

Cloudpath Enrollment System Microsoft Certificate Authority Configuration Guide, 6.0

Supporting Cloudpath Software Release 6.0

© 2024 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

CommScope and the CommScope logo are registered trademarks of CommScope and/or its affiliates in the U.S. and other countries. For additional trademark information see <https://www.commscope.com/trademarks>. All product names, trademarks, and registered trademarks are the property of their respective owners.

Patent Marking Notice

For applicable patents, see www.cs-pat.com.

Contents

New in This Document	5
Overview of Issuing Certificates with the Integration Module for Microsoft CA	7
Integration Module Specifications	9
Recommendation.....	9
Deployment Requirements.....	9
Deployment Process	11
What You Need.....	11
Configuring Policies	13
Configuring the Certificate Template for the Microsoft CA	19
Configuring Microsoft Intune in Cloudpath	25
Enhanced SAN Handling for SCEP Certificates	27
Feature Overview.....	27
Requirements.....	27
Considerations.....	27
Best Practices.....	27
Prerequisites.....	28
Configuring SAN Attributes	29
Adding RADIUS Policies to the CA Certificate Template	33
Steps to Add Policies.....	33
Policy Rules.....	34
Additional Policy Information	37
Testing Policies.....	37
Test Policy Evaluation - Example 1.....	37
Test Policy Evaluation - Example 2.....	39
Test Policy Evaluation - Example 3.....	41
Viewing Policy Information.....	43
Viewing RADIUS Attribute Information.....	45
Switching Pre-Release-5.8 Microsoft CA Certificate Templates to Policy-Assigned Templates	47
Downloading the Integration Module	49
Configuring the Web Server	51
Verify Role Services.....	51
Set Up the Integration Module Website.....	52
Multiple Certificate Templates.....	54
Testing the System	55
Troubleshooting	57
DNS.....	57
CA Name.....	57
ASP.NET Installed on the IIS Server.....	57
ASP Hosting Permissions.....	57

Restart the IIS Server.....	58
Failing Microsoft CA Test.....	58

New in This Document

The following table provides a description of new information added to this guide.

TABLE 1 Summary of Enhancements in Cloudpath Release 6.0

Feature	Description	Reference
Support for SAN attribute	The new checkbox, Use SAN values from request is available within SCEP settings to enable or disable SAN value utilization.	Configuring SAN Attributes on page 29

Overview of Issuing Certificates with the Integration Module for Microsoft CA

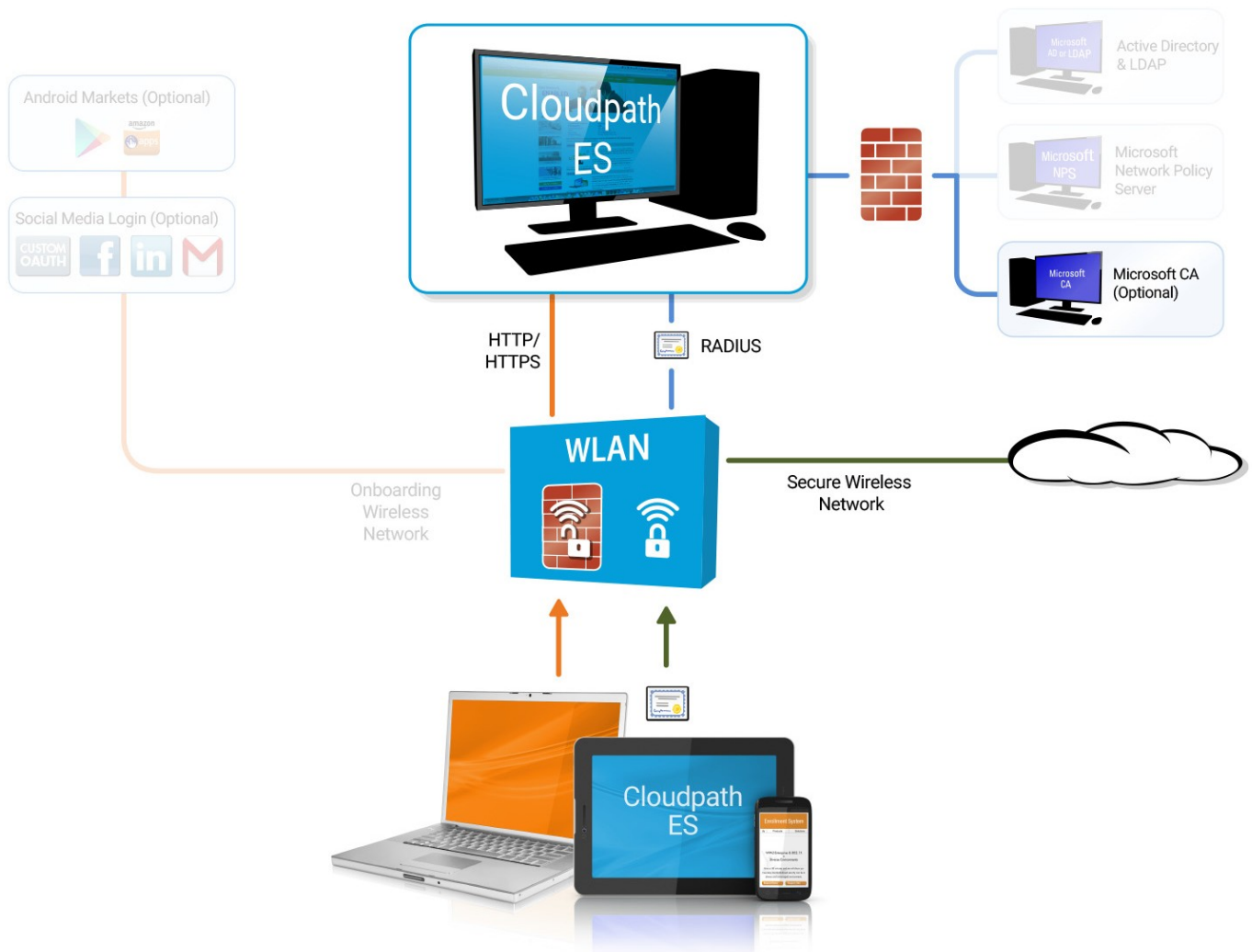
The Integration Module for Microsoft™ CA allows network administrators to issue certificates from a Microsoft CA. As a network administrator, you can configure Cloudpath for the Integration Module.

To implement certificate-based authentication on your WPA-2 Enterprise and 802.1X network, through EAP-TLS, you must set up a certificate infrastructure, which includes a certificate authority (CA) for issuing client certificates.

The Cloudpath Integration Module for Microsoft CA allows Cloudpath to request TLS client certificates from your existing Microsoft CA infrastructure.

While configuring a user's device, Cloudpath prompts the user for credentials. It then generates a CSR, authenticates to the CA, and sends the CSR to the CA via the Integration Module. The Integration Module, in coordination with the CA, authenticates the user and, if valid credentials are provided, signs a certificate for the user. The characteristics of the certificate generated are dictated by the certificate template utilized. The certificate is then streamed back to the Cloudpath Wizard, which installs it and configures the SSID to utilize it.

FIGURE 1 Cloudpath Integration Module for Microsoft CA



NOTE

The Integration Module for Microsoft CA is essentially a sibling to the Microsoft Network Device Enrollment Service (NDES). Unlike Microsoft NDES, which assigns all certificates to the SCEP_ADMIN user account, the Integration Module assigns each issued certificate to the corresponding user account.

Integration Module Specifications

Recommendation

It is recommended that you do not install the Integration Module on a domain controller. By default, you cannot run a web server on a domain controller unless you change policy settings. Also, users typically do not have LOGON_INTERACTIVE rights for domain controllers, as they do for other machines.

Deployment Requirements

- Install on a Windows Domain-joined Microsoft Windows 2008 R2 (IIS) or greater web server.
Other servers in the network including the CA and DC can be Windows 2003.
- The web server must meet Microsoft's minimum system requirements.
- The web server should contain a valid certificate to enable HTTPS communication.
- Optionally, the Integration Module can be installed directly onto the CA or RA server.
- Cloudpath must be able to interact with the CA via a URL. It strongly recommend that this URL be HTTPS to provide web server authentication and a secure communication over your network.
- The website that contains the CA's web interface should be configured for appropriate Anonymous authentication.
- To allow communication between the Enrollment Server and the CA, ensure that your firewall is configured for ports 80/443 (HTTP/HTTPS).

Deployment Process

Perform the following steps to deploy the Integration Module for Cloudpath:

- [Configuring Policies](#) on page 13
- [Configuring the Certificate Template for the Microsoft CA](#) on page 19
- [Adding RADIUS Policies to the CA Certificate Template](#) on page 33
- [Downloading the Integration Module](#) on page 49
- [Configuring the Web Server](#) on page 51
- [Testing the System](#) on page 55

What You Need

You need the following information to set up the Integration Module for Microsoft CA:

- CA Host Name of the server with which the plug-in should communicate.
- CA Name, which is the primary label for the CA within the Certification Authority snap-in.
- Requires Attributes for the certificate template.

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.

Policies can be used with EAP-TLS certificate-based authentications through configuration of the certificate template that generated the client certificate.

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.

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 2 Create RADIUS Attribute Screen

- 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: For certificate authentications, the RADIUS server replies by default with the username based on the command name (CN) of the certificate. This username is used by some WLAN infrastructures as the username displayed within the WLAN UI. Options you can select for this field are:
 - Certificate Common Name (default): Returns the certificate CN as the username.
 - Enrollment Username: Returns the username from the enrollment record as the username.
 - Enrollment Username + Device Name: Returns the username and device name from the enrollment record as the username.
 - Certificate Unique ID: Returns the unique ID of the certificate as the username. This option provides anonymity but is traceable.
 - Certificate Common Name + ID: Returns the CN of the certificate plus the unique ID of the certificate as the username.
- 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 3 Create Policy Screen

- 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.

- SSID (regex): A regular expression that lists any Wi-Fi SSID(s) to which you want to limit this policy.
- NAS Identifier: The Network access server (NAS) identifier to limit the 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.

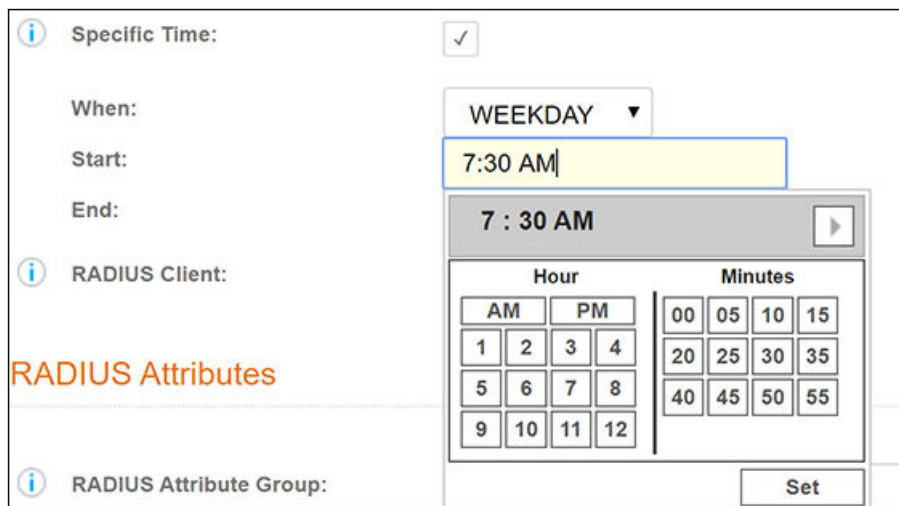
- RADIUS Realm (regex): The RADIUS realm to use in this policy, in the form of @company.com or company.com
- DPSK Reference Name (regex): A regular expression to test against the DPSK Reference Name.

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 usernames within the Active Directory that this policy allows.
- 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 4 Setting a Time for a Policy



- 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 3. The attribute group name and its attributes come from the attribute group name selected in the Create Policy Screen drop-down list. The RADIUS attribute information shown below comes from the example in Figure 2.

FIGURE 5 Policies Table Example After One Policy Is Configured

The screenshot shows a web interface for configuring policies. At the top, there is a breadcrumb 'Configuration > Policies' and a sub-tab 'RADIUS Attribute Groups'. Below this, there is a section titled 'Policies' with an 'Add Policy' button. A table displays the configured policy. The table has columns for Name, Policy, Attribute Group Name, Attributes, DPSK Rel., Cert.Template Rel., and PEAP Rel. The single entry in the table is 'Building 1 on weekdays' with a policy of 'NAS Id (Regex): 'Building 1 on weekdays', Weekdays Only From: 7:30 AM To: 6:00 PM', attribute group 'VLAN 1', and attributes 'Reply Username: 'Certificate Common Name (Default)', VLAN: '1''. Below the table, there are pagination controls showing 'Results 1 - 1 of 1' and a dropdown menu set to '15'.

	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

Configuring the Certificate Template for the Microsoft CA

The certificate template allows the certificates to be pulled from the Microsoft CA.

1. Navigate to **Certificate Authority > Manage Templates**.
2. Click **Add Certificate Template** to create a new certificate template.
3. Select **Use a Microsoft Certificate Authority**, then click **Next**. The following three screens show the complete Microsoft CA Certificate Template Information configuration screen that is displayed. Sample data is shown in these screens, then described following the screens.

FIGURE 6 Microsoft CA Certificate Template Information - Part 1 of 3

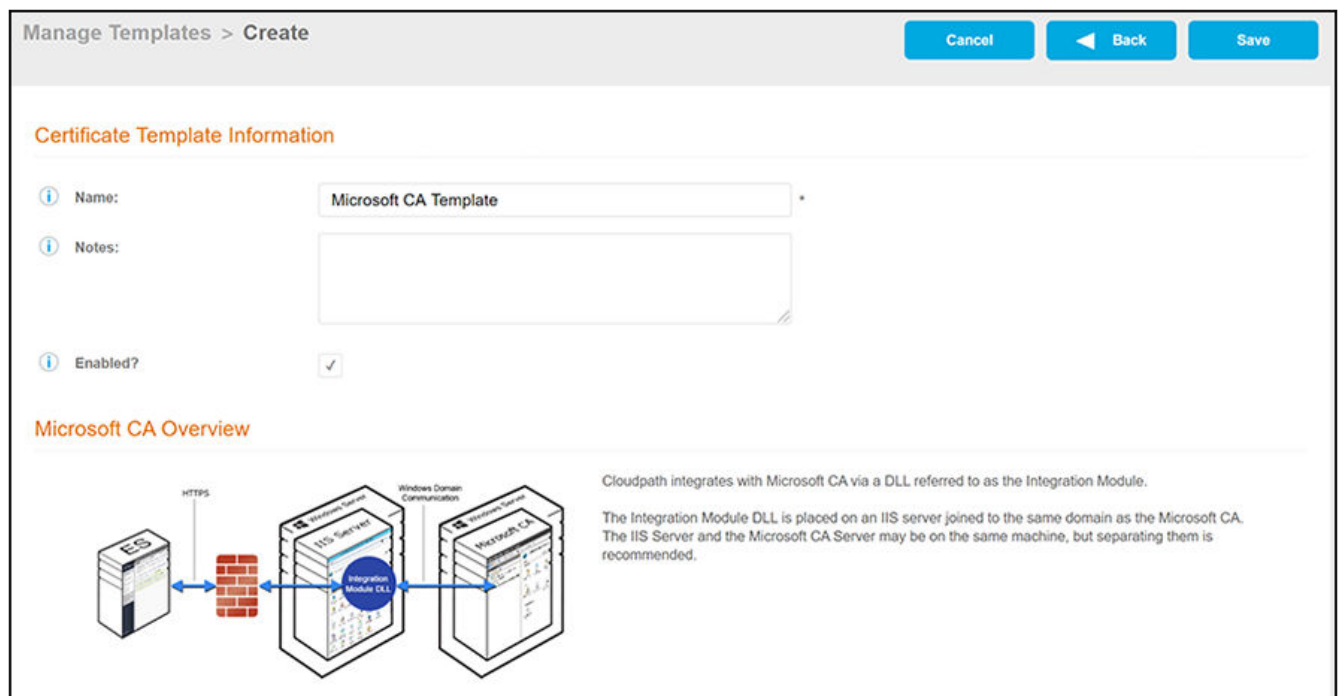


FIGURE 7 Microsoft CA Certificate Template Information - Part 2 of 3

Information Defined on IIS Server

Cloudpath will communicate with the Integration Module DLL using HTTPS. To do so, Cloudpath will need to know the URL of the DLL. This is most commonly something similar to https://server.company.com.

URL of DLL: *

Information Defined In Microsoft CA

The Integration Module DLL will communicate with Microsoft CA using domain communication. To do so, Cloudpath will need to know information about the host and the certificate authority.

CA Host Name: *

CA Name: *

Request Attributes:

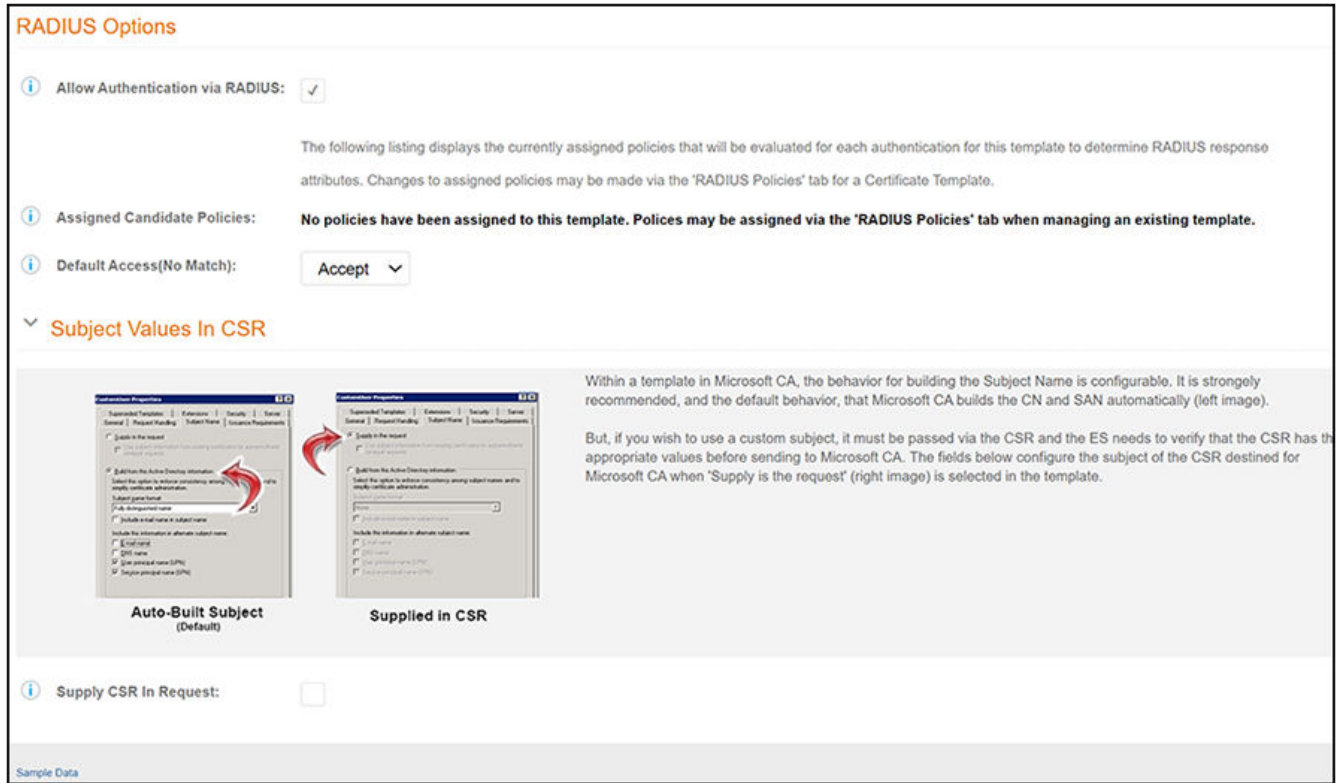
CA Chain:

Key Length:

Algorithm: ▼

Use Static Credentials?

FIGURE 8 Microsoft CA Certificate Template Information - Part 3 of 3



4. In the Certificate Template Information portion of the screen, enter the Name and Notes for the certificate template, and make sure the "Enabled" check box is selected.
5. Enter the URL of the DLL in order for Cloudpath to communicate with the Integration Module DLL using HTTPS.

NOTE

If you configure or change settings in the Microsoft CA certificate template, then you must download and install a new copy of the DLL and files.

6. Enter the "Information Defined In Microsoft CA" settings:
 - CA Host Name: The DNS name of the CA server.
 - CA Name: The name of the CA, which appears in the Certificate Authority console.

NOTE

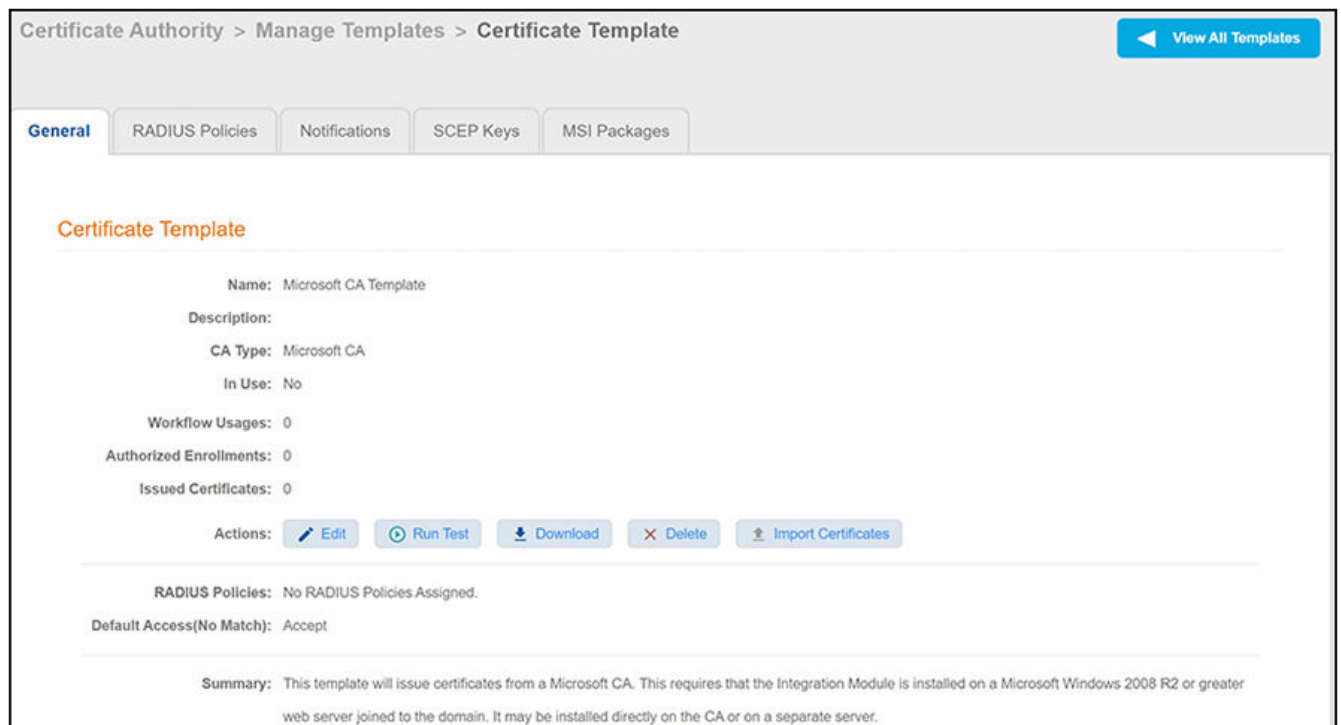
The CA Name should be the name of the CA as displayed in the Certificate Authority snap-in. On Windows, it also displays in the **Issued By** field when a certificate is viewed in the CertMgr.

- Request Attributes: The attributes used when querying the CA. This typically includes, at a minimum, the certificate template name. For example, *Certificate Template:User*.
- CA Chain: Specify the CA Chain. The client configuration must include the root, and if applicable, the intermediate CAs. The certificates should be concatenated together in PEM format.
- Key Length: The key length, as dictated by the CA, for certificate signing requests.

Configuring the Certificate Template for the Microsoft CA

- Algorithm: The algorithm, as dictated by the CA.
 - Use Static Credentials?: By default, the system uses user-provided credentials when interacting with the Microsoft CA. Check this box if you want to configure static username and password to use when interacting with the Microsoft CA.
7. The "RADIUS Options" section of the screen contains the following:
- Allow Authentication via RADIUS: If checked, the RADIUS server will contain policy information and RADIUS attributes (VLAN, Filter ID, and so on) for this certificate template.
 - Assigned Candidate Policies: Policies are not listed here until you assign one or more policies to this certificate template. After you complete the configuration of this template, you can assign policies by referring to the instructions in the [Adding RADIUS Policies to the CA Certificate Template](#) on page 33. Once added to a certificate template, policies are evaluated (in the order they are listed) for each authentication so that this template can determine the corresponding RADIUS response attributes.
 - Default Access (No Match): When no policies are assigned, or when policies are assigned but no match is found against any of the policies, the default access for authentication will either be accepted or rejected, depending on this setting.
8. Use the **Specify Subject Values in CSR** settings if you want to configure the subject of the CSR destined for Microsoft CA when the template is set to "Supply in request."
9. Click **Save**. The five-tab view of the newly created template is displayed, as in the following example:

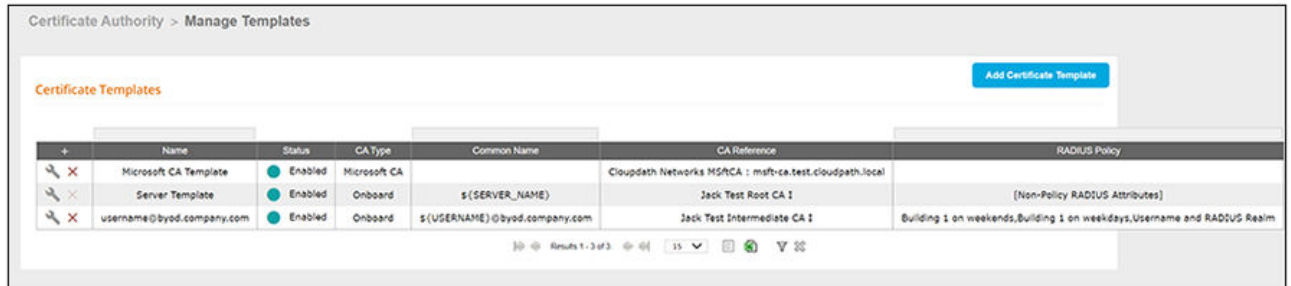
FIGURE 9 Microsoft CA Certificate Template Created



10. From this view, you can do the following:
- Assign policies by clicking the RADIUS Policies tab. For more information, refer to [Adding RADIUS Policies to the CA Certificate Template](#) on page 33.
 - Add notifications, SCEP keys, or MSI packages by clicking on the corresponding tabs.

- Click "View All Templates" in the upper right portion of the screen to return to a view of all configured templates, as shown in the example screen below:


FIGURE 10 View of All Certificate Templates



Configuring Microsoft Intune in Cloudpath

The Simple Certificate Enrollment Protocol (SCEP) provisions new or renewed certificates to a device.

1. Configure Microsoft Azure based on the instructions provided in: <https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview#set-up-third-party-ca-integration>
2. From the Cloudpath web interface, navigate to **Certificate Authority > Manage Templates**.

3. Click the  icon.

The **Certificate Template** page is displayed.

4. Navigate to the **SCEP Keys** tab.

5. Under SCEP Keys, click **Add SCEP Key**.

The **Create SCEP Key** page is displayed.

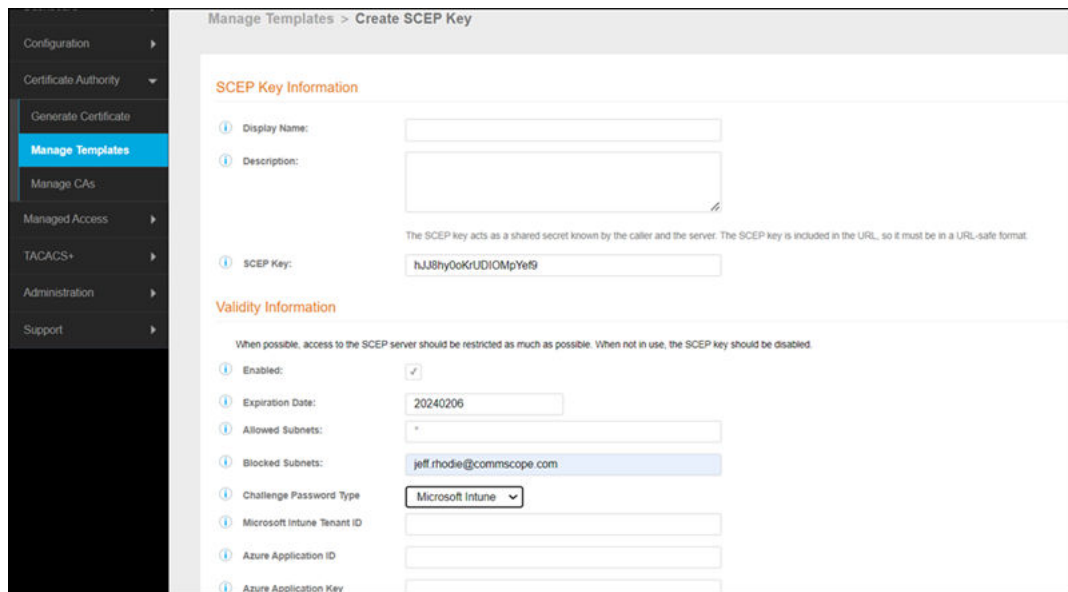
6. Under the Validity Information section, set **Challenge Password Type** to Microsoft Intune.

The following new fields are now displayed:

- Microsoft Intune Tenant ID
- Azure Application ID
- Azure Application Key

Populate these fields with the information retrieved from step 1 (App ID, Secret Key, and Tenant ID).

FIGURE 11 Microsoft Intune Configuration



7. Create a Trusted CA profile in Intune by following the instructions in: <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root#create-trusted-certificate-profiles>.

Configuring Microsoft Intune in Cloudpath

8. Configure Intune SCEP Configuration by following the instructions in: <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep>.

Configuring the **Root CA** may differ for different operating systems. For most operating systems, it is recommended to set Root CA to the Intermediate CA of the Certificate Template. For Android™, it is recommended to set Root CA of the Certificate Template's chain.

NOTE

If you get an error during SCEP enrollment (for example, if the hash value is not correct), then it is recommended to set Root CA to the Root CA of the Certificate Template's chain.

Enhanced SAN Handling for SCEP Certificates

Feature Overview

When generating certificates using the Simple Certificate Enrollment Protocol (SCEP), the systems capture and utilize Subject Alternative Name (SAN) values from the Certificate Signing Request (CSR). This helps Cloudpath to effectively leverage SAN attributes for certificate creation and authentication processes.

This feature enhances SCEP certificate generation by allowing for the pass-through of SAN values from the CSR. When Microsoft Entra or Intune is selected as the SCEP key, a new checkbox is introduced to control how SAN values are handled. The system now captures and preserves SAN values from the CSR during the certificate generation process.

The new checkbox, **Use SAN values from request** is available within SCEP settings to enable or disable SAN value utilization.

The following SAN types are supported:

- Other Name (UPN)
- RFC822 (email)
- DNS Name
- URL/URI

The process for configuring Intune and Cloudpath includes:

- Configuring Azure by following the instructions documented here: <https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview#set-up-third-party-ca-integration>.
- Creating a SCEP key in Cloudpath.
- Creating a trusted CA profile in Intune by following the instructions documented here: <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-trusted-root#create-trusted-certificate-profiles>
- Configuring Intune SCEP by following this guide: <https://learn.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep>

By effectively managing SAN values during the SCEP certificate generation process, this feature empowers organizations to optimize certificate utilization and strengthen overall security posture.

Requirements

This feature has no special hardware or software requirements for feature enablement or usage.

Considerations

This feature has no special considerations or limitations pertaining to feature enablement or usage.

Best Practices

- Use SAN attributes for certificate creation and authentication.

Enhanced SAN Handling for SCEP Certificates

Prerequisites

- Employ the device ID from Intune for authentication purposes.
- Use the Common Name (CN) as the user ID for edu roam.

Prerequisites

To use this feature, you need a Microsoft Entra ID or Intune account to access the appropriate application.

The following are the links to the Microsoft 365 Developer program and Intune:

- <https://developer.microsoft.com/en-us/microsoft-365/dev-program>.
- Configuring Azure and Intune: <https://docs.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview>.
- Configuration Necessary Infrastructure: <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-scep-configure>.
- Microsoft Troubleshooting Logs: <https://docs.microsoft.com/en-us/troubleshoot/mem/intune/troubleshoot-scep-certificate-profiles#logs-for-windows-devices>.
- Create SCEP Profile in Intune: <https://docs.microsoft.com/en-us/mem/intune/protect/certificates-profile-scep>.
- Enroll Windows 10 Devices: <https://docs.microsoft.com/en-us/mem/intune/user-help/enroll-windows-10-device>.

Configuring SAN Attributes

Follow these instructions to configure Azure: <https://learn.microsoft.com/en-us/mem/intune/protect/certificate-authority-add-scep-overview#set-up-third-party-ca-integration>.

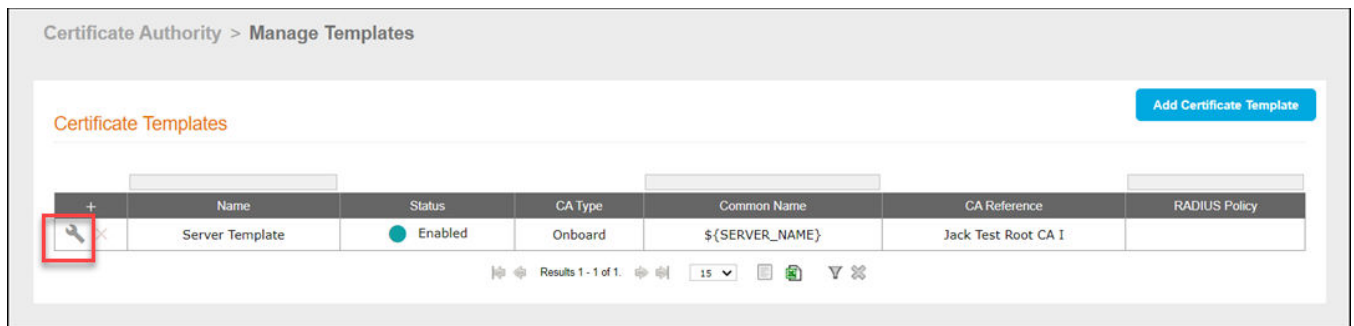
NOTE

Azure Active Directory is now called Entra ID.

Complete the following steps to configure SAN attributes.

1. From the Cloudpath Enrollment System navigation bar, go to **Certificate Authority > Manage Template**.
The **Certificate Templates** page is displayed.
2. Click the manage icon next to the certificate name.
The **Certificate Templates** page is displayed.

FIGURE 12 Managing Certificate Templates



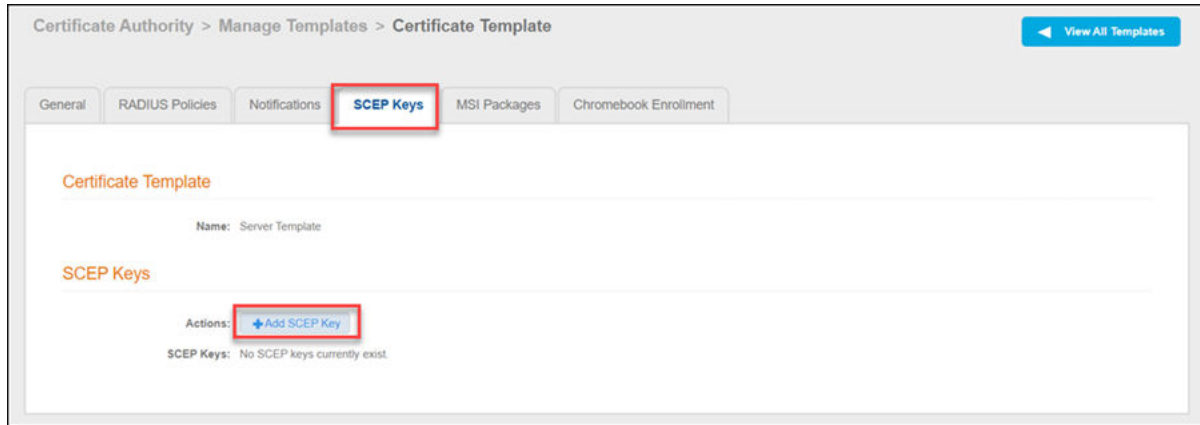
3. Click **SCEP Keys**.

Configuring SAN Attributes

4. In the **SCEP Keys** section, click **Add SCEP Key**.

The **SCEP Keys** page is displayed.

FIGURE 13 Adding SCEP Key



The **Create SCEP Key** page is displayed.

5. In the **SCEP Key Information** page, complete the following :

- **Display Name:** Enter a display name.
- **Description:** Enter a short description.

FIGURE 14 Configuring SCEP Keys to Use SAN Values

Manage Templates > Create SCEP Key

SCEP Key Information

Display Name:

Description:

The SCEP key acts as a shared secret known by the caller and the server. The SCEP key is included in the URL, so it must be in a URL-safe format.

SCEP Key:

Validity Information

When possible, access to the SCEP server should be restricted as much as possible. When not in use, the SCEP key should be disabled.

Enabled:

Expiration Date:

Allowed Subnets:

Blocked Subnets:

Challenge Password Type:

Microsoft Intune Tenant ID:

Azure Application ID:

Azure Application Key:

Use SAN values from request:

In the **Validity Information** section, complete the following information.

- **Enabled:** If enabled, the item is available for use. If disabled, the item is not available for use.
- **Expiration Date:** Set an expiration date.
- **Allowed Subnets:** If configured, only the IPs or subnets specified will be allowed to utilize the SCEP server using this key. Specify in the semi-colon separated format similar to 1.1.1.1;192.168.4.1/24.
- **Blocked Subnets:** If configured, the IPs or subnets specified will be blocked from utilizing the SCEP server using this key. Specify in the semi-colon separated format similar to 1.1.1.1;192.168.4.1/24. Blocked subnets override the allowed subnets.
- **Challenge Password Type:** Optionally specify a challenge password which must be provided by the client during the SCEP exchange.
 - **None:** No challenge password will be required.
 - **Static:** A static string challenge password will be required. The password must be 4 or more characters long.
 - **Microsoft Intune:** A valid Microsoft Intune challenge password will be required.
- **Microsoft Intune Tenant ID:** The Azure Tenant ID, this can be found in the Azure configuration portal.
- **Azure Application ID:** The Azure Application (client) ID from the Azure configuration portal.
- **Azure Application Key:** The Azure Application Key/Client Secret configured in the Azure Configuration portal.
- **Use SAN values from request:** If selected, and the SCEP request contains URI, DNS, RFC822 (email), or User Principal Name Subject Alternative Names then the first occurrence of those names will be used in the issued certificate. This will replace the SANs specified in the Certificate Template.

NOTE

The **Use SAN values from request** option is only available if a Microsoft Intune **Challenge password type** is selected.

- **Days Of Access:** Set the days of access. If greater than 0, this overrides the expiration date in the certificate template for certificates generated using this key
- **Common Name #1 Mapping:** The CSR created as part of the SCEP interaction will contain one or more common name (CN) values. The system will treat the first CN as the type of value specified. Ignore. MAC address, usable as `#{MAC_ADDRESS}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the MAC address. Username, usable as `#{USERNAME}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the username. Device identifier, usable as `#{ROLLUP_DEVICE_NAME}` in the template.
 - If selected, the CN in the CSR at the index specified will be treated as the device name. Email, usable as `#{EMAIL}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the email address. Location, usable as `#{LOCATION}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the location.
- **Common Name #2 Mapping:** The CSR created as part of the SCEP interaction will contain one or more common name (CN) values. The system will treat the second CN as the type of value specified. Ignore. MAC address, usable as `#{MAC_ADDRESS}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the MAC address. Username, usable as `#{USERNAME}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the username. Device identifier, usable as `#{ROLLUP_DEVICE_NAME}` in the template.
 - If selected, the CN in the CSR at the index specified will be treated as the device name. Email, usable as `#{EMAIL}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the email address. Location, usable as `#{LOCATION}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the location.
- **Common Name #3 Mapping:** The CSR created as part of the SCEP interaction will contain one or more common name (CN) values. The system will treat the third CN as the type of value specified. Ignore. MAC address, usable as `#{MAC_ADDRESS}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the MAC address. Username, usable as `#{USERNAME}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the username. Device identifier, usable as `#{ROLLUP_DEVICE_NAME}` in the template.
 - If selected, the CN in the CSR at the index specified will be treated as the device name. Email, usable as `#{EMAIL}` in the certificate template.
 - If selected, the CN in the CSR at the index specified will be treated as the email address. Location, usable as `#{LOCATION}` in the certificate template.. - If selected, the CN in the CSR at the index specified will be treated as the location.

6. Click **Save**.

Adding RADIUS Policies to the CA Certificate Template

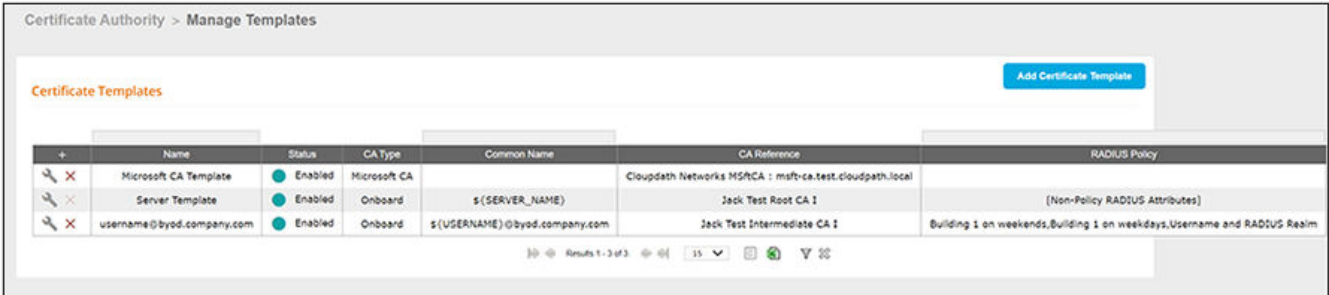
You can add as many policies as you want, but only one policy can be associated with a given user. For a user to successfully connect to the network, the user must be a match for at least one policy (or you can allow users to connect even if they do not match a policy).

Steps to Add Policies

Follow these steps to add a policy from the RADIUS Policies tab of a configured certificate template:

1. If you are not already in the RADIUS Policies tab of a configured certificate template, go to **Certificate Authority > Manage Templates** to view all existing certificate templates:

FIGURE 15 Certificate Templates View

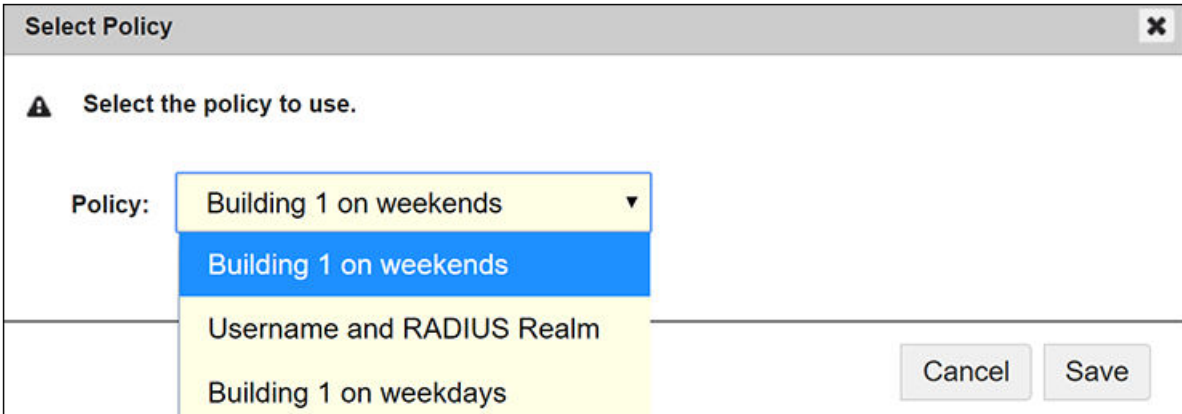


The screenshot shows the 'Certificate Authority > Manage Templates' interface. It features a table with the following columns: Name, Status, CA Type, Common Name, CA Reference, and RADIUS Policy. There are three rows of data:

Name	Status	CA Type	Common Name	CA Reference	RADIUS Policy
Microsoft CA Template	Enabled	Microsoft CA		Cloudpath Networks MS/CA : msft-ca.test.cloudpath.local	
Server Template	Enabled	Onboard	s(SERVER_NAME)	Jack Test Root CA 1	[Non-Policy RADIUS Attributes]
username@byod.company.com	Enabled	Onboard	s(USERNAME)@byod.company.com	Jack Test Intermediate CA 1	Building 1 on weekends, Building 1 on weekdays, Username and RADIUS Realm

2. Click the wrench icon for the Microsoft CA template.
3. In the ensuing screen, click the RADIUS Policies tab, then 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:

FIGURE 16 Select Policy Drop-down List



The screenshot shows a 'Select Policy' dialog box with a close button (X) in the top right corner. The main text reads 'Select the policy to use.' Below this, there is a 'Policy:' label followed by a drop-down menu. The menu is open, showing four options: 'Building 1 on weekends' (highlighted in blue), 'Building 1 on weekdays', 'Username and RADIUS Realm', and 'Building 1 on weekends'. At the bottom right of the dialog, there are 'Cancel' and 'Save' buttons.

Adding RADIUS Policies to the CA Certificate Template

Policy Rules

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 17 Policies Added to Microsoft CA Certificate Template

The screenshot shows the 'RADIUS Policies' configuration page for a 'Microsoft CA Template'. At the top, there are tabs for 'General', 'RADIUS Policies', 'Notifications', 'SCEP Keys', and 'MSI Packages'. A yellow banner indicates 'Certificate Template Policy Added'. Below this is a diagram showing a device authenticating with a laptop, with text explaining that RADIUS attributes will be returned based on the information below. The 'Certificate Template' section shows the name 'Microsoft CA Template'. The 'RADIUS Policies' section has buttons for '+ Assign Policy', 'Test Policy Evaluation', and 'Reset Counts'. Below these are three assigned candidate policies in a table:

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

When none of the policies are matched, the default access will be: **Accept**

- 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 in the template, 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

If none of the policies match a specific user, the default access setting (configured when you create a certificate template) is used to either accept or reject the user. In the example above, at the bottom of the illustration, the default access is to accept the user because that is how the field was set when the certificate template was configured.

Additional Policy Information

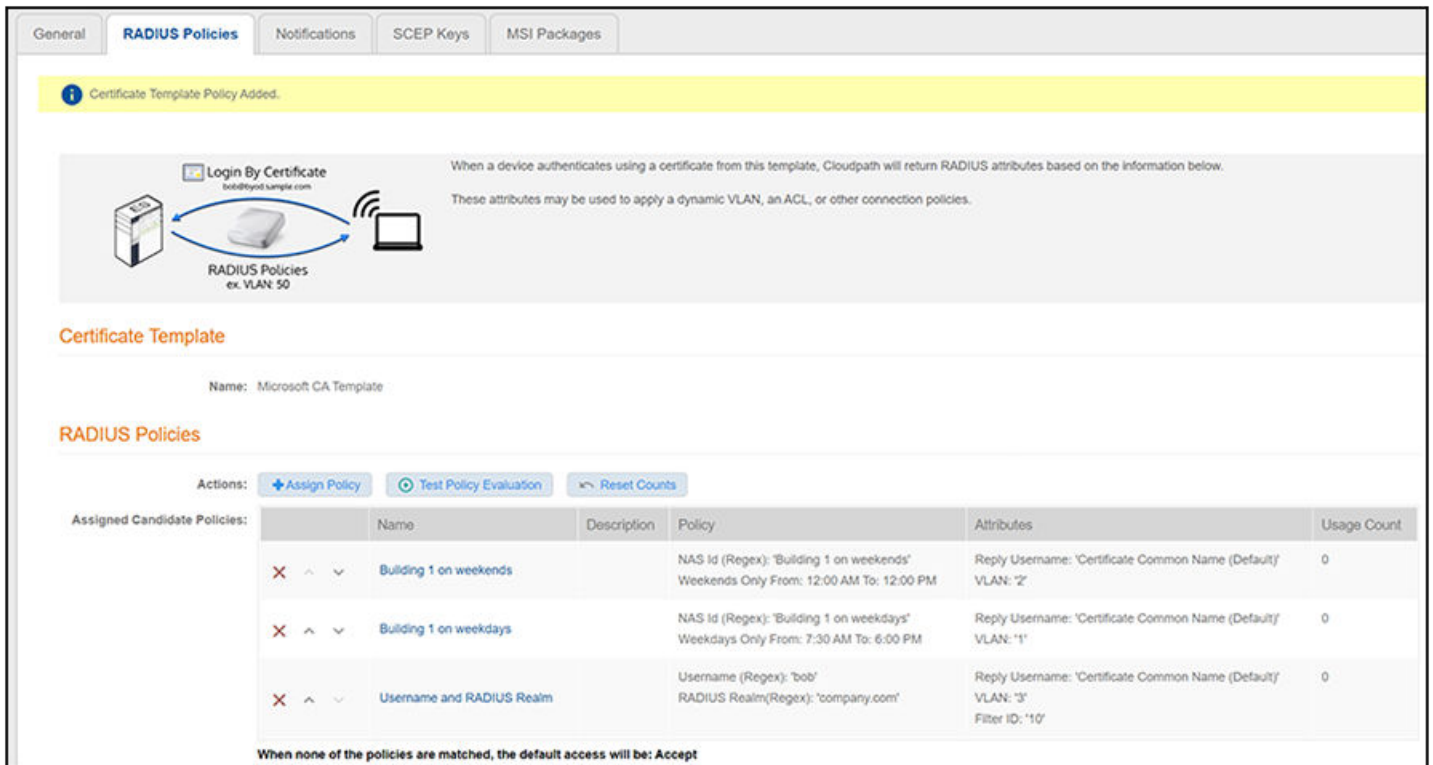
- Testing Policies..... 37
- Viewing Policy Information..... 43
- Viewing RADIUS Attribute Information..... 45

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 a Microsoft CA Certificate template. To get to this screen, go to **Certificate Authority > Manage Templates**, click the wrench icon next to the desired certificate template, then click the **RADIUS Policies** tab.

FIGURE 18 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 19 Test Policy Selection - Example 1 Values

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).

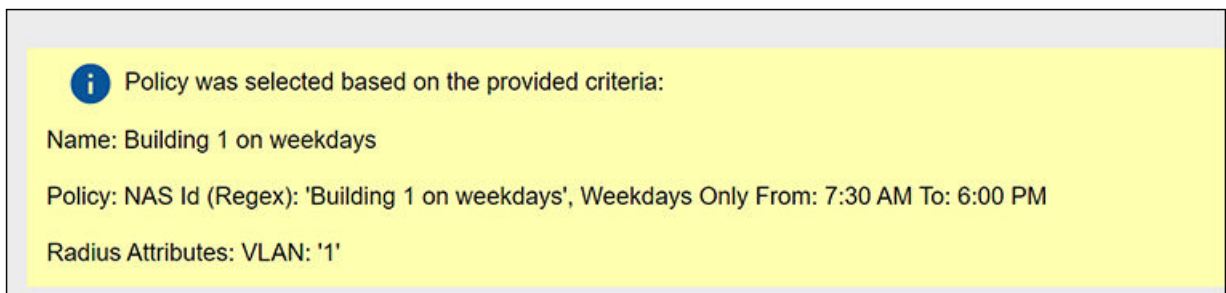
NOTE

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 20 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 21 Test Policy Selection - Example 2 Values

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'

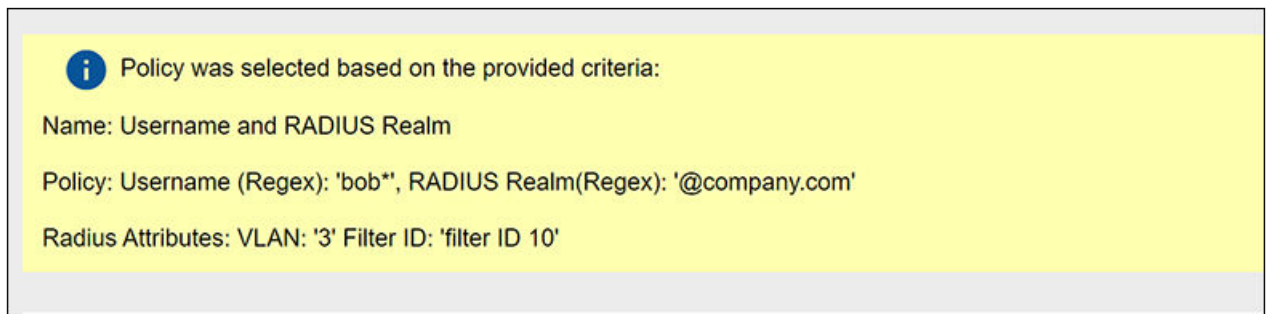
The sample values shown above have been entered to test that the "Username and RADIUS Realm" policy will be applied to users who match the criteria defined by that policy (refer to the information in the "Policy" column in the figure above).

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, 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, 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 22 Test Policy Selection - Example 2 Results



Test Policy Evaluation - Example 3

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 23 Test Policy Selection - Example 3 Values

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: james@company.com

SSID: SSID

Authentication Groups: DEMO\domain DEMO\bob DEMO\allowed BUILTIN\users

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

DPSK Reference Name: UserDevice_123

Authentication Date: 20200521

Authentication Time: 10:52 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'

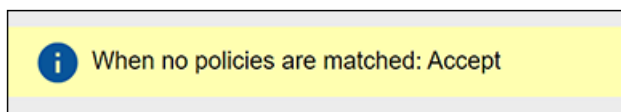
The sample values shown above have been entered to test that no policy will be applied to users who do not match the criteria defined by any of the policies belonging to the certificate template (refer to the information in the "Policy" column in the figure above).

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, 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, 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 username does not match the conditions listed for this policy, eliminating any chance of a match to this policy. Therefore, the expected behavior is that, when you click the **Apply** button, you should receive a message indicating that no policies matched, but that the user is still accepted onto the network, provided that the "Default Access (No Match)" field was configured to "Accept" a user if there was no policy match. You can confirm this is true for the example Microsoft CA Certificate template by checking [Figure 18](#).
- d. To confirm these results, now click the **Apply** button. The following response is received:

FIGURE 24 Test Policy Selection - Example 3 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 assigned to DPSK pools, certificate templates, or PEAP.

FIGURE 25 Policy Table Example

Policies									Add Policy		
	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	0				
🔍 ✎ ✕	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	0				
🔍 ✎ ✕	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	0				

🔍 ⚙️ Results 1 - 3 of 3. 📄 15 🗑️ 🔄 📄

You can use the policy table as follows:

Additional Policy Information

Viewing Policy Information

TABLE 2 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 26). You can edit the policy by clicking on the pencil icon. If the policy has not yet been assigned (such as to PEAP, a certificate template, 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 3 on page 16.
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 3 on page 16.
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 3 on page 16.
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 2 on page 14. NOTE The "Reply Username" attribute applies only to certificate templates.
DPSK Rel, Cert Template Rel, and PEAP Rel	The number of times that a policy has been assigned to each category of authentication.

FIGURE 26 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 27 RADIUS Attribute Groups Example

	Name	Description	Policy Count	Attributes	Timestamp
+ [pencil] [X]	VLAN 1		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '1'	20210118 1509 MST
+ [pencil] [X]	VLAN 2		1	Reply Username: 'Certificate Common Name (Default)', VLAN: '2'	20210118 2024 MST
+ [pencil] [X]	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 3 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 2 on page 14.
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 group is currently assigned to.

Additional Policy Information

Viewing RADIUS Attribute Information

TABLE 3 Description of RADIUS Attribute Groups Table (continued)

Column Title	Description
Attributes	<p>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 2 on page 14.</p> <p>NOTE The "Reply Username" attribute applies only to certificate authentications.</p>
Timestamp	Time that the RADIUS attribute group was created.

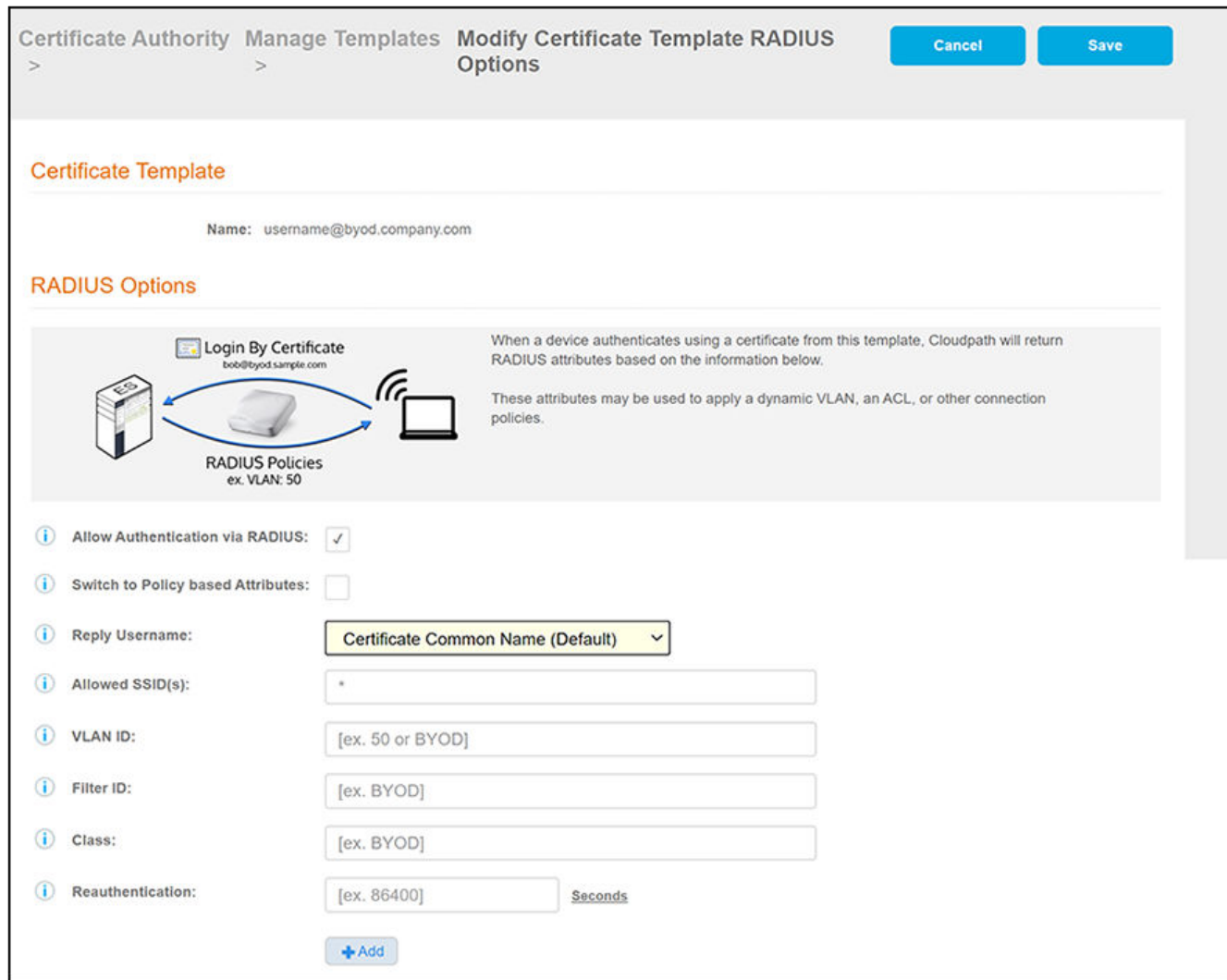
Switching Pre-Release-5.8 Microsoft CA Certificate Templates to Policy-Assigned Templates

Microsoft CA Certificate templates are created differently in Release 5.8 (and later) from prior releases. If you have older Microsoft CA Certificate templates in your system, you can continue to use them the same way in 5.8 or later, or you can convert them to the policy-type templates that are created in Release 5.8 going forward. Once you switch an old template to the new policy-type format, you cannot revert back to the pre-5.8 template configuration.

Follow the steps below to convert an old certificate template to the policy-based template:

1. In the UI, go to **Certificate Authority > Manage Templates**, then click the Wrench icon for the desired certificate template.
2. On the ensuing screen, click the **Edit RADIUS Attributes** button in the "RADIUS Attributes (Non-Policy)" portion of the screen. The following screen is then displayed.

FIGURE 28 Modify Microsoft CA Certificate Template Configuration Screen: Pre-Release 5.8 Template



NOTE

Be sure to take note of the existing values of the fields shown in the screen above because you will re-use these values when you create a new RADIUS attribute group.

3. Under RADIUS Options, check the "Switch to Policy-Based Attributes" box.
4. On the ensuing screen, select your settings in the "RADIUS Options" portion of the screen, then click **Save** to complete the process of converting the certificate template to the policy-based template.
5. Select the **RADIUS Policies** tab and add any desired policies. For instructions on adding policies, see [Adding RADIUS Policies to the CA Certificate Template](#) on page 33.

Downloading the Integration Module

The Integration Module for Microsoft CA is downloaded from the Cloudpath **Certificate Templates** page. It downloads as a compressed Zip file.

Perform the following steps to download the Integration Module:


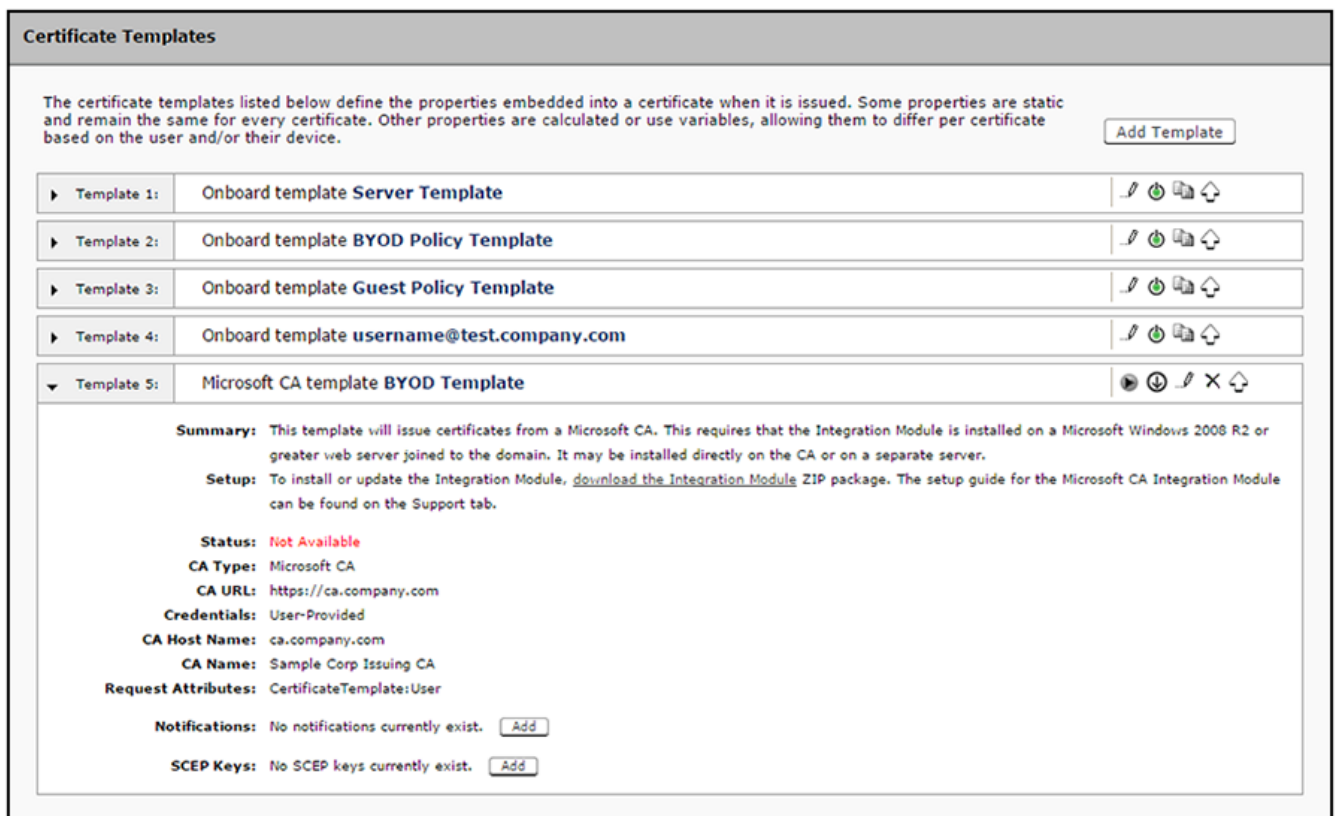
1. Go to **Certificate Authority > Certificate Templates**.
2. On the **Certificate Templates** page, click the download icon  to download the Integration Module.

FIGURE 29 Download Integration Module for Microsoft CA



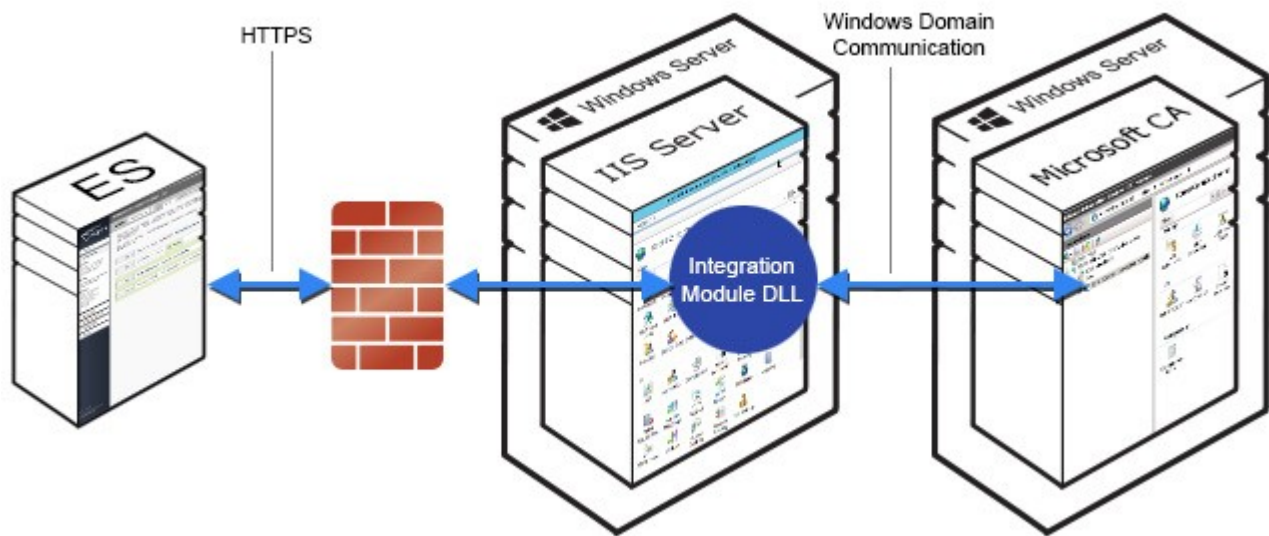
Configuring the Web Server

- [Verify Role Services.....](#) 51
- [Set Up the Integration Module Website.....](#) 52

The Integration Module is placed in IIS on a Windows 2008, 2012 or 2019 Server. The server may or may not be on the same server as the CA, but it must be on the same domain as the CA. At a minimum, the web server must have the ASP.NET role services installed.

The following diagram illustrates how the different systems work together, including the communication ports between the components, and where the different pieces of data reside.

FIGURE 30 Example of Cloudpath with Microsoft CA in a Network



Perform the steps in the following procedures to set up your IIS server.

Verify Role Services

Perform the steps in this procedure to verify the role services in the Service Manager.

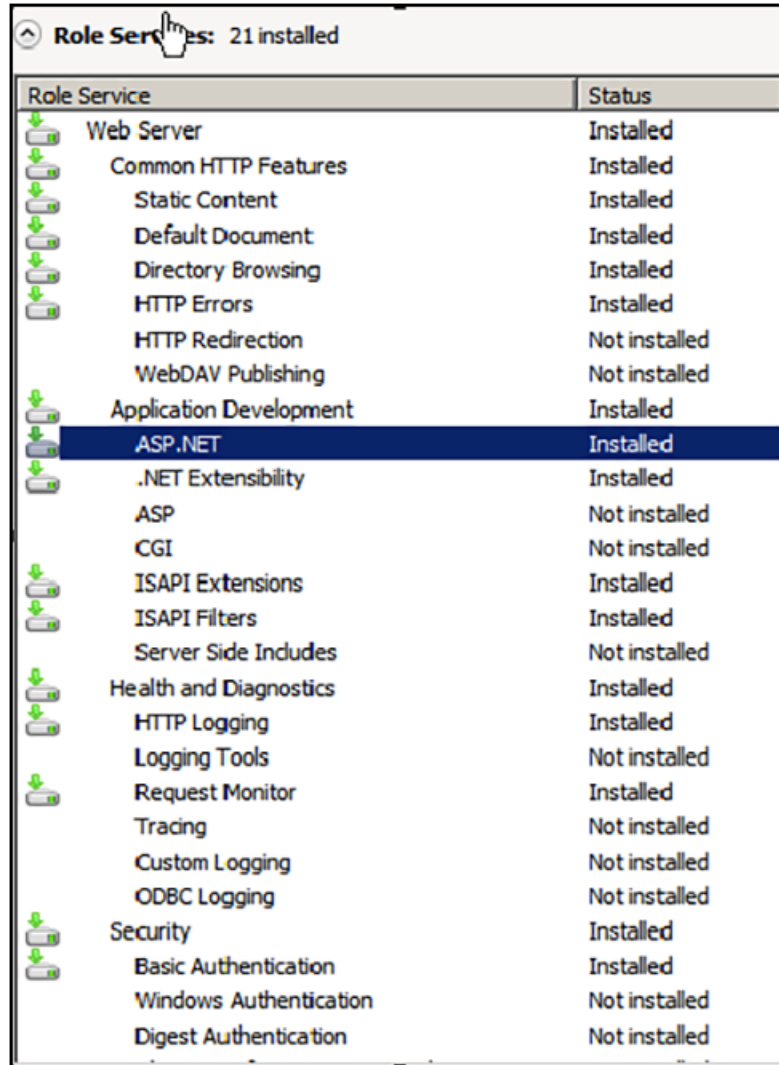
1. Open the Server Manager.

Configuring the Web Server

Set Up the Integration Module Website

2. In the left tree view, expand **Roles**, and select **Web Server (IIS)**.

FIGURE 31 Role Services Installed on the IIS



Role Service	Status
Web Server	Installed
Common HTTP Features	Installed
Static Content	Installed
Default Document	Installed
Directory Browsing	Installed
HTTP Errors	Installed
HTTP Redirection	Not installed
WebDAV Publishing	Not installed
Application Development	Installed
ASP.NET	Installed
.NET Extensibility	Installed
ASP	Not installed
CGI	Not installed
ISAPI Extensions	Installed
ISAPI Filters	Installed
Server Side Includes	Not installed
Health and Diagnostics	Installed
HTTP Logging	Installed
Logging Tools	Not installed
Request Monitor	Installed
Tracing	Not installed
Custom Logging	Not installed
ODBC Logging	Not installed
Security	Installed
Basic Authentication	Installed
Windows Authentication	Not installed
Digest Authentication	Not installed

3. In the right window, scroll down to the **Role Services** section. In the list, locate *ASP.NET*, and verify that it has the *Installed* status.

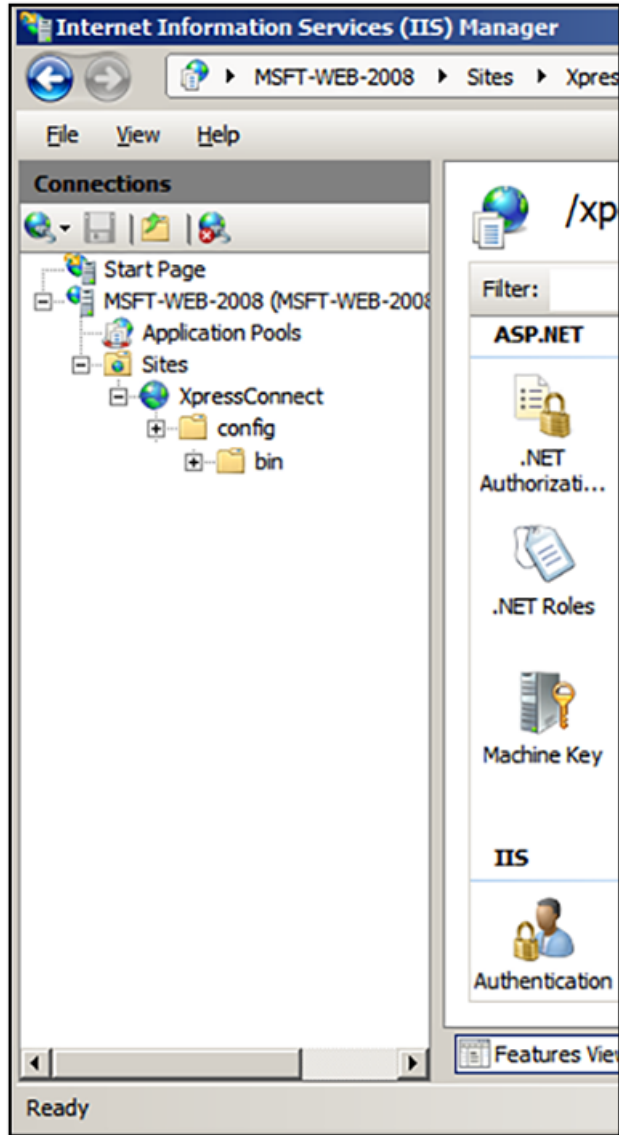
Set Up the Integration Module Website

To add the Integration Module Website, perform the following steps:

1. On the file system, locate the folder where the Integration Module will reside.
In most cases, the physical path is similar to `C:\inetpub\cloudpath`.
2. Create this folder and unzip the downloaded plug-in file into it.
The folder should contain the files `Default.aspx` and `Web.config`, among others.

3. In the IIS Manager, locate and select the **Sites** item in the left tree.
4. Right-click and select **Add Website**.
5. Name the site **Cloudpath**.

FIGURE 32 Site Structure in IIS Manager



6. Set the IP address, port, and host name appropriately.
7. Set the physical path to the folder created above (for example, C:\inetpub\cloudpath), and click **OK**.

Multiple Certificate Templates

If using multiple certificate templates (for example one for staff, `https://msft-ca.testcompany.com/ staff`, and one for guests, `https://msft-ca.testcompany.com/guests`), create a parent application for `https://msft-ca.testcompany.com`, and two child applications for staff and guests.

NOTE

The parent and child applications must be set up with *Anonymous Authentication Type*.


In multiple certificate template configurations, the parent application cannot contain the plug-in files (`Default.aspx`, `Web.config`, etc.). You must download the plug-in files into the corresponding child application directories.

For example, download the plug-in files from the staff certificate template and place them in the `https://msft-ca.testcompany.com/ staff` application directory, and download the plug-in files from the `guests` certificate template and place them in the `https://msft-ca.testcompany.com/guests` application directory.

Testing the System

After the Integration Module is deployed, you can test the communication between Cloudpath and the Microsoft CA. The query allows you to enter user credentials and verify interaction with the configured Microsoft CA.

To verify communication between Cloudpath and the Microsoft CA, perform the following steps:

1. From the **Certificate Templates** page, click the Test Integration Module icon .
2. On the **Test Microsoft CA** page, enter user credentials to verify Microsoft CA interaction with Cloudpath, and click **Continue**.

The **Microsoft CA Test** page displays the results of the query.

Troubleshooting

DNS

Verify that the Microsoft CA can resolve DNS.

CA Name

Verify that CA name is correct. The CA name is case-sensitive.

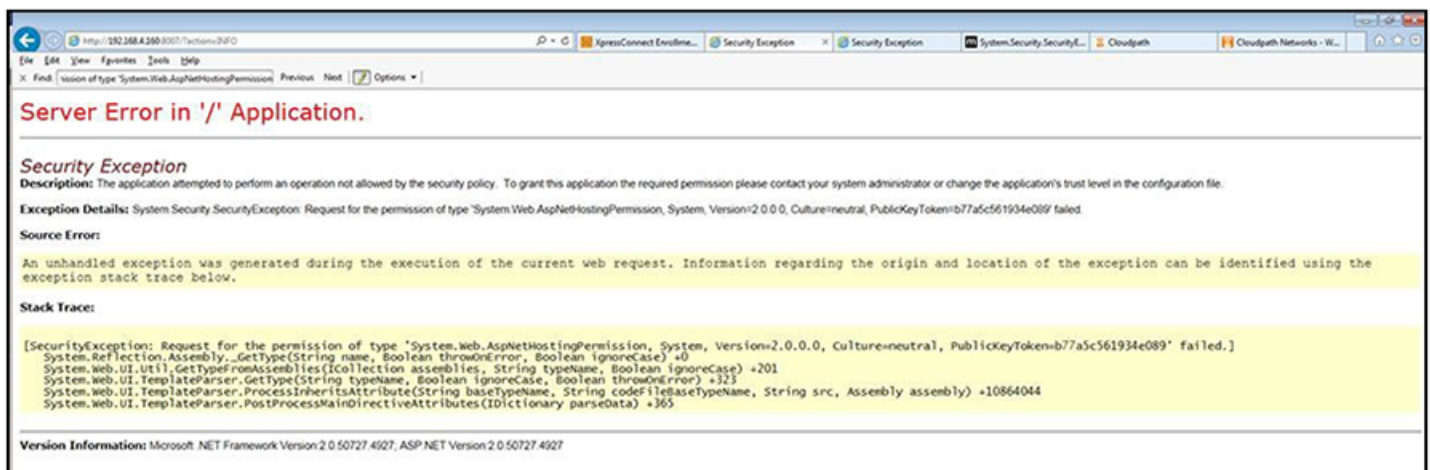
ASP.NET Installed on the IIS Server

If the Application Settings icon does not appear on the IIS server, verify that ASP.NET is installed on the IIS server. The entire ASP.NET icon set, which includes **Application Settings**, will not display if ASP.NET is not installed.

ASP Hosting Permissions

If you receive the following *Security Exception* error when trying to access `http://site/?action=INFO`, this typically indicates that the web server cannot use the files.

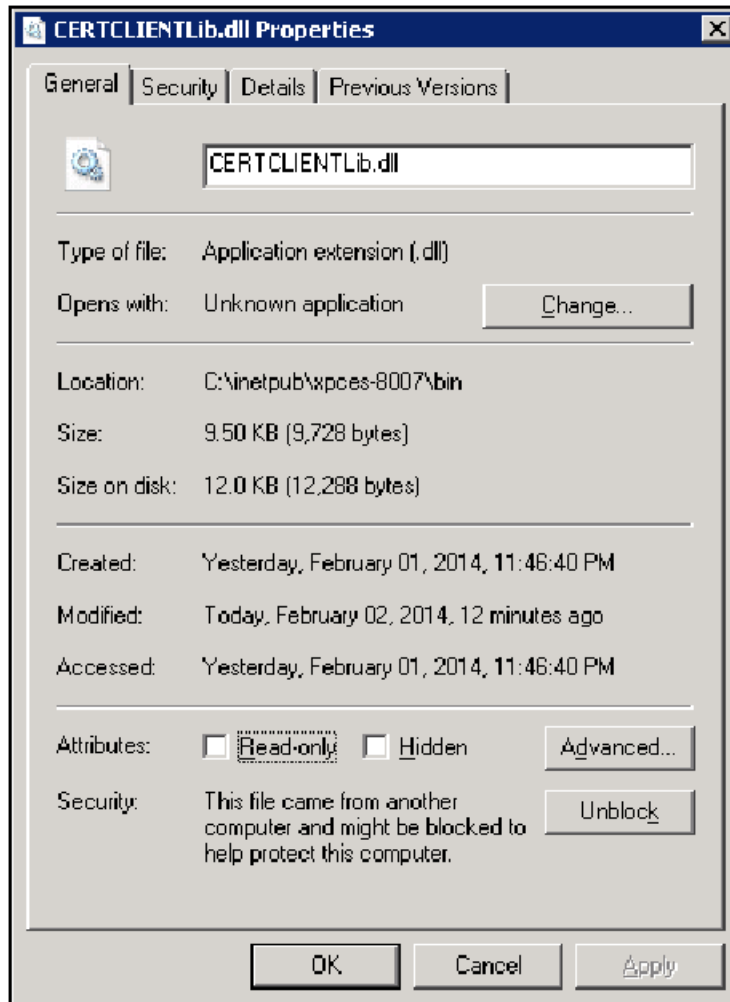
FIGURE 33 Security Exception Error



The key piece of information in this error message is *System.Web.AspNetHostingPermission*. When Internet Explorer encounters the files in the Integration Module zip files, it flags them as originating from the Internet, and blocks them.

To verify this, right-click one of the Integration Module files and view the **Properties**. With the **General** tab selected, in the **Security** section, you see a message: This file came from another computer and might be blocked to help protect this computer.

FIGURE 34 Integration Module Zip Files Properties



To correct this issue, check each file in the directory and *Unblock* any files that are listed as *Blocked*.

Restart the IIS Server

To apply these changes, the IIS Server must be restarted from the root node.

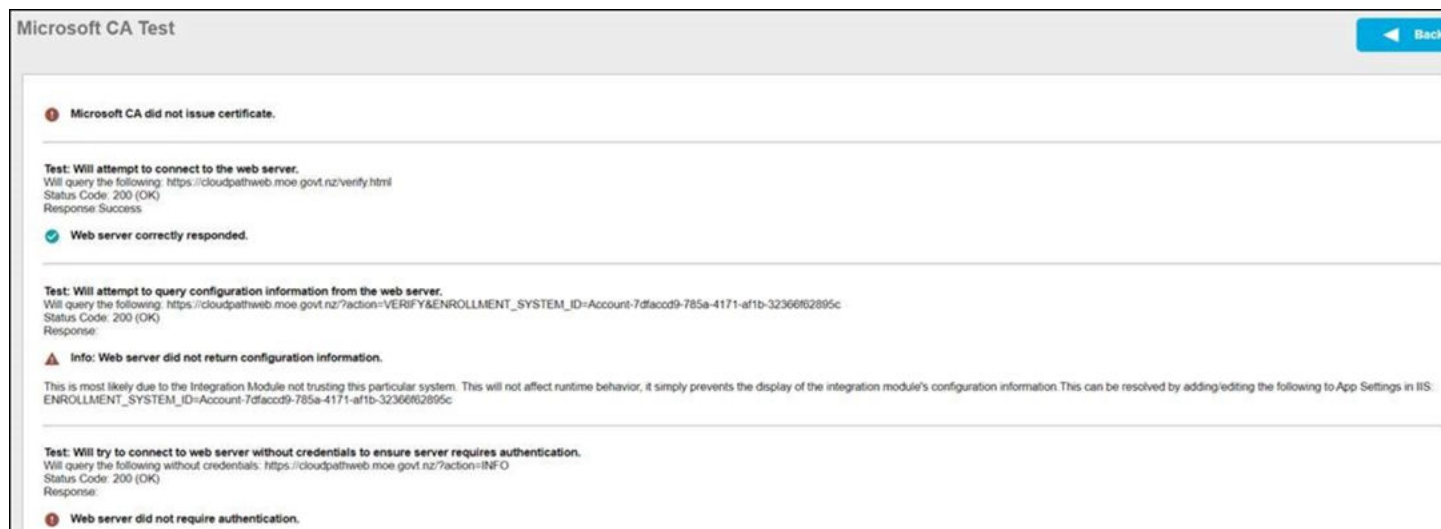
NOTE

Restarting the application does not apply the changes. You must restart the IIS server from the root node.

Failing Microsoft CA Test

Testing the Integration Module from the **Certificate Templates** page could result in failure and display a number a error messages as shown.

FIGURE 35 Sample Error Messages for Failed Microsoft CA Tests



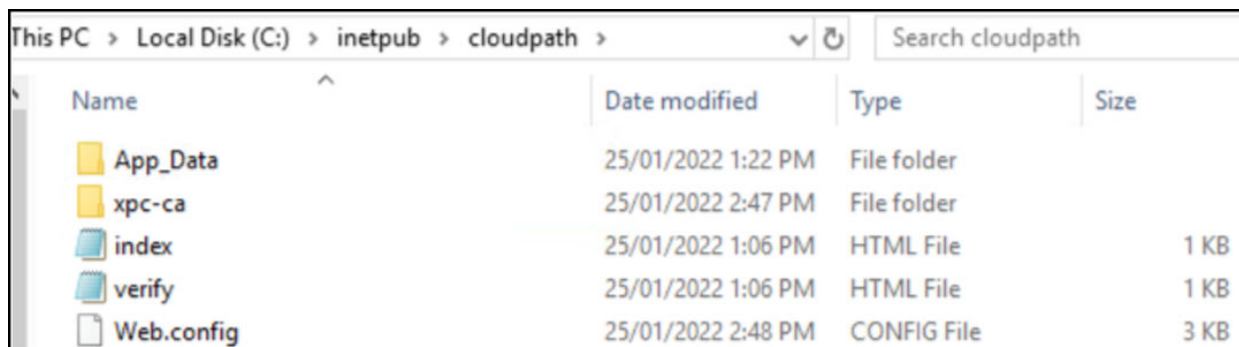
To resolve the issues, perform the following steps:

1. Download the zip files as mentioned in the [Downloading the Integration Module](#) on page 49.
2. Extract the contents of the zip file into the IIS server and added the application in the IIS Manager.

NOTE

The zip file usually contains the following information:

FIGURE 36 Contents of the Zip File



3. Add the xpc-ca directory as an application in IIS Manager.

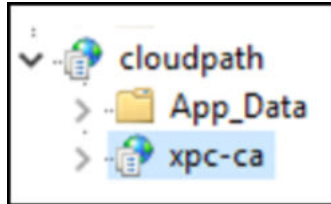
Troubleshooting

Failing Microsoft CA Test

NOTE

The xpc-ca directory icon changes after it is converted into an application as shown.

FIGURE 37 Xpc-ca Directory as An Application



4. Copy files **index.html** and **verify.html** into the xpc-ca directory.
5. Configure the URL required for Cloudpath to communicate with the Integration Module to `/cloudpath/xpc-ca`. See [Configuring the Certificate Template for the Microsoft CA](#) on page 19 for more information.

FIGURE 38 Configuring the DLL URL

Information Defined on IIS Server

Cloudpath will communicate with the Integration Module DLL using HTTPS. To do so, Cloudpath will need to know the URL of the DLL. This is most commonly something similar to `https://server.company.com`.

URL of DLL:



© 2024 CommScope, Inc. All rights reserved.
350 West Java Dr., Sunnyvale, CA 94089 USA
<https://www.commscope.com>