COMMSCOPE®

RUCKUS®

Deployment Guide

Cloudpath ES: Integration with Infiot SD-WAN

January 2022

Table of Contents

TABLE OF CONTENTS 2

INTENDED AUDIENCE 3

OVERVIEW 4

Initial Configuration on Infiot 4
Configure RADIUS Server on Infiot 4
Configure Wireless LAN on Infiot Edge 5
Configure Wired for RADIUS authentication 6

Cloudpath Configuration 7
Policy Engine Configuration 7
Apply Policies to Certificate Template 9
Workflow Creation 10

Apply Policies Based on Ruckus-User-Groups 11
Create Members to match Cloudpath 11
Create Objects to match Ruckus-User-Groups 12
Assign User Groups to Members 13
Configure Edge Policy(s) to be assigned based on User Group / Ruckus-User-Groups Attribute 13

Intended Audience

This document provides an overview of how to configure RUCKUS Cloudpath to support a RADIUS integration solution with Infiot SD-WAN. Step-by-step procedures for configuration and testing are demonstrated. Some knowledge of the Cloudpath Enrollment System, SD-WAN/Zero Trust and RADIUS is recommended.

This document is written for and intended for use by technical engineers with background in Wi-Fi design and 802.11/wireless engineering principles.

For more information on how to configure RUCKUS products, please refer to the appropriate user guide on the CommScope RUCKUS support site at https://support.ruckuswireless.com/ .

Overview

This document describes how to configure the Cloudpath Enrollment system with Infiot SD-WAN to authenticate user and apply policies on the SD-WAN based on user's identity. The document is broken into the following main categories

- Initial Configuration on Infiot
- Cloudpath Configuration
- Apply Policies Based on Ruckus-User-Groups

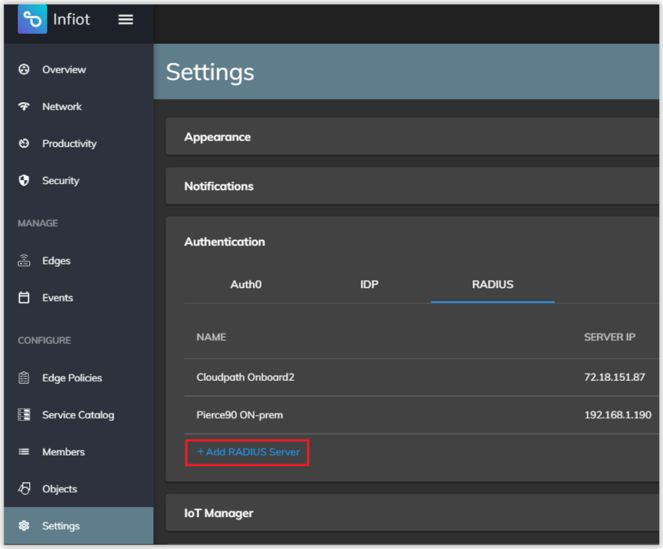
Initial Configuration on Infiot

In this integration, create the structure to allow for policies to be assigned dynamically based on Ruckus-User-Groups coming over from RADIUS. This documentation assumes a HUB and EDGE have been configured in the Infiot Environment. It is assumed you have some prior knowledge and access to Infiot SD-WAN. It is also assumed your Cloudpath Enrollment System is using HTTPS with a valid, Public CA signed SSL Web Certificate.

All configurations are done with Cloudpath version 5.9.5179.

Configure RADIUS Server on Infiot

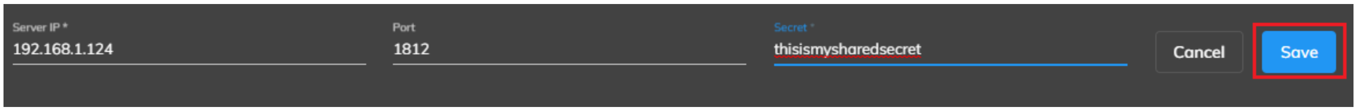
Once logged into the Infiot tenant, go to **Settings→Authentication→RADIUS→Add RADIUS Server** as shown in Figure 1.



NAME	SERVER IP
Cloudpath Onboard2	72.18.151.87
Pierce90 ON-prem	192.168.1.190

FIGURE 1

Add a reference name, IP address of the RADIUS server, the authentication port, and the shared secret. Verify all information is correct, then click **Save** as show in Figure 2.



Server IP * 192.168.1.124

Port 1812

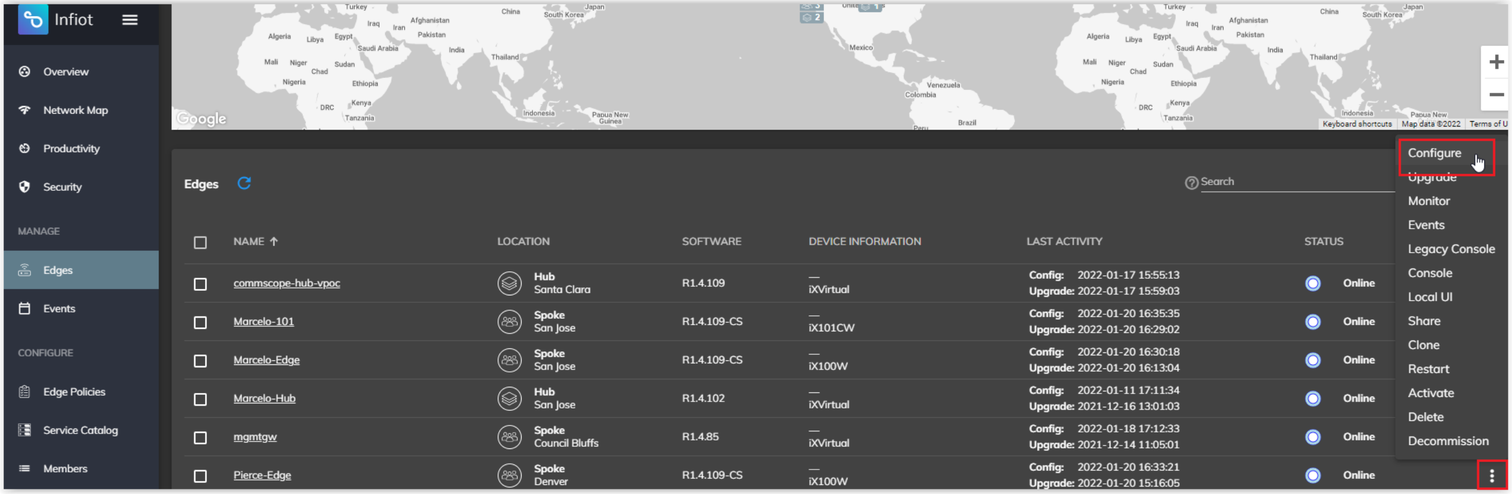
Secret * thisismysharedsecret

FIGURE 2

Configure Wireless LAN on Infiot Edge

Once the RADIUS is setup and configured on the Infiot tenant, add WLANs that will use the RADIUS server that was configured.

Click the three vertical dots by the Edge and click **Configure** as shown in Figure 3.

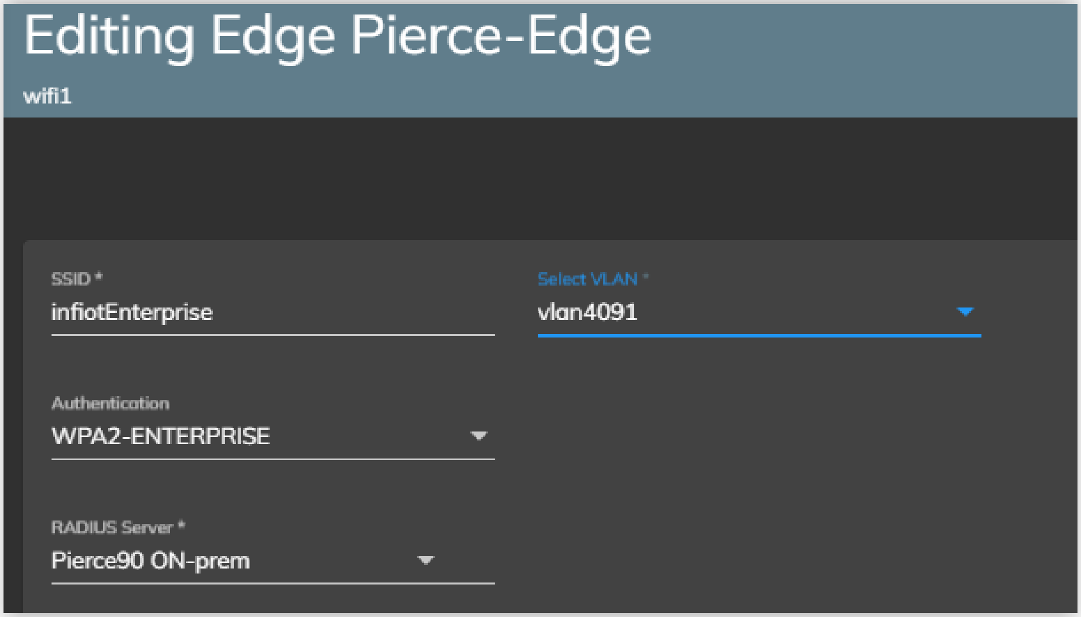


Edges

☐	NAME ↑	LOCATION	SOFTWARE	DEVICE INFORMATION	LAST ACTIVITY	STATUS
☐	commscope-hub-vpoc	Hub Santa Clara	R1.4.109	— iXVirtual	Config: 2022-01-17 15:55:13 Upgrade: 2022-01-17 15:59:03	Online
☐	Marcelo-101	Spoke San Jose	R1.4.109-CS	— iX101CW	Config: 2022-01-20 16:35:35 Upgrade: 2022-01-20 16:29:02	Online
☐	Marcelo-Edge	Spoke San Jose	R1.4.109-CS	— iX100W	Config: 2022-01-20 16:30:18 Upgrade: 2022-01-20 16:13:04	Online
☐	Marcelo-Hub	Hub San Jose	R1.4.102	— iXVirtual	Config: 2022-01-11 17:11:34 Upgrade: 2021-12-16 13:01:03	Online
☐	mgmtgw	Spoke Council Bluffs	R1.4.85	— iXVirtual	Config: 2022-01-18 17:12:33 Upgrade: 2021-12-14 11:05:01	Online
☐	Pierce-Edge	Spoke Denver	R1.4.109-CS	— iX100W	Config: 2022-01-20 16:33:21 Upgrade: 2022-01-20 15:16:05	Online

FIGURE 3

Click Interfaces icon at the top of the **Edit Edge** screen, then scroll down to Wi-Fi section. Click **Add SSID** button and fill in the required fields as shown in Figure 4.



Editing Edge Pierce-Edge

wifi1

SSID *: infiotEnterprise

Select VLAN *: vlan4091

Authentication: WPA2-ENTERPRISE

RADIUS Server *: Pierce90 ON-prem

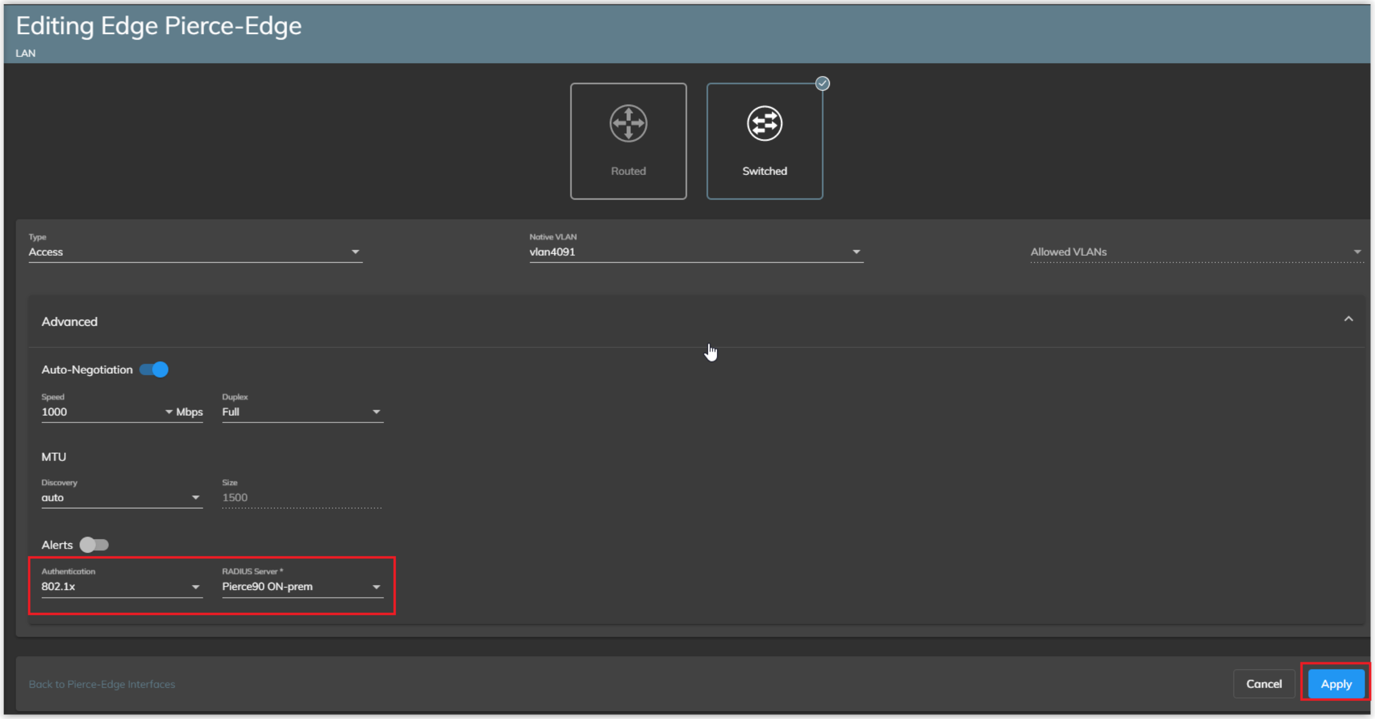
FIGURE 4

Click Apply at bottom right of the screen when all required fields have been entered. Click the Finish icon at the top of the **Edit Edge** screen, then click Save when ready to apply changes to the Edge.

Configure Wired for RADIUS authentication

RADIUS integration can be used for Wireless or Wired. In this example, we will be configuring RADIUS authentication for the Wired LAN interface on the edge.

Click the three vertical dots by the Edge and click **Configure** as shown in **Error! Reference source not found.**Figure 3



Editing Edge Pierce-Edge
LAN

Type: Access
Native VLAN: vlan4091
Allowed VLANs

Advanced

Auto-Negotiation
Speed: 1000 Mbps
Duplex: Full

MTU
Discovery: auto
Size: 1500

Alerts
Authentication: 802.1x
RADIUS Server *: Pierce90 ON-prem

FIGURE 5

Click Interfaces icon at the top of the **Edit Edge** screen, then scroll down to Interfaces section. Click **LAN** interface and fill in the required **Authentication** fields, followed by the **Apply** button as highlighted in Figure 5.

Click the Finish icon at the top of the **Edit Edge** screen, then click Save when ready to apply changes to the Edge.

Cloudpath Configuration

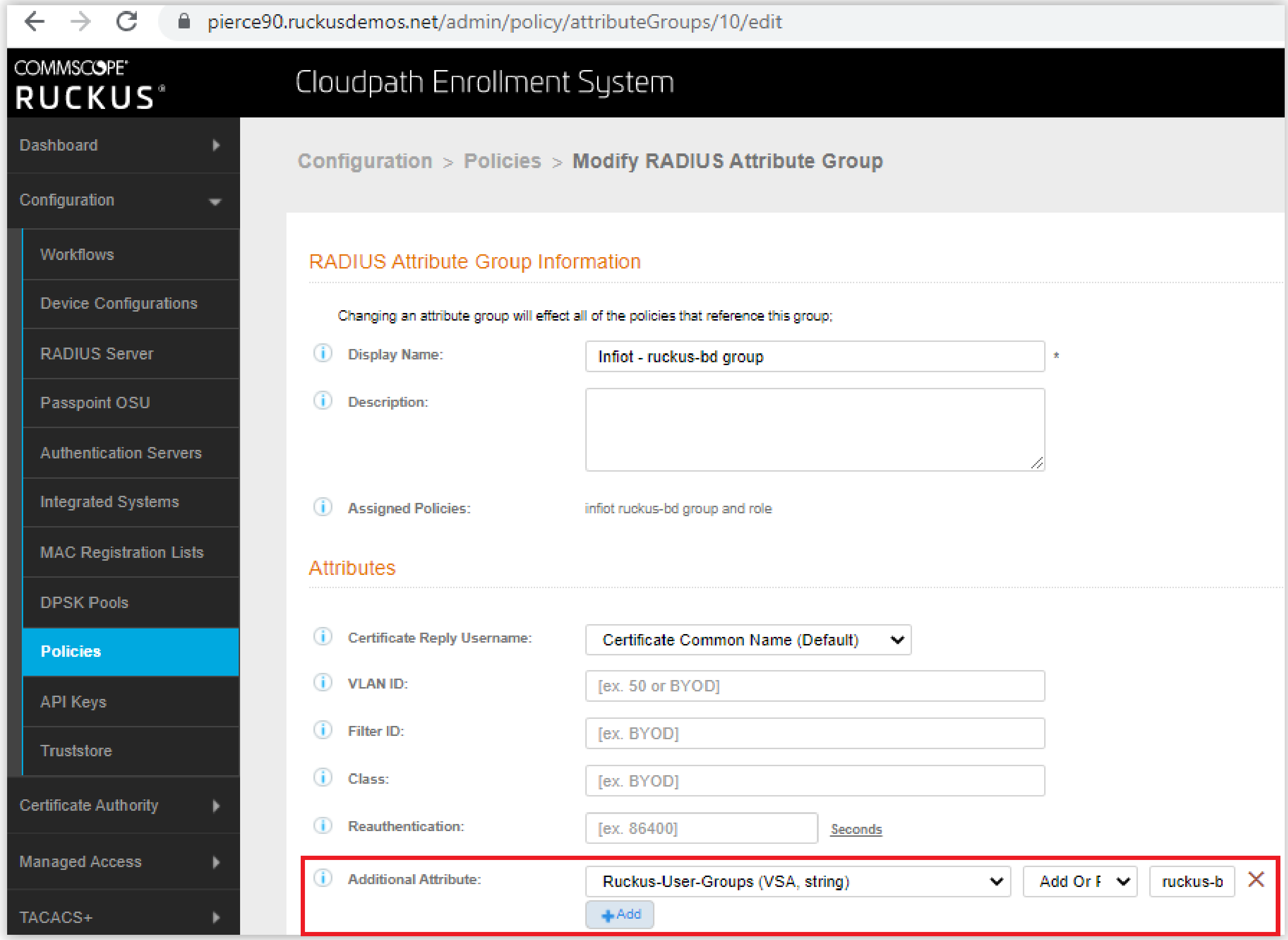
Configuration on the Cloudpath side includes configuring the Cloudpath Policy Engine to send Ruckus-User-Groups attribute through RADIUS to allow us to apply policies on the Infiot based on identity established in Cloudpath.

It is assumed you have some prior knowledge with the Cloudpath Policy Engine, Microsoft AD, RADIUS, and workflow creation in Cloudpath.

Policy Engine Configuration

In the example use case, there are three different policies where we apply a different **Ruckus-User-Groups** based on the AD group of the identity that is established in the captive portal.

Configuration→Polices→RADIUS Attribute Groups tab→Add RADIUS Attribute Group. Click the **Add** button as shown in Figure 6 and choose **Ruckus-User-Group's** attribute.



RADIUS Attribute Group Information

Changing an attribute group will effect all of the policies that reference this group;

Display Name:	Infiot - ruckus-bd group *
Description:	
Assigned Policies:	infiot ruckus-bd group and role

Attributes

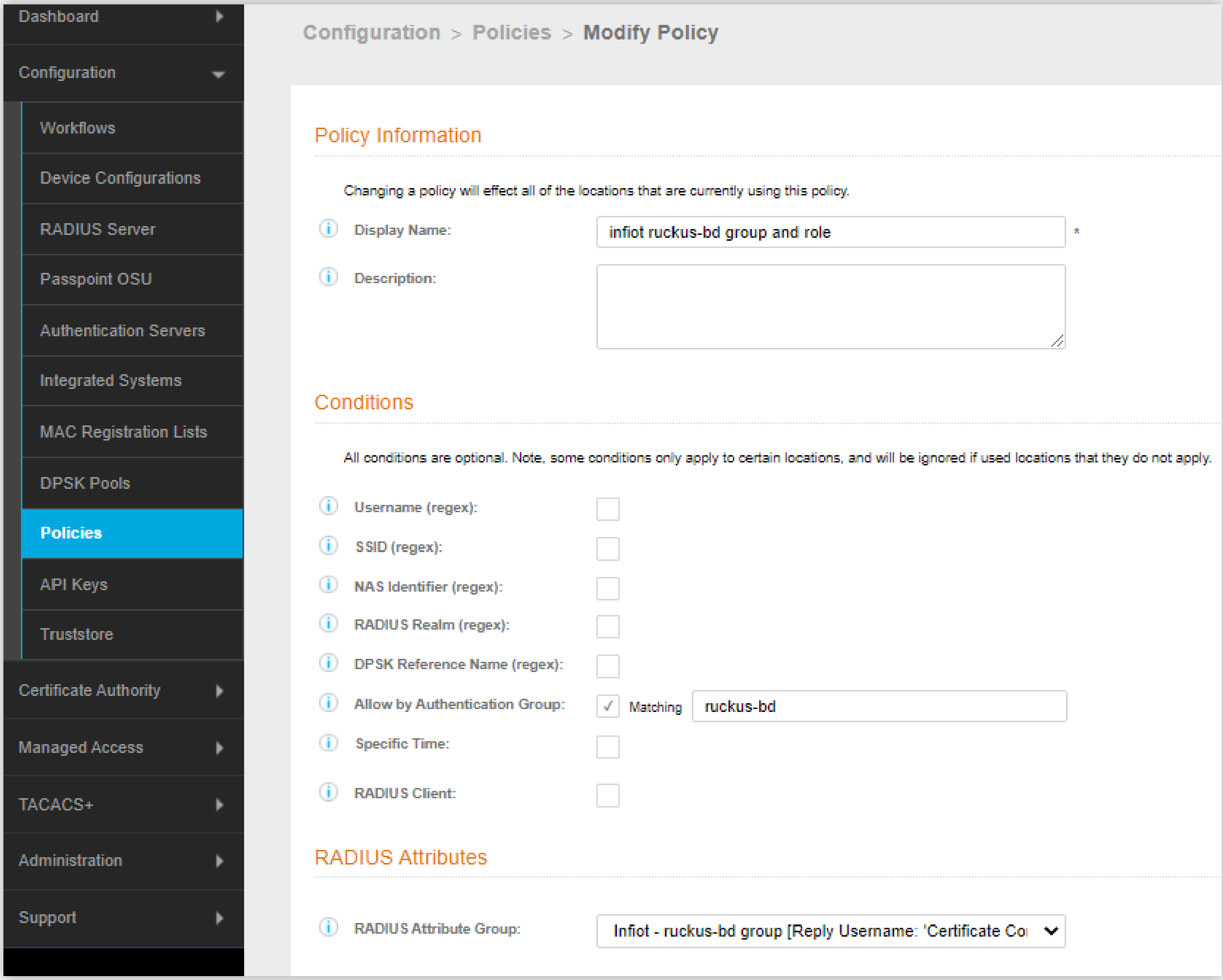
Certificate Reply Username:	Certificate Common Name (Default)
VLAN ID:	[ex. 50 or BYOD]
Filter ID:	[ex. BYOD]
Class:	[ex. BYOD]
Reauthentication:	[ex. 86400] Seconds
Additional Attribute:	Ruckus-User-Groups (VSA, string) Add Or F ruckus-b

FIGURE 6

The value of the RADIUS attribute can be any value, it just needs to match the **Object** set up in Infiot as shown later in the guide.

Once the RADIUS Attribute Group is configured, add a policy using the attribute group that was just created by clicking **Add Policy** from Configuration→Polices screen.

Policy condition can be anything, however in this example were using the **Allow by Authentication Group** condition



Configuration > Policies > Modify Policy

Policy Information

Changing a policy will effect all of the locations that are currently using this policy.

Display Name: infiot ruckus-bd group and role *

Description:

Conditions

All conditions are optional. Note, some conditions only apply to certain locations, and will be ignored if used locations that they do not apply.

Username (regex): □

SSID (regex): □

NAS Identifier (regex): □

RADIUS Realm (regex): □

DPSK Reference Name (regex): □

Allow by Authentication Group: ☑ Matching ruckus-bd

Specific Time: □

RADIUS Client: □

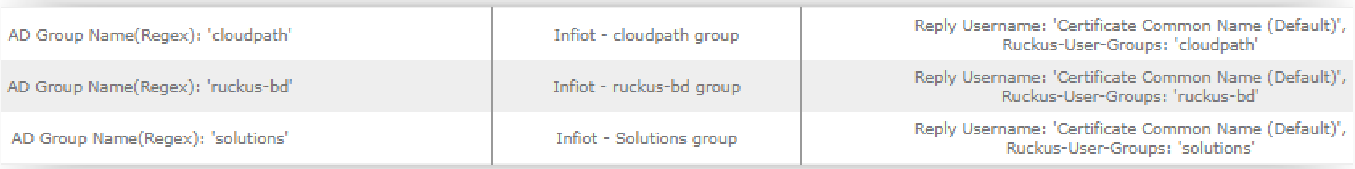
RADIUS Attributes

RADIUS Attribute Group: Infiot - ruckus-bd group [Reply Username: 'Certificate Co

FIGURE 7

as shown in Figure 7. Confirm the condition(s) and the RADIUS attribute group, then click Save.

In the use case example, repeat the Policy Configuration steps for any other Group/Objects we want configured.



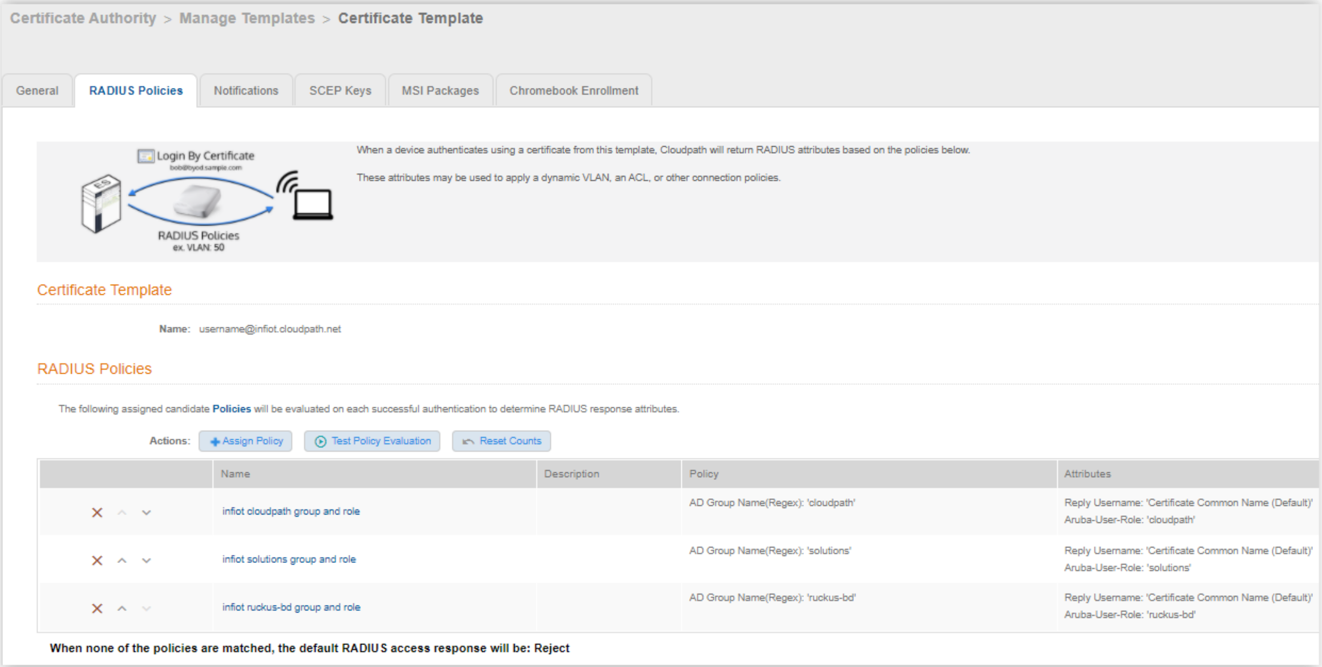
AD Group Name(Regex): 'cloudpath'	Infiot - cloudpath group	Reply Username: 'Certificate Common Name (Default)', Ruckus-User-Groups: 'cloudpath'
AD Group Name(Regex): 'ruckus-bd'	Infiot - ruckus-bd group	Reply Username: 'Certificate Common Name (Default)', Ruckus-User-Groups: 'ruckus-bd'
AD Group Name(Regex): 'solutions'	Infiot - Solutions group	Reply Username: 'Certificate Common Name (Default)', Ruckus-User-Groups: 'solutions'

FIGURE 8

There are three different policies for three different authentication groups in the use cases as shown in Figure 8.

Apply Policies to Certificate Template

The policies created must now be applied to the Certificate Template. This specific use case will be highlighting EAP-TLS authentication; however, the same process can apply to PEAP as well if we apply the policies to PEAP tab.



When a device authenticates using a certificate from this template, Cloudpath will return RADIUS attributes based on the policies below.

These attributes may be used to apply a dynamic VLAN, an ACL, or other connection policies.

Certificate Template

Name: username@infiot.cloudpath.net

RADIUS Policies

The following assigned candidate **Policies** will be evaluated on each successful authentication to determine RADIUS response attributes.

	Name	Description	Policy	Attributes
✕ ^ ˅	infiot cloudpath group and role		AD Group Name(Regex): 'cloudpath'	Reply Username: 'Certificate Common Name (Default)' Aruba-User-Role: 'cloudpath'
✕ ^ ˅	infiot solutions group and role		AD Group Name(Regex): 'solutions'	Reply Username: 'Certificate Common Name (Default)' Aruba-User-Role: 'solutions'
✕ ^ ˅	infiot ruckus-bd group and role		AD Group Name(Regex): 'ruckus-bd'	Reply Username: 'Certificate Common Name (Default)' Aruba-User-Role: 'ruckus-bd'

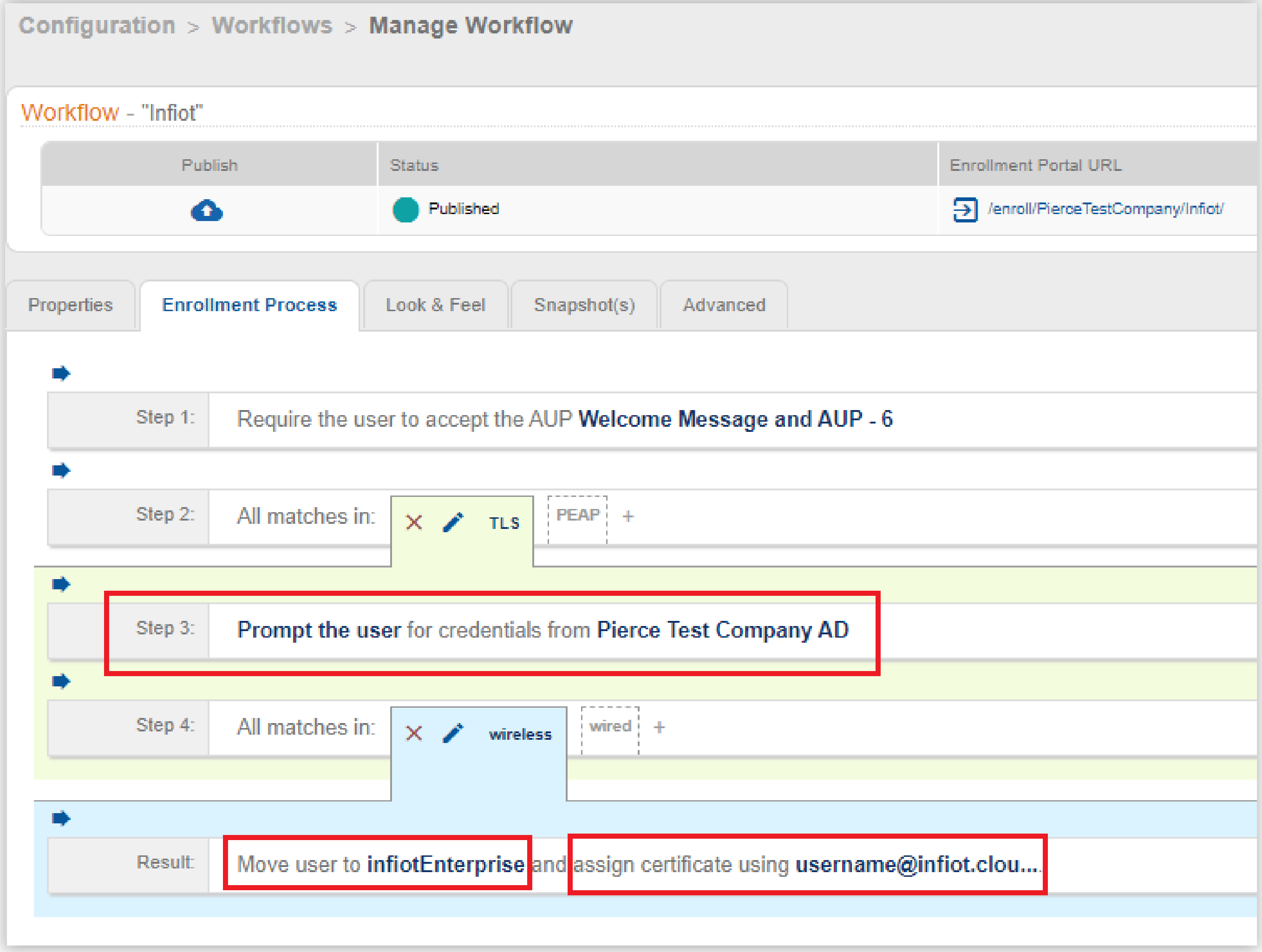
When none of the policies are matched, the default RADIUS access response will be: Reject

FIGURE 9

Certificate Authority→Manage Templates→Click wrench icon by specific certificate template that will be used. Under the RADIUS Policies tab, apply the policies previously created as shown in Figure 9.

Workflow Creation

In this use case, devices will be enrolled via the workflow (captive portal), however if the use case only uses Cloudpath for RADIUS, the certificate and WLAN profile can be pushed via SCEP or GPO. A caveat would be that Infiot SD-WAN does not have concept of captive portal, so that would need be configured on wireless controller.



Configuration > Workflows > Manage Workflow

Workflow - "Infiot"

Publish	Status	Enrollment Portal URL
	Published	/enroll/PierceTestCompany/Infiot/

Step 1: Require the user to accept the AUP **Welcome Message and AUP - 6**

Step 2: All matches in: TLS | PEAP +

Step 3: **Prompt the user** for credentials from **Pierce Test Company AD**

Step 4: All matches in: wireless | wired +

Result: Move user to **infiotEnterprise** and assign certificate using **username@infiot.clou...**

FIGURE 10

As highlighted in Figure 10, the three main components of the workflow creation will be the Microsoft AD server that has group structure to align with the policies created. As well as the certificate template that the policies were applied to, as well as creating a device configuration that includes a network profile for the wireless and/or wired network.

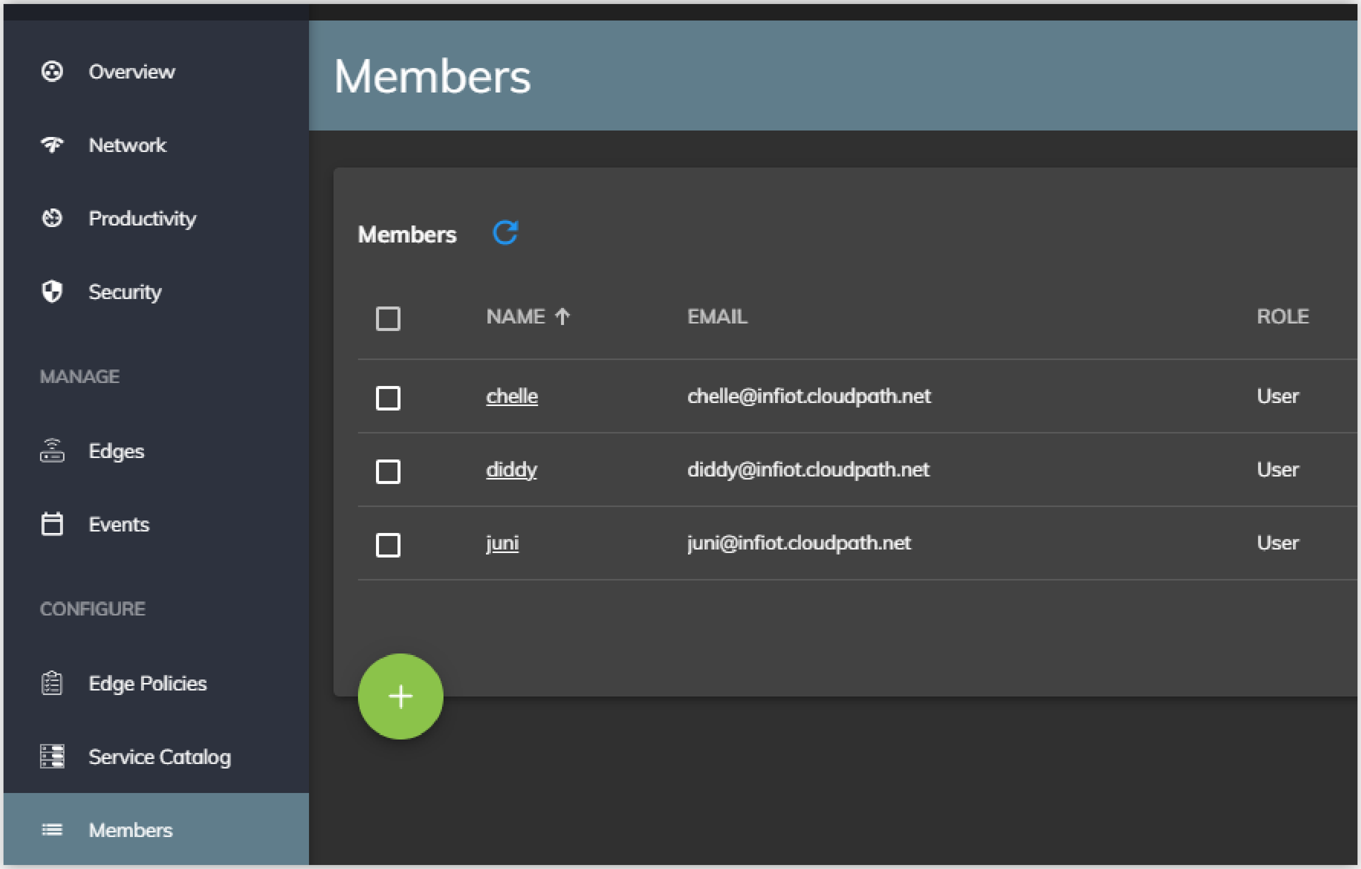
Apply Policies Based on Ruckus-User-Groups

Policies must be configured on the SD-WAN based on the Ruckus-User-Groups were sending from RADIUS. Before that can be accomplished, the policies, members and group structure must be built out on the SD-WAN.

It is assumed you have some prior knowledge and access to Infiot SD-WAN.

Create Members to match Cloudpath

Members and Objects must be created on the SD-WAN to match our user/group structure that has been configured. In this use case, three different Members and three different Objects will be added, however more can be added. This allows for policies to be applied based on the Ruckus-User-Groups being assigned during RADIUS from Cloudpath Policy Engine.



Members

Members

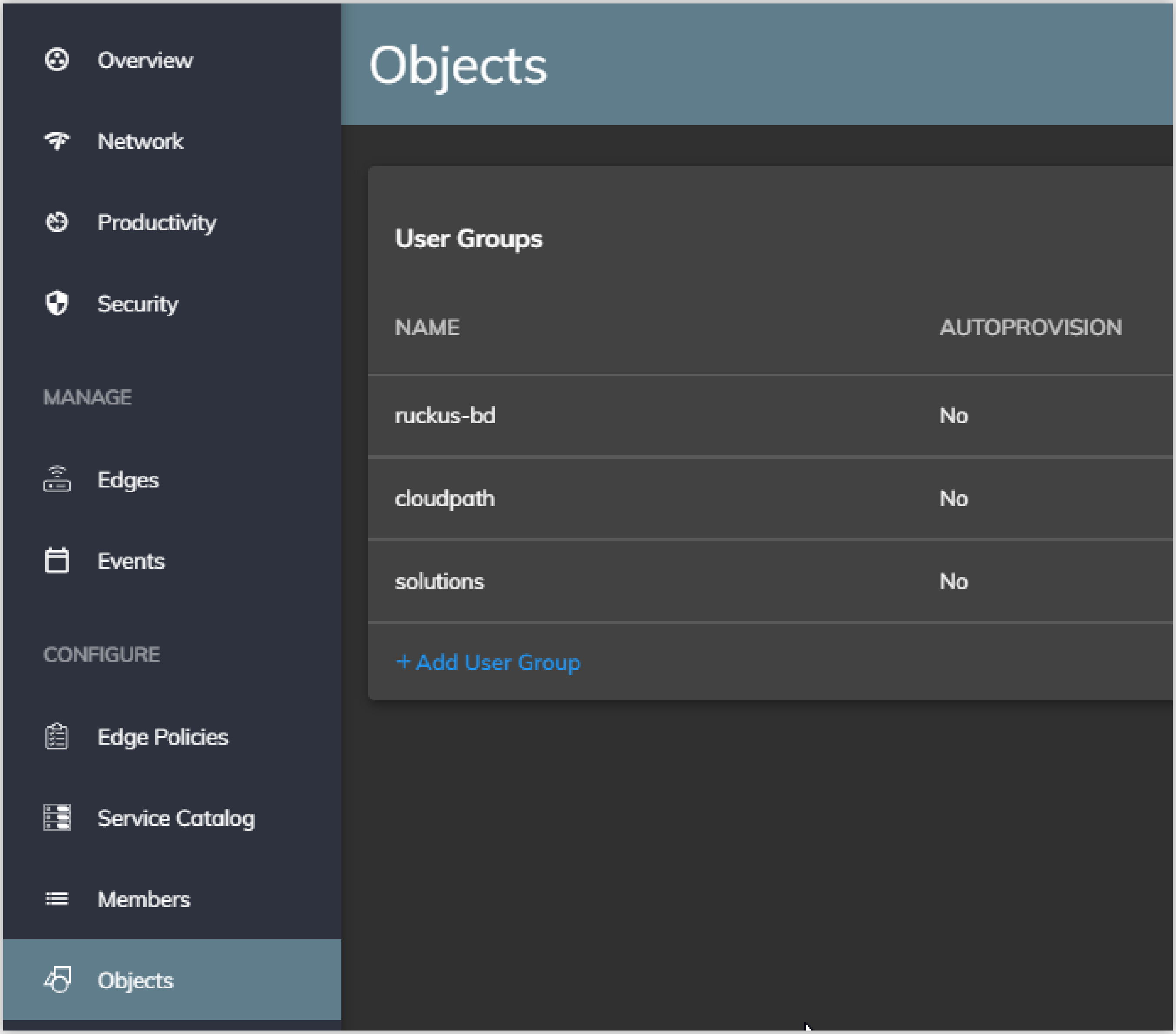
□	NAME ↑	EMAIL	ROLE
□	chelle	chelle@infiot.cloudpath.net	User
□	diddy	diddy@infiot.cloudpath.net	User
□	juni	juni@infiot.cloudpath.net	User

FIGURE 11

In the Infiot SD-WAN tenant, go to **Configure→Members→Click green + button** to add members. The name should match to a USERNAME that would be used in Cloudpath. In this example, three different users from MSFT AD are added as shown in Figure 11.

Create Objects to match Ruckus-User-Groups

Like Members, Objects must be created and match the names of the Ruckus-User-Groups we configured in Cloudpath Policy Engine (Ruckus-User-Groups listed in Figure 8 policies).



User Groups

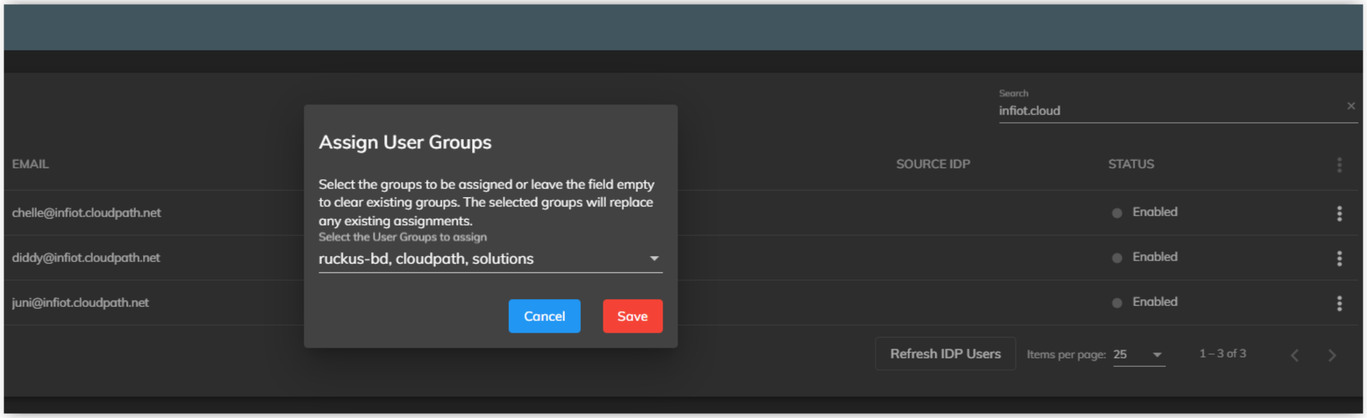
NAME	AUTOPROVISION
ruckus-bd	No
cloudpath	No
solutions	No

Figure 12

In the Infiot SD-WAN tenant, go to **Configure→Objects→Click Add User Group** button to add objects. The name should match to a Ruckus-User-Group that we defined in policy on Cloudpath. In this example, three different objects from the **Ruckus-User-Groups** configured are added as shown in Figure 12.

Assign User Groups to Members

User Groups must be assigned to the user for that User-Group to be applied dynamically through RADIUS. Based on that user-group, we can assign different Firewall policies on the SD-WAN. In the example, assign all three User Groups to three different members created on the SD-WAN.



Search: infiot.cloud

EMAIL	SOURCE IDP	STATUS
chelle@infiot.cloudpath.net		Enabled
diddy@infiot.cloudpath.net		Enabled
juni@infiot.cloudpath.net		Enabled

Assign User Groups

Select the groups to be assigned or leave the field empty to clear existing groups. The selected groups will replace any existing assignments.

Select the User Groups to assign: ruckus-bd, cloudpath, solutions

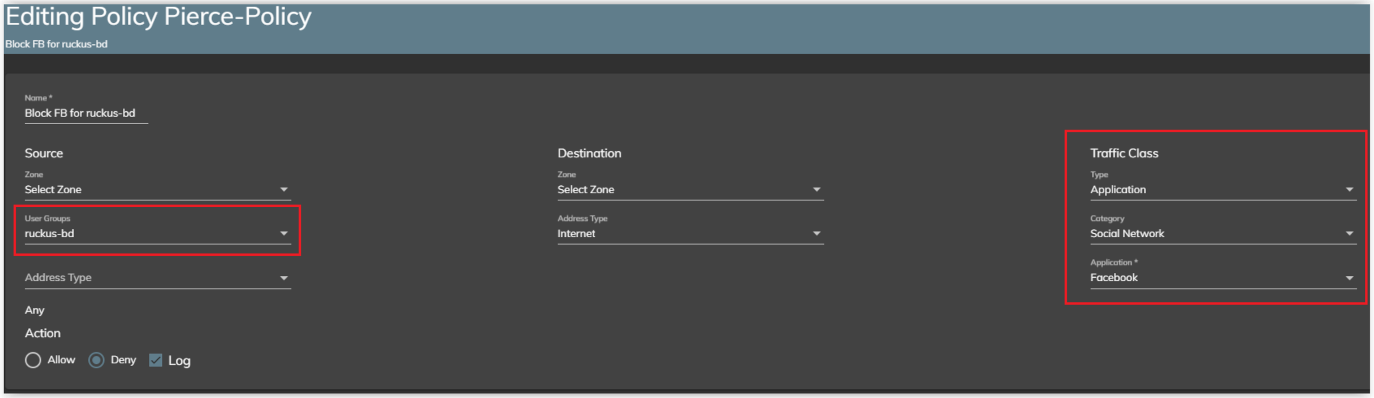
FIGURE 13

In the Infiot SD-WAN tenant, go to **Configure→Members→Click the three vertical dots by each user→Click Assign Groups** then assign all User Groups to each member as shown in Figure 13.

Configure Edge Policy(s) to be assigned based on User Group / Ruckus-User-Groups Attribute

During the initial Edge configuration, you should have a policy created to define QoS for that Edge. In the example, Firewall rules will be added based on User Group.

In the Infiot SD-WAN tenant, go to **Configure→Edge Policies→Click the Policy being used by the Edge→Security→Firewall Section→Add Rule button.**



Editing Policy Pierce-Policy

Block FB for ruckus-bd

Name *: Block FB for ruckus-bd

Source
- Zone: Select Zone
- User Groups: ruckus-bd
- Address Type
- Any

Destination
- Zone: Select Zone
- Address Type: Internet

Traffic Class
- Type: Application
- Category: Social Network
- Application *: Facebook

Action: ○ Allow ● Deny ☑ Log

FIGURE 14

The example rule shown will block access to the specific applications based on the User-Group listed during creation of the rule. Based on what is highlighted in Figure 14, specific Social Media apps will be blocked if the **ruckus-bd** Ruckus-User-Group gets sent over via RADIUS. L4 protocol can be used as well but specific applications will be shown in this example.

Repeat the **configure edge policy** steps to configure different Firewall Rules for different User-Groups that were configured in the Cloudpath Policy Engine.

Ruckus solutions are part of CommScope's comprehensive portfolio for Enterprise environments (indoor and outdoor).

We encourage you to visit **commscope.com** to learn more about:

- Ruckus Wi-Fi Access Points
- Ruckus ICX switches
- SYSTIMAX and NETCONNECT: Structured cabling solutions (copper and fiber)
- imVision: Automated Infrastructure Management
- Era and OneCell in-building cellular solutions
- Our extensive experience about supporting PoE and IoT

commscope.com

Visit our website or contact your local CommScope representative for more information.

Unless otherwise noted, all trademarks identified by ® or ™ are registered trademarks, respectively, of CommScope, Inc. This document is for planning purposes only and is not intended to modify or supplement any specifications or warranties relating to CommScope products or services. CommScope is committed to the highest standards of business integrity and environmental sustainability with a number of CommScope's facilities across the globe certified in accordance with international standards, including ISO9001, TL9000, ISO14001 and ISO45001. Further information regarding CommScope's commitment can be found at **www.commscope.com/About-Us/Corporate-Responsibility-and-Sustainability**.