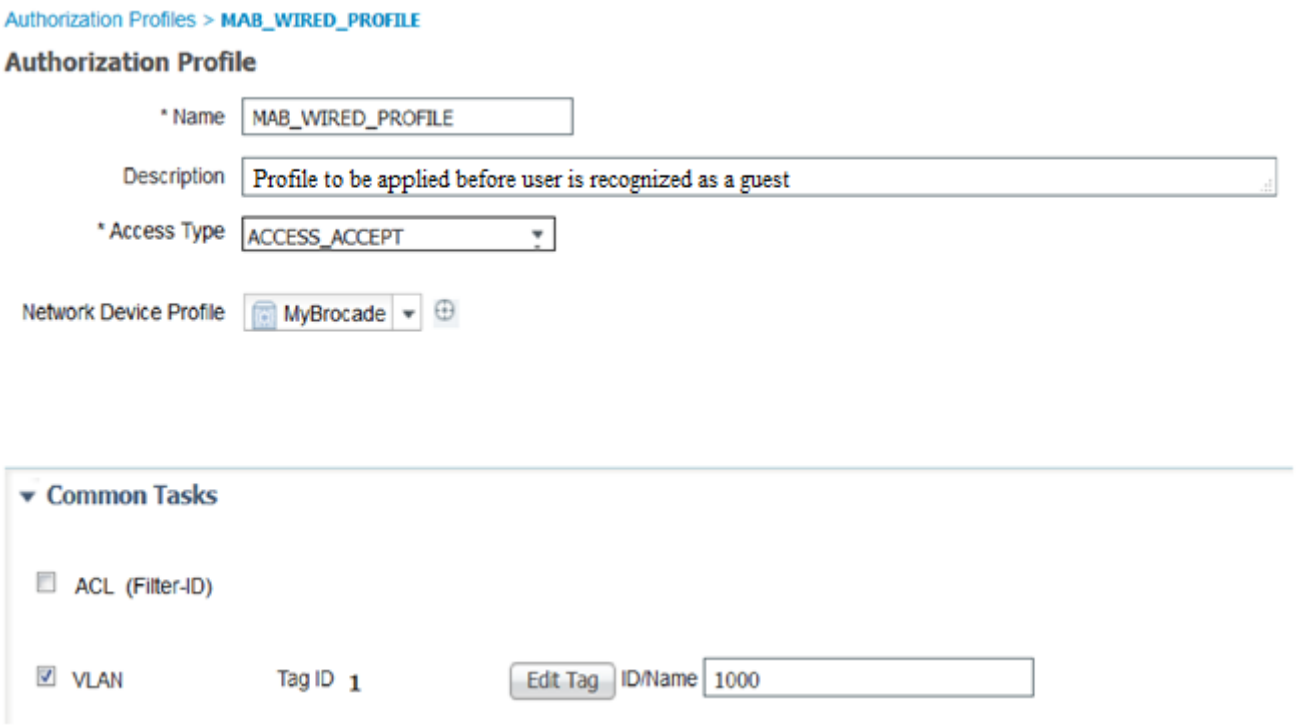
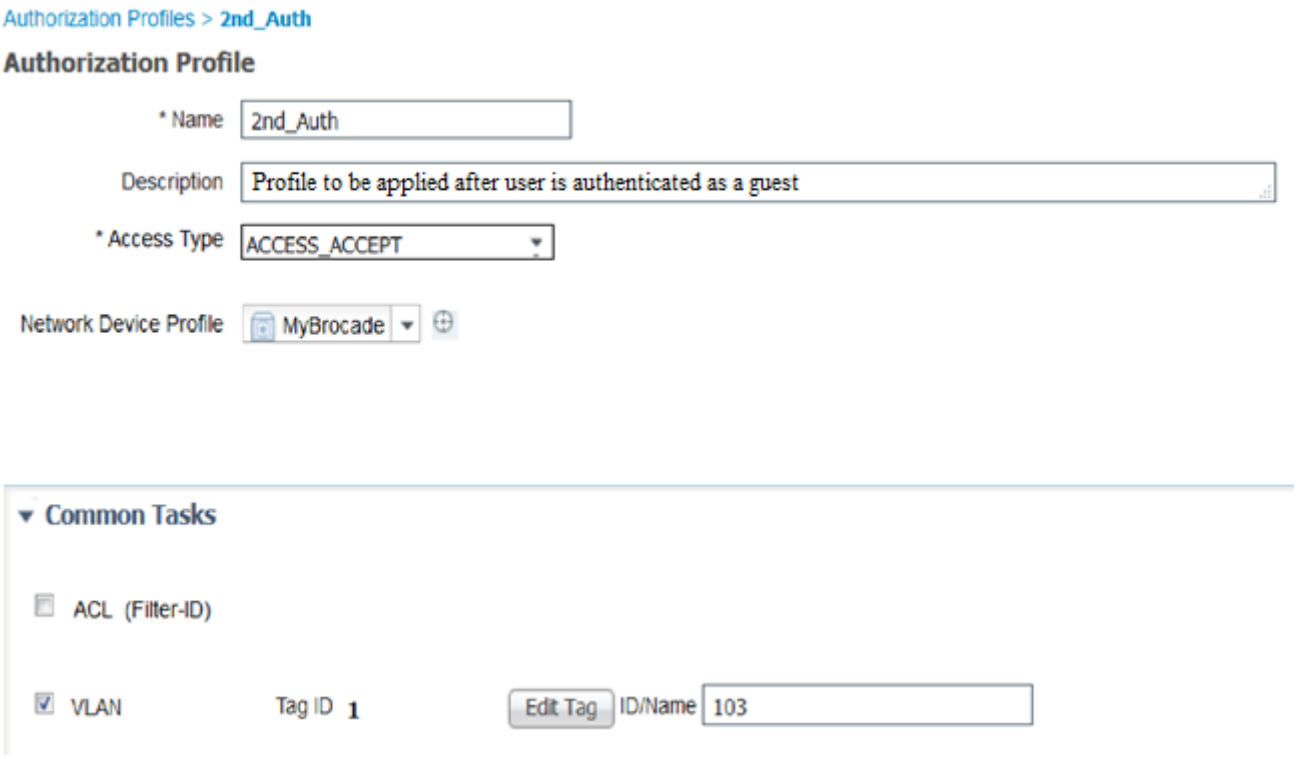


FIGURE 5 Cisco ISE Policy After Web Authentication



Sample CWA Flow

This section describes a sample CWA flow. First the client PC connects and performs MAC authentication. Because its MAC address is not known, Cisco ISE pushes the redirection attributes back to the switch. The user then opens a reachable website

and will be redirected to the Cisco ISE guest portal. After successful user login, the switch port connected to the client PC will be bounced and the user will be successfully authenticated.

1. The PC connects to the Ruckus ICX switch port.

   Once the link is connected, the PC will be authenticated by MAC authentication and the PC session will be placed in the correct VLAN. The CLI output for the Ruckus ICX switch shows the device MAC address, VLAN assignment, and state.

```
7250-U26#show mac-auth se all
------------------------------------------------------------------------------
Port    MAC             IP(v4/v6)          VLAN  Auth      ACL    Session   Age
        Addr            Addr                     State            Time
------------------------------------------------------------------------------
1/1/47  5cf3.fc4d.cc02  N/A                1000  Yes       None   5         S4
```

FIGURE 6 Output of Cisco ISE Authentication Process: Overview

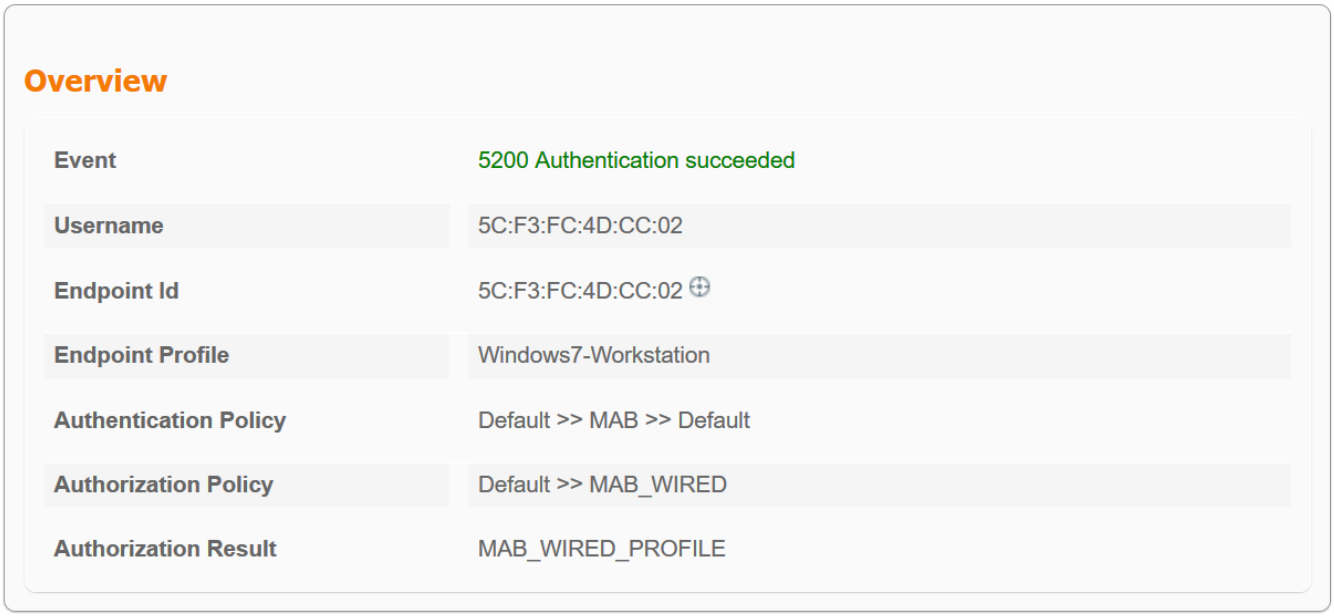


FIGURE 7 Output of Cisco ISE Authentication Process: Details

Authentication Details

Source Timestamp	2019-05-21 11:02:09.17
Received Timestamp	2019-05-21 11:02:09.171
Policy Server	CISCO-ISE
Event	5200 Authentication succeeded
Username	5C:F3:FC:4D:CC:02
User Type	Host
Endpoint Id	5C:F3:FC:4D:CC:02
Calling Station Id	5C-F3-FC-4D-CC-02
Endpoint Profile	Windows7-Workstation
Authentication Identity Store	Internal Endpoints
Identity Group	Workstation
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	7250-U26
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.176.178.41
NAS Port Id	1/1/47
NAS Port Type	Ethernet
Authorization Profile	MAB_WIRED_PROFILE
Response Time	17

FIGURE 8 Output of Cisco ISE Authentication Process: Result

2. The PC receives a valid IP address.

```
Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . : englab.brocade.com
   Link-local IPv6 Address . . . . . : fe80::212e:8966:85aa:b350%13
   IPv4 Address. . . . . . . . . . . : 10.176.178.42
   Subnet Mask . . . . . . . . . . . : 255.255.255.0
   Default Gateway . . . . . . . . . : 10.176.178.1
```

3. The PC user opens a web browser and is redirected to the Cisco ISE web guest portal.

FIGURE 9 Cisco ISE Web Guest Portal Sign-On

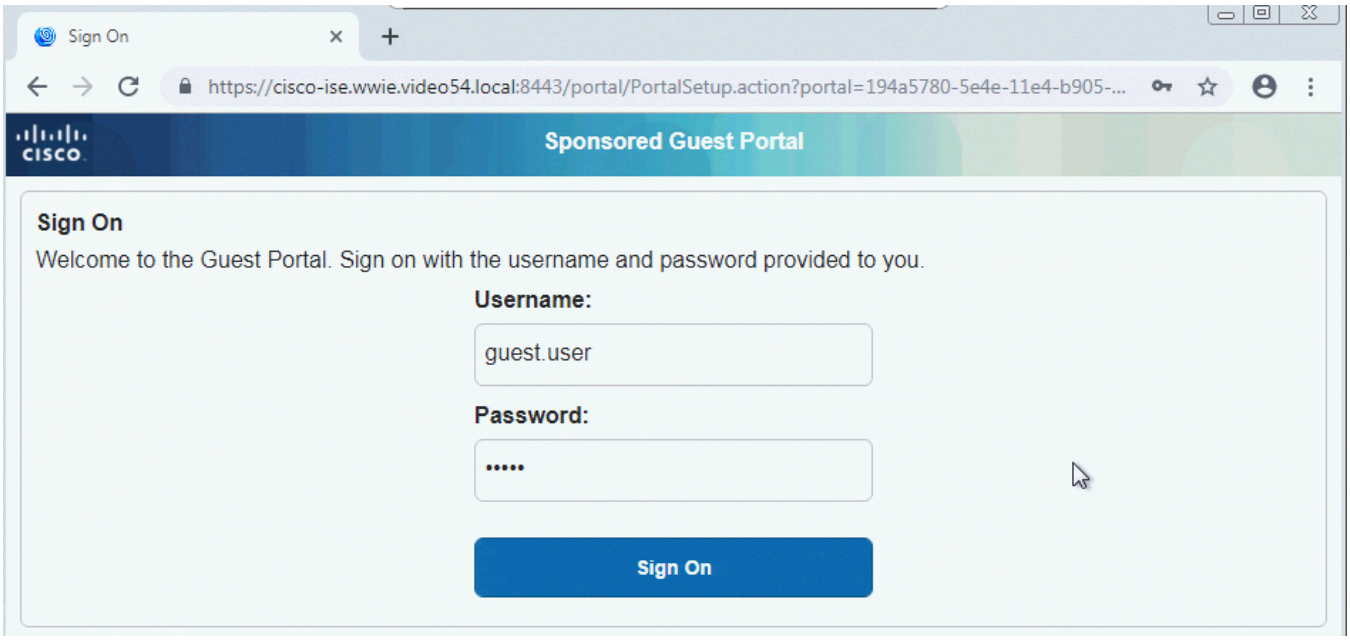


FIGURE 10 Cisco ISE Output: Overview

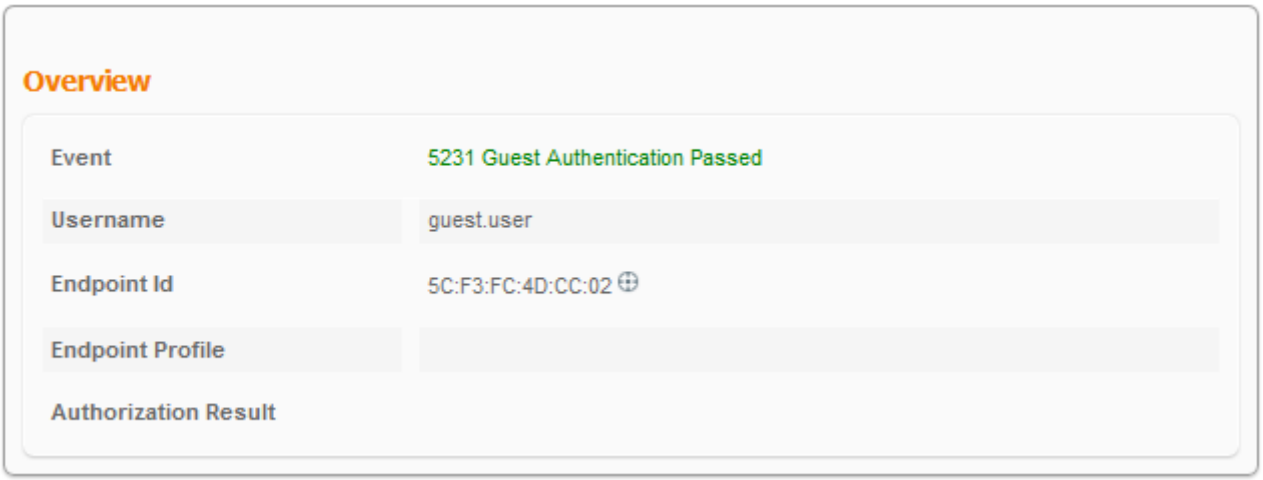
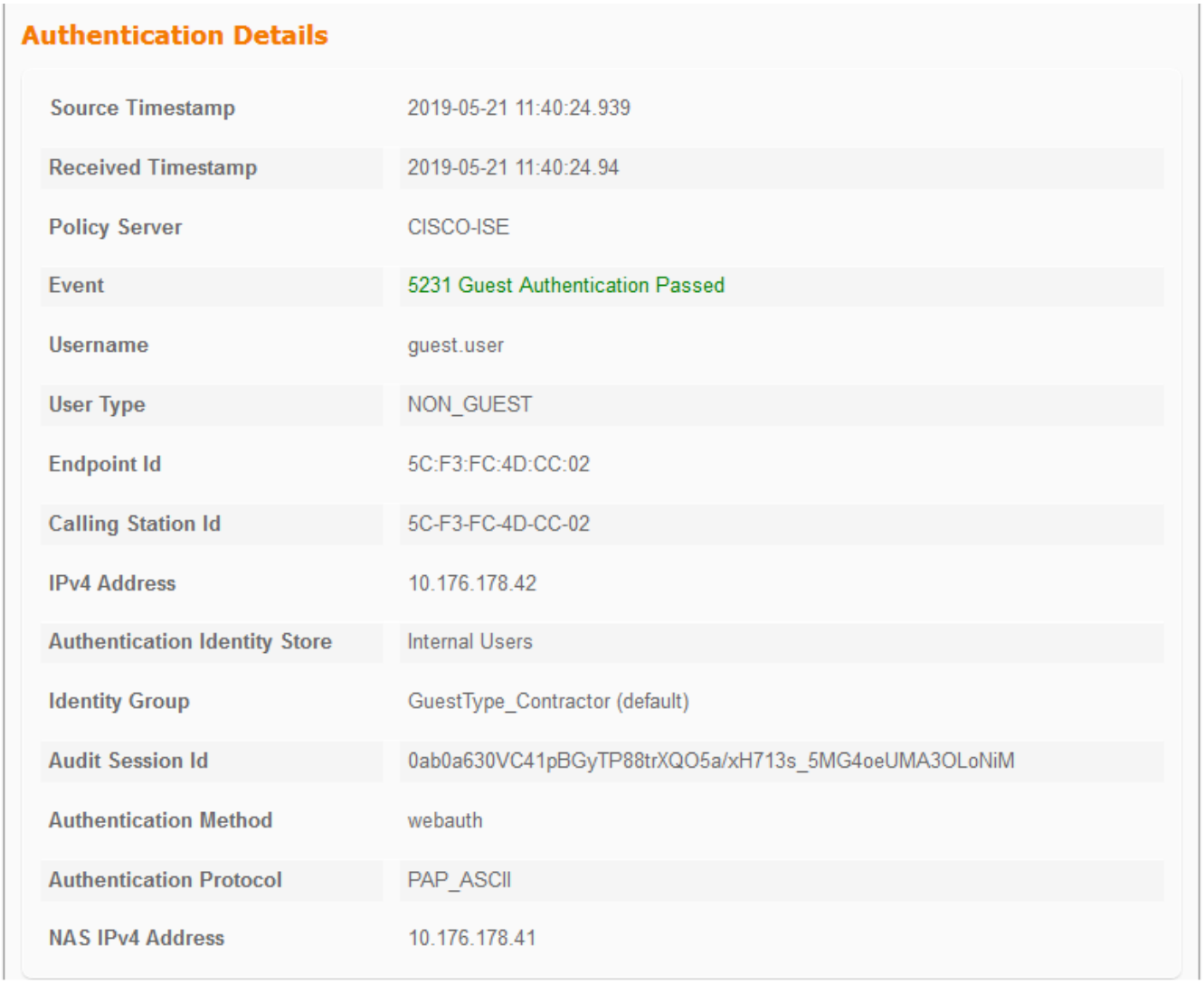


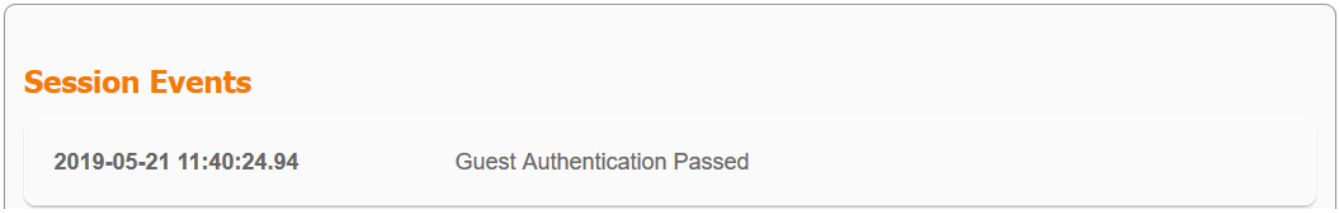
FIGURE 11 Cisco ISE Output: Authentication Details



Authentication Details

Source Timestamp	2019-05-21 11:40:24.939
Received Timestamp	2019-05-21 11:40:24.94
Policy Server	CISCO-ISE
Event	5231 Guest Authentication Passed
Username	guest.user
User Type	NON_GUEST
Endpoint Id	5C:F3:FC:4D:CC:02
Calling Station Id	5C-F3-FC-4D-CC-02
IPv4 Address	10.176.178.42
Authentication Identity Store	Internal Users
Identity Group	GuestType_Contractor (default)
Audit Session Id	0ab0a630VC41pBGyTP88trXQO5a/xH713s_5MG4oeUMA3OLoNiM
Authentication Method	webauth
Authentication Protocol	PAP_ASCII
NAS IPv4 Address	10.176.178.41

FIGURE 12 Cisco ISE Output: Session Events



Session Events

2019-05-21 11:40:24.94	Guest Authentication Passed

4. After web authentication, the switch port is disabled and then re-enabled.

   The following syslog message is received on the switch:

```
May 21 19:28:41:I:MAC-AUTH: CoA disabled and enabled (flip) the Port 1/1/47
```

FIGURE 13 Cisco ISE Output: Overview

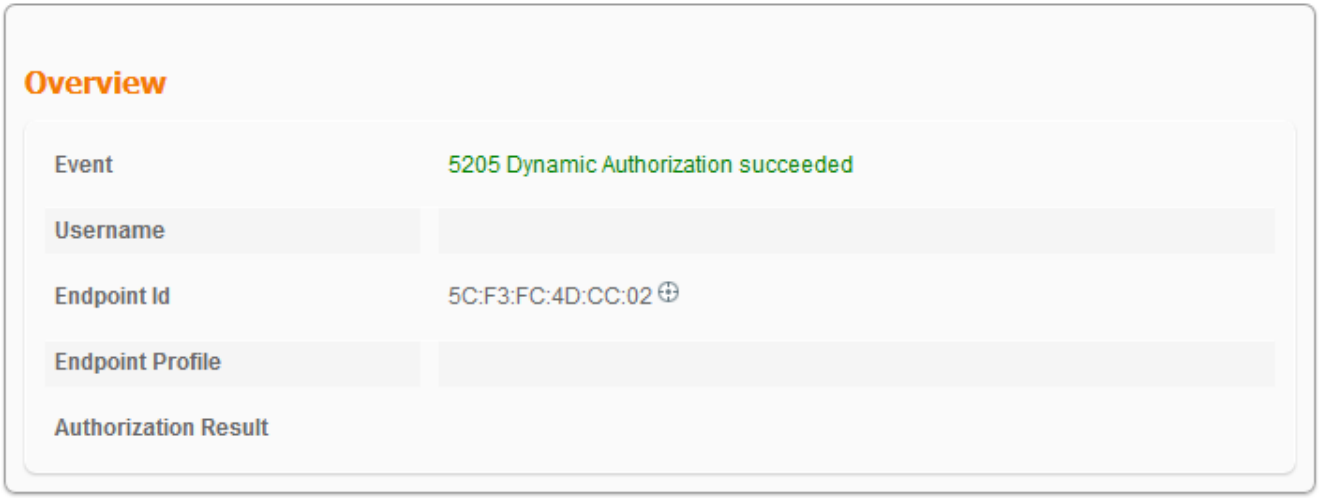


FIGURE 14 Cisco ISE Output: Authentication Details

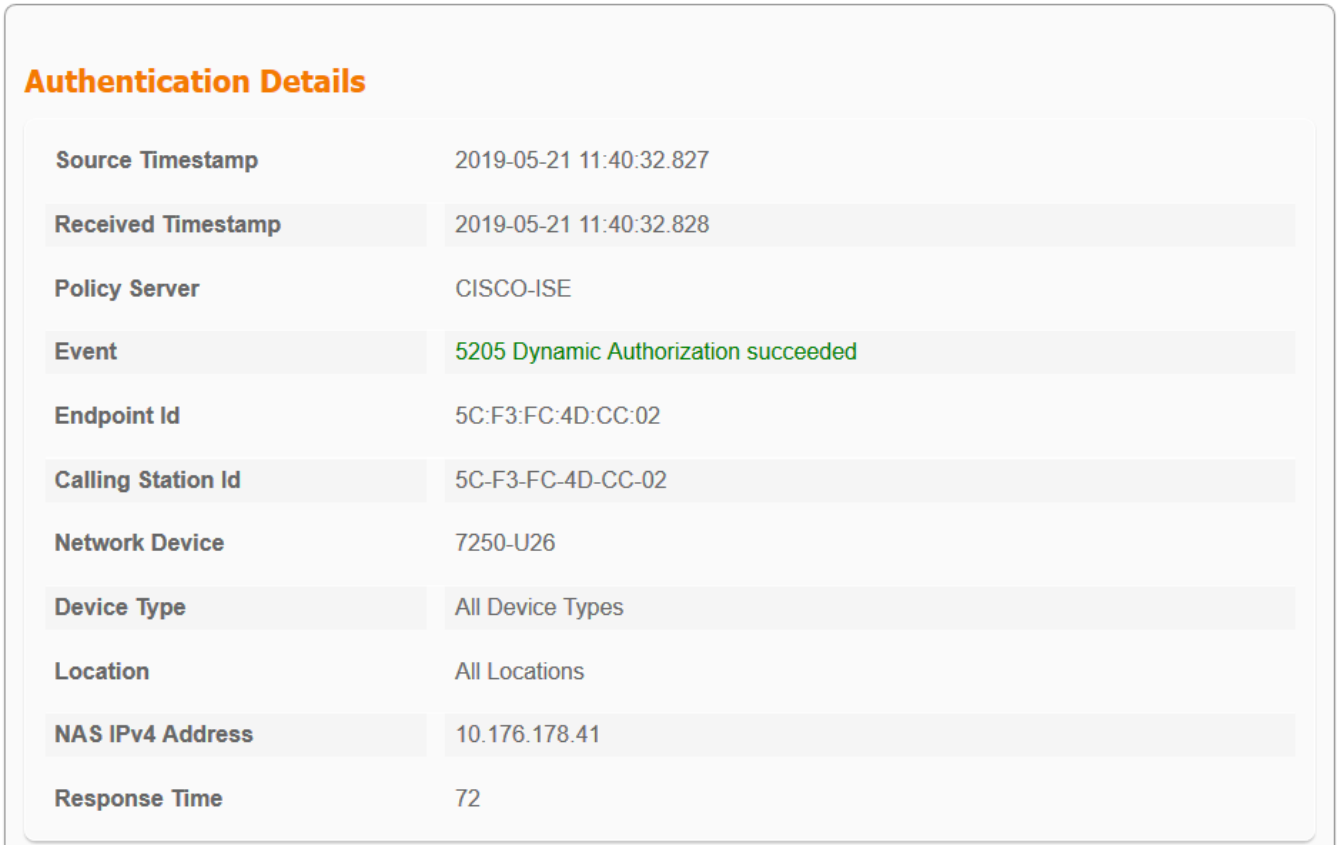
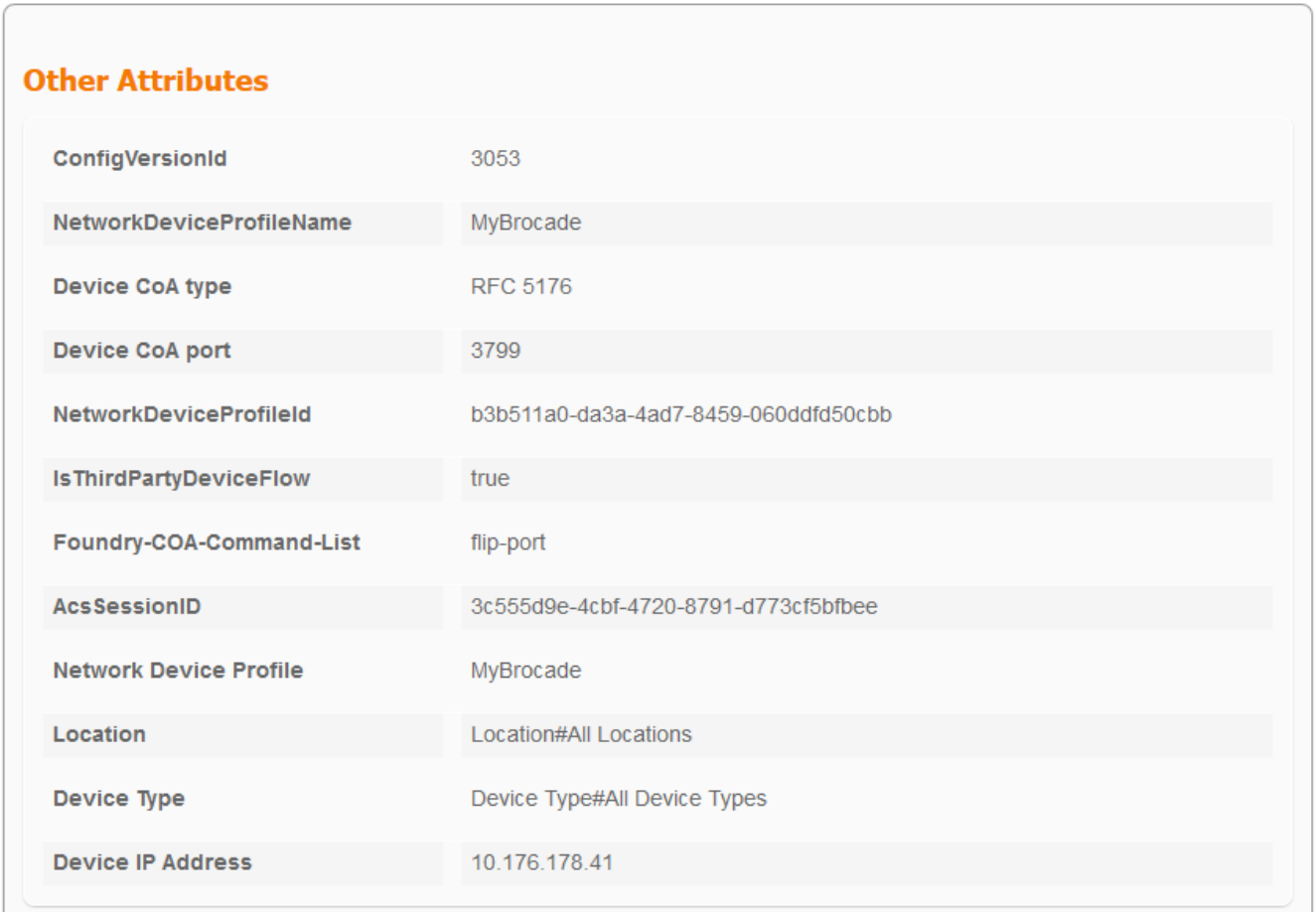


FIGURE 15 Cisco ISE Output: Other Attributes



Other Attributes

ConfigVersionId	3053
NetworkDeviceProfileName	MyBrocade
Device CoA type	RFC 5176
Device CoA port	3799
NetworkDeviceProfileId	b3b511a0-da3a-4ad7-8459-060ddfd50cbb
IsThirdPartyDeviceFlow	true
Foundry-COA-Command-List	flip-port
AcsSessionID	3c555d9e-4cbf-4720-8791-d773cf5bfbee
Network Device Profile	MyBrocade
Location	Location#All Locations
Device Type	Device Type#All Device Types
Device IP Address	10.176.178.41

5. After the switch port is bounced, the PC is authorized by MAC authentication again and the PC session is moved to a new VLAN.

   The CLI output for the Ruckus ICX switch shows the device MAC address, VLAN assignment, and state.

```
7250-U26#show mac-auth session all
------------------------------------------------------------------------------
Port     MAC              IP(v4/v6)            VLAN  Auth      ACL    Session   Age
         Addr             Addr                       State           Time
------------------------------------------------------------------------------
1/1/47   5cf3.fc4d.cc02    N/A                  103   Yes       None   7         Ena
7250-U26#
```

FIGURE 16 Cisco ISE Output: Overview

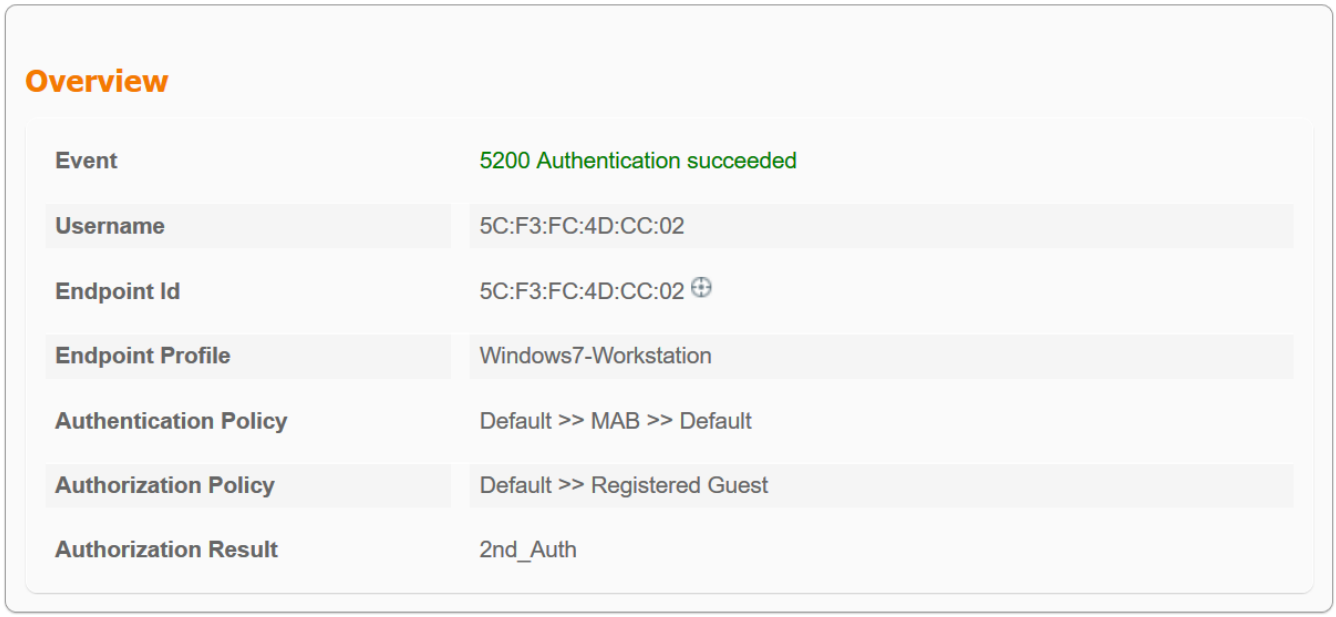


FIGURE 17 Cisco ISE Output: Authentication Details

Authentication Details

Source Timestamp	2019-05-21 11:40:37.761
Received Timestamp	2019-05-21 11:40:37.763
Policy Server	CISCO-ISE
Event	5200 Authentication succeeded
Username	5C:F3:FC:4D:CC:02
User Type	Host
Endpoint Id	5C:F3:FC:4D:CC:02
Calling Station Id	5C-F3-FC-4D-CC-02
Endpoint Profile	Windows7-Workstation
Authentication Identity Store	Internal Endpoints
Identity Group	GuestEndpoints
Authentication Method	mab
Authentication Protocol	Lookup
Service Type	Call Check
Network Device	7250-U26
Device Type	All Device Types
Location	All Locations
NAS IPv4 Address	10.176.178.41
NAS Port Id	1/1/47
NAS Port Type	Ethernet
Authorization Profile	2nd_Auth
Response Time	16

FIGURE 18 Cisco ISE Output: Result

6. The PC receives a new IP address after the PC session is moved to a new VLAN. The PC user can now access the Internet.

```
Ethernet adapter Local Area Connection 3:

   Connection-specific DNS Suffix  . : brocade.com
   Link-local IPv6 Address . . . . . : fe80::212e:8966:85aa:b350%13
   IPv4 Address. . . . . . . . . . . : 103.0.0.1
   Subnet Mask . . . . . . . . . . . : 255.0.0.0
   Default Gateway . . . . . . . . . : 103.1.1.1
```

Sample Ruckus NAD Profile

The following figures show a sample Ruckus Network Access Device (NAD) profile.

FIGURE 19 Network Device Profile

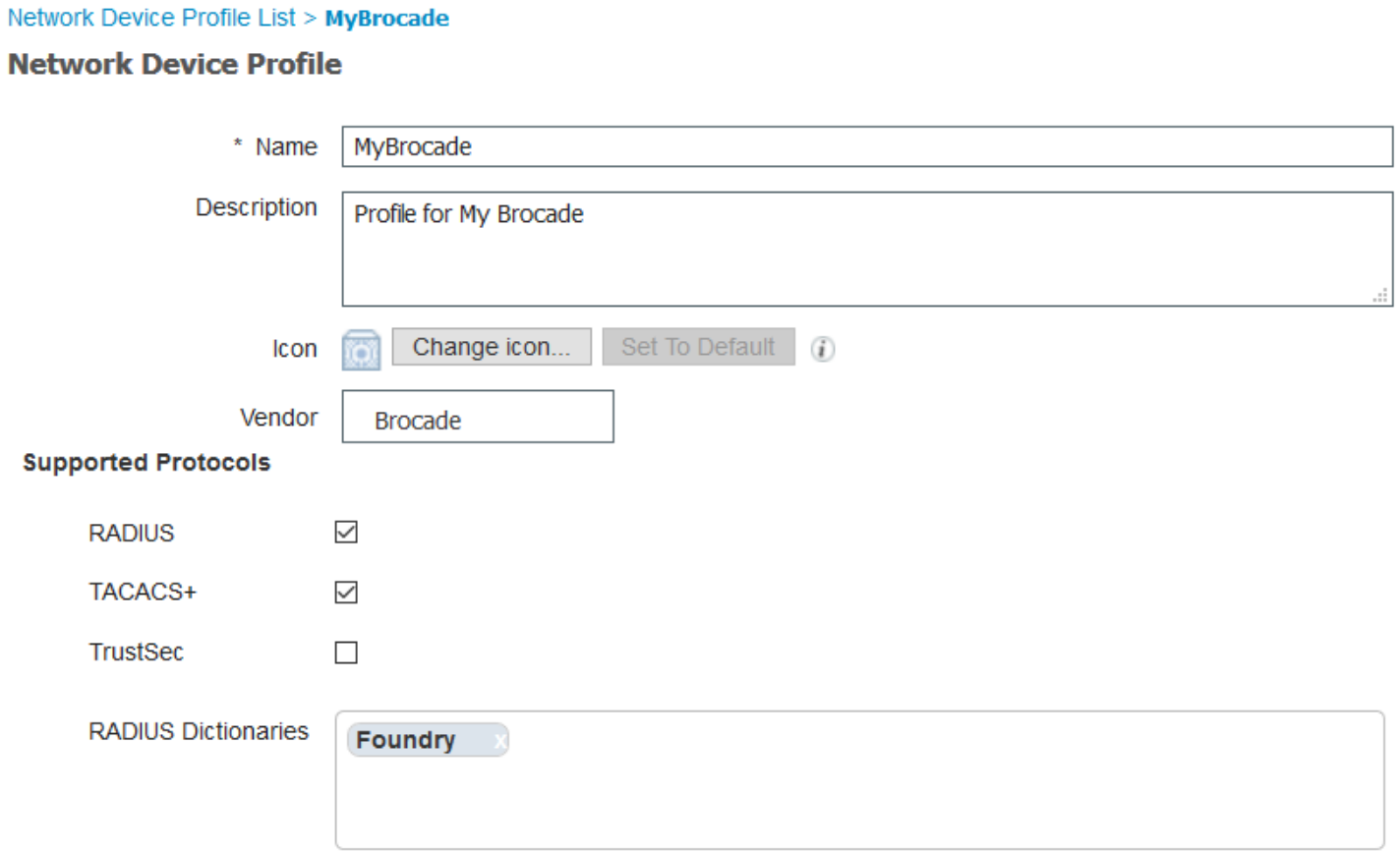


FIGURE 20 Templates

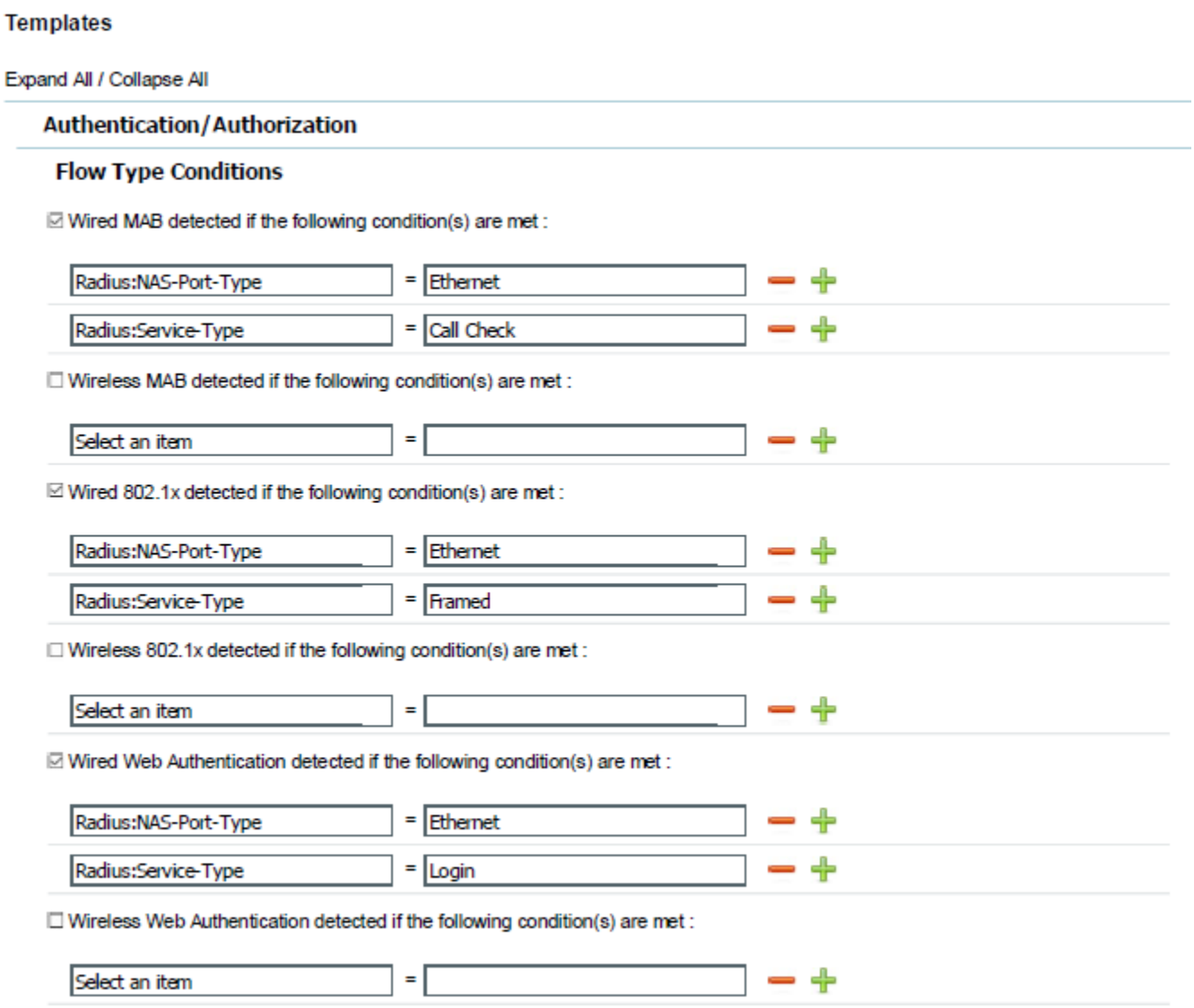


FIGURE 21 Attribute Aliasing

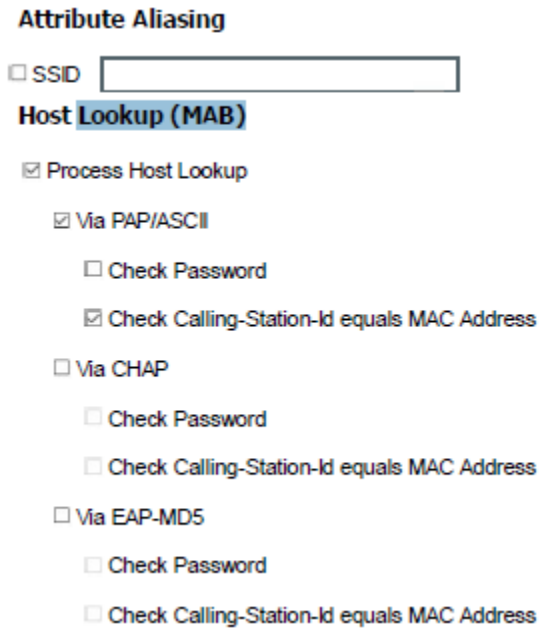


FIGURE 22 Permissions

FIGURE 23 Change of Authorization

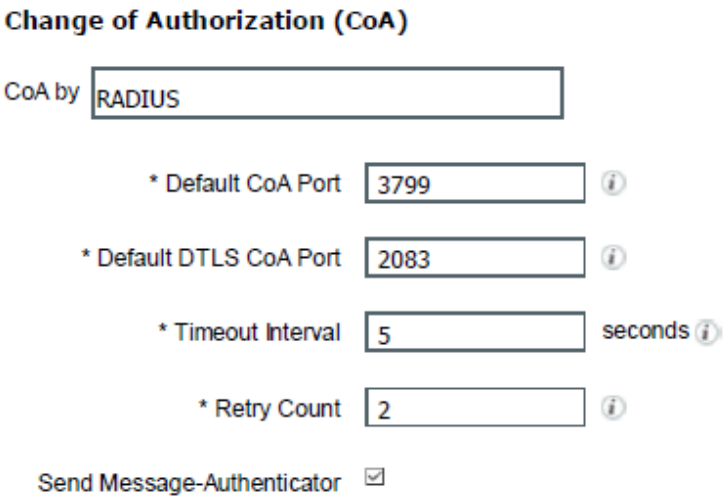


FIGURE 24 Disconnect

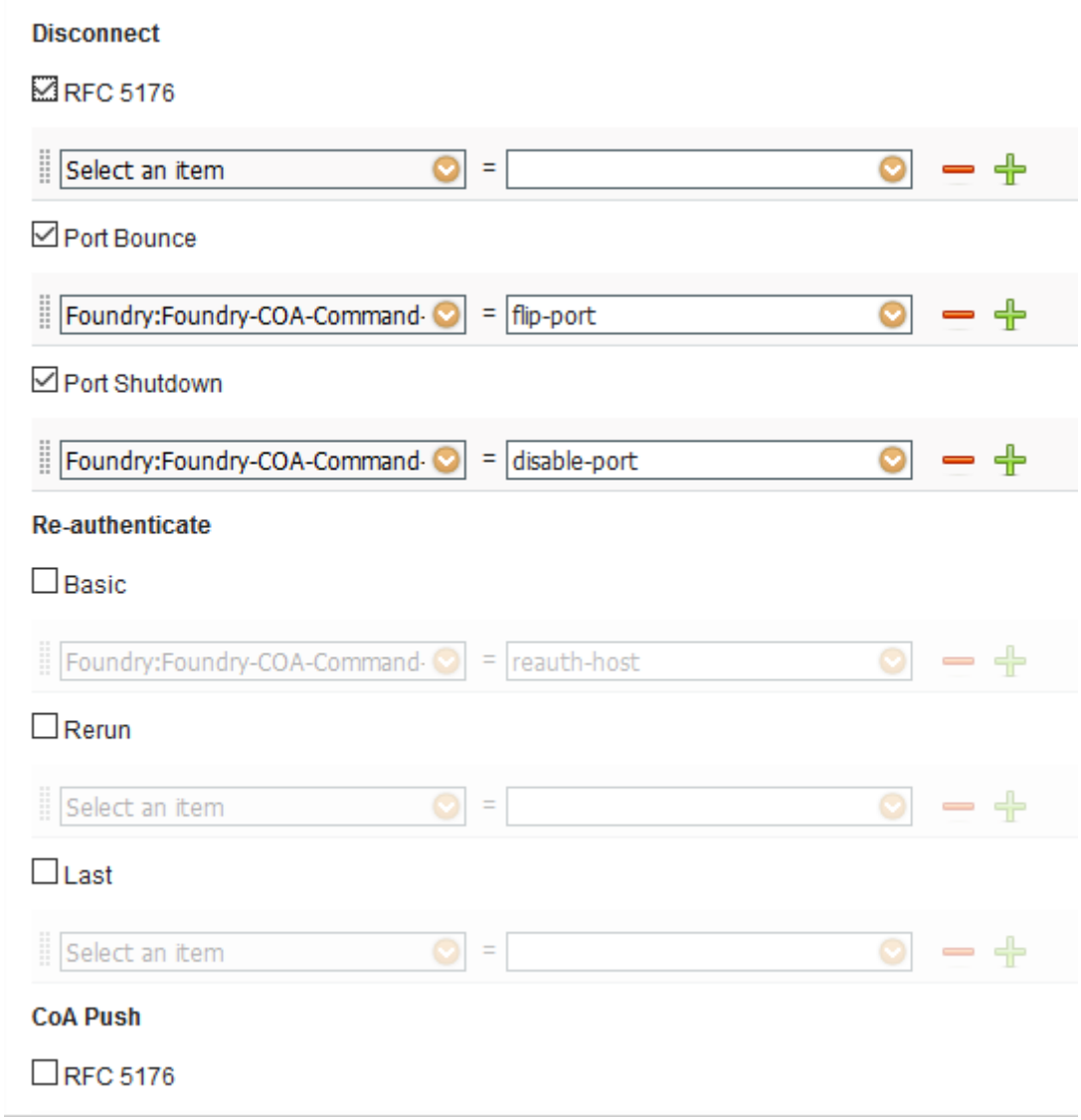
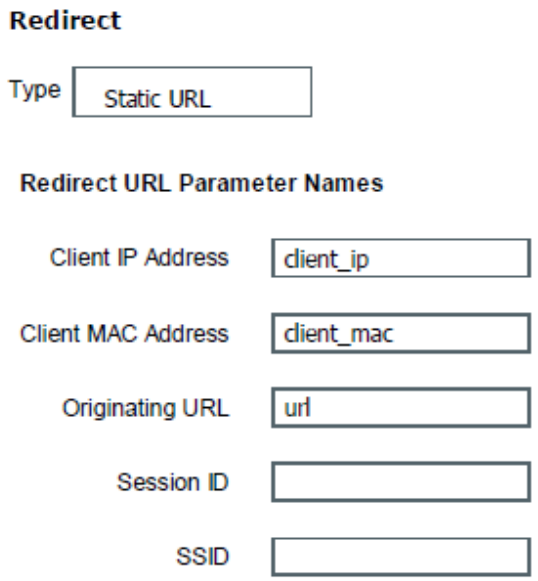


FIGURE 25 Redirect



Summary

This document shows the configurations and steps necessary to configure CWA on Cisco ISE and a Ruckus ICX switch. It also gives the details of the CWA flow for better understanding and easy deployment of CWA in the existing network infrastructure.

Ruckus Wireless, Inc., a wholly owned subsidiary of ARRIS International plc.
350 West Java Dr., Sunnyvale, CA 94089 USA
www.ruckuswireless.com