



[COGNITIVE CAMPUS](#) > [AGNI](#)  
([/ARISTACOMMUNITY/S/TOPIC/0...](#)) ([/ARISTACOMMUNITY/S/TOPIC/0...](#))

**Title**

Configuring RadSec profile in EOS

**Article Type**

Configuration

**Author**

[Karl-Magnus Olsson \(/AristaCommunity/s/profile/00521000008eeKJQAY\)](#)

**Language**

English

**Published Date**

September 5, 2023

**Updated Date**

January 17, 2025

**Table of Contents**

- [Configuring RadSec profile in EOS](#)
  - [Generate certificates](#)
    - [Method 1 - CSR \(Certificate Signing Request\)](#)
      - [Copy certificates to the switch](#)
    - [Method 2 - Direct certificate generation](#)
      - [Copy certificates to the switch](#)
    - [Create a SSL profile](#)
  - [RadSec profile configuration](#)
  - [Example Configuration](#)
  - [Verify the RadSec connection](#)
  - [Troubleshooting](#)

**Content**

# Configuring RadSec profile in EOS

Arista Switches can form a RadSec tunnel using SSL encryption with AGNI. RadSec is a protocol that supports RADIUS over TCP and TLS. For mutual authentication it is required to install a client certificate with corresponding private key as well as your AGNI CA certificate. The steps below assumes the usage of AGNI's internal PKI.

Major steps to create, upload and establish the RadSec tunnel.

1. Generate private key and CSR
2. Generate client certificate for the Switch in AGNI.
3. Upload the Certificate to the Switch.
4. Configure an SSL profile and RadSec profile

## Generate certificates

### Method 1 - CSR (Certificate Signing Request)

A pair of two keys ( public and private key) is generated using a public-key cryptosystem. EOS supports the RSA algorithm with key lengths of 2,048, 3,072, or 4,096 bit.

A certificate signing request (CSR) is issued specifying properties like the common name (CN) and DNS. The CSR is then submitted to the CA (AGNI). AGNI will generate a certificate that must be uploaded and installed on the switch

It is also necessary to upload AGNI's root certificate to the switch trust list.

- Generate the Key pair

```
switch01#security pki key generate rsa 2048 rit311.key
```

- Generate the certificate signing request using the key just created.

**Note. Common Name must correspond to the Switch MAC address and the DNS needs to match the hostname of the switch**

```

rit311...17:18:39(config)#security pki certificate generate si
Common Name for use in subject: 2c:dd:e9:fe:cd:68
Two-Letter Country Code for use in subject: US
State for use in subject: NC
Locality Name for use in subject: RTP
Organization Name for use in subject: Arista
Organization Unit Name for use in subject: Lab
Email address for use in subject:
IP addresses (space separated) for use in subject-alternative-
DNS names (space separated) for use in subject-alternative-nam
Email addresses (space separated) for use in subject-alternati
URIs (space separated) for use in subject-alternative-name:
-----BEGIN CERTIFICATE REQUEST-----
MIICzDCCAbQCAQAwYzELMAkGA1UEBhMCVVMxCzAJBgNVBAGMAk5DMQwwCgYDVQ
DANSVFAXDzANBgNVBAoMBkFyaXN0YTEMMAoGA1UECwwDTGFiMR0wGAYDVQQDD
BZypkZDplOTpmZTpjZDo2ODCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCgg
AM+QJPWIMHNj0LJ8aChLVX5F1m6Ce5/bLCmaZgZrhYBGAW47GTiyCbsFCEwYNT
0nZq/LGuy5yX2fUdL+L9bXbgRFzdZLoMFCCfXulK4fUJX0lzVmIlEPpycS11wD
aW9oEludsE+j8+zW0blhDWKRL75eSRIcdYgm5yWrcdAVVWhrm0kM9iKcuc5LYK
/eaqzc7Ef70Nrjt89JAn+M7wNiMTVbEfUwFRpuPQjpUSHnvREEUGN0vQIrBhdP
KWJ30yFhX3Ers6xLHSv2RcdHPSc2qsH6rEjaNMiu4MLMaTjux0Mya2FqX0ATkG
MJvMDN13DKrrIj9a41+buhECAwEAAaAkMCIGCSqGSIb3DQEJJDjEVMbMwEQYDVR
BAowCIIGcm10MzExMA0GCSqGSIb3DQEBCwUAA4IBAQDE12j/6CA0LXVXS1zqig
EsSf2H8IZDq+8ZaMzKX+8zDWQ9UySsS6DdTr+H72SXtBCclpsImgwxRDHt8r0P
ZwLpAXD0Xkt0hPrRiNsM2evo78FUxbwN2NxLcyZmsWIa5VDCQ4nqmmU7Sjqt0f
XXpCkxEUTu/01PhgmtUo5+lSgI7eJLU6MCaP8kELPz/8L8R2zFTGL8ZKv2y3ps
HG9jGiGEGIXU0wkI103CHiUzaobJeYZd02N7l/Z0o7R5F1s00C88yX08Mff90R
r/Wiqh8QWoQCRctCsLQyLXhTdFbbfYEgZQukxtH4SUfg0hPc8024tN+z7FkUXE
-----END CERTIFICATE REQUEST-----

```

- Copy the certificate including the text “-----BEGIN CERTIFICATE REQUEST-----” and “-----END CERTIFICATE REQUEST-----”
- Select your **Access Device** from the list and select **Get Client Certificate**.
- Select Use CSR (Single Device) and Past CSR.

Note 1. CSR can also be uploaded from file by selecting action **Upload CSR File**

Note 2. For signing multiple CSRs select **Upload Zip with multiple CSRs**

CloudVision

agni

Karl-Magnus Olsson - Arista

MONITORING

Dashboard

Sessions

ACCESS CONTROL

Networks

Segments

ACLs

IDENTITY

Identity Provider

User

Client

CONFIGURATION

Access Devices

Devices

Device Groups

Certificates

System

CONCOURSE

Explore

Installed Apps

Generate RadSec Client Certificate

Fill in the details to generate RadSec client certificate for the Access Device

Generate Certificate:

☐ Generate
 ☒ Use CSR (Single Device)
 ☐ Upload Zip with multiple CSRs

Access Device

rit311

Select Action:

☐ Upload CSR File
 ☒ Paste CSR

Paste CSR

```

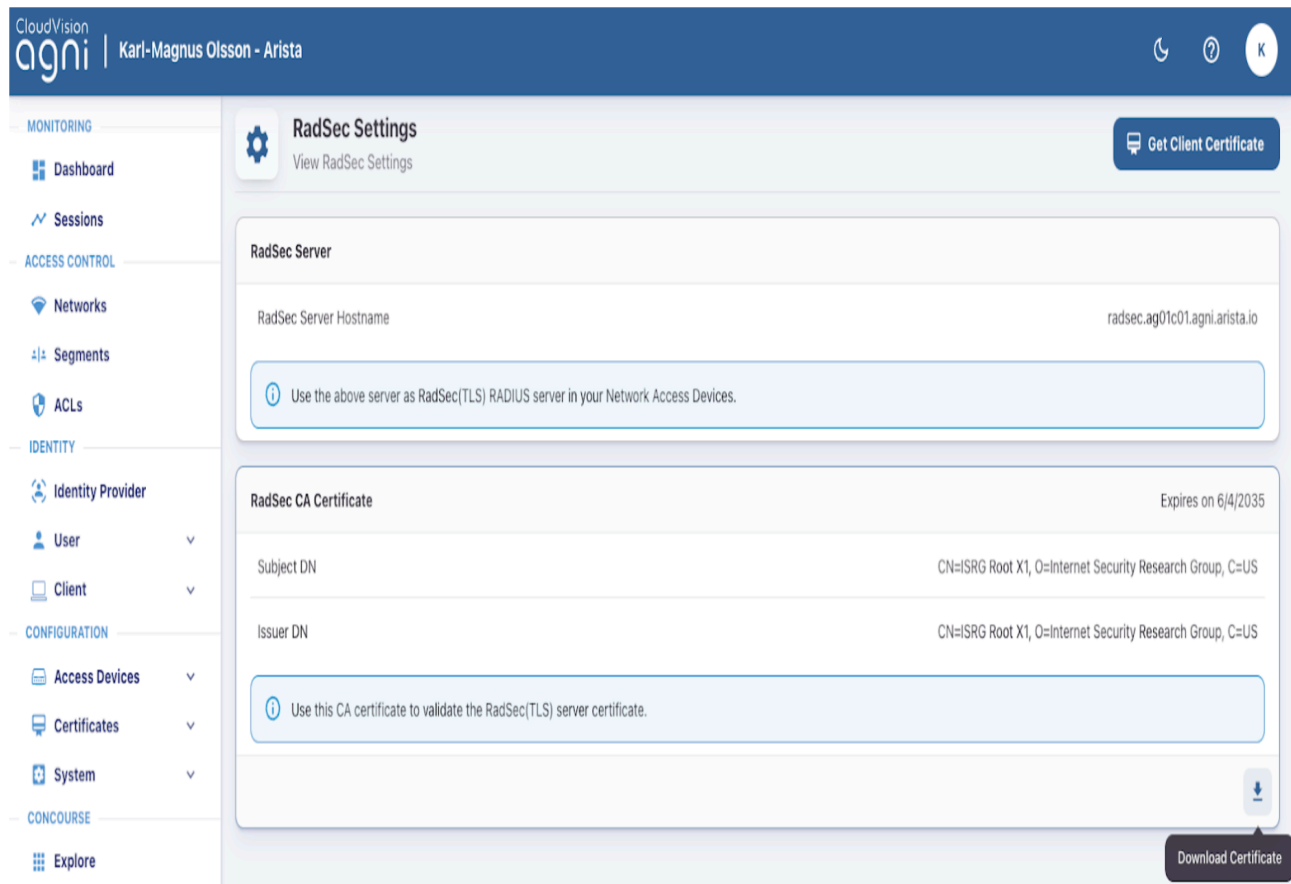
-----BEGIN CERTIFICATE REQUEST-----
MIICZDCCAbQCAQAwYzELMAkGA1UEBhMCVVMxChAJBqNVBAgMAk5DMQwwCgYDVQQH
DANSVFAXDzANBgNVBAoMBkFvaXN0YTEMMGA1UECwwDTGFmRowGAYDVQQDDBEy
YzpkZDplOTpmZTpjZDo2ODCCASlwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEB
AM+QJPWIMHNIOLJ8aChLVX5F1m6Ce5/bLCmaZgZrhYBGAW47GTivCbsFEwYNTRL
OnZq/LGuy5yX2fUdL+L9bXbqRFzdZLoMFCCfXulk4fUJXOlzVmlEPpycS11wDUU
aW9oEludsE+j8+zW0bldWKRl75eSRlCdYam5WrcdAVVWhrm0kM9Kcuc5iYKJb
/eaqzc7Ef7ONrit89JAn+M7wNIMTVbEfUwfrPupQjpUSHnvREEUGNOvQlrBhdP5N
KWJ3OyFhX3Ers6xLHSv2RcdHPSc2qsH6rEjaNMiu4MLMaTjux0Mya2FqX0ATkG8T
MJvMDN13DKrrj9a41+buhECAwEAaAkMCIGCSqGSib3DQEJDJEVMBMwEQYDVROR
BAowCIIgcmlOMzExMA0GCsGqGSib3DQEBCwUA4IBAQDE12j/6CA0LXVXSizqigVd
EsSf2H8lZDq+8ZaMzKX+8zDWQ9UySs56DdTr+H72SXtBCclpsImgwXRdHt8rOPL1
ZwLpAXDOXkTOhPrINsM2evo78FuxbwN2NxLcyZmsWla5VDCQ4ngmmU7Siat0f45
XXpCkxEUTu/01PhgmtUo5+ISqI7eJLU6MCAp8kEIPz/8L8R2zFTG8Zkv2v3psOV
HG9IGIGEGIXUOwk103CHIuZaobJeYzd02N7j/ZOo7R5F1s0OC88yXO8Mff9ORwf
r/Wiah8QWoQCRctCsLQvLXhTdFbbfYEqZQukxtH4SUfoOhPc8O24tN+z7FKUXEq6
-----END CERTIFICATE REQUEST-----

```

Cancel

Generate Certificate

- Click **Generate Certificate**. A certificate [Access device].pem will be generated and downloaded.
- Go to **RadSec Setting** in the Navigator under Administration section to download the CA certificate.
- Download the RadSec CA certificate (radsec\_ca\_certificate.pem) by clicking **Download Certificate**.



## Copy certificates to the switch

The certificate and root certificate need to be copied to the switch flash using SCP.

- Prerequisites

Settings on switch to be able to SCP over the certs.

```
#username USER privilege 15 role network-admin secret SECRET
#aaa authentication login console local
#aaa authorization exec default local
```

- Copy the certificates

```
#scp rit311.pem radsec_ca_certificate.pem <user>@<switch-ip>:/
```

- Now you are ready to create a SSL profile

## Method 2 - Direct certificate generation

Generate a RadSec client certificate for the switch from AGNI by following the procedure.

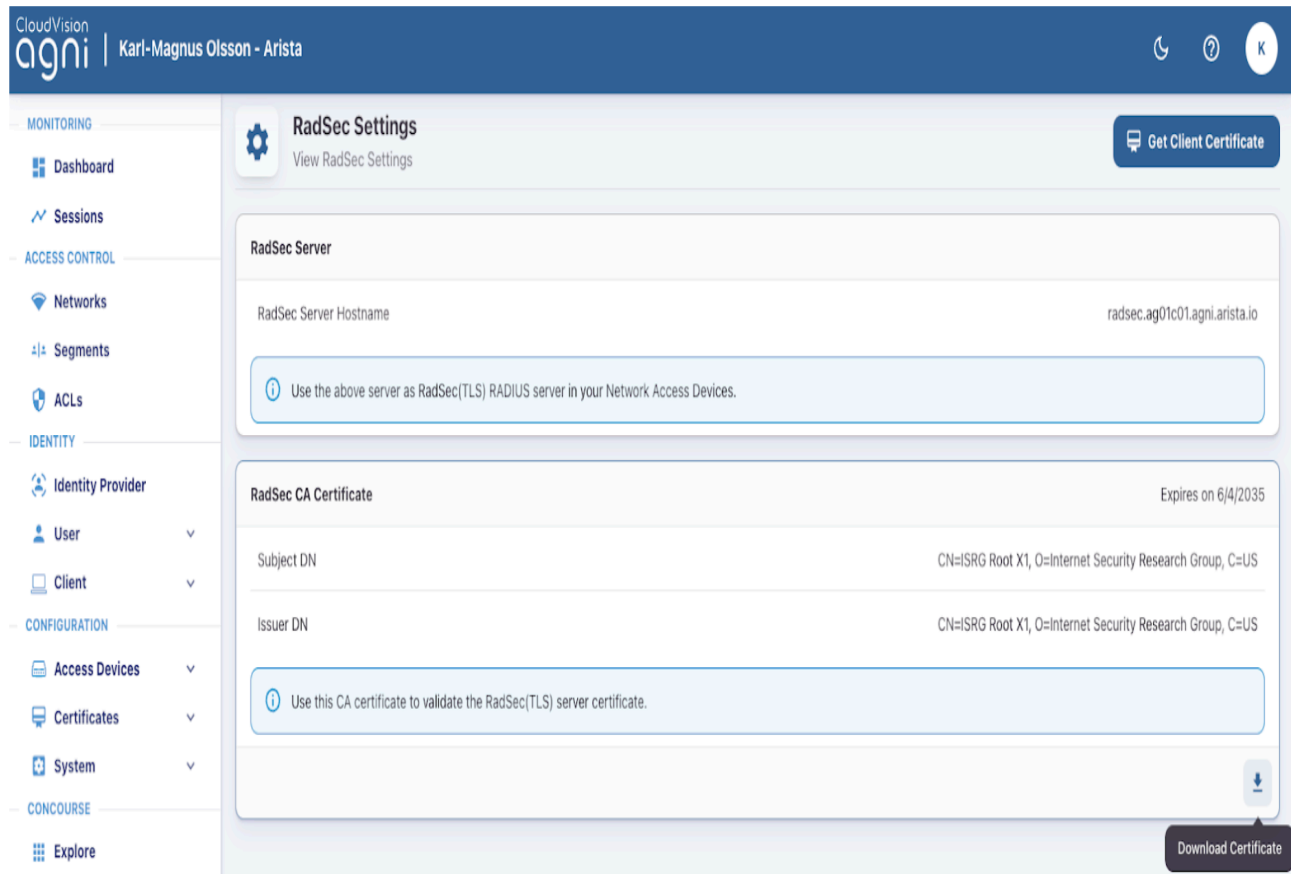
- Select your **Access Device** from the list and select **Get Client Certificate**.

- Select **Generate**. Define password and DNS name.

Note. The DNS name needs to match the switch host name

The screenshot shows the CloudVision interface with the 'Generate RadSec Client Certificate' form. The left sidebar contains navigation links under 'MONITORING' (Dashboard, Sessions), 'ACCESS CONTROL' (Networks, Segments, ACLs), 'IDENTITY' (Identity Provider, User, Client), and 'CONFIGURATION' (Access Devices, Devices, Device Groups). The main panel has a title 'Generate RadSec Client Certificate' and a subtitle 'Fill in the details to generate RadSec client certificate for the Access Device'. A 'Back' button is in the top right. The form includes three radio buttons for 'Generate Certificate': 'Generate' (selected), 'Use CSR (Single Device)', and 'Upload Zip with multiple CSRs'. There are three input fields: 'Access Device' (containing 'rit311'), 'Password' (masked with dots), and 'DNS Names' (containing 'rit311'). A 'Cancel' button and a 'Generate Certificate' button are at the bottom right.

- Click **Generate Certificate**. A certificate [Access device].pem will be generated.
- Go to **RadSec Setting** in the Navigator under Administration section to download the CA certificate.
- Download the RadSec CA certificate (radsec\_ca\_certificate.pem) by clicking **Download Certificate**.



- Break out the private key

Split the certificate into switch.crt and switch.key using the openssl commands described. The following commands are run in terminal (Linux, MacOS or Windows)

```
#openssl pkcs12 -in rit311.p12 -out rit311.crt -clcerts -nokey
#openssl pkcs12 -in rit311.p12 -out rit311.key -nocerts -nodes
```

Note. Running openssl on newer MacOS release might require -legacy flag to be added to the commands above.

## Copy certificates to the switch

The certificate, key and CA certificate files need to be copied to the switch flash using scp.

- Prerequisites

Settings on switch to be able to SCP over the certs.

```
#username USER privilege 15 role network-admin secret SECRET
#aaa authentication login console local
#aaa authorization exec default local
```

- Copy the certificates.

```
#scp rit311.crt rit311.key radsec_ca_certificate.pem  
<user>@<switch-ip>:/mnt/flash
```

## Create a SSL profile

- SSH to the switch and create the SSL profile by executing the commands below. All steps except for copying the key to the key storage is required for both method 1 and 2.

```
rit311#copy flash:rit311.pem certificate:  
rit311#copy flash:rit311.key sslkey: (Not necessary if certifi  
rit311#copy flash:radsec_ca_certificate.pem certificate:  
rit311#config  
rit311(config)#management security  
rit311(config-mgmt-security)#ssl profile agni-server  
rit311(config-mgmt-sec-ssl-profile-server)#certificate rit311.  
rit311(config-mgmt-sec-ssl-profile-server)#trust certificate r
```

- Test your management security profile

```
rit311#show management security ssl profile agni-server
```

Profile	State
-----	
agni-server	valid

## RadSec profile configuration

- Configure AGNI as a RadSec server in the switch and use the above configured SSL profile.



```

rit311(config)#radius-server host radsec.ag01c01.agni.arista.i
rit311(config)#aaa group server radius agni-server-group
rit311(config-sg-radius-agni-server-group)# server radsec.ag01
rit311(config)#aaa authentication dot1x default group radius
rit311(config)#aaa accounting dot1x default start-stop group r

```

## Example Configuration

```

management security
    ssl profile agni-server
        certificate rit311.pem key rit311.key
        trust certificate radsec_ca_certificate.pem
!
radius-server host radsec.beta.agni.arista.io (http://radsec.b
!
aaa group server radius agni-server-group
    server radsec.ag01c01.agni.arista.io (http://radsec.ag01c01
!

aaa authentication dot1x default group radius
aaa accounting dot1x default start-stop group radius

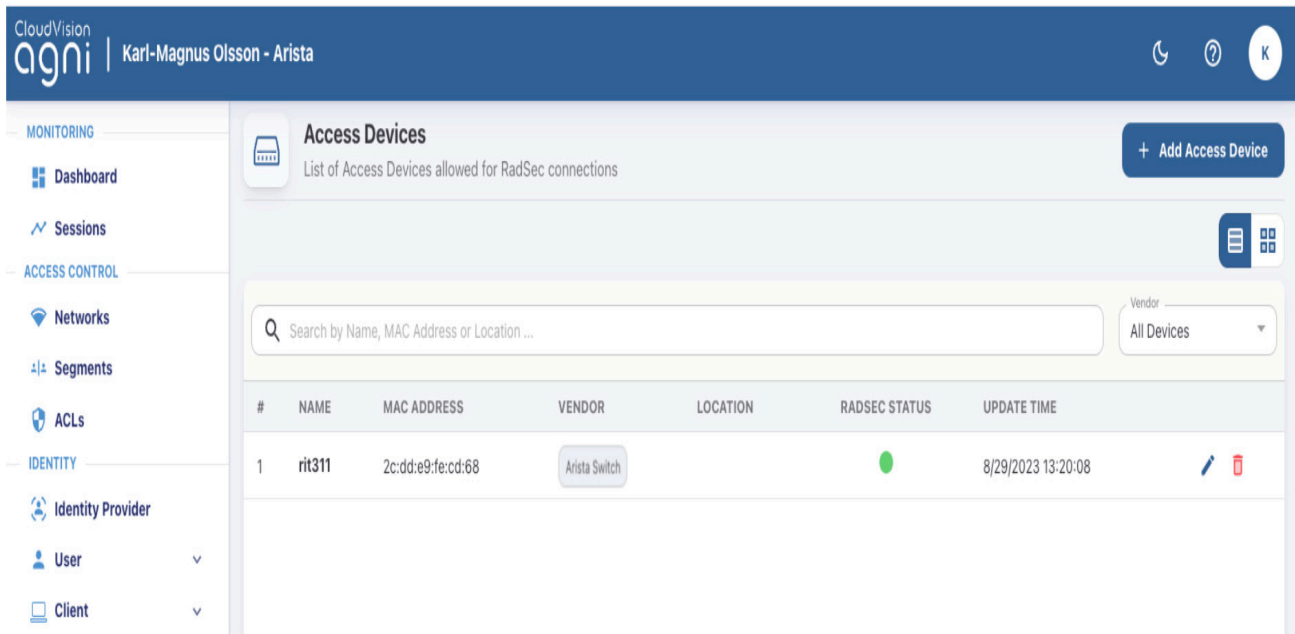
!

```

## Verify the RadSec connection

The status of the RadSec tunnel can be verified from: Configuration > Access Devices > Devices page in AGNI. Solid green under RadSec status means that the tunnel is UP.

The RadSec tunnel stays Down [Solid Gray], unless the Access Device is using it. Meaning, SSIDs using RadSec should be turned ON.



## Troubleshooting

- Client certificate missing or wrong.

List available certificates.

```
#dir certificate:
```

List available Keys.

```
#dir sslkey:
```

Make sure your certificate and key pair is valid.

```
#sh management security ssl profile agni-server
```

```
KM710(config-mgmt-sec-ssl-profile-agni-server)#end
KM710#sh management security ssl profile agni-server
  Profile      State      Additional Info
-----
  agni-server  invalid  Certificate 'switch2.crt' does not match
                                with key
```

Example output of certificate and key mismatch

This command displays the status of the SSL profile server. Problems like Certificate does not exist, Certificate expired, incorrect certificate chain, Certificate is not yet valid, etc can be revealed using this command

"Certificate not yet valid" is generally a symptom of incorrect date and time on the switch.

- Make sure Switch Host name is present in client certificate.

```
#show management security ssl certificate rit311.pem
```

```
b223f5ae35f9bba11
X509v3 extensions:
  subjectKeyIdentifier:
    D5:D4:2C:3E:14:F3:D5:28:8D:3F:D0:60:B4:05:F6:60:46:9D:25:5C
  keyUsage: Critical
    Digital Signature
  authorityKeyIdentifier:
    keyid:6C:4C:E0:E3:29:1D:95:14:49:BF:5B:AB:E3:CF:AB:82:F7:78:8B:4B
  extendedKeyUsage:
    TLS Web Client Authentication, Any Extended Key Usage
  subjectAltName:
    DNS:rit311
  basicConstraints: Critical
    CA:FALSE
```

Snippet of client certificate showing the DNS matching switch host name (here rit311)

- Root CA certificate of Server missing on client side

Make sure Root CA is trusted in your SSL profile

```
rit311..16:36:12(config)#sh run section ssl
management security
  ssl profile agni-server
    certificate rit311.pem key rit311.key
    trust certificate radsec_ca_certificate.pem
```

Further info on troubleshooting TLS

<https://www.arista.com/en/um-eos/eos-control-plane-security#xx1001547>  
(<https://www.arista.com/en/um-eos/eos-control-plane-security#xx1001547>)

Cognitive Campus  
(/AristaCommunity/s/topic/0TO2I00...

Campus Switches  
(/AristaCommunity/s/topic/0TO2I00...

AGNI  
(/AristaCommunity/s/topic/0TO5w0...

Was this article helpful?



1



0



F (0). (/AristaCommunity/s/relatedlist/ka0Uw0000006yO5IAI/AttachedContentDocuments).



## Related Articles

Enable RadSec (/AristaCommunity/s/article/Enable-RadSec)

1.02K

How to Troubleshoot “No Internet” issue on Client when connected to Wi-Fi (/AristaCommunity/s/article/How-to-Troubleshoot-No-Internet-issue)

703

Analysis of MAC Randomization Schemes in Wi-Fi Clients (/AristaCommunity/s/article/Analysis-of-MAC-Randomization-Schemes-in-Wi-Fi-Clients)

398

Configure and Troubleshoot DNS on EOS (/AristaCommunity/s/article/configure-and-troubleshoot-dns-on-eos)

5.28K

How to configure Link Aggregation Groups in EOS (/AristaCommunity/s/article/how-to-configure-link-aggregation-groups-in-eos)

10.92K

## Trending Articles

**DCS-7050SX3-48YC8/48C8 and 7050TX3-48C8: Logical port usages and limitations**

(/AristaCommunity/s/article/DCS-7050SX3-48YC8-and-7050TX3-48C8-Logical-port-usages-and-limitations).

**Wireshark for Troubleshooting - Part2**

(/AristaCommunity/s/article/Wireshark-for-troubleshooting-Part2).

**Understanding CloudVision APIs and accessing NetDB data**

(/AristaCommunity/s/article/Understanding-CloudVision-APIs-and-accessing-NetDB-data).

**VXLAN-EVPN Troubleshooting Guidebook**

(/AristaCommunity/s/article/VxLAN-EVPN-Troubleshooting-Guidebook).

**VeloCloud SD-WAN: VCE Links DEAD briefly after certificate renewal**

(/AristaCommunity/s/article/Velocloud-SD-WAN-VCE-Links-DEAD-briefly-after-certificate-renewal).

## Trending Topics



### Routing/Switching

13

([AristaCommunity/s/topic/0TO2I000000DaWGWA0/routingswitching](https://AristaCommunity/s/topic/0TO2I000000DaWGWA0/routingswitching)).

Get In Touch Today

Contact Us (<https://www.arista.com/en/company/contact-us>)

# ARISTA



(<https://www.facebook.com/AristaNW>)



(<https://twitter.com/AristaNetworks>)



(<https://www.linkedin.com/company/arista-networks-inc>)

## Support

### Support & Services

(<https://www.arista.com/en/support/customer-support>).

### Training

(<https://www.arista.com/en/partner/partner-portal/training>).

### Product Documentation

(<https://www.arista.com/en/support/product-documentation>).

### Software Downloads

(<https://www.arista.com/en/support/software-download>).

## Contacts & Help

### Contact Arista

(<https://www.arista.com/en/company/contact-us>).

### Contact Technical Support

(<https://www.arista.com/en/support/customer-support>).

Order Status (<https://orders.arista.com/>).

## News

### News Room

[. \(https://www.arista.com/en/company/news/in-the-news\)](https://www.arista.com/en/company/news/in-the-news)

### Events

[. \(https://www.arista.com/en/company/news/events\)](https://www.arista.com/en/company/news/events)  
[Blogs \(https://www.arista.com/blogs\)](https://www.arista.com/blogs)

## About Arista

### Company

[. \(https://www.arista.com/en/company/company-overview\)](https://www.arista.com/en/company/company-overview)

### Management Team

[. \(https://www.arista.com/en/company/management-team\)](https://www.arista.com/en/company/management-team)

### Careers

[. \(https://www.arista.com/en/careers\)](https://www.arista.com/en/careers)

### Investor Relations

[. \(https://investors.arista.com/\)](https://investors.arista.com/)

© 2025 Arista Networks, Inc. All rights reserved.

[Terms of Use \(https://www.arista.com/en/terms-of-use\)](https://www.arista.com/en/terms-of-use), [Privacy Policy \(https://www.arista.com/en/privacy-policy\)](https://www.arista.com/en/privacy-policy).