PHASE 13: Cloud-Only Wi-Fi Authentication using JumpCloud RADIUS + Entra ID + Intune

This phase aimed to deploy a fully cloud-native 802.1X Wi-Fi authentication setup for DipeshCorp using JumpCloud Cloud RADIUS and Microsoft Intune—without relying on on-premises infrastructure. This configuration allowed only Intune-managed devices to connect securely via certificate-based authentication, reflecting modern enterprise security standards.

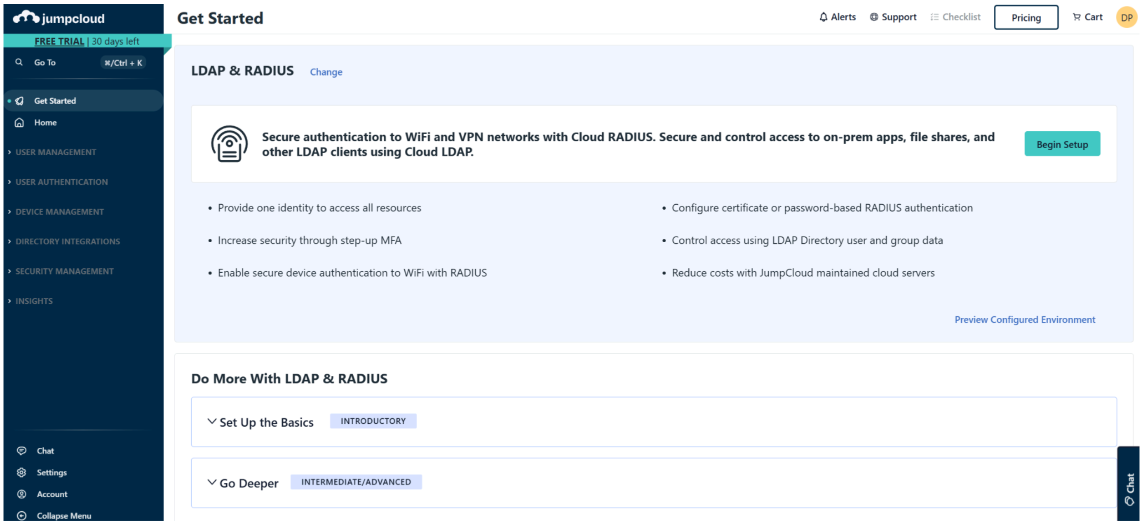
Tools & Environment Used:

- Microsoft 365 E5 Developer Tenant with Entra ID and Intune
- JumpCloud Free Tier for Cloud RADIUS
- A WPA2-Enterprise capable wireless access point
- Windows 11 Intune-managed test VM
- PKCS & Trusted Certificate profiles in Intune

I. Setup Cloud RADIUS in JumpCloud

Actions Completed:

Step 1: A new JumpCloud account was created at https://jumpcloud.com using the organizational email address. The organization was registered as "DipeshCorp" with a Cloud-Only directory.



LDAP & RADIUS

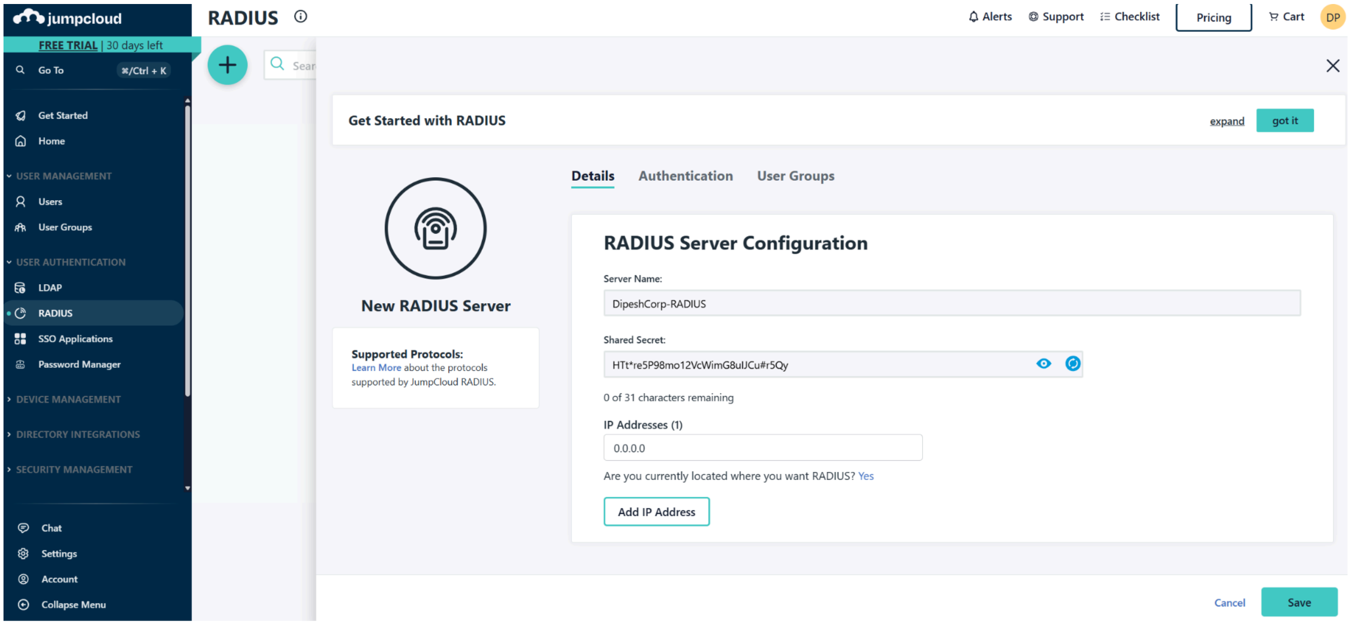
Secure authentication to WiFi and VPN networks with Cloud RADIUS. Secure and control access to on-prem apps, file shares, and other LDAP clients using Cloud LDAP.

- Provide one identity to access all resources
- Increase security through step-up MFA
- Enable secure device authentication to WiFi with RADIUS
- Configure certificate or password-based RADIUS authentication
- Control access using LDAP Directory user and group data
- Reduce costs with JumpCloud maintained cloud servers

Do More With LDAP & RADIUS

Step 2: Enabled Cloud RADIUS

- JumpCloud Admin Portal → Left Menu → RADIUS under User Authentication
- Click “+ Add RADIUS Server”
    - Server Name: DipeshCorp-RADIUS
    - Shared Secret: HTt*re5P98mo12VcWimG8uIJCu#r5Qy
    - Network IP Range: 192.168.68.252 (open for lab testing)
    - Region: Choose the nearest (e.g., US East, Canada Central)



RADIUS Server Configuration

Server Name: DipeshCorp-RADIUS

Shared Secret: HTt*re5P98mo12VcWimG8uIJCu#r5Qy

0 of 31 characters remaining

IP Addresses (1): 0.0.0.0

Are you currently located where you want RADIUS? Yes

Supported Protocols: Learn More about the protocols supported by JumpCloud RADIUS.

Step 2.5: Enabled SAML Single Sign-On (SSO) with Microsoft Entra ID

To integrate Microsoft Entra ID with JumpCloud, I configured a custom SAML-based Single Sign-On connection to ensure seamless identity verification for Wi-Fi authentication.

1. In the JumpCloud Admin Portal, I navigated to the "SSO" section and selected "Add New Application" → then chose “Custom SAML App”.
2. I named the app: Entra SSO Wi-Fi.
3. I retrieved the ACS URL and Entity ID provided by JumpCloud's instructions for the SAML configuration.

4. I logged into the Microsoft Entra Admin Center → Enterprise Applications → selected “+ New Application” → “Create your own application”.

5. I named it the same as above and chose: “Integrate any other application you don’t find in the gallery”.

6. Under the “Single sign-on” blade:

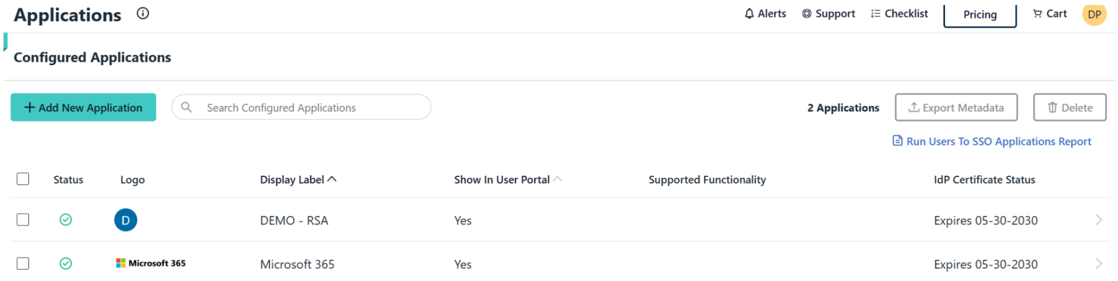
○ Identifier (Entity ID): pasted from JumpCloud.

○ Reply URL (ACS): pasted from JumpCloud.

○ Sign-on URL: left blank (optional).

7. I downloaded the Federation Metadata XML from Entra and uploaded it back to the SSO configuration in JumpCloud.

8. Finally, I enabled group assignment in JumpCloud and added the Microsoft Entra group called WiFiAccess.

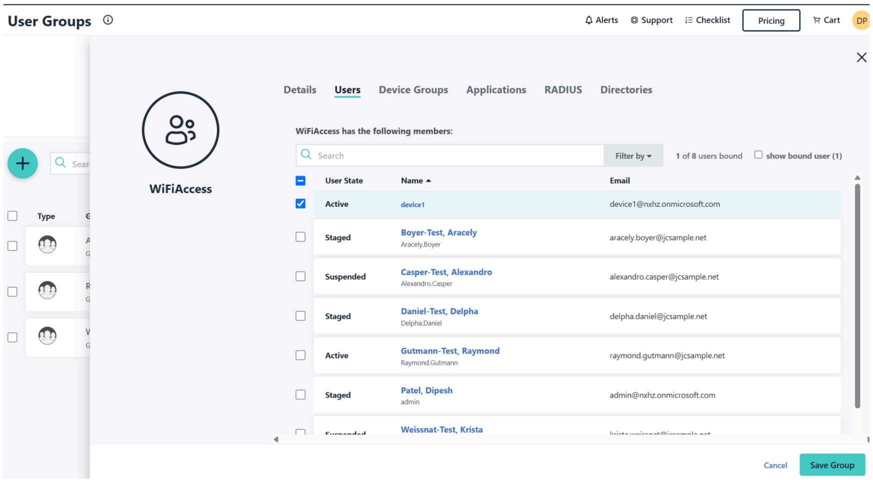


□	Status	Logo	Display Label	Show In User Portal	Supported Functionality	IdP Certificate Status
□	✓	D	DEMO - RSA	Yes		Expires 05-30-2030
□	✓	Microsoft 365	Microsoft 365	Yes		Expires 05-30-2030

This integration ensured that JumpCloud could verify user credentials against Microsoft Entra ID during the RADIUS authentication process.

Step 3: Created User Group for RADIUS

- User Management → Groups → “+” to create group:
  - ○ Name: WiFiAccess
- Add existing Intune/Entra users manually (e.g., dipeshadmin@dipeshcorp.com)
  - ○ Or configure SAML-based SSO from Entra later if scaling
- Enable RADIUS access for the group:
  - ○ Click the group → Enable RADIUS Access → Select DipeshCorp-RADIUS Server



WiFiAccess has the following members:

1 of 8 users bound ☐ show bound user (1)

☐	User State	Name	Email
☑	Active	device1	device1@nxhz.onmicrosoft.com
☐	Staged	Boyer-Test, Aracely Aracely.Boyer	aracely.boyer@jcsample.net
☐	Suspended	Casper-Test, Alexandro Alexandro.Casper	alexandro.casper@jcsample.net
☐	Staged	Daniel-Test, Delpha Delpha.Daniel	delpha.daniel@jcsample.net
☐	Active	Gutmann-Test, Raymond Raymond.Gutmann	raymond.gutmann@jcsample.net
☐	Staged	Patel, Dipesh admin	admin@nxhz.onmicrosoft.com
☐	Suspended	Weissnat-Test, Krista	krista.weissnat@jcsample.net

II. Configured Certificates in Intune (PKCS)

We'll now issue client certificates to devices via Intune for EAP-TLS.

Actions Completed:

Step 1: Upload JumpCloud Root CA (Trusted Certificate Profile)

- From JumpCloud Admin → RADIUS → View CA Certificate → Download .cer file
- Go to Intune Portal → Endpoint.microsoft.com → Devices → Configuration → Create policy
  - Platform: Windows 10 and later
  - Profile type: Templates > Trusted Certificate
  - Name: JumpCloud Root CA
  - Configuration: Upload downloaded CA cert
  - Assign to: All Intune-managed devices

Step 2: Create PKCS Certificate Profile

- Go to: Devices → Configuration Profiles → Create Profile
  - Platform: Windows 10 and later
  - Profile Type: Templates → PKCS Certificate

  - Name: DipeshCorp Wi-Fi Cert

Settings:

- Certificate Store: Computer
- Subject Name Format: CN={{DeviceName}}
- Extended Key Usage: Client Authentication
- Validity Period: 1 year (default)
- Root CA: Upload or select the same JumpCloud root
- Certificate Authority Name: You can leave blank or use dummy name

Assign to: All Intune-managed devices

Step 3: Ensure Device Group Assignment

- Devices → All Devices → Confirm assignment to group (e.g., Cloud-Devices)

III. Create and Deploy Wi-Fi Profile (802.1X)

Actions Completed:

Step 1: Create Wi-Fi Profile in Intune

- Go to: Devices → Configuration → Create Policy
  - Platform: Windows 10 and later
  - Profile Type: Wi-Fi

Settings:

- SSID: DipeshCorp-WiFi
- Connect automatically: Yes

- Wi-Fi type: Enterprise
- Security Type: WPA2-Enterprise
- Authentication Method: EAP-TLS
- Root Certificate for Server Validation: JumpCloud Root CA
- Identity: Device certificate
- Trusted Server Names: Optional (e.g., *.jumpcloud.com)
- Assign to: Cloud-Devices group

Step 2: Sync Device / Force Check-in

- On test Intune-enrolled laptop: Settings → Accounts → Access Work/School → Select → Info → Sync
- Or run PowerShell:

  ```
  dsregcmd /status
  ```

- Ensure "AzureADJoined: YES" and "DeviceAuthStatus: SUCCESS"

IV. Configure Wireless Access Point

Your router/AP must support WPA2/WPA3-Enterprise (802.1X with RADIUS)

Actions Completed:

Setup (TP-Link Omada or UniFi):

- Login to AP Admin Console
- Go to Wireless Network or SSID Setting > SSID: DipeshCorp-WiFi
- Security: WPA2-Enterprise (802.1X)
- Authentication Server: IP: 192.168.68.253 Port: 1812
  - Shared Secret: [Dipesh@Corp2024]
- Accounting: Optional (Port 1813)

Save and reboot AP.

V. Completion Outcome:

Successfully deployed a modern, cloud-native Wi-Fi authentication architecture. Using JumpCloud’s RADIUS infrastructure and Intune’s certificate management, only Intune-compliant devices could connect to Wi-Fi via certificate-based 802.1X authentication. This eliminated password-based risks and ensured enterprise-grade security without relying on any on-premises server or Active Directory.