

Cloudpath Enrollment System PEAP With Onboard RADIUS Server Configuration Guide, 5.11

Supporting Cloudpath Software Release 5.11

Copyright, Trademark and Proprietary Rights Information

© 2022 CommScope, Inc. All rights reserved.

No part of this content may be reproduced in any form or by any means or used to make any derivative work (such as translation, transformation, or adaptation) without written permission from CommScope, Inc. and/or its affiliates ("CommScope"). CommScope reserves the right to revise or change this content from time to time without obligation on the part of CommScope to provide notification of such revision or change.

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, COMMSCOPE 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. CommScope 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. CommScope 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 CommScope 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 COMMSCOPE, COMMSCOPE 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 COMMSCOPE 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, COMMSCOPE, RUCKUS, RUCKUS WIRELESS, the Ruckus logo, the Big Dog design, BEAMFLEX, CHANNELFLY, FASTIRON, ICX, SMARTCELL and UNLEASHED are trademarks of CommScope, Inc. and/or its affiliates. Wi-Fi Alliance, Wi-Fi, the Wi-Fi logo, Wi-Fi Certified, the Wi-Fi CERTIFIED logo, Wi-Fi Protected Access, the Wi-Fi Protected Setup logo, Wi-Fi Protected Setup, Wi-Fi Multimedia and WPA2 and WMM are trademarks or registered trademarks of Wi-Fi Alliance. All other trademarks are the property of their respective owners.

Contents

Overview	4
Considerations for Replication	4
Requirements for Setting Up Cross-Realm Trusts	5
Creating An Authorization Server	5
Configuring DNS and Verifying Readiness for Cloudpath to Join Active Directory Domain	7
Adding an Active Directory Authentication Server	7
PEAP Realm Ports Used	10
Using Policies	11
Configuring Policies.....	11
Adding Policies to RADIUS Server Configuration.....	15
Testing Policies.....	17
Viewing Policy Information.....	21
Viewing RADIUS Attribute Information.....	23
Checking a User Record	24

Overview

You can use PEAP authentication with the Cloudpath onboard RADIUS server. Only Active Directory (AD) authentication servers are supported with this PEAP implementation.

Two of the advantages of using Cloudpath PEAP with AD are:

- It removes the requirement to deploy NPS as a RADIUS server in front of AD for 802.1X EAP-PEAP credential-based authentication.
- It provides a consolidated approach to migrating users from EAP-PEAP to EAP-TLS .

With this type of authentication, you can set up any number of active directories to which your Cloudpath system can communicate. You then configure the Cloudpath onboard RADIUS server to support PEAP. You can also configure an unlimited number of policies, but only one policy will be assigned to a user, depending on which criteria that you specify matches a given user trying to connect to Cloudpath. For each policy, you assign a RADIUS attribute group that can contain many attributes including VLAN ID.

The basic steps to follow to use PEAP with the Cloudpath onboard RADIUS server are:

- Set up your active directory servers.
- [Creating An Authorization Server](#) on page 5: This section covers the requirements to set up at least one authorization server.
- [Adding an Active Directory Authentication Server](#) on page 7: This section describes how to add a server to the PEAP configuration within the RADIUS Server portion of the Cloudpath UI.
- [Adding Policies to RADIUS Server Configuration](#) on page 15: This section describes how to add policies to the PEAP configuration within the RADIUS Server portion of the Cloudpath UI.
- [Checking a User Record](#) on page 24: This section shows you how to view information about users who have been enrolled or attempted to enroll into the Cloudpath system using this PEAP authentication process.

Considerations for Replication

You can use PEAP internal RADIUS authentication in a replicated environment, but the following guidelines must be followed:

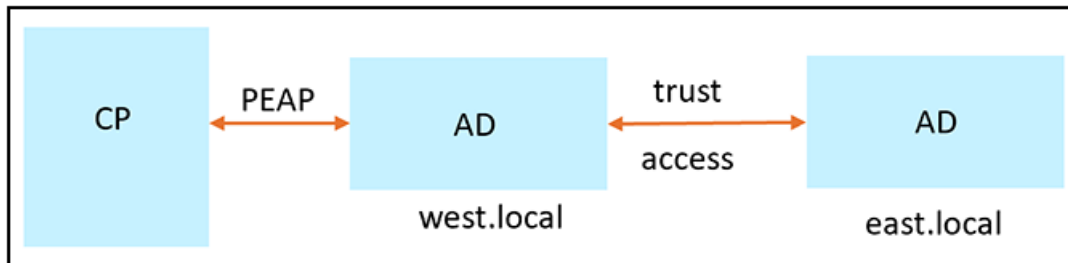
- A two-node replication cluster is the only supported topology, although it can be an active-active or an active-standby configuration.
- If you have already have a PEAP domain configured on a single Cloudpath system, you must disable (unjoin) the PEAP AD domain before configuring your replication cluster, then you must enable (join) the PEAP domain after the replication configuration is complete.

For instructions on setting up a cluster, refer to the *Cloudpath Enrollment System Replication Configuration Guide*.

Requirements for Setting Up Cross-Realm Trusts

PEAP Authentication is supported across realms that have been set up to trust each other, as the following illustration depicts.

FIGURE 1 Cross-REALM PEAP Support



Follow these guidelines, which use the environment depicted in the illustration as an example, to use PEAP authentication for trusted realms:

- Set up west.local and east.local to trust each other.
- Choose only one domain as the Cloudpath PEAP domain for Cloudpath to join; for example west.local. Cloudpath will be able to authenticate all identities on west.local and its trusted domain east.local
- You do not need to add the east.local domain controller to Cloudpath.
- Verifications for readiness to join west.local should be conducted on the west.local domain controller only.
- LDAP user authentication tests in the **Configuration > Authentication Servers** of the Cloudpath UI works only for test users in the west.local domain.
- Users on the PEAP default domain (west.local in this example) can be authenticated without specifying the domain name (for example, a user called *john* can be authenticated using only the name john as well as john@west.local or WEST\john).
- Users on the trusted domain (east.local in this example) must be authenticated with the domain name specified (for example: EAST\bob or bob@east.local).
- Cloudpath can retrieve user groups for identities on the trusted domains. Therefore, group policies can be applied to the trusted domains.

Creating An Authorization Server

You must have at least one active directory authorization server for PEAP authentication using the onboard RADIUS server, but you can configure as many authorization servers as you want.

NOTE

It is strongly recommended to *not* place the AD server on the other side of any type of NAT device because AD over NAT has not been tested by Microsoft.

To set up an active directory for user with PEAP, follow these steps:

1. In the Cloudpath UI, go to **Configuration > Authentication Servers**.
2. Click **Add Server**.
3. On the ensuing Authentication Server Configuration screen, you can first click one of the "Sample data" options at the very bottom of the screen, then tweak the information as needed for your system. An example of this screen after the "AD using LDAPS" item has been clicked is shown below.

Creating An Authorization Server

4. In the AD Host field, enter the fully qualified domain name, which is `ldaps://msft-dc-2012.demo.sample.local` in this example .

FIGURE 2 Configuring An Authentication Server

The screenshot shows the 'Authentication Server Configuration' window. It is divided into several sections:

- Connect to Active Directory:** This section is selected with a radio button. Below it, there is a text box for 'Default AD Domain' containing 'demo.sample.local', a text box for 'AD Host' containing 'ldaps://msft-dc-2012.demo.sample.local', a text box for 'AD DN' containing 'dc=demo,dc=sample,dc=local', and a dropdown menu for 'AD Username Attribute' set to 'SAM Account Name'.
- Verify Account Status On Each Authentication:** This section contains a checkbox for 'Perform Status Check' which is currently unchecked.
- Additional Logins:** This section contains three checkboxes: 'Configured for PEAP Login' (set to 'No'), 'Use For Admin Logins' (unchecked), and 'Use For Sponsor Logins' (checked).
- Test Authentication:** This section contains a checkbox for 'Run Authentication Test?' (checked), a text box for 'Test Username' containing 'bob', and a text box for 'Test Password' containing '****'.
- VLAN Configuration:** This section contains a checkbox for 'Use VLAN Range' which is currently unchecked.

5. Click **Save**.

NOTE

The "Configured for PEAP Login" will be set to No until you join the server to the PEAP domain (shown later).

6. On the ensuing Server Certificate Information screen, Click **Save**.

Configuring DNS and Verifying Readiness for Cloudpath to Join Active Directory Domain

Perform the following steps to configure DNS and verify that the Active Directory server is ready to be joined by Cloudpath:

1. Configure DNS. Active Directory uses DNS in the background to locate other domain controllers and services, such as Kerberos. Therefore, Active Directory domain members and servers must be able to resolve the Active Directory DNS zones. The following describes how to manually configure Cloudpath to use DNS servers:
 - a. Log into your Cloudpath system from the command line as `cpn_service`.
 - b. Run the **show config** command. Check if there is a DNS (*nameserver*) entry for your Active Directory server. Typically, the existing `/etc/resolv.conf` file contains only the DNS nameserver entry of the local host. If your Active Directory server is in a different DNS nameserver, follow the next step to add the Active Directory nameserver.
 - c. Run the command: **config network STATIC dns nameserver_ip1 nameserver_ip2** to add nameservers into the `/etc/resolv.conf` file, as follows:
 - `nameserver_ip1`
 - `nameserver_ip2`

If there is more than one nameserver for multiple Active Directory servers in the PEAP domain, you can add multiple nameservers. However, the `/etc/resolv.conf` file has a limit of three nameserver entries.
 - d. Run the **show config** command again. Verify that the *nameservers* are correctly configured.
2. Test DNS resolution: On the Cloudpath UI, go to **Support > Diagnostics**, then click the **DNS Lookup** tab.
 - Forward lookup: Enter the fully qualified domain name (FQDN) of your AD server (such as `msft-dc-2012.demo.sample.local`) in the Server DNS field, then click the **Run** button. Check that the returned IP address is the IP address of the AD server.
 - Reverse lookup: Enter the IP address of your AD server in the Server DNS field, then click the **Run** button. Check that the returned name is the host name of the AD server.
3. Ping the AD server. Verify that you can ping the FQDN under the Ping tab in the **Support > Diagnostics** portion of the UI. If the ping is not successful, check the network connectivity between the Cloudpath server and your AD server.
4. Test the Cloudpath connection to the AD Server:
 - a. Go to the **Configuration > Authentication Servers** portion of the UI.
 - b. Click the right-pointing green arrow to the right of the AD whose connection you are testing.
 - c. On the ensuing "Test" popup window, enter the credentials for a user in that AD, then click **Continue**.
 - d. You will receive a success or failure message, along with other pertinent information.

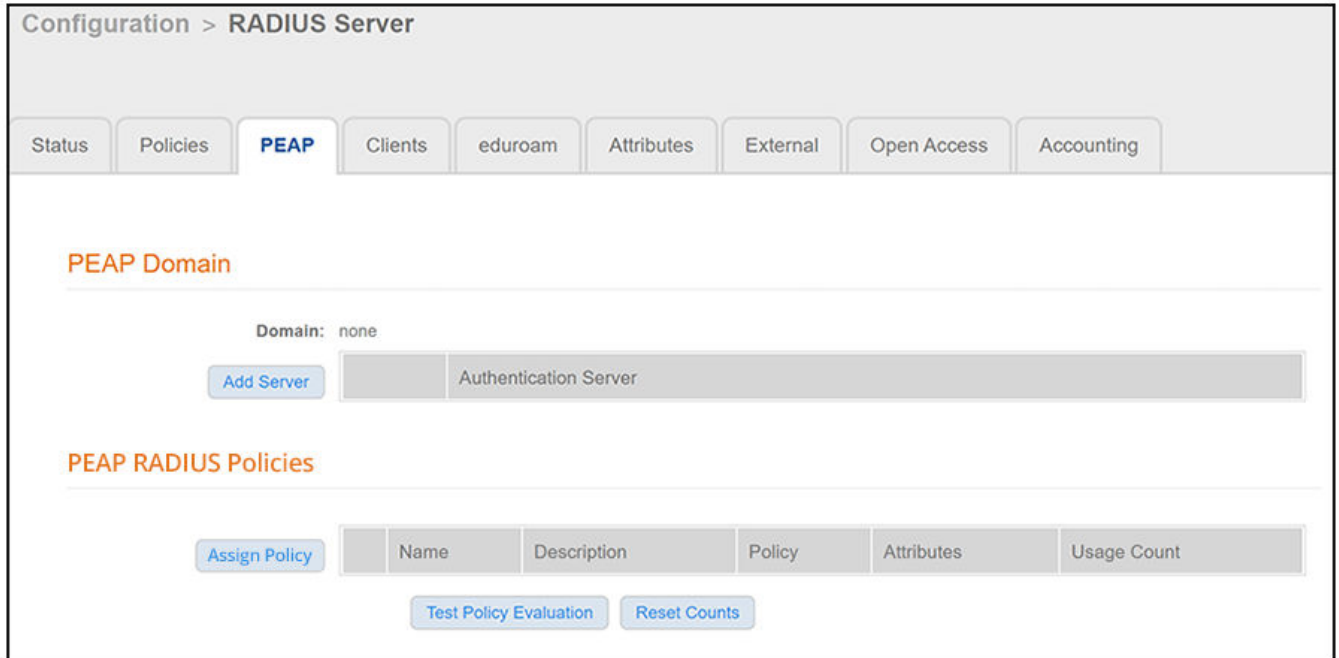
Adding an Active Directory Authentication Server

You need to add at least one authentication server to the PEAP realm.

Follow the steps below:

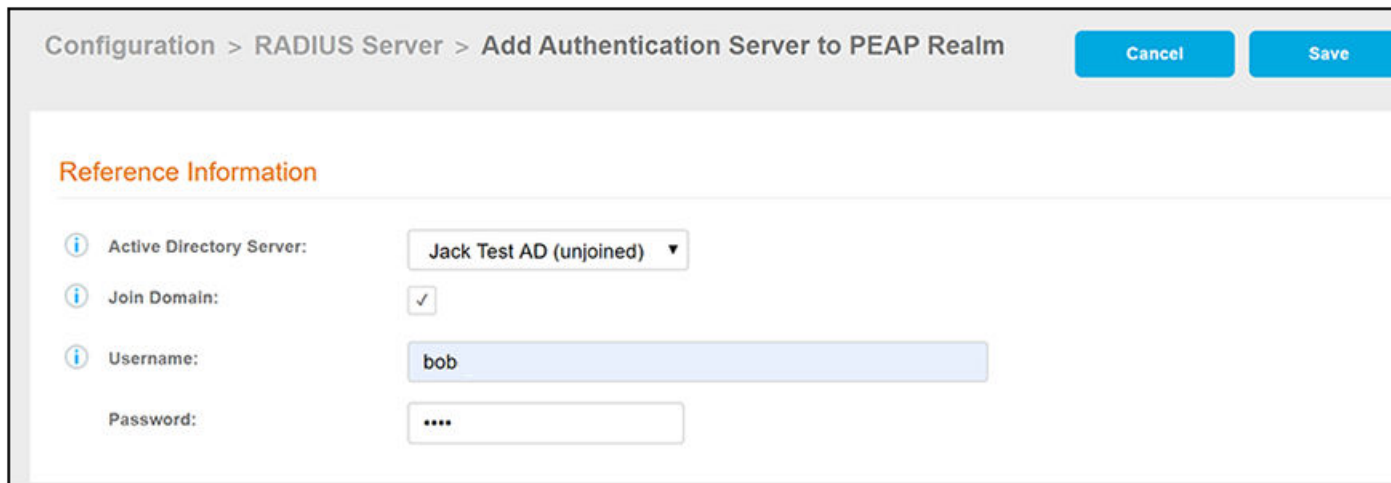
1. In the Cloudpath UI, go to **Configuration > RADIUS Server**.
2. Click the **PEAP** tab.
3. The first time you go here, you may be presented with a button called **ENABLE PEAP**. Click this button to proceed. You should then arrive at the following screen :

FIGURE 3 PEAP Domain and PEAP Policies Screen



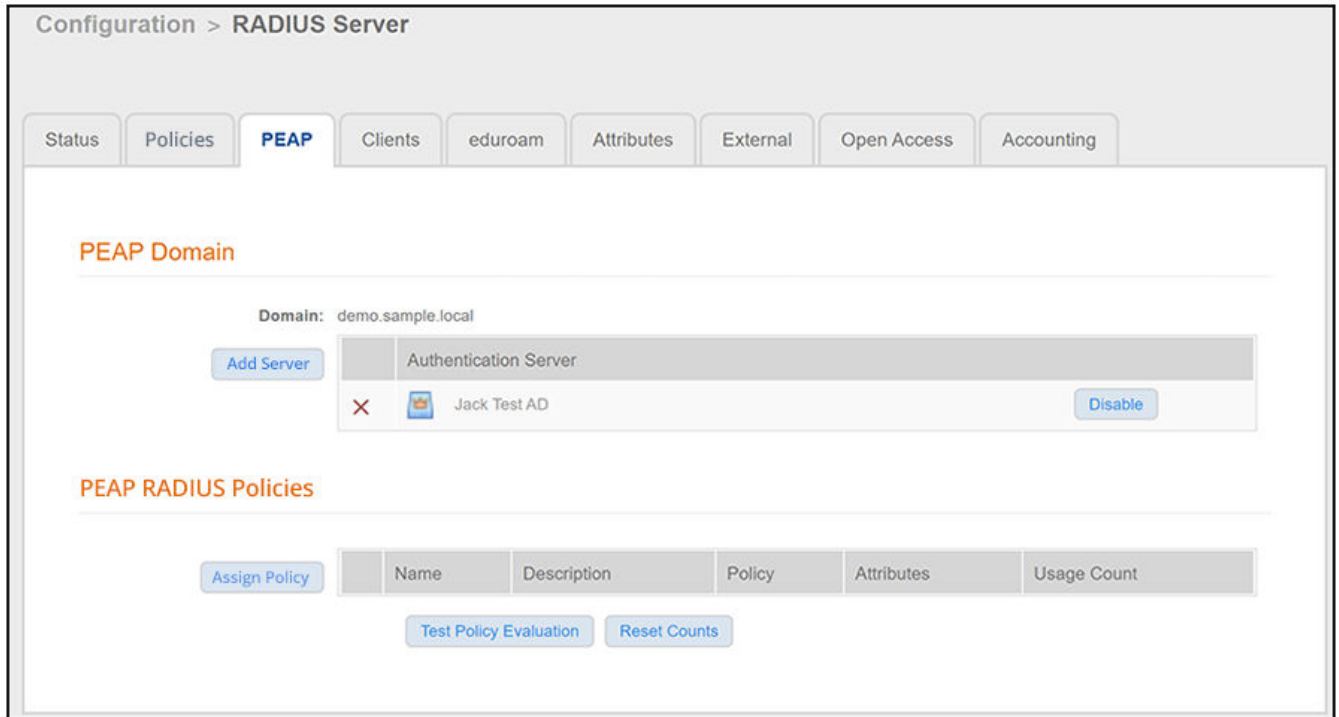
4. In the PEAP Domain section of the screen, click **Add Server**.
5. On the ensuing Add Authentication Server to PEAP Realm screen (see the completed example figure below), do the following:
 - From the Active Directory Server drop-down, select the active directory server that you want to join the PEAP domain.
 - Check the Join Domain box.
 - For Username and Password, enter the credentials for an Active Directory user (with domain join permissions) to enable this server for PEAP.

FIGURE 4 Adding Active Directory Server to PEAP Realm



6. Click **Save**.
7. The PEAP Domain portion of the screen should now indicate the realm (domain), as shown in the example below:

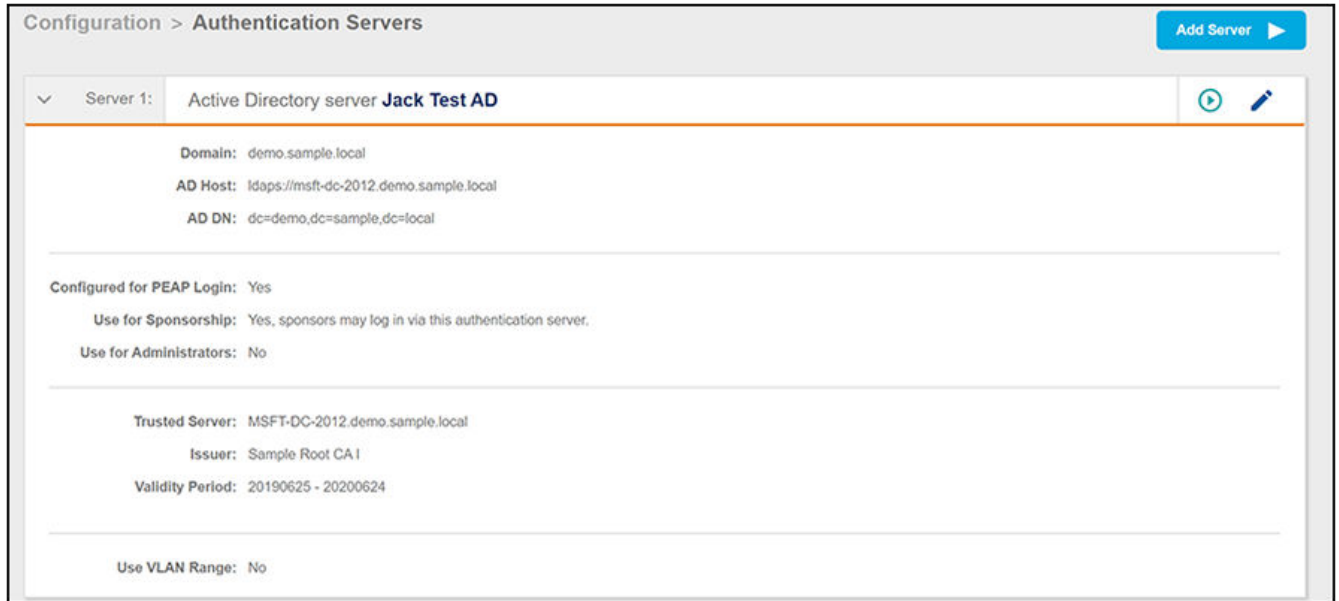
FIGURE 5 Authentication Server Successfully Added to PEAP Domain



The crown icon to the left of the server name indicates that it is the master server because it is the first one added to the PEAP domain. If you have multiple servers in the domain, and you wish to remove them, the master server needs to be the last one that you remove.

8. You can now go back to the Authentication Server configuration (**Configuration > Authentication Servers**), and the "Configured for PEAP Login" field should now have the "yes" value, as shown below:

FIGURE 6 Authentication Server Now Configured for PEAP Login



PEAP Realm Ports Used

Once you have enabled PEAP and successfully added an authentication server to the PEAP realm, port 445 over TCP and port 445 over UDP are opened. To confirm that this has occurred, go to **Administration > Firewall Requirements**, then check the inbound traffic. The screen below includes the applicable information:

FIGURE 7 PEAP Realm Ports

Traffic:		Inbound to this System		
Purpose	System Address	External Address	Protocol	Reason
Web Interface	jeff243.cloudpath.net:443		TCP / HTTP(s)	Administrator, API, and end-user access to the web interface.
PEAP Realm	jeff243.cloudpath.net:445		TCP	Microsoft-DS Active Directory, Windows shares.
PEAP Realm	jeff243.cloudpath.net:445		UDP	Microsoft-DS SMB file sharing.

Using Policies

Configuring Policies

Policies allow for mapping incoming successful RADIUS authentication requests to a set of RADIUS response attributes based on dynamic conditions of the request. Each policy has an associated RADIUS attribute group which defines the RADIUS response attributes (such as VLAN ID, filter ID, and class). Each authentication is matched against an assigned list of candidate policies in sequential order. Criteria of a policy can include dynamic conditions such as a user's physical location, username, or the time of day.

As of this release, policies can be used for PEAP authentication with the Cloudpath onboard RADIUS server.

The following procedure guides you first through creating RADIUS attribute groups for your policies, then creating the policies themselves. You must create at least one RADIUS attribute group before you can configure a policy because a policy needs to have at least one RADIUS attribute group available for selection.

NOTE

If none of your policies are a match for a prospective user, the user's attempt to join the network is declined.

1. In the Cloudpath UI, go to **Configuration > Policies**.
2. Select the **RADIUS Attribute Groups** tab, then click the **Add RADIUS Attribute Group** button.
3. In the ensuing Create Radius Attribute Group screen, enter the information to create the group, then click **Save**.

NOTE

You can configure as many RADIUS Attribute groups as you want. One RADIUS Attribute group will later be assigned to each policy you create.

An example screen and field descriptions follow:

FIGURE 8 Create RADIUS Attribute Screen

Configuration > Policies > Create RADIUS Attribute Group

RADIUS Attribute Group Information

Display Name: VLAN 1

Description:

Assigned Policies:

Attributes

Certificate Reply Username: Certificate Common Name (Default)

VLAN ID: 1

Filter ID: [ex. BYOD]

Class: [ex. BYOD]

Reauthentication: [ex. 86400] Seconds

+ Add

- Display Name: The name of the RADIUS attribute group. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this RADIUS attribute group. It is visible only to Cloudpath administrators.
- Assigned Policies: This field lists the names of all the policies that are using this RADIUS attribute group. There will be no policies listed here during the initial configuration of the group.
- Certificate Reply Username: This setting is applied only when the RADIUS attribute group is associated with certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.
- VLAN ID: If this field is populated, the VLAN ID is included in the RADIUS reply to the controller for successful authentications. Cloudpath sends Tunnel-Type, Tunnel-Medium-Type, and Tunnel-Private-Group-ID. If your network policy is wireless, the Tunnel-Type value is VLAN, the Tunnel-Medium-Type value is 802 (this includes all 802 media plus Ethernet canonical format), and the Tunnel-Private-Group-ID is the integer that represents the VLAN number to which group members will be assigned.

If the VLAN ID field is left blank, Cloudpath will not return a VLAN ID in the RADIUS reply; therefore the controller assigns the VLAN ID based on its own configuration.
- Filter ID: If this field is populated, the Filter ID is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Filter ID in the RADIUS reply.
- Class: If this field is populated, the Class is included in the RADIUS reply for successful authentications. If this field is left blank, Cloudpath will not return a Class in the RADIUS reply.
- Reauthentication: The number of seconds included in the RADIUS reply for successful authentications. If the device stays connected for longer than this period, the WLAN or switch requires that the device be reauthenticated. In wireless devices, this causes the encryption keys to rotate.
- Additional Attributes: You can add other attributes in the "Attributes" section of the screen by clicking the + button, and selecting the desired fields and values. These attributes will be returned to the controller in an access-accept RADIUS server packet.

4. Configure your policies:
 - a. In the **Configuration > Policies** area of the UI, select the **Policies** tab, then click **Add Policies**.
 - b. In the ensuing Create Policy screen, enter the information to create the policy, then click **Save**.

NOTE

You can configure as many policies as you want.

An example screen and field descriptions follow:

FIGURE 9 Create Policy Screen

The screenshot shows the 'Create Policy' configuration screen. At the top, there is a breadcrumb 'Configuration > Policies > Create Policy' and two buttons: 'Cancel' and 'Save'. The screen is organized into three main sections:

- Policy Information:** Contains a 'Display Name' field with the value 'Building 1 on weekdays' and an empty 'Description' text area.
- Conditions:** Includes a note: 'All conditions are optional. Note, some conditions only apply to certain locations, and will be ignored if used locations that they do not apply.' Below this are several conditions with checkboxes:
 - Username (regex):
 - SSID (regex):
 - NAS Identifier (regex): Matching Building 1 on weekdays
 - RADIUS Realm (regex):
 - DPSK Reference Name (regex):
 - Allow by AD Group:
 - Specific Time:
 - When: WEEKDAY
 - Start: 7:30 AM
 - End: 6:00 PM
 - RADIUS Client:
- RADIUS Attributes:** Contains a 'RADIUS Attribute Group' dropdown menu with the selected value 'VLAN 1 [Reply Username: 'Certificate Common Name (D)']'.

- Display Name: The name of the policy. This should be a descriptive name. It is visible only to Cloudpath administrators
- Description: Optionally, enter a description of this policy. It is visible only to Cloudpath administrators.

- "Conditions": In the Conditions section, use any or all of these fields to create the matching criteria you desire so that the appropriate policy gets applied to each user.

NOTE

You can use the asterisks that appear in some of the Conditions fields, when selected, to denote that any value is acceptable in the place of the asterisk.

- Username Regex: When the user is prompted for credentials, the username specified by the user will be verified against this regular expression for proper format. For example, `^d{8}$` will ensure that the user enters an 8-digit ID.

NOTE

Due to the complexity of regular expressions, it is recommended to use this field only if you are experienced with regular expressions. If you need assistance creating a regular expression to match your needs, contact support.

- NAS Identifier: A regex that defines the network access service (NAS) identifier to limit this policy..

NOTE

If you use this field, and no NAS Identifier is provided in the response, the policy will be "false" and will not get applied to a user.

- RADIUS Realm (regex): The RADIUS realm to use in this policy, in the form of `@company.com` or `company.com`
- DPSK Reference Name (regex): A regular expression to test against the DPSK Reference Name.

NOTE

This field is applicable only when the policy is applied to a DPSK pool.

- Allow by AD Group: A regular expression that defines the groups within the Authentication Server that this policy allows.

NOTE

Active Directory is the only authentication server supported for PEAP

- Specific Time: If checked, drop-downs appear where you can specify the days and times that this policy allows enrollment. Be sure to click the **Set** button to set the desired time (see the following illustration):

FIGURE 10 Setting a Time for a Policy

Specific Time:

When: WEEKDAY ▾

Start: 7:30 AM

End: 7 : 30 AM

RADIUS Client:

RADIUS Attributes

RADIUS Attribute Group:

Set

Hour				Minutes			
AM	PM	00	05	10	15		
1	2	3	4	20	25	30	35
5	6	7	8	40	45	50	55
9	10	11	12				

- RADIUS Client: If you check this box, you are presented with a drop-down where you can then select a RADIUS client if you have already configured this client in the **Configuration > RADIUS Server > Clients** tab. This RADIUS client would then be associated with this policy.
- RADIUS Attribute Group: From this drop-down, select the attribute group that you want associated with this policy.

The following illustration shows the Policies tab after one policy has been added. The information shown in the table represents the policy configuration shown in the example in [Figure 9](#). The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. (The "Certificate Reply Username" applies only to certificate-based authentications, and is therefore described in the Cloudpath documentation of certificate templates.) The RADIUS attribute information shown below comes from the example in [Figure 8](#).

FIGURE 11 Policies Table Example After One Policy Is Configured



	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert. Template Rel.	PEAP Rel.
	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	0	0	0

Adding Policies to RADIUS Server Configuration

You can add as many policies as you want, but only one policy can be associated with a given user. For a user to successfully connect to the network, the user must be a match for at least one policy.

Steps to Add Policies

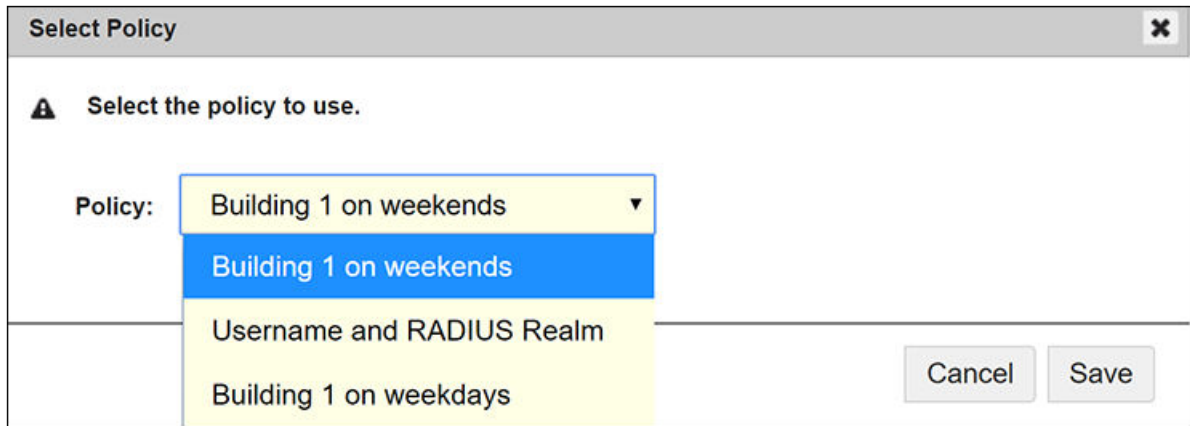
Follow these steps to add a policy:

1. In the Cloudpath UI, go to **Configuration > RADIUS Server**.
2. Click the **PEAP** tab.
3. Click **Assign Policy**. The Select Policy Drop-down List appears, as shown in the following example list. The policies that you have already configured are available for you to add:

Using Policies

Adding Policies to RADIUS Server Configuration

FIGURE 12 Select Policy Drop-down List



4. Select the policy you wish to add, then click **Save**.
5. Continue to add policies as you desire. If you have added all available policies, you will receive the message: " All Defined Policies have been assigned."

Policy Rules

The following illustration shows an example of how the page appears after three policies have been added:

FIGURE 13 PEAP Policies Added Via RADIUS Server PEAP Tab

PEAP Domain

Domain: demo.sample.local

Add Server

Authentication Server

Jack Test AD Disable

PEAP RADIUS Policies

Assign Policy

	Name	Description	Policy	Attributes	Usage Count
✕ ^ v	Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'	0
✕ ^ v	Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'	0
✕ ^ v	Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): 'company.com'	VLAN: '3' Filter ID: 'filter ID 10'	0

Test Policy Evaluation Reset Counts

- There may be many policies whose criteria are matched by a user, but the first policy that is a match is the one that gets applied. For example, if you have three policies, as shown above, the order in which you have them listed is the order in which they will be tested for matches with an enrolling user.

NOTE

You can use the arrows in the screen show above to list the policies in the desired order. If you want to remove a policy from being used with PEAP, click the X next to the policy, then confirm the removal of the policy when prompted.

- Because the "Building 1 on weekends" policy is listed first, the matching criteria in that policy (listed in the Policy column) will first be checked against an enrolling user. If there is a match, the policy is applied to the user (meaning that the attributes listen in the Attributes column are applied to the user). If there is no match, the next policy ("Building 1 on weekdays") is checked against the enrolling user, and so on.

NOTE

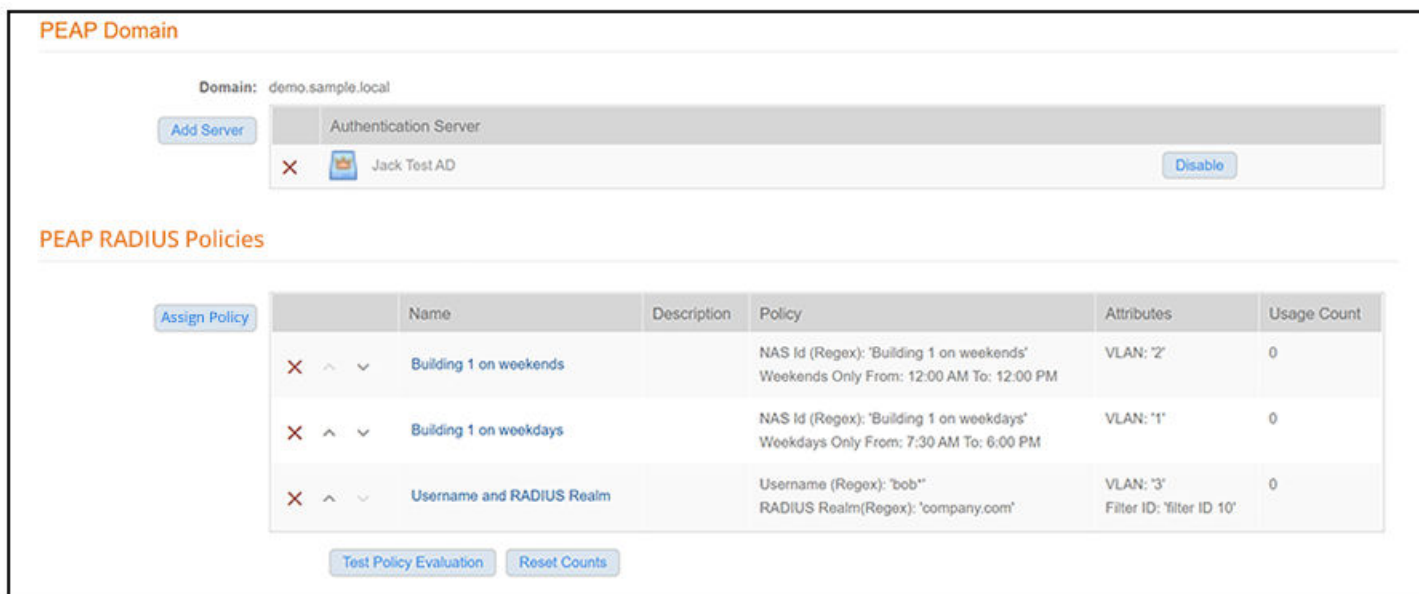
Even though this example shows only three policies for simplicity sake, *you must configure policies so that all users will be a match for at least one policy. If a user matches at least once policy, the user will be given network access because all policies are "allow only."* However, if a user does not match **any** policy, the user is denied network access.

Testing Policies

You can test your policies to be sure they are working as desired before you implement them in a live environment.

The following screen shows an example of three policies that have been added to PEAP via the **Configuration > RADIUS Server** PEAP tab of the UI:

FIGURE 14 Three-Policy Example



Test Policy Evaluation - Example 1

1. Click the **Test Policy Evaluation** button (see the screen above).
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 15 Test Policy Selection Example 1

Configuration > DPSK Pools > DPSKs > Test Policy Selection Cancel Apply ▶

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

i Username:

i SSID:

i Authentication Groups:

i NAS ID:

i DPSK Reference Name:

i Authentication Date:

i Authentication Time:

i Client Short Name:

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

The sample values shown above have been entered to test that the "Building 1 on weekdays" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

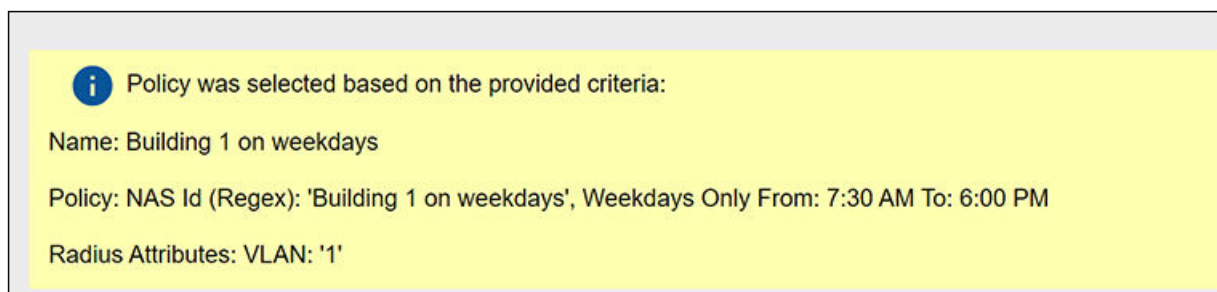
NOTE

The sample values can include fields that are not configured in a policy, and could still be a match for the policy. For example, there could be a value entered in the Client Short Name field in the example above, and it would have no impact on the results of the policy evaluation test because none of the three policies shown above show a value for Client Short Name (as evidenced by the values shown in the Policy column for each policy).

- Username (required): Must be a valid username that your Cloudpath system will accept when this user attempts enrollment.
- SSID: Matches the Wi-Fi SSID name for the connecting device. If this field is populated, this will match only the Wi-Fi based connections.

- Authentication Groups (required): The list of groups returned from a user (as configured in your authorization server; you need a workflow step that requires authentication to an authorization server for the user to have groups).
 - NAS ID: The NAS ID that is expected to be returned from the controller. In the example above, the value "Building 1 on weekdays" is entered because it matches the NAS ID of the "Building 1 on weekdays" policy.
 - Authentication Date: The date on which the user would attempt to authenticate. In the example above, the date is on a weekday because the "Building 1 on weekdays" policy specifies weekdays only for authentication.
 - Authentication Time: The time when the user would attempt to authenticate. In the example above, the time is 5:10 p.m., which falls in the range of 7:30 a.m. to 6 p.m. that the policy specifies for authentication.
 - Client Short Name: RADIUS Client-Shortname expected to be returned from the controller.
3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
- a. The values entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy.
 - b. The values entered are next compared to the second policy in the list, which is the "Building 1 on weekdays" policy. You can see that the values entered for testing all *do* match those listed for this policy. Therefore, the expected behavior is that, when you click the **Apply** button, the "Building 1 on weekdays" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
 - c. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 16 Test Policy Selection Example 1 Results



Test Policy Evaluation - Example 2

1. Click the **Test Policy Evaluation** button.
2. In the ensuing Test Policy Selection screen, enter the values that would be provided during user enrollment to determine which policy, if any, is a match. The screen below contains sample values, which are described below the screen:

FIGURE 17 Test Policy Selection Example 2

Configuration > DPSK Pools > DPSKs > Test Policy Selection

Cancel Apply

User, Radius and Controller Values

Provide the values below that the user, RADIUS and the controller would provide and the matching policy will be determined.

Username: bobb@company.com

SSID: SSID

Authentication Groups: DEMO\domain users DEMO\bob

NAS ID: 54-EC-2F-D9-D5-4C

DPSK Reference Name: UserDevice_123

Authentication Date: 20200512

Authentication Time: 5:10 PM

Client Short Name: 0.0.0.0/0

Policies

Name	Description	Policy	Attributes
Building 1 on weekends		NAS Id (Regex): 'Building 1 on weekends' Weekends Only From: 12:00 AM To: 12:00 PM	VLAN: '2'
Building 1 on weekdays		NAS Id (Regex): 'Building 1 on weekdays' Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN: '1'
Username and RADIUS Realm		Username (Regex): 'bob*' RADIUS Realm(Regex): '@company.com'	VLAN: '3' Filter ID: 'filter ID 10'

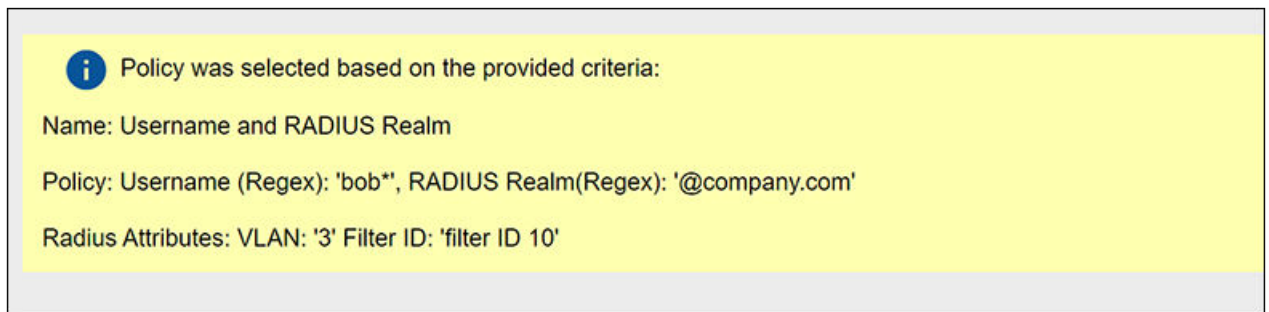
The sample values shown above have been entered to test that the "Username and RADIUS Realm" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

3. Before you click the **Apply** button, check the values you have entered. In the above example, the expected behavior is:
 - a. The values you entered in the upper portion of the screen are first compared to the policy named "Building 1 on weekends" because that is the policy listed first (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekends" policy. For example, the "Building 1 on weekends" policy includes a Regex value of "Building 1 on weekends," but the sample test values entered in the screen above do not include any value for NAS ID, therefore eliminating any chance of a match to this policy.
 - b. The values entered in the upper portion of the screen are next compared to the policy named "Building 1 on weekdays" because that is the next policy listed (see Policies section in the screen above). However, you can see that the values entered for testing do not match the conditions shown in the Policy column for the "Building 1 on weekdays" policy either. For example, the "Building 1 on

weekdays" policy includes a Regex value of "Building 1 on weekdays," but the sample test values entered in the screen above do not include any value for NAS ID, therefore eliminating any chance of a match to this policy.

- c. The values entered are next compared to the third policy in the list, which is the "Username and RADIUS Realm" policy. You can see that the values entered for testing all *do* match the conditions listed for this policy: A username in the form of bob* (where the * can be replaced with any value) and a RADIUS realm (in the username field for the sample test values) in the form of company.com. Therefore, the expected behavior is that, when you click the **Apply** button, the "Username and RADIUS Realm" will indicate a successful match, and the corresponding attributes would be applied to the enrolling user.
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 18 Test Policy Selection Example 2 Results



Viewing Policy Information

To view your currently configured policies, go to **Configuration > Policies** in the UI, and be sure to highlight the Policies tab.

The following table shows you an example of what a policy table looks like after three different policies have been created, and have been assigned to PEAP and/or DPSK pools.

FIGURE 19 Policy Table Example

	Name	Policy	Attribute Group Name	Attributes	DPSK Rel.	Cert.Template Rel.	PEAP Rel.
	Building 1 on weekdays	NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM	VLAN 1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	1	0	1
	Building 1 on weekends	NAS Id (Regex): 'Building 1 on weekends', Weekends Only From: 12:00 AM To: 12:00 PM	VLAN 2	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	1	0	1
	Username and RADIUS Realm	Username (Regex): 'bob', RADIUS Realm(Regex): 'company.com'	VLAN 3 and Filter ID	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	1	0	1

You can use the policy table as follows:

Using Policies

Viewing Policy Information

TABLE 1 Description of Policy Table

Column Title	Description
+	<ul style="list-style-type: none">You can view details of the policy by clicking on the magnifying glass icon (for an example of the Policy Information screen that gets invoked, see Figure 20).You can edit the policy by clicking on the pencil icon.If the policy has not yet been assigned (such as to PEAP or a DPSK pool), there will be a X next to the policy name. Clicking that X deletes the policy. However, in the example above, all three policies are in use; therefore the - sign denotes that you cannot delete the policy as long as it remains in use. You would first need to remove the policy from where it is being used before you can delete the policy from the table shown above.
Name	The name of the policy as configured in the Display Name field in the Policy configuration screen, an example of which is shown in Figure 9 on page 13.
Policy	All the conditions that you set when you created the policy are listed in this column. For example, the "Building 1 on weekdays" policy conditions are the ones that were configured in the example shown in Figure 9 on page 13
Attribute Group Name	The name of the group that has been selected in the RADIUS Attribute Group drop-down when the policy was created. For the "Building 1 on weekdays" policy shown in this example, the group name VLAN 1 matches the selection that was shown in the example in Figure 9 on page 13.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 8 on page 12.
DPSK Rel, Cert Template Rel, and PEAP Rel	The number of times that a policy has been assigned to each category of authentication.

FIGURE 20 Policy Information Screen Example

Policy Information

Name: Building 1 on weekdays

Description:

Conditions: NAS Id (Regex): 'Building 1 on weekdays',
Weekdays Only From: 7:30 AM To: 6:00 PM

RADIUS Attribute Group: Reply Username: 'Certificate Common Name (Default)',
VLAN: '1'

Relationships

Type	Location	Usage Count
PEAP	PEAP	0
DPSK	DPSK Pool 17	0
CERTIFICATE	username@byod.company.com	0

The screen above indicates that the policy is currently being used by PEAP, one DPSK pool, and one certificate. The "Location" column of this screen in the UI provides live links to the specific configuration areas where the policy is used.

The Usage column will be incremented each time a device is assigned to the policy in question. Also, If a device then gets assigned to a different policy and later gets reassigned to its original policy, the usage count of the original policy will be incremented.

Viewing RADIUS Attribute Information

To view your currently configured RADIUS attribute groups, go to **Configuration > Policies** in the UI, and be sure to select the RADIUS Attribute Groups tab.

The following table shows you an example of what a RADIUS Attribute Groups table looks like after three different RADIUS attribute groups have been created.

FIGURE 21 Radius RADIUS Groups Example

+	Name	Description	Policy Count	Attributes	Timestamp
	VLAN 1		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	20210118 1509 MST
	VLAN 2		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	20210118 2024 MST
	VLAN 3 and Filter ID		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '3', Filter ID: '10'	20210118 2025 MST

You can use the RADIUS Attribute Groups table as follows:

TABLE 2 Description of RADIUS Attribute Groups Table

Column Title	Description
+	<ul style="list-style-type: none"> You can edit the RADIUS attribute group by clicking on the pencil icon. If the RADIUS attribute group has not yet been assigned to any policy, there will be a X next to the name. Clicking that X deletes the group. However, in the example screen shown above, all the groups have already been assigned to at least one policy; therefore the X is not selectable, which denotes that you cannot delete the group as long as it remains in use by one or more policies. You would have to edit the policy itself to remove the RADIUS attribute from the policy if you then want to delete the RADIUS attribute.
Name	The name of the radius attribute group as configured in the Display Name field in the Radius Attribute Group configuration screen, an example of which is shown in Figure 8 on page 12.
Description	Any optional description that was entered in the configuration of the Radius attribute group.
Policy Count	The number of policies that the Radius attribute is currently assigned to.
Attributes	Lists all the attributes that were set for the corresponding RADIUS attribute group name. For the "VLAN 1" attribute group name shown in this example, the attribute "VLAN 1" is listed because that is the only attribute that was set during the configuration of the VLAN 1 RADIUS attribute group name, as shown in Figure 8 on page 12.
Timestamp	Time that the radius attribute group was created.

Checking a User Record

You can check the record of a user for various information, including the PEAP policy that has been applied to the user upon a successful enrolment.

To view a user's record, go to **Dashboard > Users & Devices** in the UI, then click the magnifying glass icon for the user whose information you wish to view. An example of the record for a user named bob is shown in the figure below. Toward the bottom of the record, the PEAP authentication date and PEAP policy used are shown.

NOTE

If there was no policy applied to a user, the PEAP Policy Used column will indicate: "no match," denoting that the user has not been allowed into the Cloudpath system. You must configure your policies so that at least one policy will be a match for any given user who needs access.

FIGURE 22 User Information Includes PEAP Policy Used

The screenshot displays a 'User Information' page for a user named 'bob'. The page lists various attributes such as Username, Email Address, Blocked status, Common Name, Distinguished Name, Office Name, Department, Company, Server Name, Server Type, Domain, PEAP Authentication Date, PEAP Policy Used, and Groups. The PEAP Policy Used is 'students' and the PEAP Authentication Date is '2/2/20 9:42 PM'. There is also a 'Block' button next to the 'Blocked' status.

Field	Value
Username:	bob
Email Address:	bob@cloudpath.net
Blocked:	No. Block
Common Name:	Bob Smith
Distinguished Name:	CN=Bob Smith,CN=Users,DC=demo,DC=sample,DC=local
Office Name:	Bob Office
Department:	Bob Dep
Company:	Bob Corp
Server Name:	Jack Test AD
Server Type:	Active Directory
Domain:	demo.sample.local
PEAP Authentication Date:	2/2/20 9:42 PM
PEAP Policy Used:	students
Groups:	BYOD-EMPLOYEE Allowed RODC Password Replication Group Administrators

Additional Information:

- In the user table, if the user does not already have a user record (onboarded a device previously), then a new user record gets created.
- If the user already exists, an updated user record will show the most recent PEAP authentication date and the PEAP policy matched (or "no match").



© 2022 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>