

Configure Juniper Mist Cloud

This guide describes how to set up and test your Juniper Mist environment so you can use it with Orion Wifi:

- Log in to the Mist Dashboard as a user with administrative privileges.
- Configure the Wireless LAN, Hotspot 2.0 and RadSec service options.
- Upgrade Mist APs to support Hotspot 2.0

Log in to the Juniper Mist Dashboard

To start the configuration process, log in to the Mist dashboard as admin. For existing environments with additional users, log in as a user with administrative privileges.



Email

Password

[Forgot your password?](#)

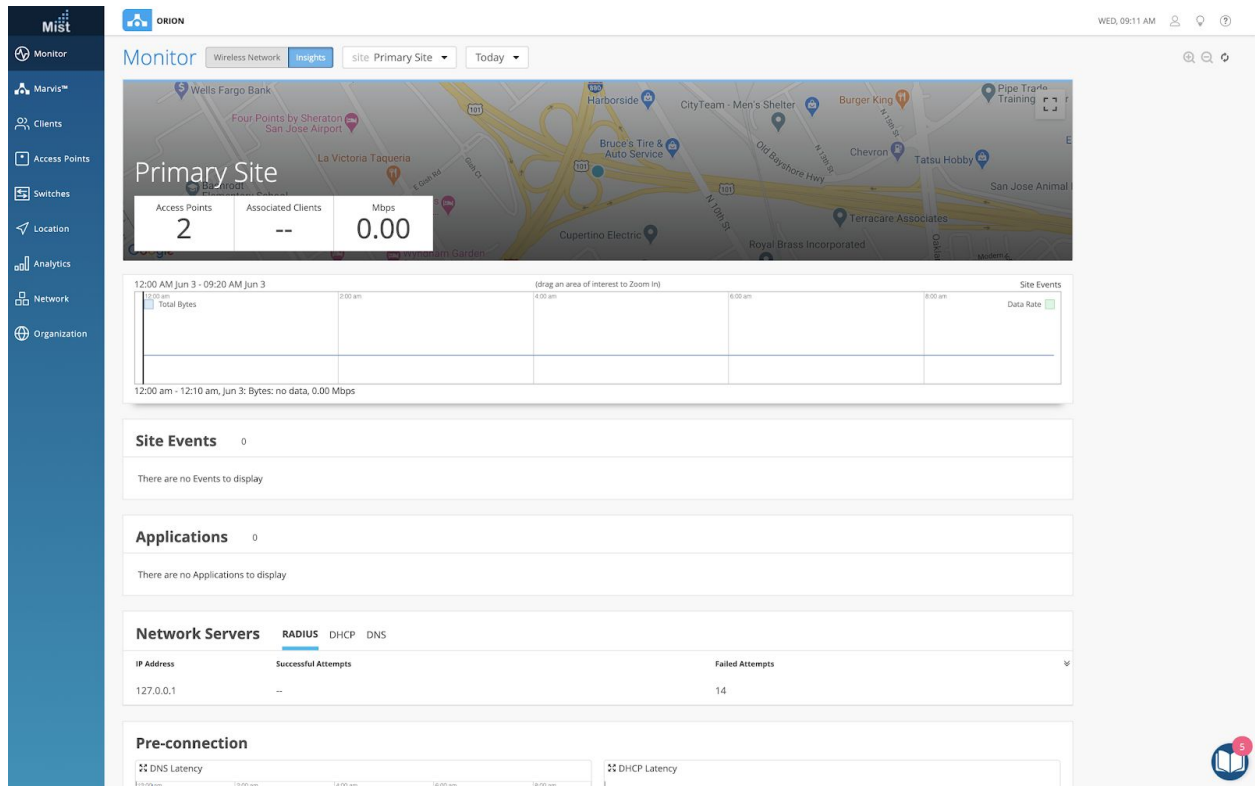
Sign In

or



Need a Mist account? [Create Account](#)

The Juniper Mist dashboard appears.



Set WLAN, SSID, and RadSec server options

Site identifier

Orion WiFi uses the NAS identifier (NAS-ID) to identify your venue (a site location) with each RADIUS access request. If you're new to Orion WiFi, we recommend creating a new SSID to avoid impacting any existing SSID configurations running in production.

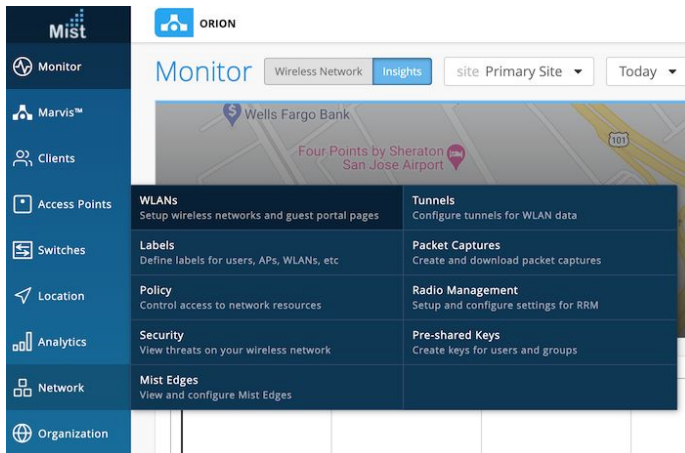
RadSec connection

It's important to set up a secure RADIUS connection between Mist APs and Orion WiFi.

Orion WiFi uses RadSec (RADIUS over TLS) to ensure end-to-end encryption of AAA traffic. Mist natively supports RadSec, AAA traffic is directed directly to Orion's RadSec server inside an encrypted RadSec tunnel.

Note: There are a number of options to set. Only the options that require your input are shown. Default values are used for options that don't need adjustment.

1. Select **Network > WLANs** from the Juniper Mist Dashboard.

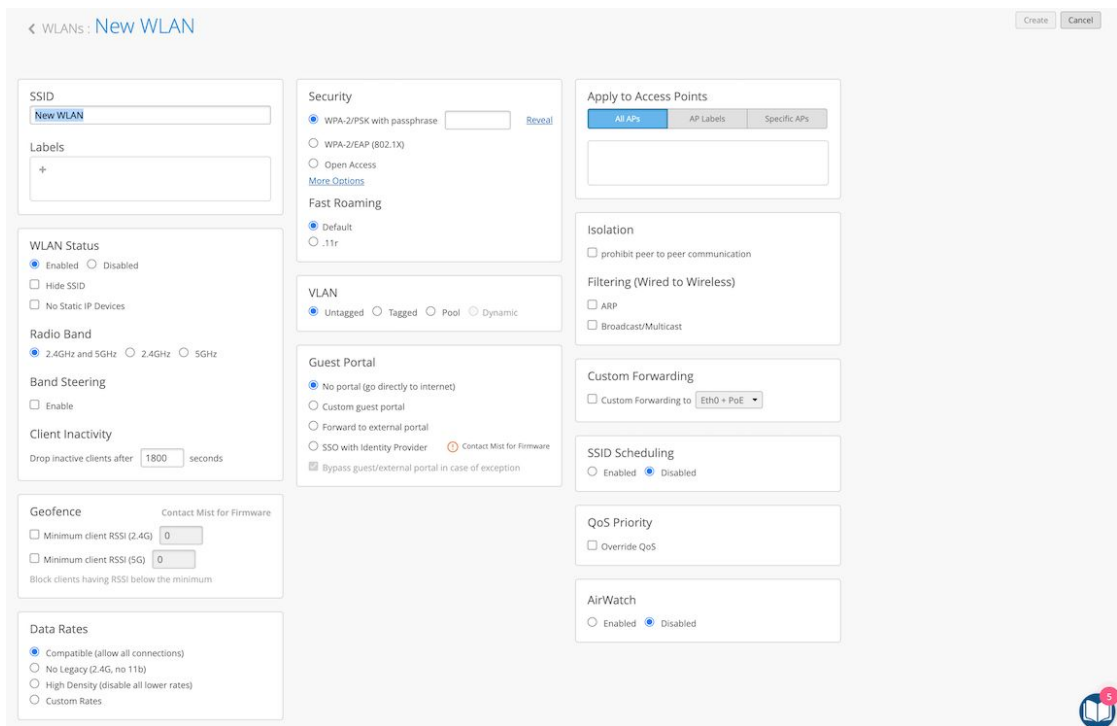


The **WLANs** page appears.

2. Select the **Site** to use at the top left and click **Add WLAN** in the top right corner. In this example, the site is “Primary Site”.



The **New WLAN** page appears.

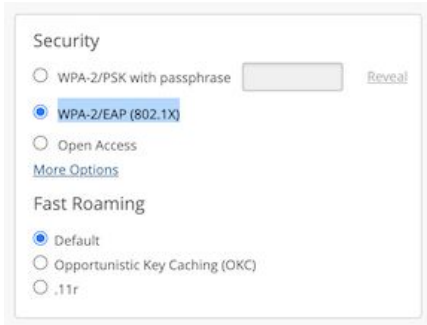


3. For **SSID**, enter “Orion” or any other name to your liking, it is not important.



A screenshot of a configuration form. The 'SSID' field contains the text 'Orion'. Below it, the 'Labels' field contains a '+' sign.

4. For Security, select **WPA-2/EAP (802.1X)**.

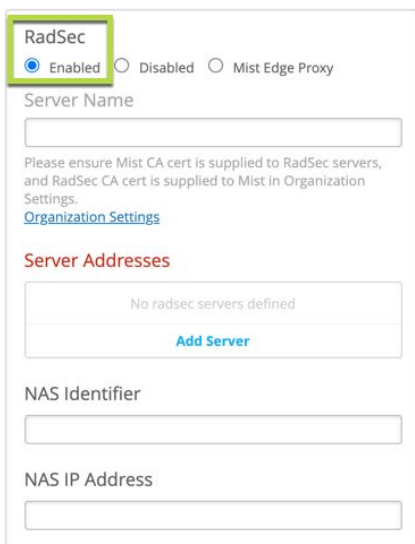


A screenshot of a 'Security' configuration section. The 'WPA-2/EAP (802.1X)' option is selected with a blue radio button. Other options include 'WPA-2/PSK with passphrase', 'Open Access', 'Fast Roaming' (with 'Default' selected), and '.11r'. There is a 'Reveal' button next to the passphrase field and a 'More Options' link.

Red text appears at the top left indicating that you have to add at least one RADIUS authentication server.

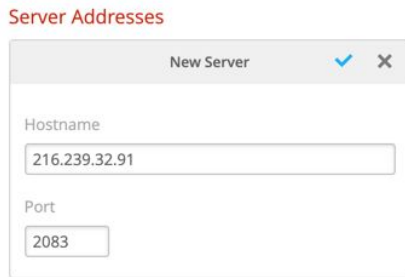


5. For **RadSec**, verify that RadSec is **Enabled**, and click **Add a Server** under **Server Addresses**:



A screenshot of the 'RadSec' configuration section. The 'RadSec' header is highlighted with a green box. Below it, the 'Enabled' radio button is selected. There are fields for 'Server Name', 'NAS Identifier', and 'NAS IP Address'. A section titled 'Server Addresses' shows 'No radsec servers defined' and an 'Add Server' button. A note at the bottom states: 'Please ensure Mist CA cert is supplied to RadSec servers, and RadSec CA cert is supplied to Mist in Organization Settings. Organization Settings'.

The **New Server** dialog box appears:



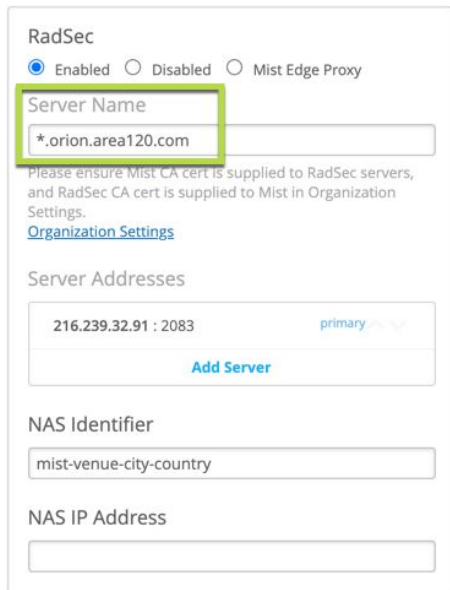
Server Addresses

New Server ✓ ✕

Hostname
216.239.32.91

Port
2083

Please configure the Server Name field. This is required by the Mist APs to verify RadSec server identity:



RadSec

Enabled Disabled Mist Edge Proxy

Server Name
*.orion.area120.com

Please ensure Mist CA cert is supplied to RadSec servers, and RadSec CA cert is supplied to Mist in Organization Settings.
[Organization Settings](#)

Server Addresses

216.239.32.91 : 2083 primary

Add Server

NAS Identifier
mist-venue-city-country

NAS IP Address

6. Enter the RadSec service values shown for the primary server, and click **OK**.

Primary RadSec server values:

Name	Description	Value
Host	Orion RadSec IP address or an FQDN <i>See Deploy and configure RadSec</i>	216.239.32.91
Port	Port for RadSec secure tunnel	2083 (default)

Server Name	RadSec server certificate name used to verify Orion server identity	*.orion.area120.com
-------------	---	---------------------

- To add a secondary radsec server for redundancy/HA, click **add a server** again under **RadSec Servers** to add a backup server - 216.239.34.91.
- For a **NAS Identifier**, enter a meaningful description of the access point and site, such as "Shopping-Center_123-Main-Street_City_State_Zip". Because this identifier is limited to 48 characters, full addresses might not be possible. Note that NAS ID is used as a network identifier in Orion WiFi and important to be distinct and unique.
- Enable "**Hotspot 2.0**" and enable operator "Google" from the drop-down. Venue Name field can be left blank, in which case "Site Name" will be automatically used as the venue-name.

Hotspot 2.0

Enabled Disabled

Operators

Google × +

Venue Name

The **New WLAN** page should look like this example.

< WLANs: **New WLAN**

SSID

Labels

WiFi SLE

 Exclude this WLAN from WiFi SLEs (except AP Update SLE)

WLAN Status

Enabled Disabled

Hide SSID

Broadcast AP name

Radio Band

2.4 GHz and 5 GHz 2.4 GHz 5 GHz

Band Steering

Enable

Client Inactivity

Drop inactive clients after seconds

Geofence Contact Mist for Firmware

Minimum client Signal Strength (2.4G)

Minimum client Signal Strength (5G)

Block clients having Signal Strength below the minimum

Data Rates

Compatible (allow all connections)

No Legacy (2.4G, no 11b)

High Density (disable all lower rates)

Custom Rates

WiFi Protocols

WiFi-6 Enabled Disabled

WLAN Rate Limit

Limit uplink to Mbps

Limit downlink to Mbps

Per-Client Rate Limit

Security

WPA-2/PSK with passphrase [Reveal](#)

WPA-2/EAP (802.1X)

Open Access

[More Options](#)

Prevent banned clients from associating
(Contact Mist for firmware)
Edit banned clients in [Network Security Page](#)

Fast Roaming

Default

Opportunistic Key Caching (OKC)

.11r

802.1X Web Redirect

Allow 802.1X Web Redirect for quarantine or posture assessment based on RADIUS server response containing url-redirect-URL

Enabled Disabled

Hotspot 2.0

Enabled Disabled

Operators

Venue Name

Apply to Access Points

All APs AP Labels Specific APs

Isolation

prohibit peer to peer communication

Filtering (Wireless)

ARP

Broadcast/Multicast

Ignore Broadcast SSID Probe Requests

DTIM Period

DTIM period

Custom Forwarding

Custom Forwarding to

SSID Scheduling

Enabled Disabled

QoS Priority

Override QoS

Multimedia Extensions

WMM Enabled Disabled

APSD Enabled Disabled

AirWatch

Enabled Disabled

Application QoS

[Add Application](#)

Applications

No Applications have been defined

RadSec

Enabled Disabled Mist Edge Proxy

Server Name

Please ensure Mist CA cert is supplied to RadSec servers, and RadSec CA cert is supplied to Mist in Organization Settings.

[Organization Settings](#)

Server Addresses

primary

[Add Server](#)

NAS Identifier

NAS IP Address

CoA/DM Server

10. To complete the New WLAN creation process, click **Create** in the top right corner.

THU, 01:10 AM

The **WLANs** page appears and displays the new Orion SSID.

Filter	SSID	Enabled	Band	Security	VLAN ID	WLAN Limit	Client Limit	WLAN Labels
	Mist-Test	⊙	2.4GHz and 5GHz	WPA-2/EAP (802.1X)		Unlimited / Unlimited	Unlimited / Unlimited	
	Mist-Test-2	⊙	2.4GHz and 5GHz	WPA-2/EAP (802.1X)		Unlimited / Unlimited	Unlimited / Unlimited	
	Orion	⊙	2.4GHz and 5GHz	WPA-2/EAP (802.1X)		Unlimited / Unlimited	Unlimited / Unlimited	

Provision Orion RadSec certificates to the Mist Cloud

To enable secure and trusted RadSec communication between Mist APs and Orion's RadSec servers, it is required to provision Orion's SSL certificates to the Mist Cloud.

On the Orion settings page click on the **"Generate RadSec Certificates"** button to download a zip file containing all the necessary files:

RadSec Certs

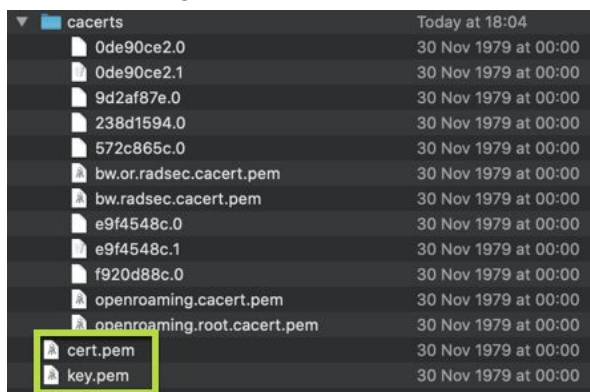
Please click on the button below to generate new certificates. These will be used during deployment to enable RadSec (Radius over TLS) connections to the Orion WiFi service.

[Generate RadSec Certificates](#)

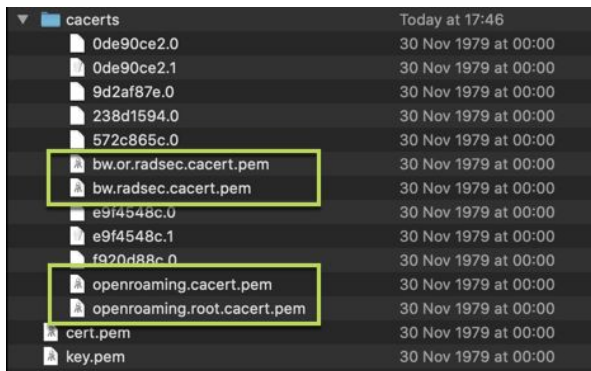
The first step is to prepare the certificate files. Unpack the zip archive.

There are two important parts required to provision all certificates to the Mist Cloud:

1. **AP (client) certificate and private key** – this is the certificate that is unique to your particular Orion account, and will be presented by each Mist AP that belongs to the same Mist Org:

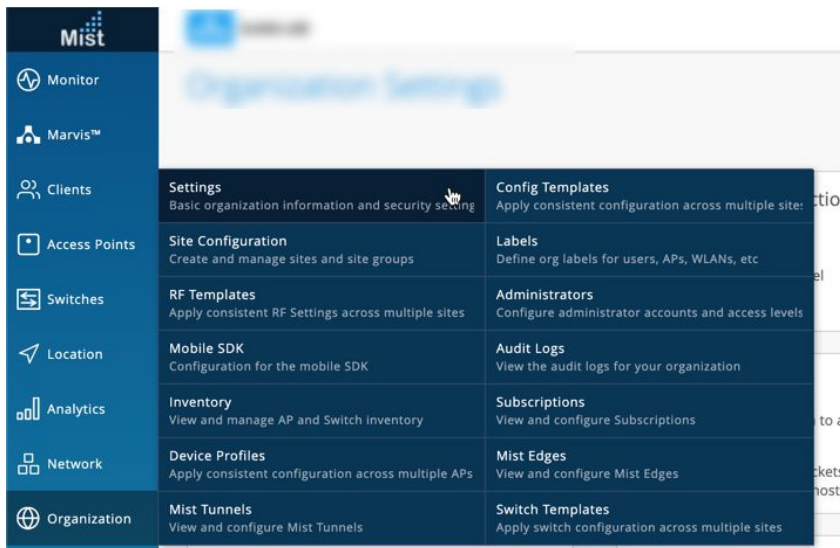


2. **Orion's Root CA certificates** – these are the root CA certificates that we need to include in the trust chain for the Mist APs to verify the validity of Orion's RadSec server certificates:



Open each of the above files in any text editor to get ready for the next step. The following process can be used to easily publish Orion RadSec certificates to the Mist Cloud.

3. On the Mist Dashboard navigate to **Organization > Settings**



4. Scroll down to the RadSec Certificates section. Click on the “Add AP RadSec Certificate” and paste contents of the **key.pem** file to the Private Key field, and contents of the **cert.pem** to the Signed Certificate field. Save after you are done.:

Mist Certificate
CA certificate for use by RadSec servers to validate certificates presented by Mist APs. Copy this certificate to all RadSec servers.
[View Certificate](#)

RadSec Certificates
CA certificates for use by Mist APs to validate certificates presented by RadSec servers.
[Add a RadSec certificate](#)

AP RadSec Certificate
Signed certificate for use by Mist APs to identify themselves to RadSec servers.
[Add AP RadSec certificate](#)

AP RadSec Certificate

Private Key

```
-----BEGIN EC PRIVATE KEY-----
MHcCAQEEIC8ZRilExvBGH6Od2xlwYbYnTObN/iQdPkM9ZzK/LcGBoAoGCC
qGSM49
AwEHoUJODQgAEIwZ80bwYBG/cN5gdtBCN6DupsB7Q0sPi1PrroD85iu5iwUj
F6Yyhu
4o07QF8VFRZMJ4+appP2bsawT1jvHXzN4w==
-----END EC PRIVATE KEY-----
```

Signed Certificate

```
DAgeAMBMG
A1UdjQQMMAoGCCsGAQUFBwMCAwGA1UdEwEB/wQCAAwKAQYDV
R0RBCewH4IdbWlz
dHN5c3RlbnMub3Jpb24uYXJlYTEyMC5jb20wCgYIKoZlZj0EAWIDRwAwRAI
gDdS2
Np3JRBFS8M72EQPRMmtjN8oRda5jq4elZnSROYCIF43z0qAZFYQHsnz4
E46K3sk
vtYtu3pGgtAWjrV/cK1L
-----END CERTIFICATE-----
```

Save Cancel

- Now click on the “Add a RadSec Certificate” link and add each and every CA certificate that you downloaded from Orion, one by one:

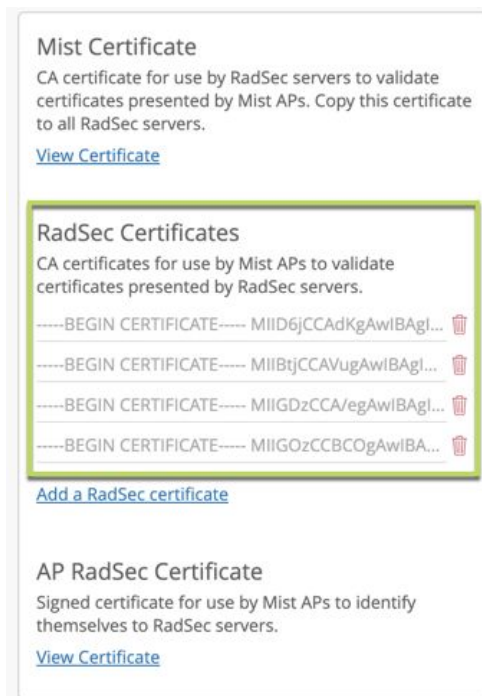
Mist Certificate
CA certificate for use by RadSec servers to validate certificates presented by Mist APs. Copy this certificate to all RadSec servers.
[View Certificate](#)

RadSec Certificates
CA certificates for use by Mist APs to validate certificates presented by RadSec servers.
[Add a RadSec certificate](#)

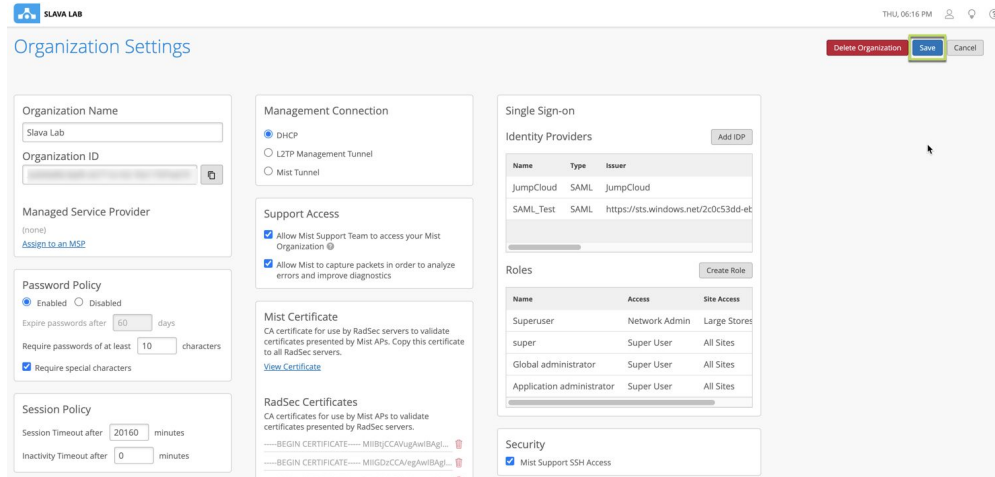
AP RadSec Certificate
Signed certificate for use by Mist APs to identify themselves to RadSec servers.
[View Certificate](#)



Repeat the same steps for **bw.radsec.cacert.pem**, **openroaming.cacert.pem**, **openroaming.root.cacert.pem**. At the end you should see 4 RadSec certificates showing up:



Do not forget to save all changes in the top right corner of the screen:



Note that after this procedure is complete, any Mist AP (existing or new) that is claimed to your Organization will automatically have Orion RadSec certificate provisioned and ready to be used.

Upgrade your Mist APs to support Hotspot 2.0

In order to support Hotspot2.0 a Mist AP needs to run **0.8.21116** or higher firmware. In order to upgrade your APs manually navigate to Access Points tab, select all or several APs you would like to upgrade and initiate the upgrade procedure. It is also possible to set your auto-upgrade image under Site settings to make sure all new APs will be upgraded to the same version.

Note it takes about 20 seconds for the Mist AP to reboot to apply a new firmware:

