Configure TLS Certificate for QRadar Webpage

IBM Federal Sales Engineering

By: Christian L. Reyes

Date: June 15, 2023

Table of Contents

Disclaimer

NOTE: While the IBM QRadar “Installing a new SSL certificate” article (https://www.ibm.com/docs/en/qsip/7.5?topic=certificates-installing-new-ssl-certificate) is mostly correct, it is missing a major component. This component is the generation of the certificate signing request (CSR) with a subject alternate name (SAN). Modern browsers have enforcement of SAN within a certificate. This means that if you generate a CSR and corresponding certificate via the above listed article, it will never be trusted by the browser, regardless of if you have the root CA in the trusted authorities of the browser. A SAN is required for the certificate to be trusted. This how to guide will demonstrate how to create a san file.

Prerequisites

NOTE: Prior to attempting this guide ensure your customer has access to both DNS and the relevant Certificate Authority. Access to DNS and the Certificate authority will be needed to complete this task. If the end customer does not have access to these systems, ensure they have coordinated with the appropriate individuals who do have access.

1. Ensure a DNS A record exists for QRadar, within DNS server.

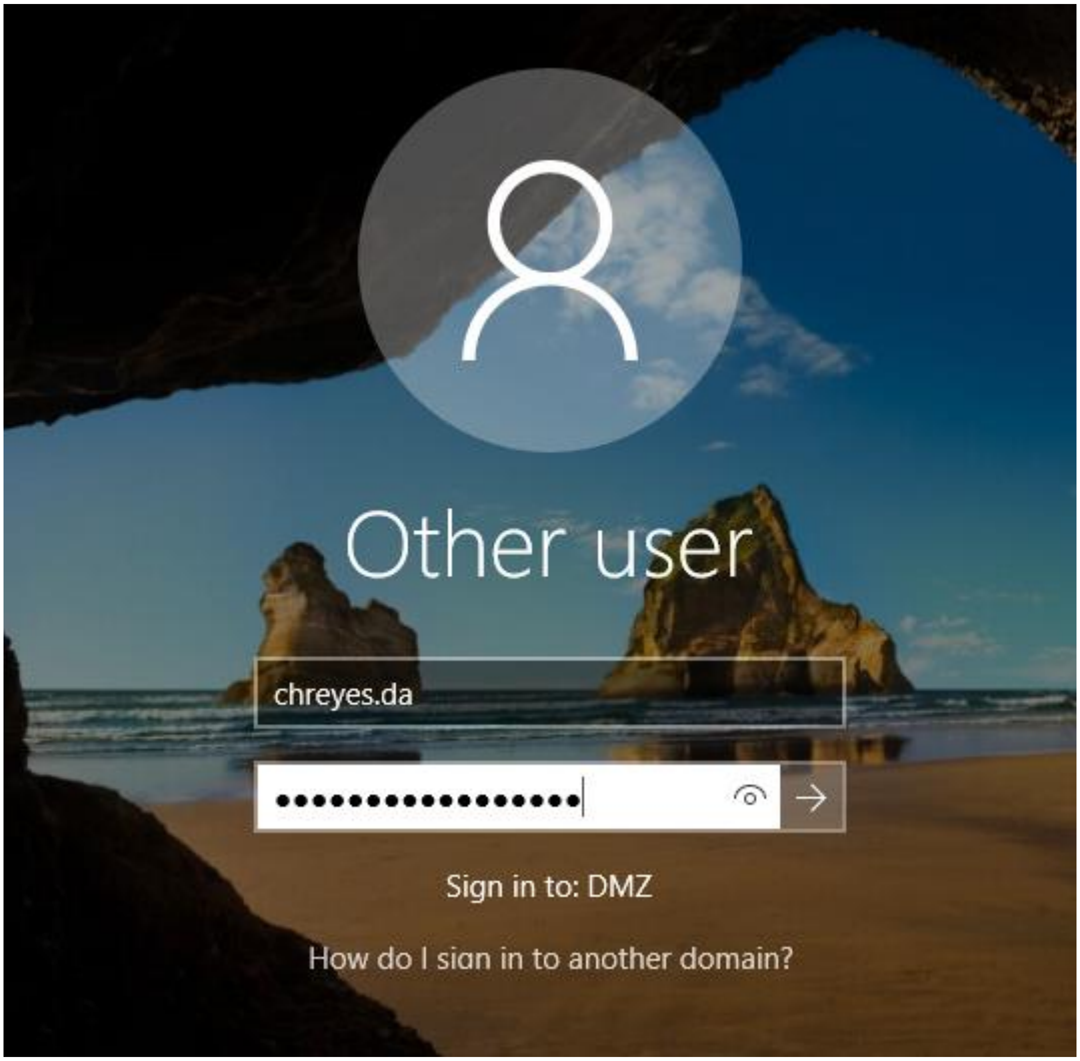
2. Ensure QRadar user has root access to CLI.

3. Ensure someone has access to Certificate Authority.

Create DNS A Record

NOTE: This step only needs to be completed if and only if the DNS record for QRadar doesn't already exist. Most customers will have a DNS A record for QRadar. Talk to the customer and validate an A record exists. If they do not have a DNS A record, then you may proceed with this section and assist the customer with building one out. If an DNS A record already exists, then you may skip ahead to the "Generate a CSR" section.

1. Log into Domain Controller that is hosting the DNS service, with a Domain Admin account.



Other user

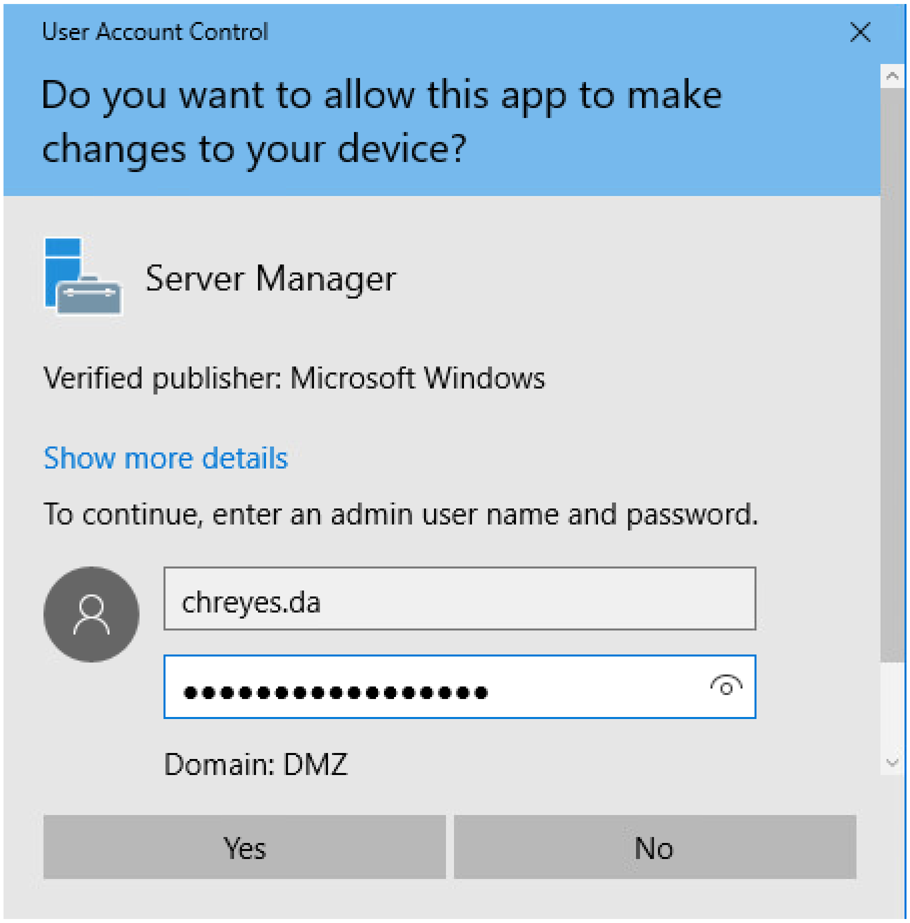
chreyes.da

•••••••••••••••••

Sign in to: DMZ

How do I sign in to another domain?

2. Enter the Domain Admin credentials again, to open the Server Manager.



User Account Control

Do you want to allow this app to make changes to your device?

Server Manager

Verified publisher: Microsoft Windows

Show more details

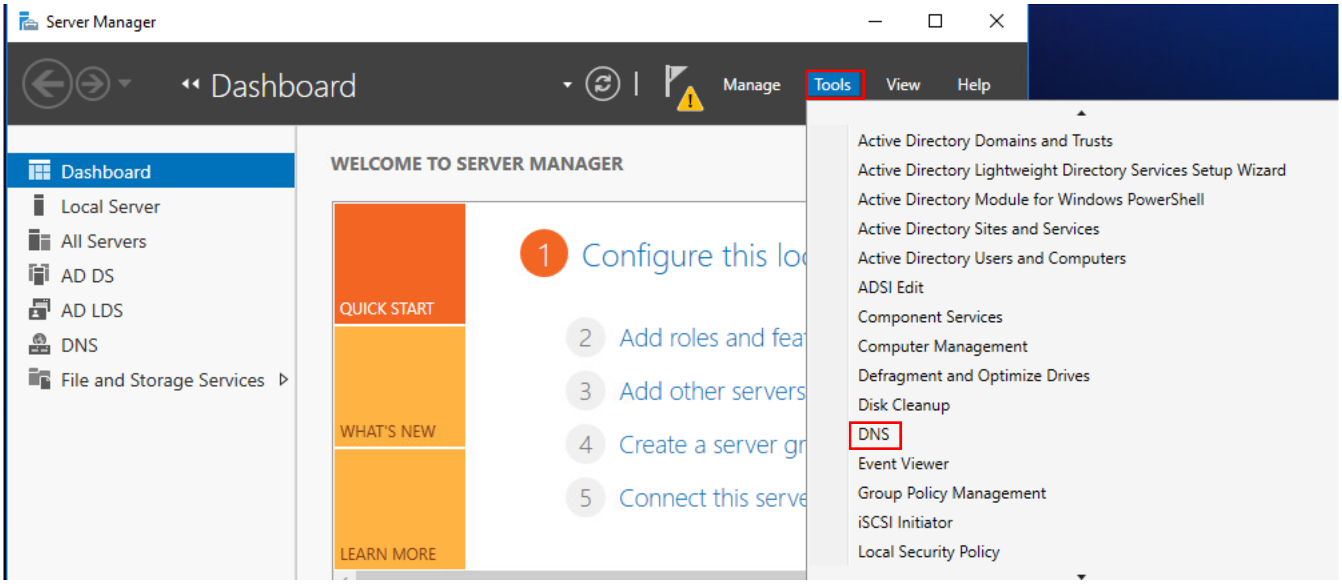
To continue, enter an admin user name and password.

chreyes.da

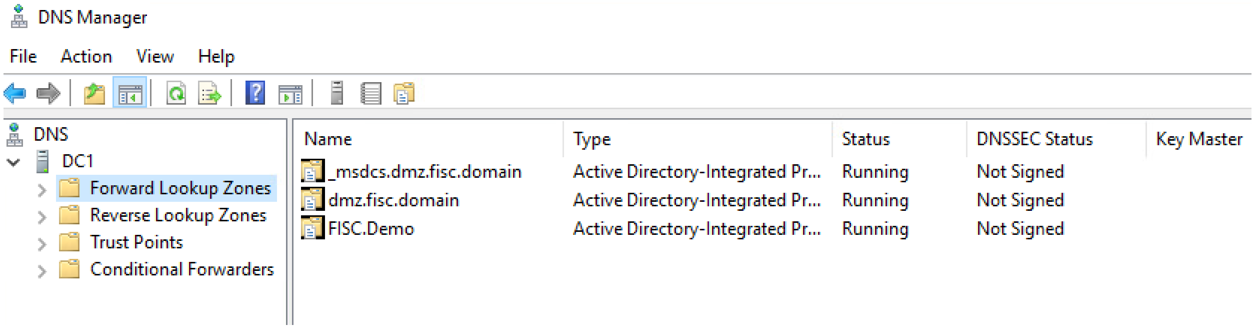
●●●●●●●●●●●●●●●●●

Domain: DMZ

3. Server Manager will open, next Click “Tools” and then “DNS”.

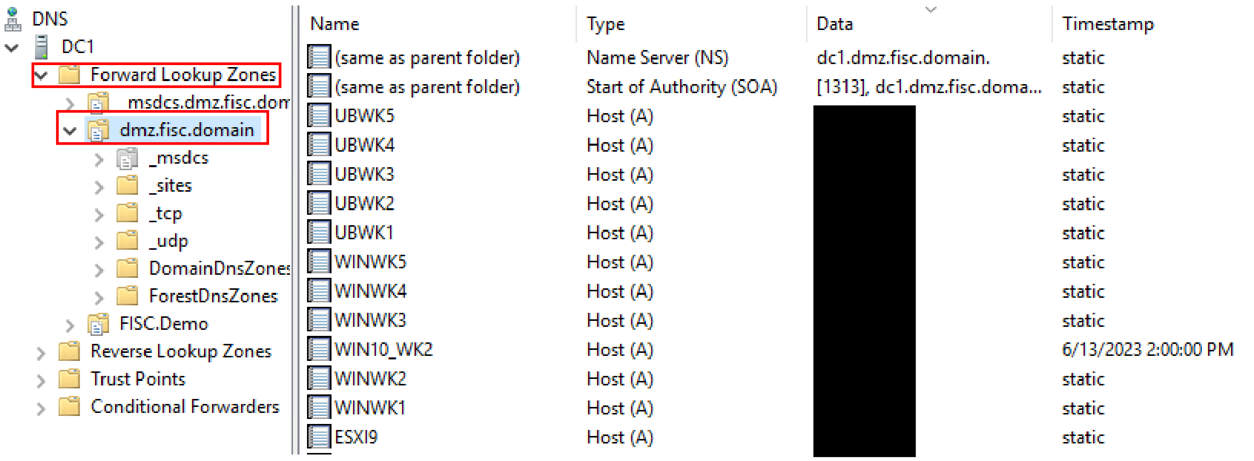


4. DNS Manager will open, as shown.



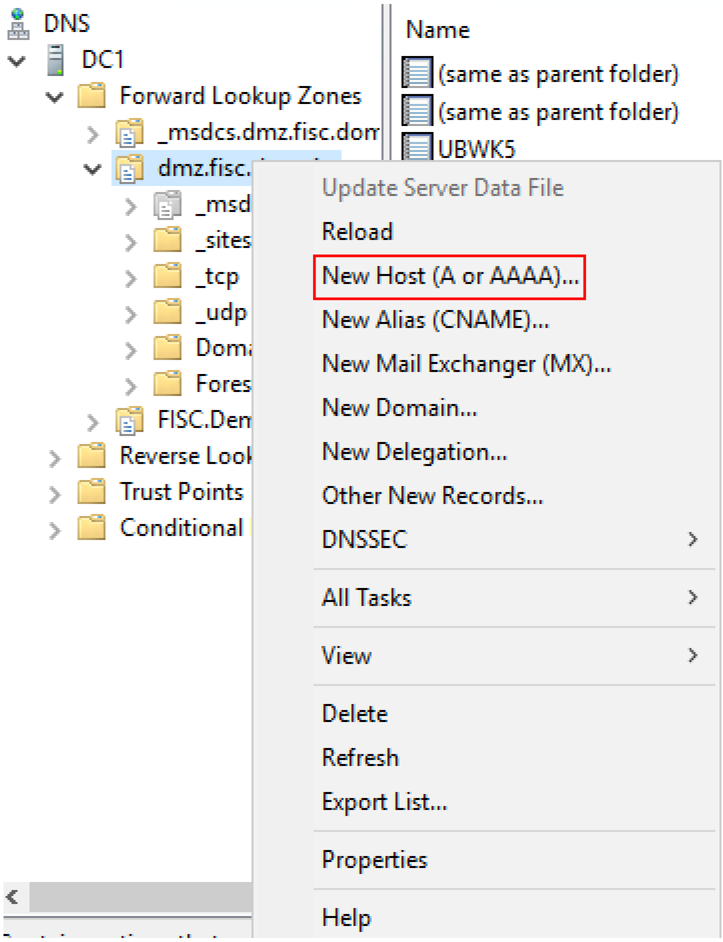
Name	Type	Status	DNSSEC Status	Key Master
_msdcs.dmz.fisc.domain	Active Directory-Integrated Pr...	Running	Not Signed	
dmz.fisc.domain	Active Directory-Integrated Pr...	Running	Not Signed	
FISC.Demo	Active Directory-Integrated Pr...	Running	Not Signed	

5. Expand the "Forward Lookup Zones", locate the domain you are looking for and expand that as well.



Name	Type	Data	Timestamp
(same as parent folder)	Name Server (NS)	dc1.dmz.fisc.domain.	static
(same as parent folder)	Start of Authority (SOA)	[1313], dc1.dmz.fisc.doma...	static
UBWK5	Host (A)	[redacted]	static
UBWK4	Host (A)	[redacted]	static
UBWK3	Host (A)	[redacted]	static
UBWK2	Host (A)	[redacted]	static
UBWK1	Host (A)	[redacted]	static
WINWK5	Host (A)	[redacted]	static
WINWK4	Host (A)	[redacted]	static
WINWK3	Host (A)	[redacted]	static
WIN10_WK2	Host (A)	[redacted]	6/13/2023 2:00:00 PM
WINWK2	Host (A)	[redacted]	static
WINWK1	Host (A)	[redacted]	static
ESXI9	Host (A)	[redacted]	static

6. Right click on the desire domain, the following menu will appear. Select "New Host (A or AAAA)…".



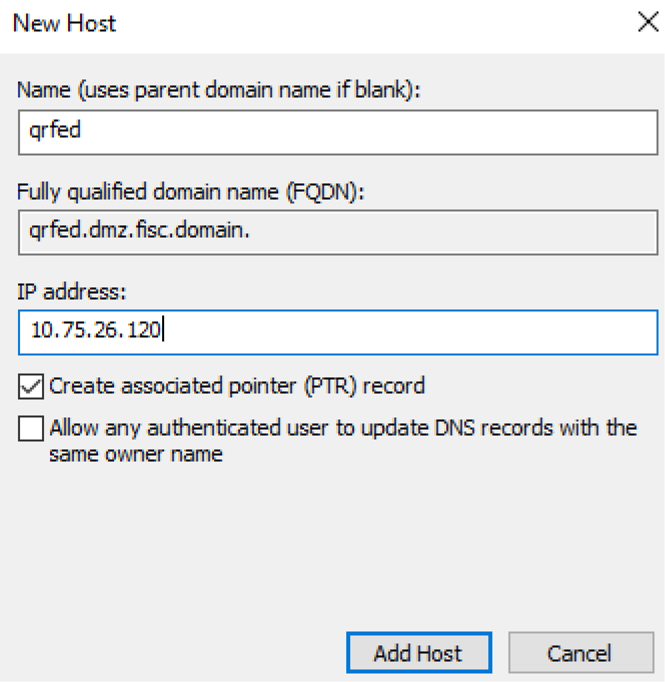
7. The “New Host” pop-up window will appear as shown. Enter the below information:

   a. Name = DNS Name of server, example: qrfed

   b. IP Address: = IP Address of QRadar Console

   c. Check Mark “Create associated pointer (PTR) record

   d. Click “Add Host”



New Host

Name (uses parent domain name if blank):

qrfed

Fully qualified domain name (FQDN):

qrfed.dmz.fisc.domain.

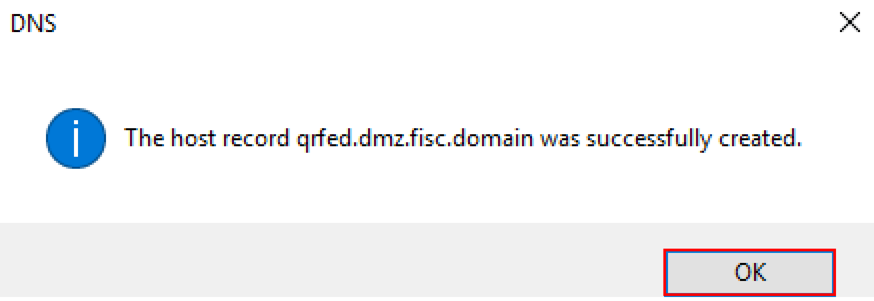
IP address:

10.75.26.120

☑ Create associated pointer (PTR) record

□ Allow any authenticated user to update DNS records with the same owner name

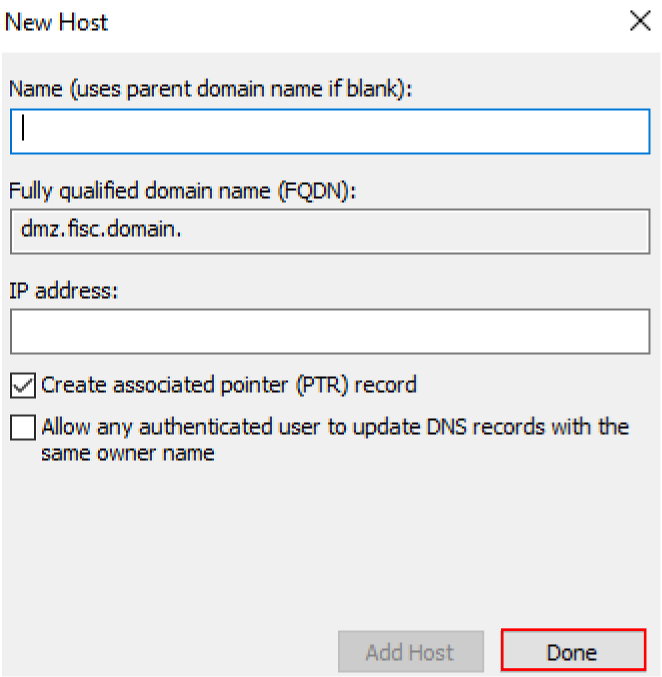
8. After clicking “Add Host”, ensure you receive the following message that the host record was successfully created. Click “OK” to exit.



DNS

The host record qrfed.dmz.fisc.domain was successfully created.

9. After clicking “OK”, you will be returned to the “New Host” pop-up window. Click “Done” to exit.



New Host

Name (uses parent domain name if blank):

Fully qualified domain name (FQDN):

dmz.fisc.domain.

IP address:

☑ Create associated pointer (PTR) record

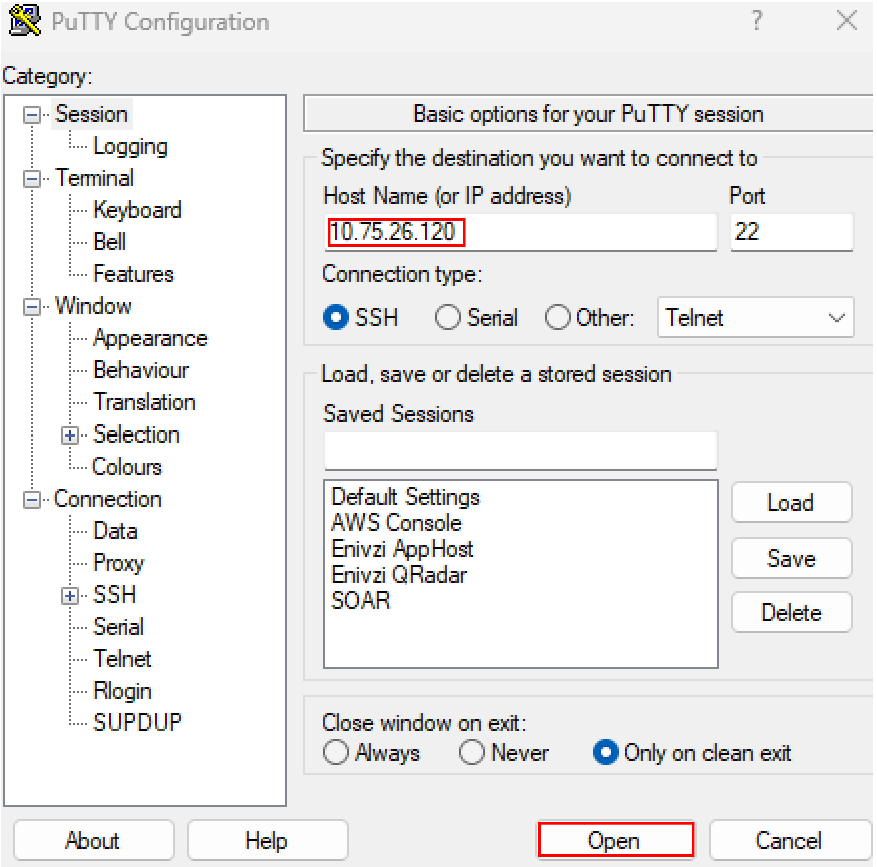
□ Allow any authenticated user to update DNS records with the same owner name

10. Close out of the “DNS Manager” and log out of the Domain Controller. Proceed to the next section.

Generate CSR

1. Open Putty or other terminal emulator.

2. Enter the QRadar Console IP Address in the “Host Name (or IP address)” space and click “Open”.



PuTTY Configuration

Category:

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.75.26.120

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

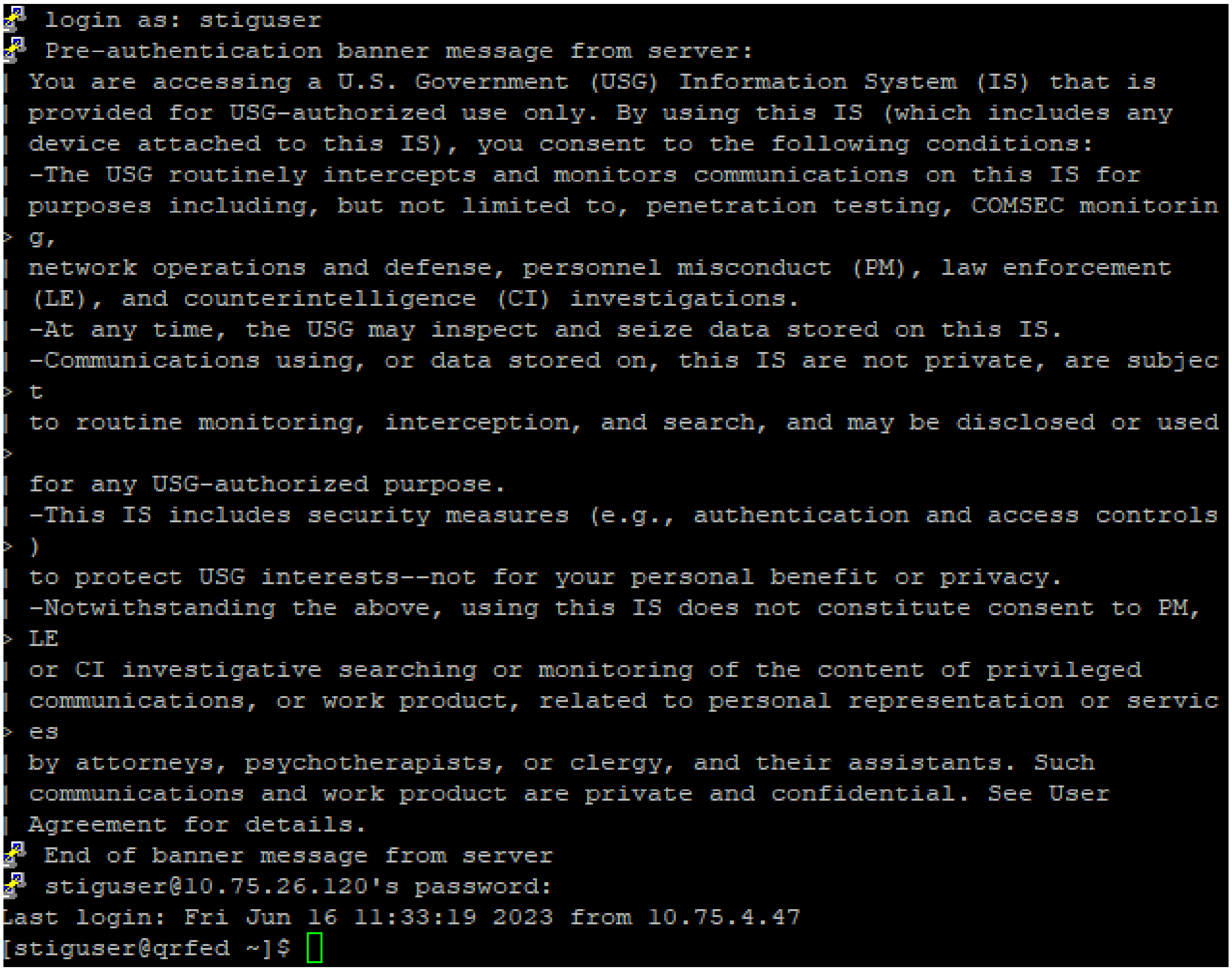
Load, save or delete a stored session

Saved Sessions

Default Settings
AWS Console
Enivzi AppHost
Enivzi QRadar
SOAR

Close window on exit: ○ Always ○ Never ● Only on clean exit

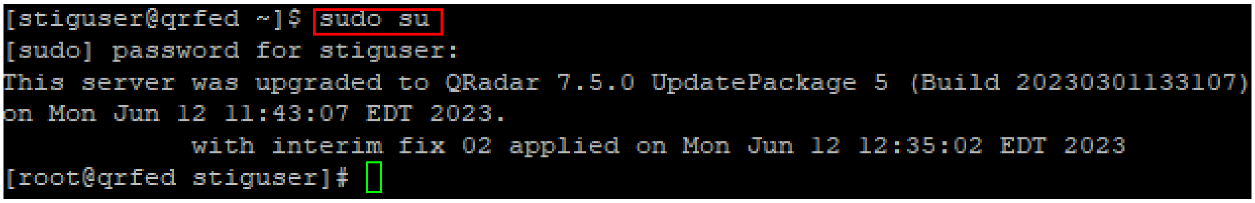
3. If the host is already STIG compliant you will have to login as stiguser or the user, the customer created during the STIG process. If the system is not STIG compliant then you may login as root. This example is done on a STIG compliant system.



```
 login as: stiguser
 Pre-authentication banner message from server:
 You are accessing a U.S. Government (USG) Information System (IS) that is
 provided for USG-authorized use only. By using this IS (which includes any
 device attached to this IS), you consent to the following conditions:
 -The USG routinely intercepts and monitors communications on this IS for
 purposes including, but not limited to, penetration testing, COMSEC monitorin
 g,
 network operations and defense, personnel misconduct (PM), law enforcement
 (LE), and counterintelligence (CI) investigations.
 -At any time, the USG may inspect and seize data stored on this IS.
 -Communications using, or data stored on, this IS are not private, are subjec
 t
 to routine monitoring, interception, and search, and may be disclosed or used

 for any USG-authorized purpose.
 -This IS includes security measures (e.g., authentication and access controls
 )
 to protect USG interests--not for your personal benefit or privacy.
 -Notwithstanding the above, using this IS does not constitute consent to PM,
 LE
 or CI investigative searching or monitoring of the content of privileged
 communications, or work product, related to personal representation or servic
 es
 by attorneys, psychotherapists, or clergy, and their assistants. Such
 communications and work product are private and confidential. See User
 Agreement for details.
 End of banner message from server
 stiguser@10.75.26.120's password:
Last login: Fri Jun 16 11:33:19 2023 from 10.75.4.47
[stiguser@qrfed ~]$
```

4. Escalate to root privileges via the sudo su command, as shown.

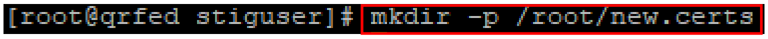
   - command: sudo su



```
[stiguser@qrfed ~]$ sudo su
[sudo] password for stiguser:
This server was upgraded to QRadar 7.5.0 UpdatePackage 5 (Build 20230301133107)
on Mon Jun 12 11:43:07 EDT 2023.
            with interim fix 02 applied on Mon Jun 12 12:35:02 EDT 2023
[root@qrfed stiguser]#
```

5. Create a new directory named new.certs within the root directory.

   - command: mkdir -p /root/new.certs

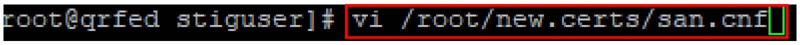


```
[root@qrfed stiguser]# mkdir -p /root/new.certs
```

6. IMPORTANT NOTCIE: The following steps in creating the san.cnf file is critical for proper registering with modern browsers. If you utilize the IBM “Install a new SSL certificate” article https://www.ibm.com/docs/en/qsip/7.5?topic=certificates-installing-new-ssl-certificate, it will not work properly and regardless of web browser will come up saying the certificate is invalidate and cannot be trusted. This is due to recently all browsers requires a SAN or Subject Alternate Name for all certificates.

7. Create san.cnf configuration file within the /root/new.certs directory.

   - command: vi /root/new.certs/san.cnf



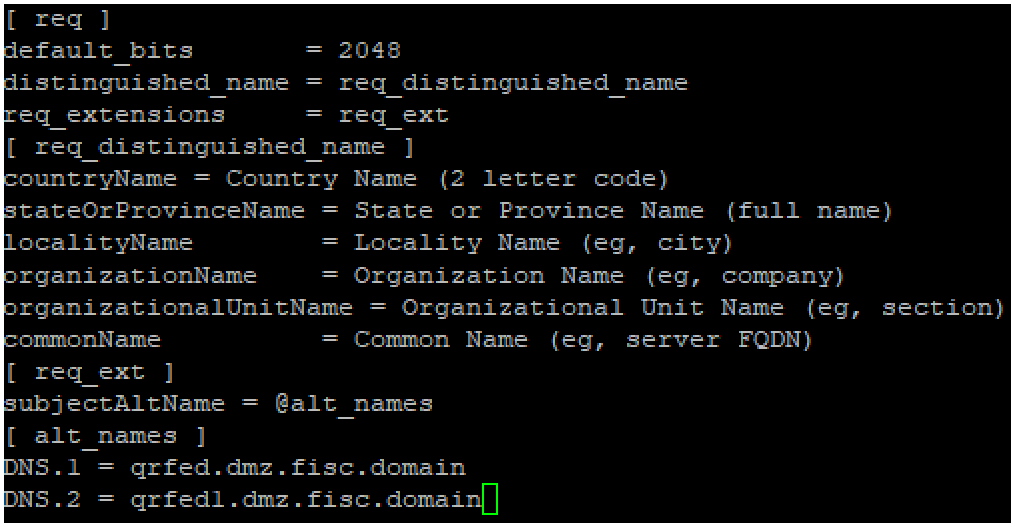
```
root@qrfed stiguser]# vi /root/new.certs/san.cnf
```

8. Type the i key, this will bring you into insert mode and allow you to edit the file.

   - Command: i

```
-- INSERT --
```

9. Enter the following information shown in the screen shot. For the last section of DNS.1 & DNS.2, enter the customers DNS name for the QRadar Console.



```
[ req ]
default_bits       = 2048
distinguished_name = req_distinguished_name
req_extensions     = req_ext
[ req_distinguished_name ]
countryName = Country Name (2 letter code)
stateOrProvinceName = State or Province Name (full name)
localityName         = Locality Name (eg, city)
organizationName     = Organization Name (eg, company)
organizationalUnitName = Organizational Unit Name (eg, section)
commonName           = Common Name (eg, server FQDN)
[ req_ext ]
subjectAltName = @alt_names
[ alt_names ]
DNS.1 = qrfed.dmz.fisc.domain
DNS.2 = qrfed1.dmz.fisc.domain
```

10. Press the esc key, this will stop editing mode, as shown.

```
~
```

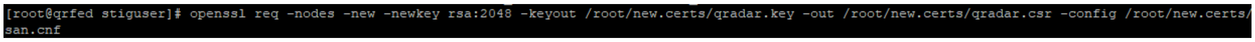
11. Save and exit the file.

    - command: :wq!

```
:wq!
```

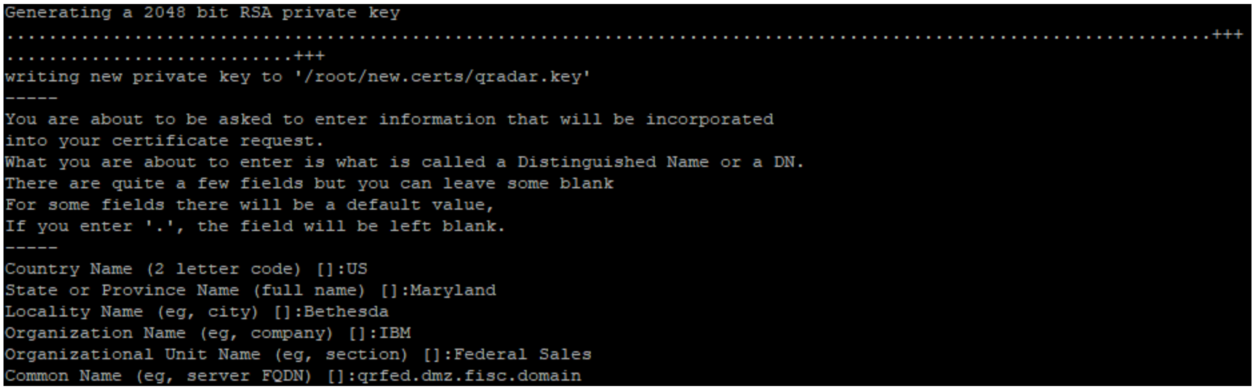
12. Generate the CSR via the following command:

    - command: openssl req -nodes -new -newkey rsa:2048 -keyout /root/new.certs/qradar.key -out /root/new.certs/qradar.csr -config /root/new.certs/san.cnf



```
[root@qrfed stiguser]# openssl req -nodes -new -newkey rsa:2048 -keyout /root/new.certs/qradar.key -out /root/new.certs/qradar.csr -config /root/new.certs/
san.cnf
```

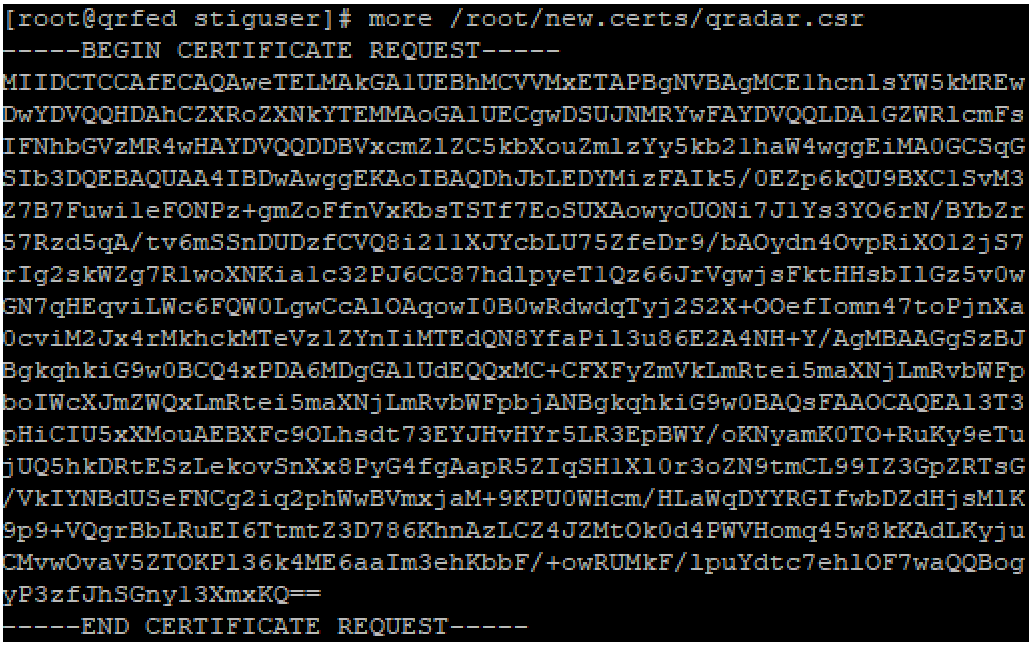
13. You will have to enter the following information. Enter the customers information, not what is shown in the screen shot, this is just an example.



```
Generating a 2048 bit RSA private key
................................................................................................................+++
...........................+++
writing new private key to '/root/new.certs/qradar.key'
-----
You are about to be asked to enter information that will be incorporated
into your certificate request.
What you are about to enter is what is called a Distinguished Name or a DN.
There are quite a few fields but you can leave some blank
For some fields there will be a default value,
If you enter '.', the field will be left blank.
-----
Country Name (2 letter code) []:US
State or Province Name (full name) []:Maryland
Locality Name (eg, city) []:Bethesda
Organization Name (eg, company) []:IBM
Organizational Unit Name (eg, section) []:Federal Sales
Common Name (eg, server FQDN) []:qrfed.dmz.fisc.domain
```

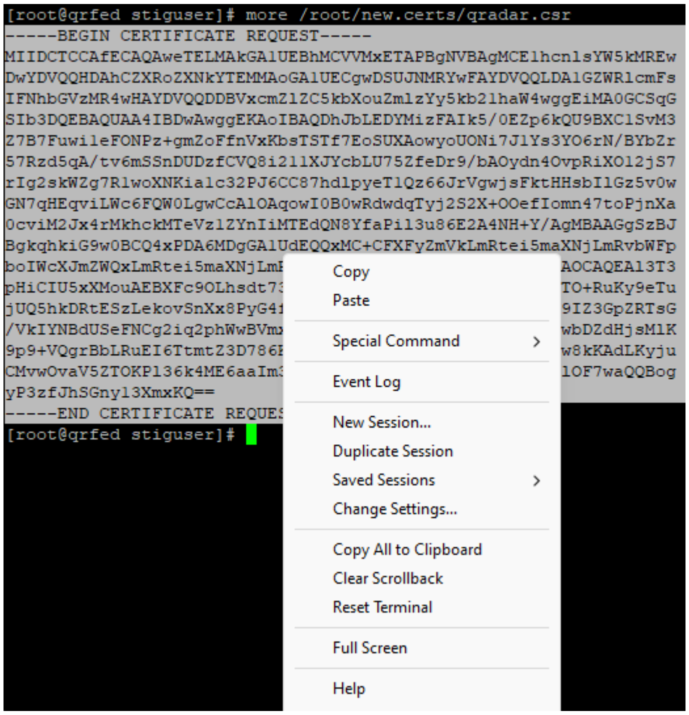
14. Next, you will copy and paste the qradar.csr information into a note pad, or you can make a copy of the qradar.csr file and place it in the /home/stiguser directory to export it via WinSCP or Filezilla. This example will show just copying the contents of the qradar.csr file to a notepad.

    - command: more /root/new.certs/qradar.csr



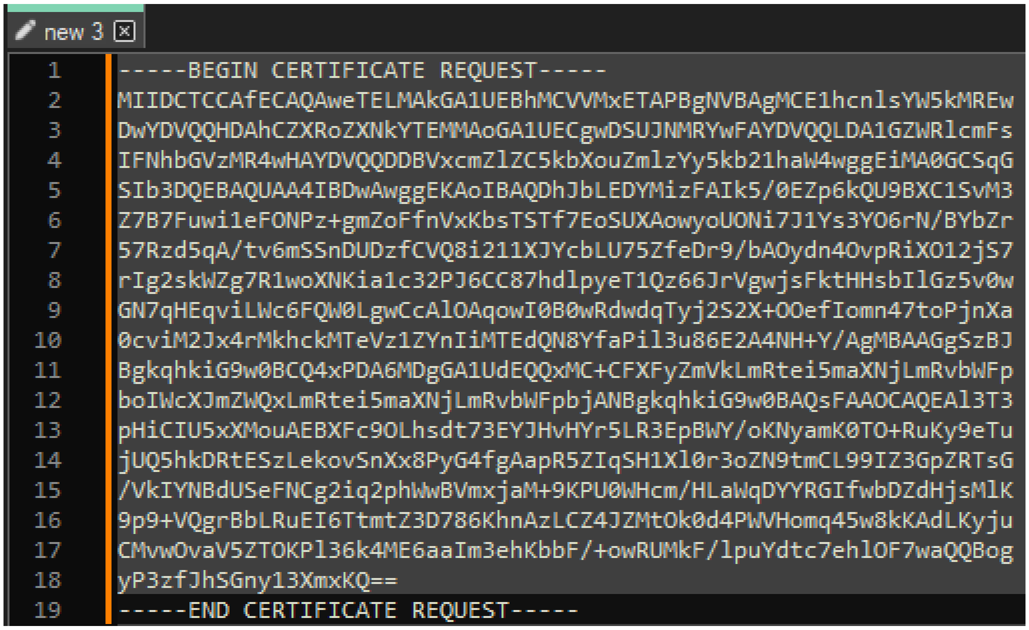
```
[root@qrfed stiguser]# more /root/new.certs/qradar.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDCTCCAfECAQAweTELMAkGA1UEBhMCVVMxETAPBgNVBAgMCElhcnlsYW5kMREw
DwYDVQQHDAhCZXRoZXNkYTEMMAoGA1UECgwDSUJNMRYwFAYDVQQLDA1GZWR1cmFs
IFNhbGVzMR4wHAYDVQQDDBVxcmZlZC5kbXouZmlzYy5kb21haW4wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDhJbLEDYMizFAIk5/0EZp6kQU9BXC1SvM3
Z7B7FuwileFONPz+gmZoFfnVxKbsTSTf7EoSUXAowyoUONi7J1Ys3YO6rN/BYbZr
57Rzd5qA/tv6mSSnDUDzfCVQ8i2llXJYcbLU75ZfeDr9/bAOydn4OvpRiXOl2jS7
rIg2skWZg7RlwoXNKialc32PJ6CC87hdlpyeTlQz66JrVgwjsFktHHsbIlGz5v0w
GN7qHEqviLWc6FQW0LgwCcAlOAqowI0B0wRdwdqTyj2S2X+OOefIomn47toPjnXa
0cviM2Jx4rMkhckMTeVzlZYnIiMTEdQN8YfaPil3u86E2A4NH+Y/AgMBAAGgSzBJ
BgkqhkiG9w0BCQ4xPDA6MDgGA1UdEQQxMC+CFXFyZmVkLmRtei5maXNjLmRvbWFp
boIWcXJmZWQxLmRtei5maXNjLmRvbWFpbjANBgkqhkiG9w0BAQsFAAOCAQEA13T3
pHiCIU5xXMouAEBXFc9OLhsdt73EYJHvHYr5LR3EpBWY/oKNyamK0TO+RuKy9eTu
jUQ5hkDRtESzLekovSnXx8PyG4fgAapR5ZIqSH1X10r3oZN9tmCL99IZ3GpZRTsG
/VkIYNBdUSeFNCg2iq2phWwBVmxjaM+9KPU0WHcm/HLaWqDYYRGIfwbDZdHjsM1K
9p9+VQgrBbLRuEI6TtmtZ3D786KhnAzLCZ4JZMtOk0d4PWVHomq45w8kKAdLKyju
CMvwOvaV5ZTOKP136k4ME6aaIm3ehKbbF/+owRUMkF/1puYdtc7ehlOF7waQQBog
yP3zfJhSGnyl3XmxKQ==
-----END CERTIFICATE REQUEST-----
```

15. Highlight all the text present and hold Ctrl key and right click, select to “copy” as shown.



```
[root@qrfed stiguser]# more /root/new.certs/qradar.csr
-----BEGIN CERTIFICATE REQUEST-----
MIIDCTCCAfECAQAweTELMAkGA1UEBhMCVVMxETAPBgNVBAgMCElhcnlsYW5kMREw
DwYDVQQHDAhCZXRoZXNkYTEMMAoGA1UECgwDSUJNMRYwFAYDVQQLDA1GZWR1cmFs
IFNhbGVzMR4wHAYDVQQDDBVxcmZlZC5kbXouZmlzYy5kb21haW4wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDhJbLEDYMizFAIk5/0EZp6kQU9BXC1SvM3
Z7B7FuwileFONPz+gmZoFfnVxKbsTSTf7EoSUXAowyoUONi7J1Ys3YO6rN/BYbZr
57Rzd5qA/tv6mSSnDUDzfCVQ8i2llXJYcbLU75ZfeDr9/bAOydn4OvpRiXOl2jS7
rIg2skWZg7RlwoXNKialc32PJ6CC87hdlpyeTlQz66JrVgwjsFktHHsbIlGz5v0w
GN7qHEqviLWc6FQW0LgwCcAlOAqowI0B0wRdwdqTyj2S2X+OOefIomn47toPjnXa
0cviM2Jx4rMkhckMTeVzlZYnIiMTEdQN8YfaPil3u86E2A4NH+Y/AgMBAAGgSzBJ
BgkqhkiG9w0BCQ4xPDA6MDgGA1UdEQQxMC+CFXFyZmVkLmRtei5maXNjLmRvbWFp
boIWcXJmZWQxLmRtei5maXNjLmR                                 AOCAQEA13T3
pHiCIU5xXMouAEBXFc9OLhsdt73                                 TO+RuKy9eTu
jUQ5hkDRtESzLekovSnXx8PyG4f                                 9IZ3GpZRTsG
/VkIYNBdUSeFNCg2iq2phWwBVmx                                 wbDZdHjsM1K
9p9+VQgrBbLRuEI6TtmtZ3D786K                                 w8kKAdLKyju
CMvwOvaV5ZTOKP136k4ME6aaIm3                                 lOF7waQQBog
yP3zfJhSGnyl3XmxKQ==
-----END CERTIFICATE REQUES
[root@qrfed stiguser]#
```

16. Paste the contents into a Notepad or Notepad++, as shown.



```
-----BEGIN CERTIFICATE REQUEST-----
MIIDCTCCAfECAQAweTELMAkGA1UEBhMCVVMxETAPBgNVBAgMCE1hcnlsYW5kMREw
DwYDVQQHDAhCZXRoZXNkYTEMMAoGA1UECgwDSUJNMRYwFAYDVQQLDA1GZWRlcmFs
IFNhbGVzMR4wHAYDVQQDDBVxcmZlZC5kbXouZmlzYy5kb21haW4wggEiMA0GCSqG
SIb3DQEBAQUAA4IBDwAwggEKAoIBAQDhJbLEDYMizFAIk5/0EZp6kQU9BXC1SvM3
Z7B7Fuwi1eFONPz+gmZoFfnVxKbsTSTf7EoSUXAowyoUONi7J1Ys3YO6rN/BYbZr
57Rzd5qA/tv6mSSnDUDzfCVQ8i211XJYcbLU75ZfeDr9/bAOydn4OvpRiXO12jS7
rIg2skWZg7R1woXNKia1c32PJ6CC87hdlpyeT1Qz66JrVgwjsFktHHsbIlGz5v0w
GN7qHEqviLWc6FQW0LgwCcAlOAqowI0B0wRdwdqTyj2S2X+OOefIomn47toPjnXa
0cviM2Jx4rMkhckMTeVz1ZYnIiMTEdQN8YfaPil3u86E2A4NH+Y/AgMBAAGgSzBJ
BgkqhkiG9w0BCQ4xPDA6MDgGA1UdEQQxMC+CFXFyZmVkLmRtei5maXNjLmRvbWFp
boIWcXJmZWQxLmRtei5maXNjLmRvbWFpbjANBgkqhkiG9w0BAQsFAAOCAQEAl3T3
pHiCIU5xXMouAEBXFc9OLhsdt73EYJHvHYr5LR3EpBWY/oKNyamK0TO+RuKy9eTu
jUQ5hkDRtESzLekovSnXx8PyG4fgAapR5ZIqSH1Xl0r3oZN9tmCL99IZ3GpZRTsG
/VkIYNBdUSeFNCg2iq2phWwBVmxjaM+9KPU0WHcm/HLaWqDYYRGIfwbDZdHjsMlK
9p9+VQgrBbLRuEI6TtmtZ3D786KhnAzLCZ4JZMtOk0d4PWVHomq45w8kKAdLKyju
CMvwOvaV5ZTOKPl36k4ME6aaIm3ehKbbF/+owRUMkF/lpuYdtc7ehlOF7waQQBog
yP3zfJhSGny13XmxKQ==
-----END CERTIFICATE REQUEST-----
```

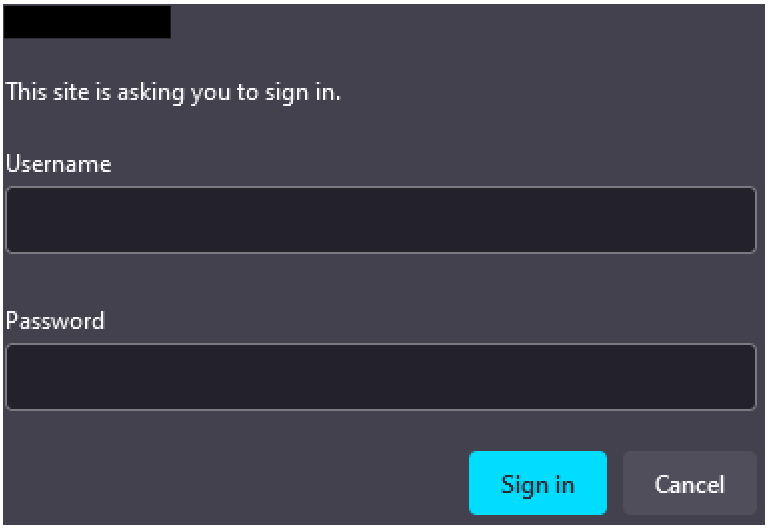
17. Save this file as a .csr and provide it to the Certificate Authority administrator. Or provide the exported file to the Certificate Authority administrator.

18. If the client has admin authority to generate certificates procedure to the next section. If they do not and require someone else to generate the certificate, ensure your client informs the CA admin that the entire p7b chain is required.

Generate Certificate

Note: This step is only to be done by the certificate authority administrator. If you client has the permissions, they can follow this section and create the certificate.

1. Log into the certificate authority with the correct privileges.



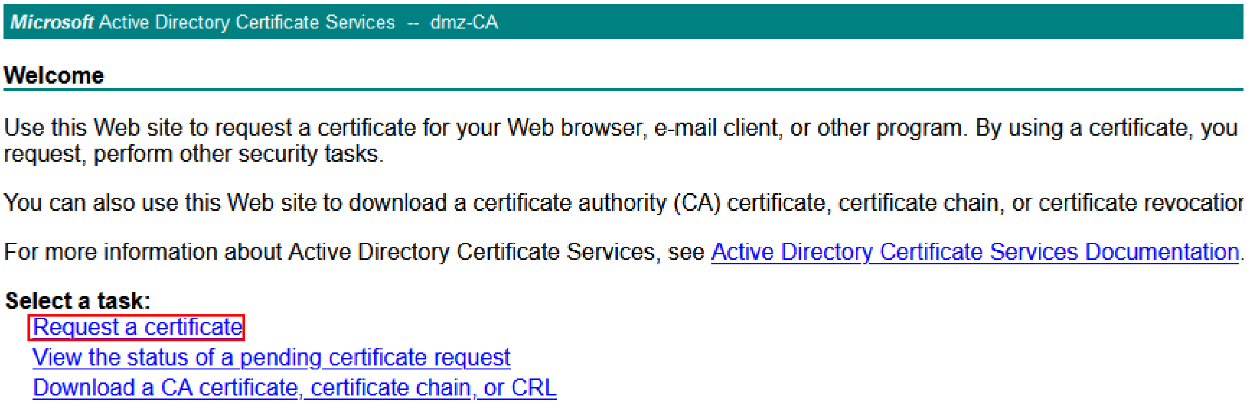
[redacted]

This site is asking you to sign in.

Username

Password

2. After logging in you will be brought to the certificate authority page as shown. Click on “Request a certificate”, as shown.



Microsoft Active Directory Certificate Services -- dmz-CA

Welcome

Use this Web site to request a certificate for your Web browser, e-mail client, or other program. By using a certificate, you request, perform other security tasks.

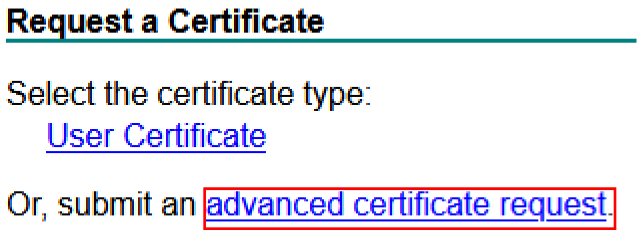
You can also use this Web site to download a certificate authority (CA) certificate, certificate chain, or certificate revocatior

For more information about Active Directory Certificate Services, see Active Directory Certificate Services Documentation.

Select a task:

Request a certificate
View the status of a pending certificate request
Download a CA certificate, certificate chain, or CRL

3. The “Request a Certificate” page will appear. Click “advanced certificate request”, as shown.

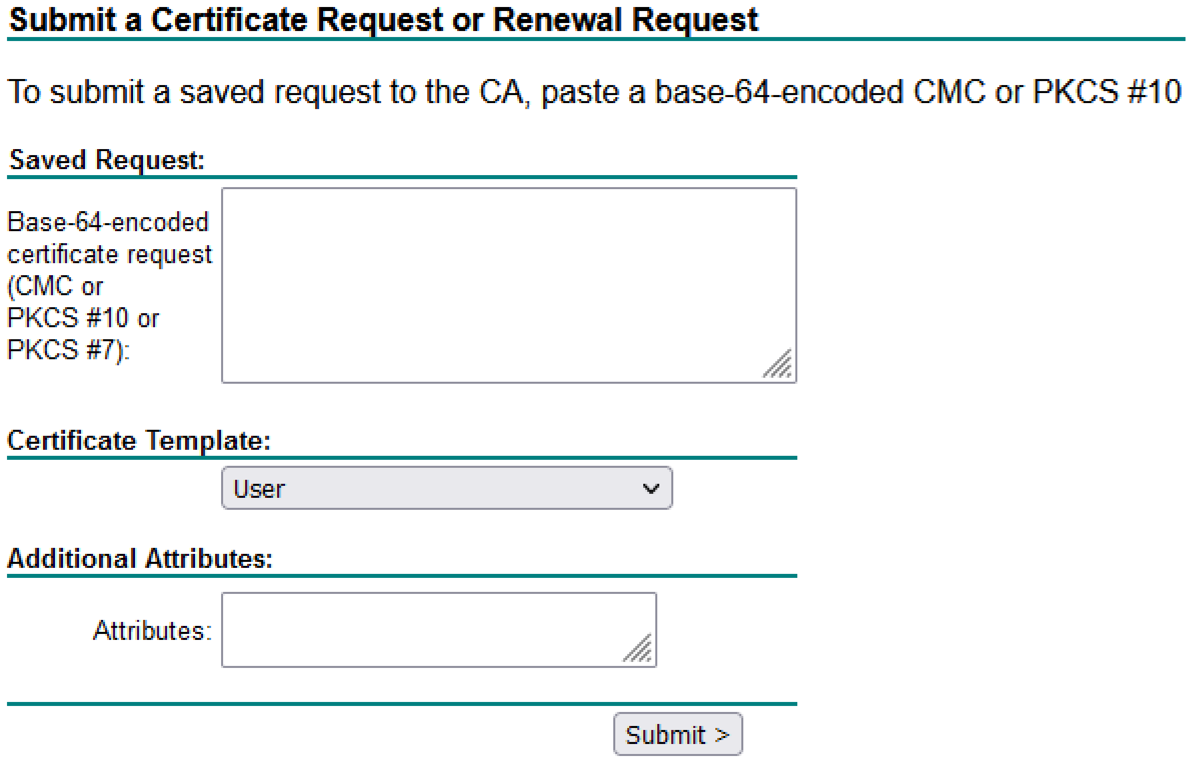


Request a Certificate

Select the certificate type:
User Certificate

Or, submit an advanced certificate request.

4. You will be brought to the “Submit a Certificate Request or Renewal Request” page, as shown.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

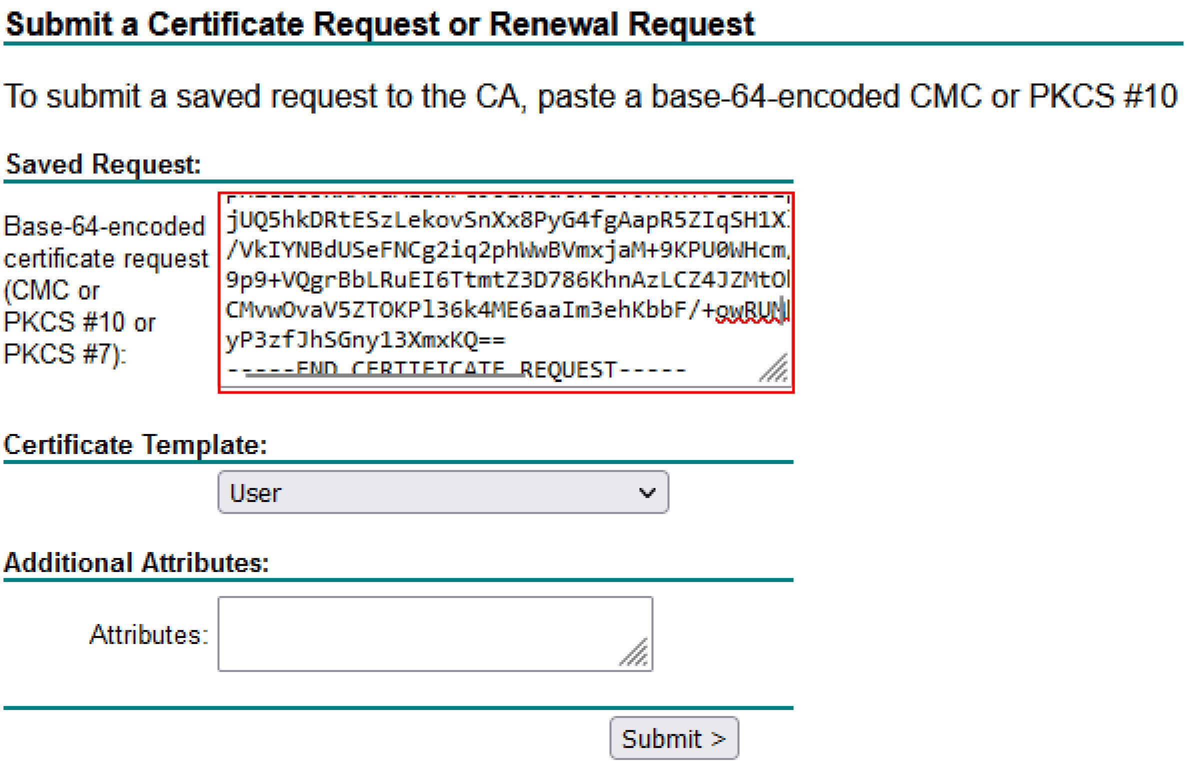
Certificate Template:

User

Additional Attributes:

Attributes:

5. Within the “Base-64-encoded certificate request” box, copy and paste in the contents of the qradar.csr, as shown.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
jUQ5hkDRtESzLekovSnXx8PyG4fgAapR5ZIqSH1X
/VkIYNBdUSeFNCg2iq2phWwBVmxjaM+9KPU0WHcm
9p9+VQgrBbLRuEI6TtmtZ3D786KhnAzLCZ4JZMtO
CMvwOvaV5ZTOKPl36k4ME6aaIm3ehKbbF/+owRUN
yP3zfJhSGny13XmxKQ==
-----END CERTIFICATE REQUEST-----
```

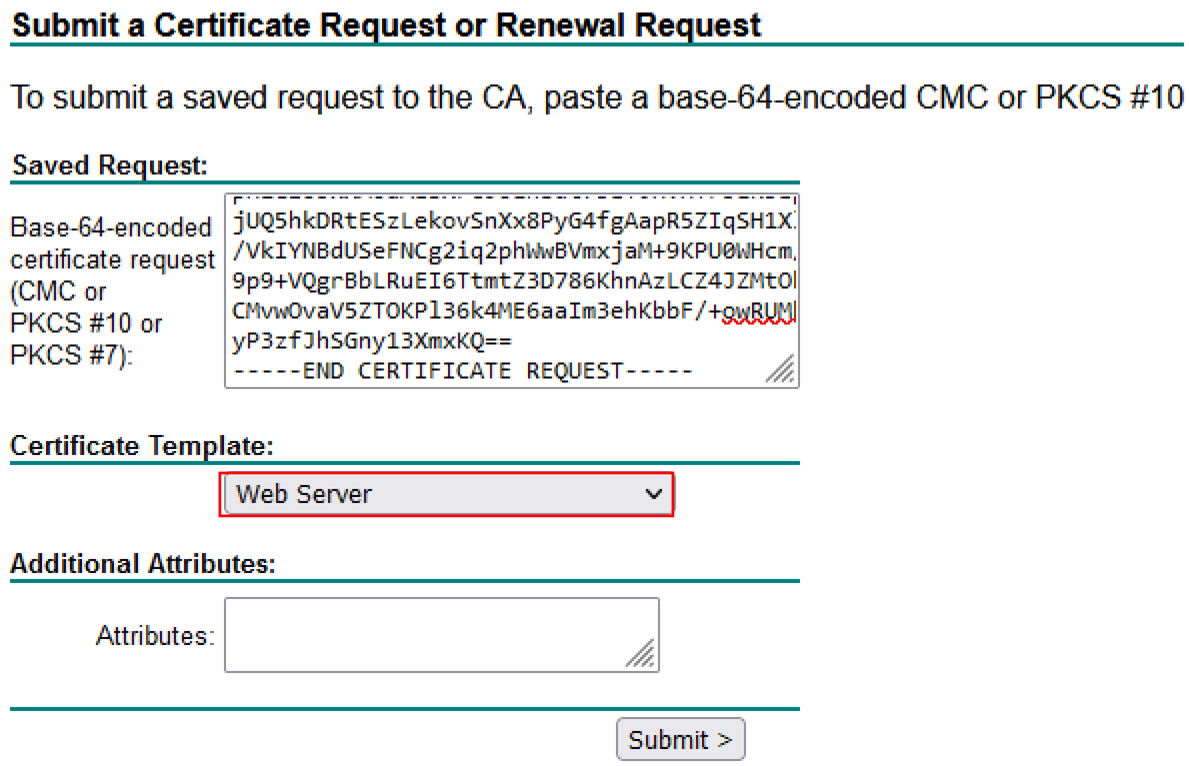
Certificate Template:

User

Additional Attributes:

Attributes:

6. Next, click the drop-down menu for “Certificate Template” section and select “Web Server”, as shown.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
jUQ5hkDRtESzLekovSnXx8PyG4fgAapR5ZIqSH1X
/VkIYNBdUSeFNCg2iq2phWwBVmxjaM+9KPU0WHcm
9p9+VQgrBbLRuEI6TtmtZ3D786KhnAzLCZ4JZMtO
CMvwOvaV5ZTOKPl36k4ME6aaIm3ehKbbF/+owRUM
yP3zfJhSGny13XmxKQ==
-----END CERTIFICATE REQUEST-----
```

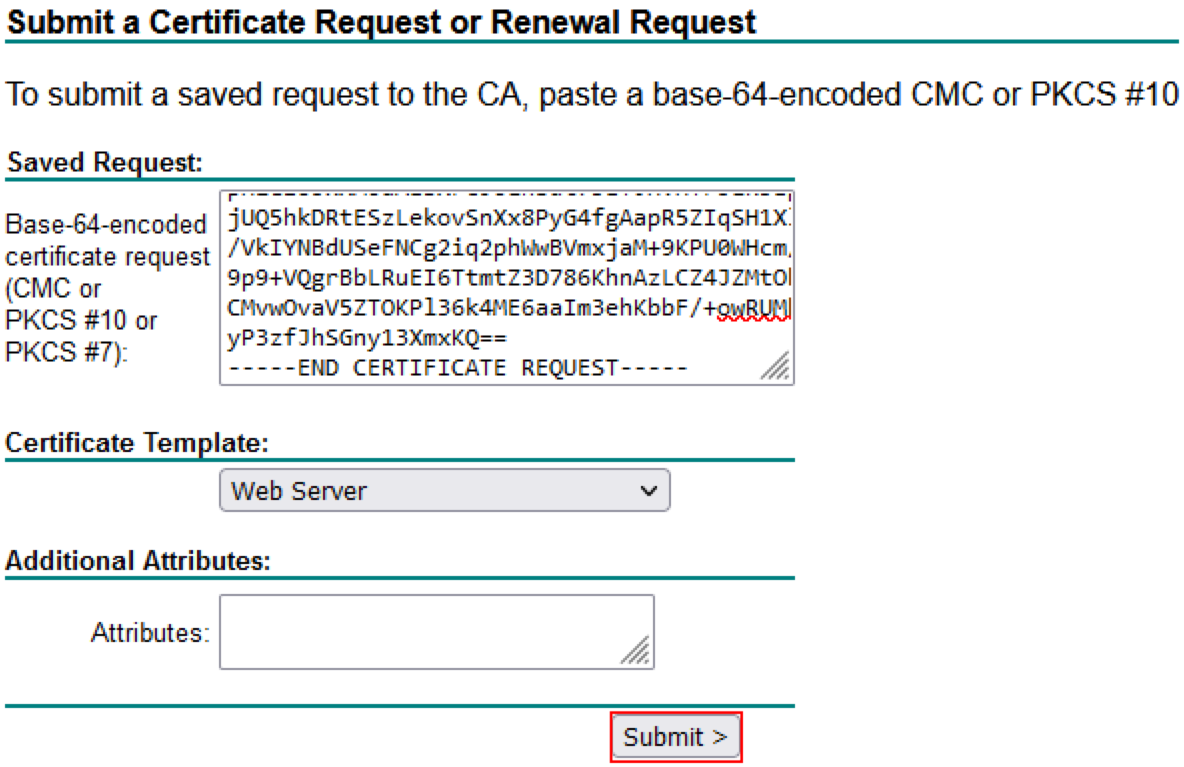
Certificate Template:

Web Server

Additional Attributes:

Attributes:

7. After entering in the csr content and making the certicate template web server, next click the “Submit >” button, as shown.



Submit a Certificate Request or Renewal Request

To submit a saved request to the CA, paste a base-64-encoded CMC or PKCS #10

Saved Request:

Base-64-encoded certificate request (CMC or PKCS #10 or PKCS #7):

```
jUQ5hkDRtESzLekovSnXx8PyG4fgAapR5ZIqSH1X
/VkIYNBdUSeFNCg2iq2phWwBVmxjaM+9KPU0WHcm
9p9+VQgrBbLRuEI6TtmtZ3D786KhnAzLCZ4JZMtO
CMvwOvaV5ZTOKPl36k4ME6aaIm3ehKbbF/+qwRUM
yP3zfJhSGny13XmxKQ==
-----END CERTIFICATE REQUEST-----
```

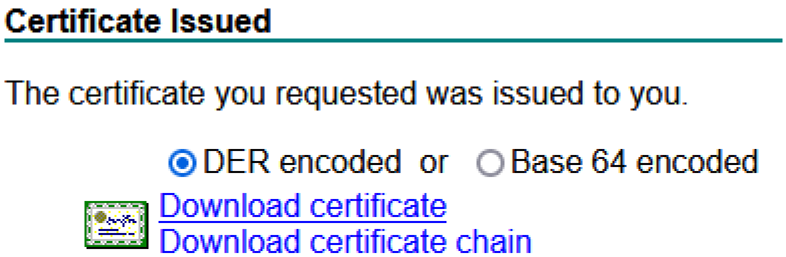
Certificate Template:

Web Server

Additional Attributes:

Attributes:

8. After clicking submit you will be taken to the “Certificate Issued” page, as shown.



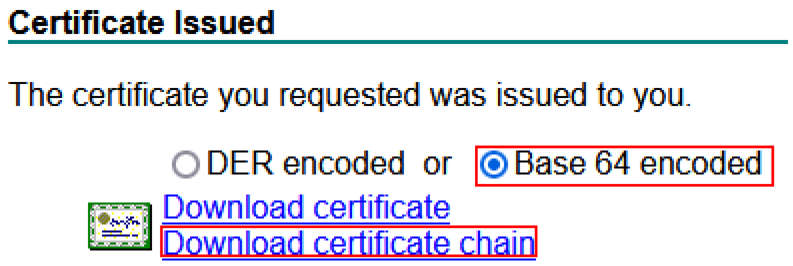
Certificate Issued

The certificate you requested was issued to you.

● DER encoded or ○ Base 64 encoded

.

9. Have the certificate authority administer select the “Base 64 encoded” radial button and click on “Download certificate chain”, as shown.



Certificate Issued

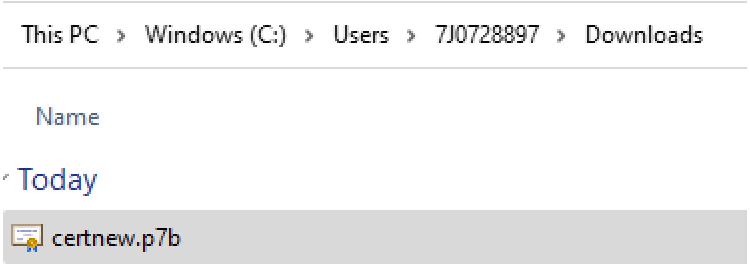
The certificate you requested was issued to you.

○ DER encoded or ● Base 64 encoded

Download certificate

Download certificate chain

10. Clicking on the “Download certificate chain” will download the p7b chain to the users Downloads folder, as shown.



This PC › Windows (C:) › Users › 7J0728897 › Downloads

Name

Today

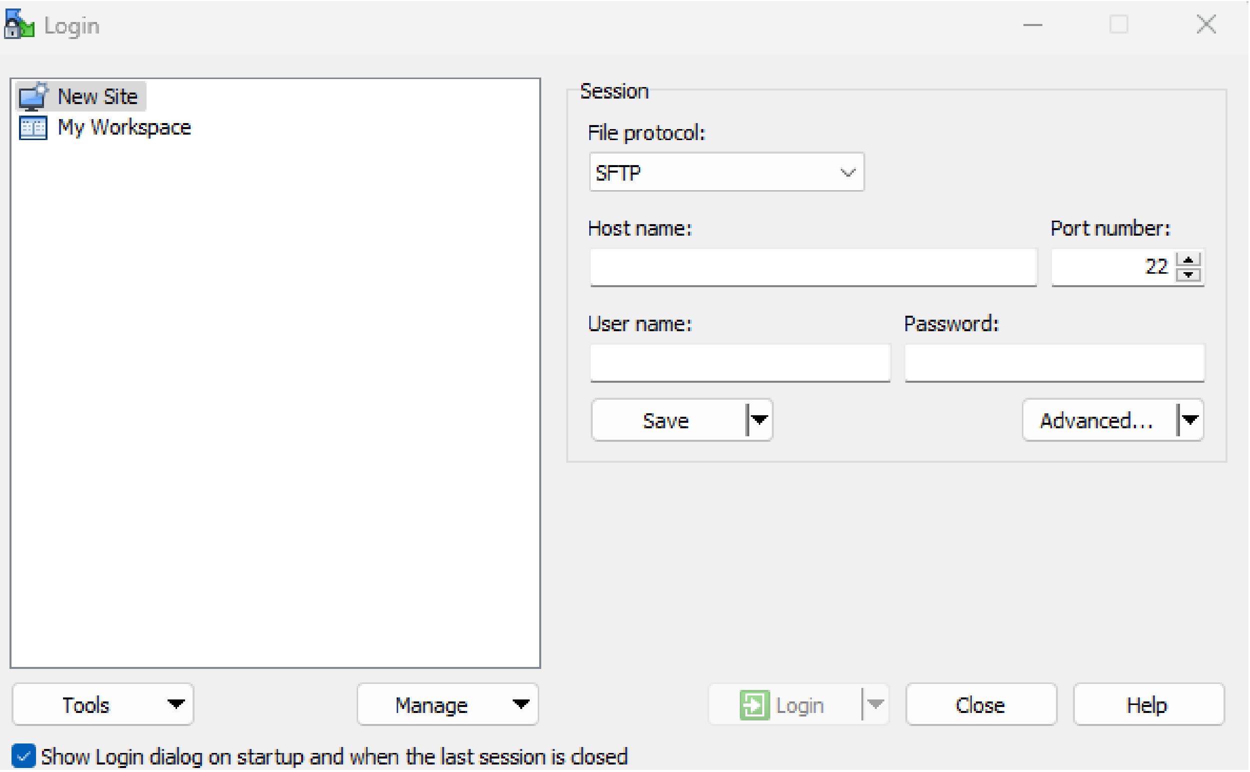
certnew.p7b

11. Ensure your client has access to this .p7b file. Proceed to the next section.

Import and Convert Certificate

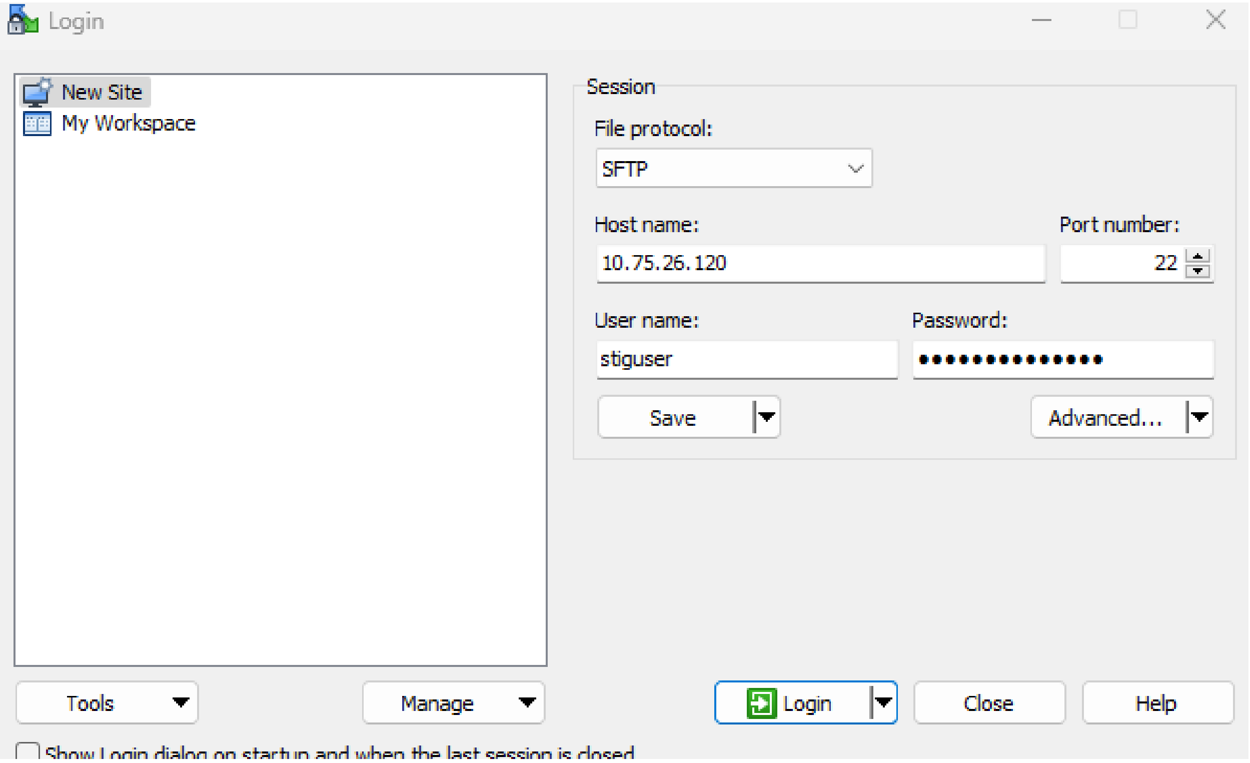
1. Open WinSCP or other file transferring application.

2. The WinSCP login page will appear, as shown.



3. Enter the QRadar Console ip address, the desired username and password for the username. If the appliance is STIG compliant you will have to use that user which was created and password. There are additional steps when a host is STIG compliant which will be provided here.

   - Host name: ip address of QRadar console
   - User name: root or the user created during STIG
   - Password: password of the user
   - Click “Login”



File protocol: SFTP

Host name: 10.75.26.120

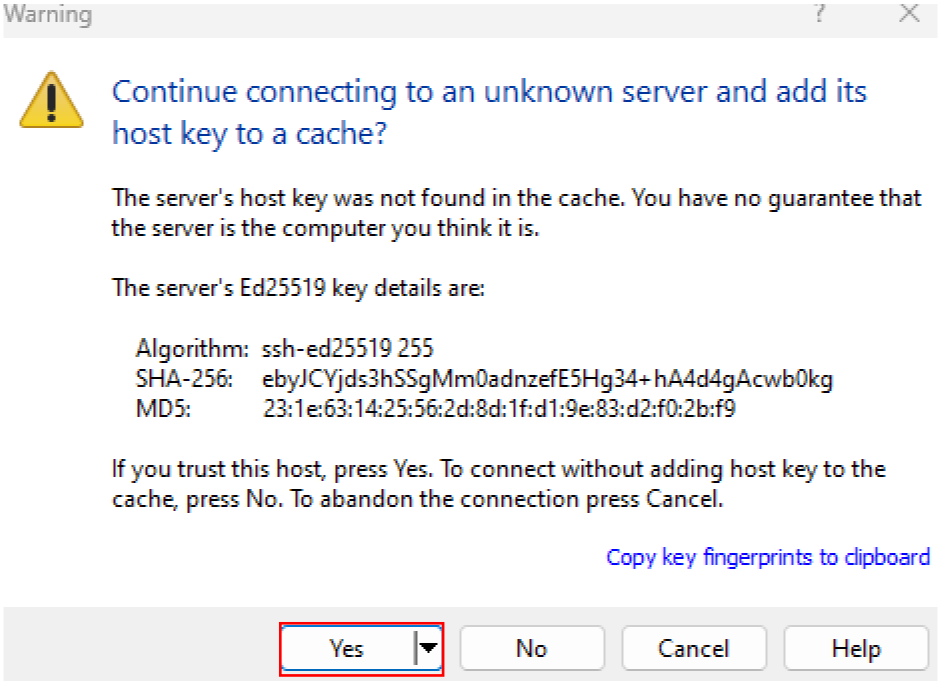
Port number: 22

User name: stiguser

Password: ••••••••••••••

□ Show Login dialog on startup and when the last session is closed

4. If the file transfer application has never made a connection with the QRadar Console before, you will be prompted with the following Warning pop-up, click “Yes”.



Continue connecting to an unknown server and add its host key to a cache?

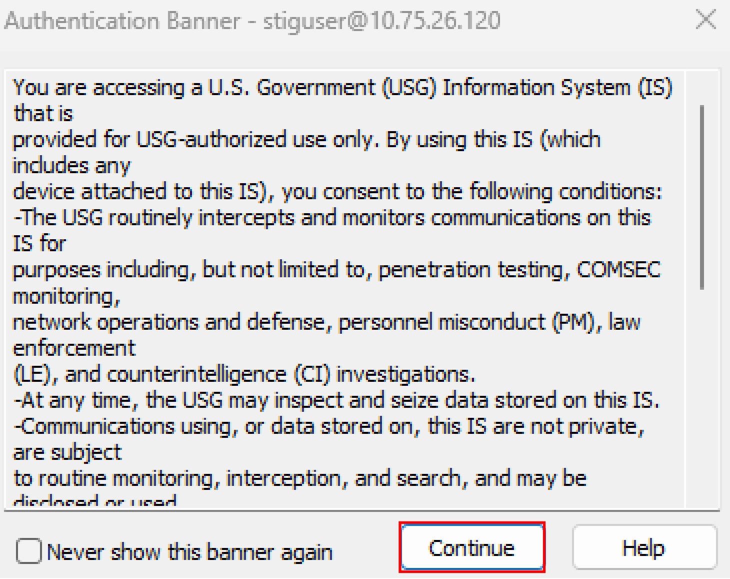
The server's host key was not found in the cache. You have no guarantee that the server is the computer you think it is.

The server's Ed25519 key details are:

```
Algorithm:  ssh-ed25519 255
SHA-256:    ebyJCYjds3hSSgMm0adnzefE5Hg34+hA4d4gAcwb0kg
MD5:        23:1e:63:14:25:56:2d:8d:1f:d1:9e:83:d2:f0:2b:f9
```

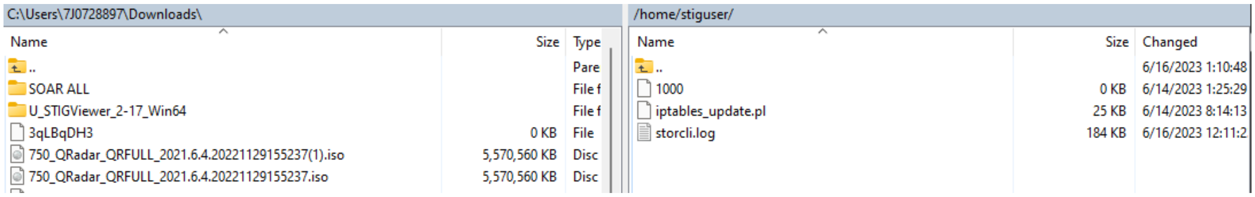
If you trust this host, press Yes. To connect without adding host key to the cache, press No. To abandon the connection press Cancel.

5. If the appliance is STIG compliant, you will receive the DoD warning banner. Click “Continue”, as shown.



You are accessing a U.S. Government (USG) Information System (IS) that is
provided for USG-authorized use only. By using this IS (which includes any
device attached to this IS), you consent to the following conditions:
-The USG routinely intercepts and monitors communications on this IS for
purposes including, but not limited to, penetration testing, COMSEC monitoring,
network operations and defense, personnel misconduct (PM), law enforcement
(LE), and counterintelligence (CI) investigations.
-At any time, the USG may inspect and seize data stored on this IS.
-Communications using, or data stored on, this IS are not private, are subject
to routine monitoring, interception, and search, and may be
disclosed or used

6. Once logged in you will be able to see the files within the QRadar Console /home/stiguser directory, as shown.



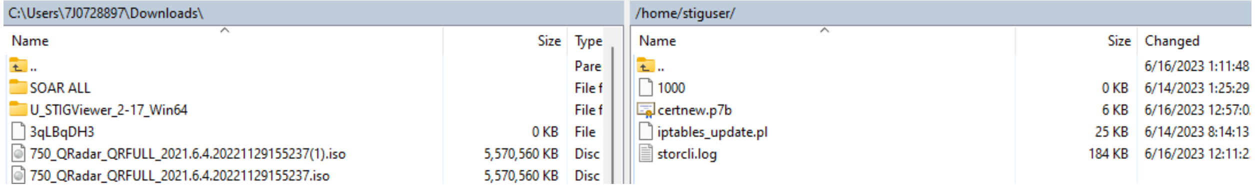
C:\Users\7J0728897\Downloads\

Name	Size	Type
..		Pare
SOAR ALL		File f
U_STIGViewer_2-17_Win64		File f
3qLBqDH3	0 KB	File
750_QRadar_QRFULL_2021.6.4.20221129155237(1).iso	5,570,560 KB	Disc
750_QRadar_QRFULL_2021.6.4.20221129155237.iso	5,570,560 KB	Disc

/home/stiguser/

Name	Size	Changed
..		6/16/2023 1:10:48
1000	0 KB	6/14/2023 1:25:29
iptables_update.pl	25 KB	6/14/2023 8:14:13
storcli.log	184 KB	6/16/2023 12:11:2

7. Locate the “certnew.p7b” file in the “Downloads” folder and drag and drop it into the /home/stiguer directory, as shown.



C:\Users\7J0728897\Downloads\

Name	Size	Type
..		Pare
SOAR ALL		File f
U_STIGViewer_2-17_Win64		File f
3qLBqDH3	0 KB	File
750_QRadar_QRFULL_2021.6.4.20221129155237(1).iso	5,570,560 KB	Disc
750_QRadar_QRFULL_2021.6.4.20221129155237.iso	5,570,560 KB	Disc

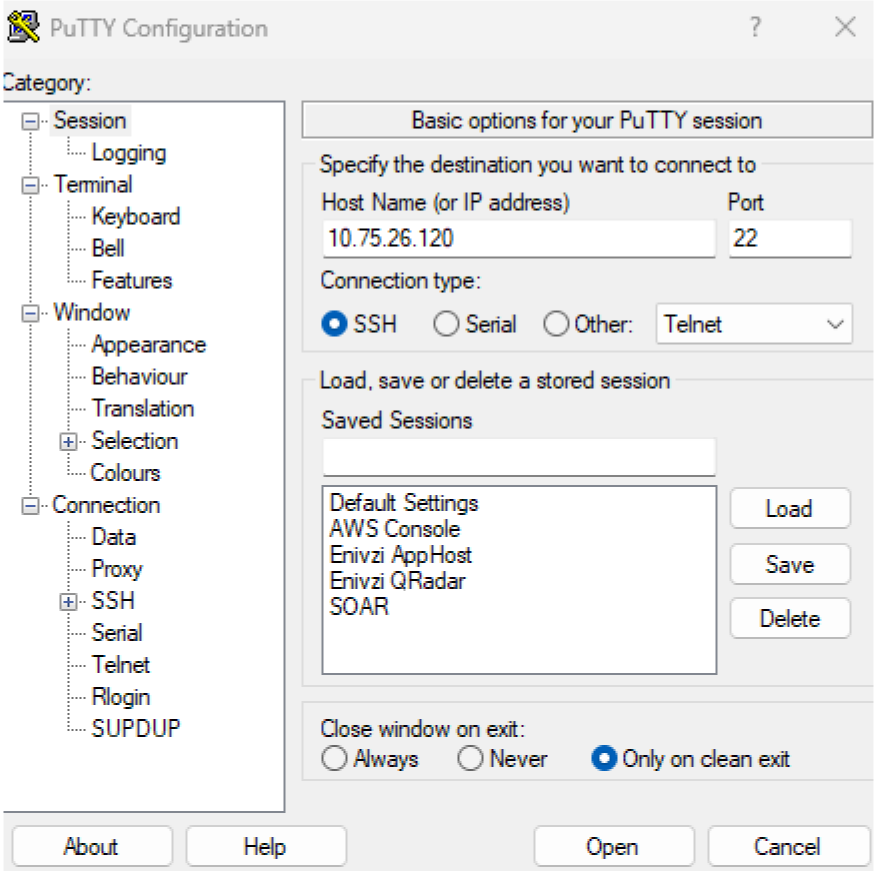
/home/stiguser/

Name	Size	Changed
..		6/16/2023 1:11:48
1000	0 KB	6/14/2023 1:25:29
certnew.p7b	6 KB	6/16/2023 12:57:0
iptables_update.pl	25 KB	6/14/2023 8:14:13
storcli.log	184 KB	6/16/2023 12:11:2

8. Having transferred the file into the /home/stiguser directory on the QRadar Console, you can close out the file transfer application.

9. Open Putty or another terminal emulator.

10. Within the “Host name (or IP address)” section enter the IP address of the QRadar console and click “Open”, as shown.



PuTTY Configuration

Basic options for your PuTTY session

Specify the destination you want to connect to

Host Name (or IP address): 10.75.26.120

Port: 22

Connection type: ● SSH ○ Serial ○ Other: Telnet

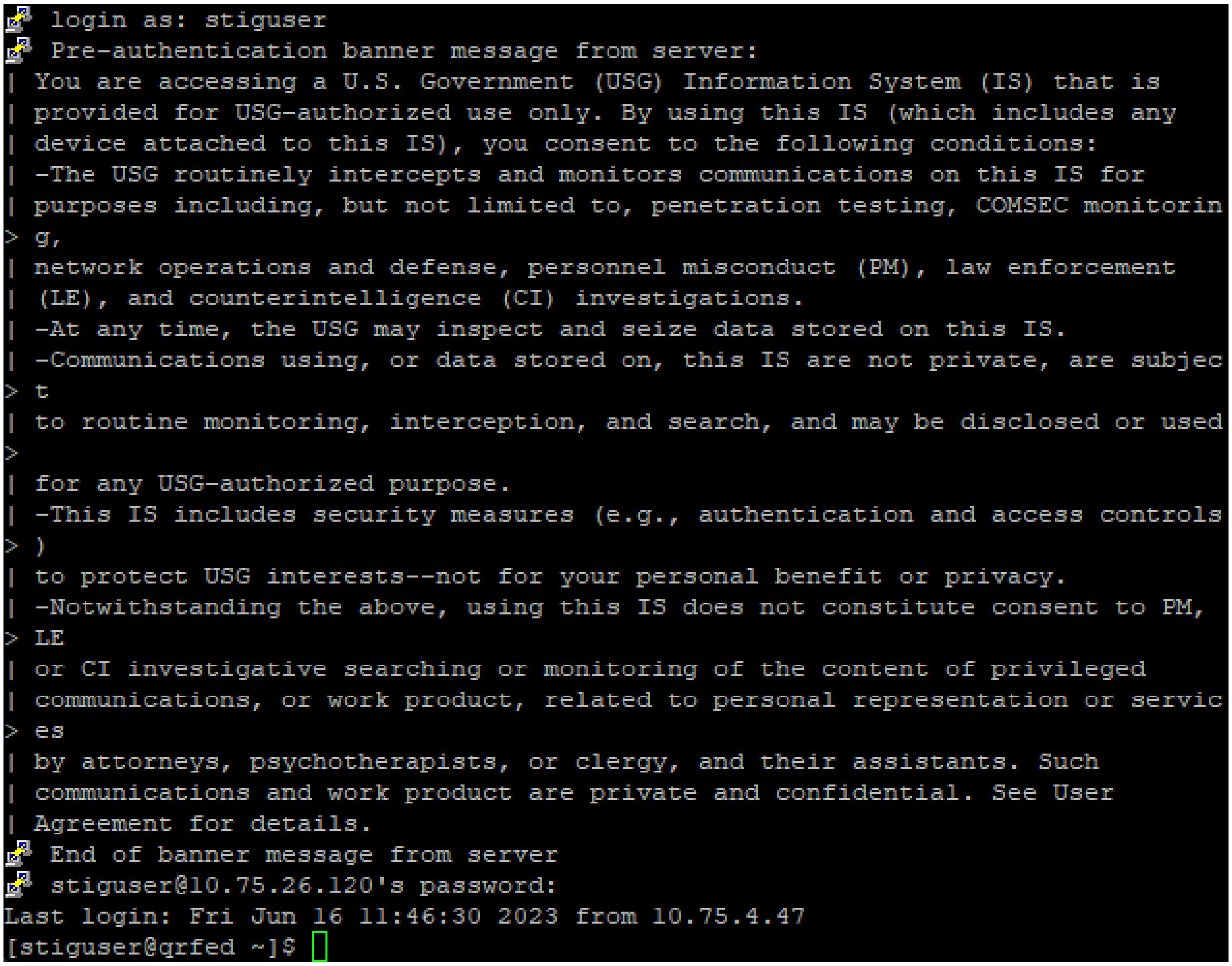
Load, save or delete a stored session

Saved Sessions

Default Settings
AWS Console
Enivzi AppHost
Enivzi QRadar
SOAR

Close window on exit: ○ Always ○ Never ● Only on clean exit

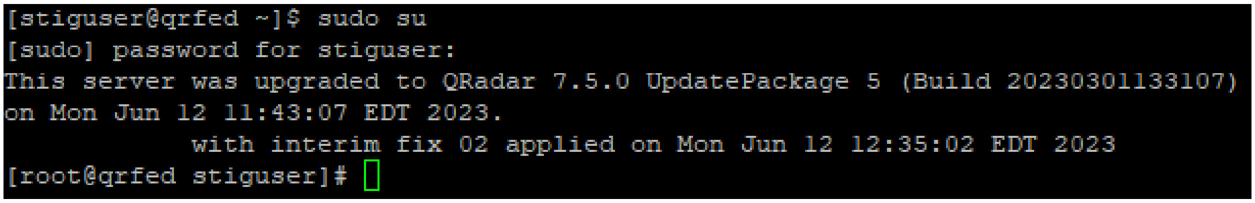
11. Login either via root or for STIG compliant appliances, log in with the user created during the stig process. This example is of a STIG compliant appliance.



```
  login as: stiguser
  Pre-authentication banner message from server:
| You are accessing a U.S. Government (USG) Information System (IS) that is
| provided for USG-authorized use only. By using this IS (which includes any
| device attached to this IS), you consent to the following conditions:
| -The USG routinely intercepts and monitors communications on this IS for
| purposes including, but not limited to, penetration testing, COMSEC monitorin
> g,
| network operations and defense, personnel misconduct (PM), law enforcement
| (LE), and counterintelligence (CI) investigations.
| -At any time, the USG may inspect and seize data stored on this IS.
| -Communications using, or data stored on, this IS are not private, are subjec
> t
| to routine monitoring, interception, and search, and may be disclosed or used
>
| for any USG-authorized purpose.
| -This IS includes security measures (e.g., authentication and access controls
> )
| to protect USG interests--not for your personal benefit or privacy.
| -Notwithstanding the above, using this IS does not constitute consent to PM,
> LE
| or CI investigative searching or monitoring of the content of privileged
| communications, or work product, related to personal representation or servic
> es
| by attorneys, psychotherapists, or clergy, and their assistants. Such
| communications and work product are private and confidential. See User
| Agreement for details.
  End of banner message from server
  stiguser@10.75.26.120's password:
Last login: Fri Jun 16 11:46:30 2023 from 10.75.4.47
[stiguser@qrfed ~]$ 
```

12. Escalate privileges to root, via the sudo su command.

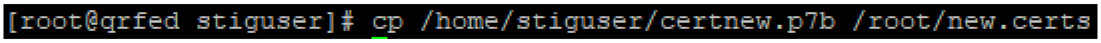
- command: sudo su



```
[stiguser@qrfed ~]$ sudo su
[sudo] password for stiguser:
This server was upgraded to QRadar 7.5.0 UpdatePackage 5 (Build 20230301133107)
on Mon Jun 12 11:43:07 EDT 2023.
            with interim fix 02 applied on Mon Jun 12 12:35:02 EDT 2023
[root@qrfed stiguser]# 
```

13. Copy the certnew.p7b file over to the /root/new.certs/ directory as shown.

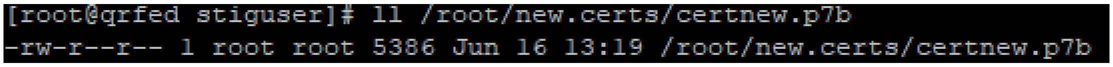
    - command: cp /home/stiguser/certnew.p7b /root/new.certs



```
[root@qrfed stiguser]# cp /home/stiguser/certnew.p7b /root/new.certs
```

14. Verify the certnew.p7b file was transferred successfully to the /root/new.certs/ and its permissions are correct, as shown.

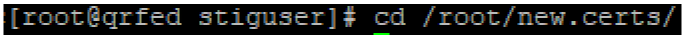
    - command: ll /root/new.certs/certnew.p7b



```
[root@qrfed stiguser]# ll /root/new.certs/certnew.p7b
-rw-r--r-- 1 root root 5386 Jun 16 13:19 /root/new.certs/certnew.p7b
```

15. Change directories to the /root/new.certs directory, as shown.

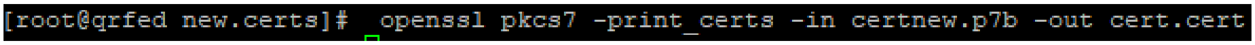
    - command: cd /root/new.certs/



```
[root@qrfed stiguser]# cd /root/new.certs/
```

16. Convert the p7b file into a cert, as shown.

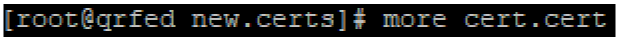
    - command: openssl pkcs7 -print_certs -in certnew.p7b -out cert.cert



```
[root@qrfed new.certs]#  openssl pkcs7 -print_certs -in certnew.p7b -out cert.cert
```

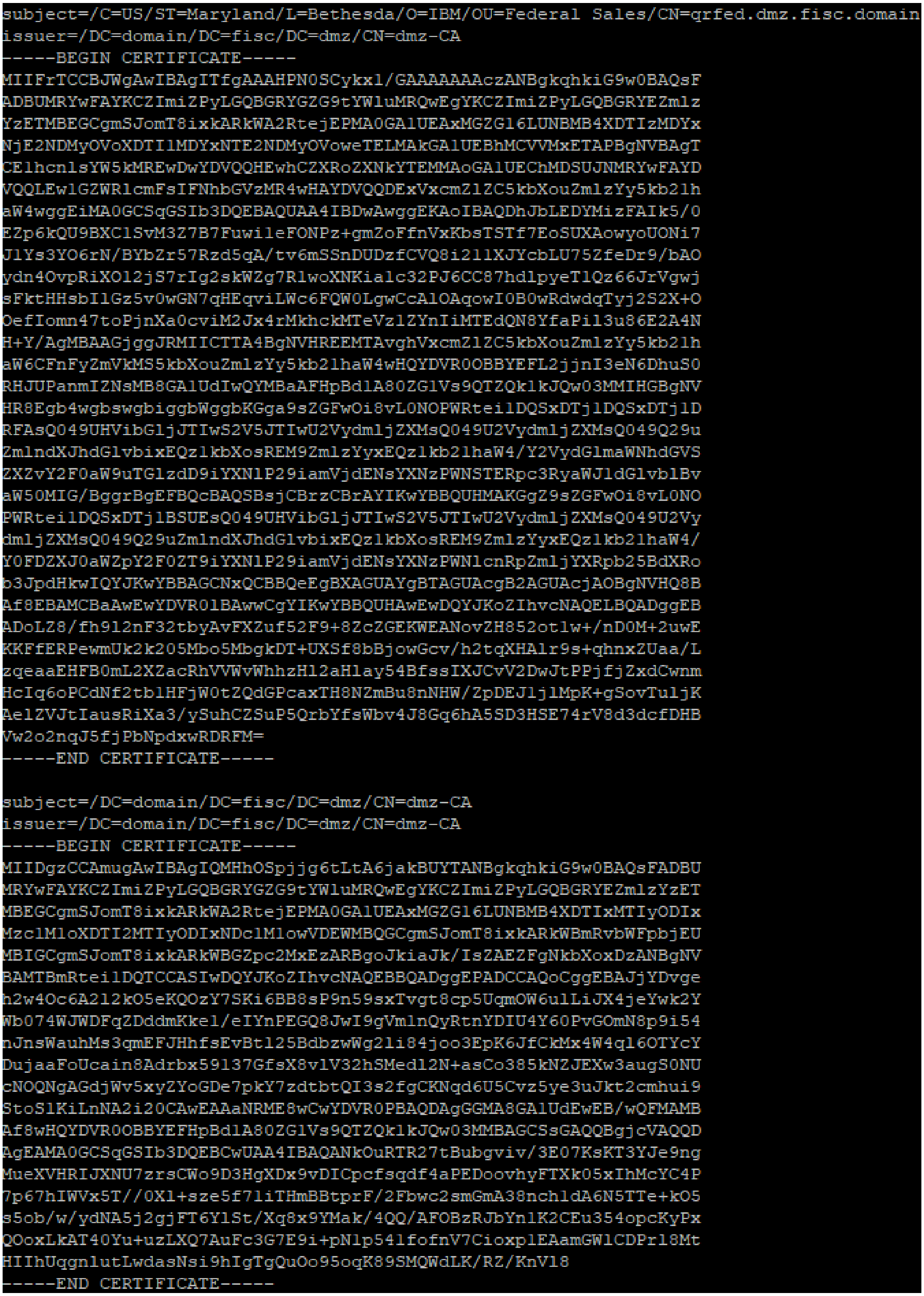
17. Verify the contents of the cert.cert file via the following command.

    - command: more cert.cert



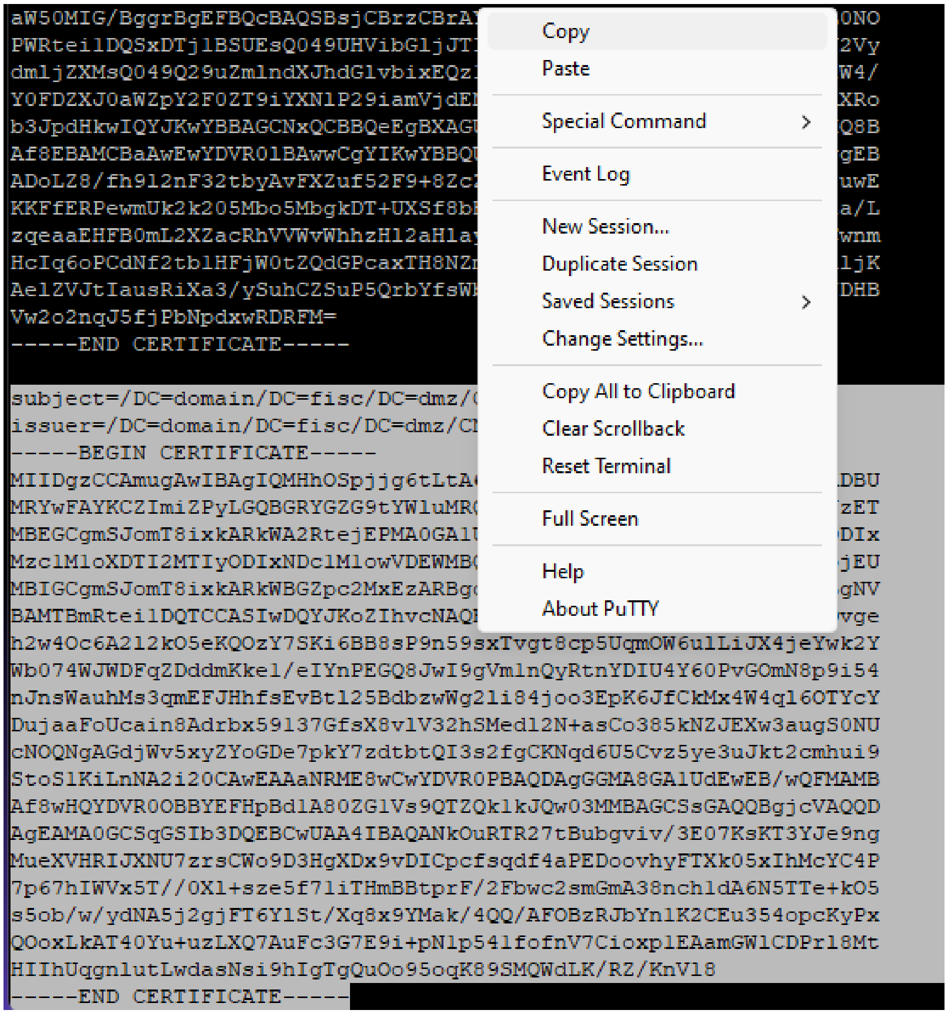
```
[root@qrfed new.certs]# more cert.cert
```

18. Due to the p7b being a chain file, both the QRadar Console certificate and the Root CA public certificate will be present in the file as shown.



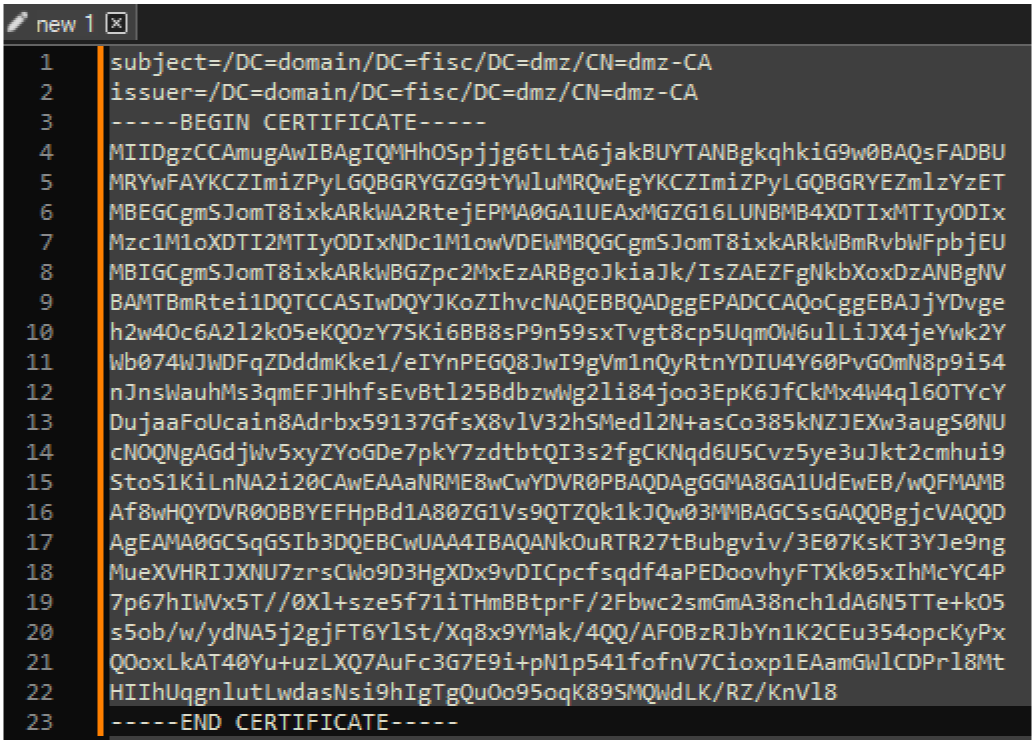
```
subject=/C=US/ST=Maryland/L=Bethesda/O=IBM/OU=Federal Sales/CN=qrfed.dmz.fisc.domain
issuer=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
-----BEGIN CERTIFICATE-----
MIIFrTCCBJWgAwIBAgITfgAAAHPN0SCykxl/GAAAAAAAczANBgkqhkiG9w0BAQsF
ADBUMRYwFAYKCZImiZPyLGQBGRYGZG9tYWluMRQwEgYKCZImiZPyLGQBGRYEZmlz
YzETMBEGCgmSJomT8ixkARkWA2RtejEPMA0GA1UEAxMGZG16LUNBMB4XDTIzMDYx
NjE2NDMyOVoXDTI1MDYxNTE2NDMyOVoweTELMAkGA1UEBhMCVVMxETAPBgNVBAgT
CE1hcnlsYW5kMREwDwYDVQQHEwhCZXRoZXNkYTEMMAoGA1UEChMDSUJNMRYwFAYD
VQQLEw1GZWRlcmFsIFNhbGVzMR4wHAYDVQQDExVxcmZlZC5kbXouZmlzYy5kb21h
aW4wggEiMA0GCSqGSIb3DQEBAQUAA4IBDwAwggEKAoIBAQDhJbLEDYMizFAIk5/0
EZp6kQU9BXClSvM3Z7B7FuwileFONPz+gmZoFfnVxKbsTSTf7EoSUXAowyoUONi7
JlYs3YO6rN/BYbZr57Rzd5qA/tv6mSSnDUDzfCVQ8i2llXJYcbLU75ZfeDr9/bAO
ydn4OvpRiXOl2jS7rIg2skWZg7RlwoXNKia1c32PJ6CC87hdlpyeTlQz66JrVgwj
sFktHHsbIlGz5v0wGN7qHEqviLWc6FQW0LgwCcAlOAqowI0B0wRdwdqTyj2S2X+O
OefIomn47toPjnXa0cviM2Jx4rMkhckMTeVzlZYnIiMTEdQN8YfaPil3u86E2A4N
H+Y/AgMBAAGjggJRMIICTTA4BgNVHREEMTAvghVxcmZlZC5kbXouZmlzYy5kb21h
aW6CFnFyZmVkMS5kbXouZmlzYy5kb21haW4wHQYDVR0OBBYEFL2jjnI3eN6DhuS0
RHJUPanmIZNsMB8GA1UdIwQYMBaAFHpBdlA80ZGlVs9QTZQklkJQw03MMIHGBgNV
HR8Egb4wgbswgbiggbWggbKGga9sZGFwOi8vL0NOPWRteilDQSxDTjlDQSxDTjlD
RFAsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2VydmljZXMsQ049Q29u
ZmlndXJhdGlvbixEQzlkbXosREM9ZmlzYyxEQzlkb21haW4/Y2VydGlmaWNhdGVS
ZXZvY2F0aW9uTGlzdD9iYXNlP29iamVjdENsYXNzPWNSTERpc3RyaWJ1dGlvblBv
aW50MIG/BggrBgEFBQcBAQSBsjCBrzCBrAYIKwYBBQUHMAKGgZ9sZGFwOi8vL0NO
PWRteilDQSxDTjlBSUEsQ049UHVibGljJTIwS2V5JTIwU2VydmljZXMsQ049U2Vy
dmljZXMsQ049Q29uZmlndXJhdGlvbixEQzlkbXosREM9ZmlzYyxEQzlkb21haW4/
Y0FDZXJ0aWZpY2F0ZT9iYXNlP29iamVjdENsYXNzPWNlcnRpZmljYXRpb25BdXRo
b3JpdHkwIQYJKwYBBAGCNxQCBBQeEgBXAGUAYgBTAGUAcgB2AGUAcjAOBgNVHQ8B
Af8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQUHAwEwDQYJKoZIhvcNAQELBQADggEB
ADoLZ8/fh9l2nF32tbyAvFXZuf52F9+8ZcZGEKWEANovZH852otlw+/nD0M+2uwE
KKFfERPewmUk2k205Mbo5MbgkDT+UXSf8bBjowGcv/h2tqXHAlr9s+qhnxZUaa/L
zqeaaEHFB0mL2XZacRhVVWvWhhzHl2aHlay54BfssIXJCvV2DwJtPPjfjZxdCwnm
HcIq6oPCdNf2tblHFjW0tZQdGPcaxTH8NZmBu8nNHW/ZpDEJljlMpK+gSovTuljK
AelZVJtIausRiXa3/ySuhCZSuP5QrbYfsWbv4J8Gq6hA5SD3HSE74rV8d3dcfDHB
Vw2o2nqJ5fjPbNpdxwRDRFM=
-----END CERTIFICATE-----

subject=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
issuer=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQMHhOSpjjg6tLtA6jakBUYTANBgkqhkiG9w0BAQsFADBU
MRYwFAYKCZImiZPyLGQBGRYGZG9tYWluMRQwEgYKCZImiZPyLGQBGRYEZmlzYzET
MBEGCgmSJomT8ixkARkWA2RtejEPMA0GA1UEAxMGZG16LUNBMB4XDTIxMTIyODIx
MzclMloXDTI2MTIyODIxNDclMlowVDEWMBQGCgmSJomT8ixkARkWBmRvbWFpbjEU
MBIGCgmSJomT8ixkARkWBGZpc2MxEzARBgoJkiaJk/IsZAEZFgNkbXoxDzANBgNV
BAMTBmRteilDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJjYDvge
h2w4Oc6A2l2kO5eKQOzY7SKi6BB8sP9n59sxTvgt8cp5UqmOW6ulLiJX4jeYwk2Y
Wb074WJWDFqZDddmKkel/eIYnPEGQ8JwI9gVmlnQyRtnYDIU4Y60PvGOmN8p9i54
nJnsWauhMs3qmEFJHhfsEvBtl25BdbzwWg2li84joo3EpK6JfCkMx4W4ql6OTYcY
DujaaFoUcain8Adrbx59137GfsX8vlV32hSMedl2N+asCo385kNZJEXw3augS0NU
cNOQNgAGdjWv5xyZYoGDe7pkY7zdtbtQI3s2fgCKNqd6U5Cvz5ye3uJkt2cmhui9
StoSlKiLnNA2i20CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFHpBdlA80ZGlVs9QTZQklkJQw03MMBAGCSsGAQQBgjcVAQQD
AgEAMA0GCSqGSIb3DQEBCwUAA4IBAQANkOuRTR27tBubgviv/3E07KsKT3YJe9ng
MueXVHRIJXNU7zrsCWo9D3HgXDx9vDICpcfsqdf4aPEDoovhyFTXk05xIhMcYC4P
7p67hIWVx5T//0Xl+sze5f7liTHmBBtprF/2Fbwc2smGmA38nchldA6N5TTe+kO5
s5ob/w/ydNA5j2gjFT6YlSt/Xq8x9YMak/4QQ/AFOBzRJbYnlK2CEu354opcKyPx
QOoxLkAT40Yu+uzLXQ7AuFc3G7E9i+pNlp54lfofnV7CioxplEAamGWlCDPrl8Mt
HIIhUqgnlutLwdasNsi9hIgTgQuOo95oqK89SMQWdLK/RZ/KnVl8
-----END CERTIFICATE-----
```

19. Copy the contents of the root CA. Highlight all the text, click and hold Ctrl and then right click on the mouse. Select “copy” as shown.



```
aW50MIG/BggrBgEFBQcBAQSBsjCBrzCBrA                          0NO
PWRteilDQSxDTjlBSUEsQ049UHVibGljJT                          2Vy
dmljZXMsQ049Q29uZmlndXJhdGlvbixEQz                          W4/
Y0FDZXJ0aWZpY2F0ZT9iYXN1P29iamVjdE                          XRo
b3JpdHkwIQYJKwYBBAGCNxQCBBQeEgBXAG                          Q8B
Af8EBAMCBaAwEwYDVR0lBAwwCgYIKwYBBQ                          gEB
ADoLZ8/fh912nF32tbyAvFXZuf52F9+8Zc                          uwE
KKFfERPewmUk2k205Mbo5MbgkDT+UXSf8b                          a/L
zqeaaEHFB0mL2XZacRhVVWvWhhzH12aHla                          wnm
HcIq6oPCdNf2tblHFjW0tZQdGPcaxTH8NZ                          1jK
Ae1ZVJtIausRiXa3/ySuhCZSuP5QrbYfsW                          DHB
Vw2o2nqJ5fjPbNpdxwRDRFM=
-----END CERTIFICATE-----

subject=/DC=domain/DC=fisc/DC=dmz/
issuer=/DC=domain/DC=fisc/DC=dmz/C
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQMHhOSpjjg6tLtA                          DBU
MRYwFAYKCZImiZPyLGQBGRYGZG9tYWluMR                          zET
MBEGCgmSJomT8ixkARkWA2RtejEPMA0GA1                          DIx
MzclMloXDTI2MTIyODIxNDclMlowVDEWMB                          jEU
MBIGCgmSJomT8ixkARkWBGZpc2MxEzARBg                          gNV
BAMTBmRteilDQTCCASIwDQYJKoZIhvcNAQ                          vge
h2w4Oc6A212kO5eKQOzY7SKi6BB8sP9n59sxTvgt8cp5UqmOW6ulLiJX4jeYwk2Y
Wb074WJWDFqZDddmKkel/eIYnPEGQ8JwI9gVmlnQyRtnYDIU4Y60PvGOmN8p9i54
nJnsWauhMs3qmEFJHhfsEvBtl25BdbzwWg2li84joo3EpK6JfCkMx4W4ql6OTYcY
DujaaFoUcain8Adrbx59137GfsX8vlV32hSMed12N+asCo385kNZJEXw3augS0NU
cNOQNgAGdjWv5xyZYoGDe7pkY7zdtbtQI3s2fgCKNqd6U5Cvz5ye3uJkt2cmhui9
StoSlKiLnNA2i20CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFHpBdlA80ZGlVs9QTZQklkJQw03MMBAGCSsGAQQBgjcVAQQD
AgEAMA0GCSqGSIb3DQEBCwUAA4IBAQANkOuRTR27tBubgviv/3E07KsKT3YJe9ng
MueXVHRIJXNU7zrsCWo9D3HgXDx9vDICpcfsqdf4aPEDoovhyFTXk05xIhMcYC4P
7p67hIWVx5T//0Xl+sze5f71iTHmBBtprF/2Fbwc2smGmA38nchldA6N5TTe+kO5
s5ob/w/ydNA5j2gjFT6Y1St/Xq8x9YMak/4QQ/AFOBzRJbYnlK2CEu354opcKyPx
QOoxLkAT40Yu+uzLXQ7AuFc3G7E9i+pN1p541fofnV7CioxplEAamGW1CDPrl8Mt
HIIhUqgnlutLwdasNsi9hIgTgQuOo95oqK89SMQWdLK/RZ/KnV18
-----END CERTIFICATE-----
```

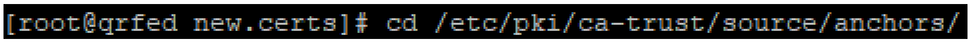
20. Paste the contents into a text file, as shown.



```
subject=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
issuer=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQMHhOSpjjg6tLtA6jakBUYTANBgkqhkiG9w0BAQsFADBU
MRYwFAYKCZImiZPyLGQBGRYGZG9tYWluMRQwEgYKCZImiZPyLGQBGRYEZmlzYzET
MBEGCgmSJomT8ixkARkWA2RtejEPMA0GA1UEAxMGZG16LUNBMB4XDTIxMTIyODIx
Mzc1M1oXDTI2MTIyODIxNDc1M1owVDEWMBQGCgmSJomT8ixkARkWBmRvbWFpbjEU
MBIGCgmSJomT8ixkARkWBGZpc2MxEzARBgoJkiaJk/IsZAEZFgNkbXoxDzANBgNV
BAMTBmRtei1DQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJjYDvge
h2w4Oc6A2l2kO5eKQOzY7SKi6BB8sP9n59sxTvgt8cp5UqmOW6ulLiJX4jeYwk2Y
Wb074WJWDFqZDddmKke1/eIYnPEGQ8JwI9gVm1nQyRtnYDIU4Y60PvGOmN8p9i54
nJnsWauhMs3qmEFJHhfsEvBtl25BdbzwWg2li84joo3EpK6JfCkMx4W4ql6OTYcY
DujaaFoUcain8Adrbx59137GfsX8vlV32hSMedl2N+asCo385kNZJEXw3augS0NU
cNOQNgAGdjWv5xyZYoGDe7pkY7zdtbtQI3s2fgCKNqd6U5Cvz5ye3uJkt2cmhui9
StoS1KiLnNA2i20CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFHpBd1A80ZG1Vs9QTZQk1kJQw03MMBAGCSsGAQQBgjcVAQQD
AgEAMA0GCSqGSIb3DQEBCwUAA4IBAQANkOuRTR27tBubgviv/3E07KsKT3YJe9ng
MueXVHRIJXNU7zrsCWo9D3HgXDx9vDICpcfsqdf4aPEDoovhyFTXk05xIhMcYC4P
7p67hIWVx5T//0Xl+sze5f71iTHmBBtprF/2Fbwc2smGmA38nch1dA6N5TTe+kO5
s5ob/w/ydNA5j2gjFT6YlSt/Xq8x9YMak/4QQ/AFOBzRJbYn1K2CEu354opcKyPx
QOoxLkAT40Yu+uzLXQ7AuFc3G7E9i+pN1p541fofnV7Cioxp1EAamGWlCDPrl8Mt
HIIhUqgnlutLwdasNsi9hIgTgQuOo95oqK89SMQWdLK/RZ/KnVl8
-----END CERTIFICATE-----
```

21. Change directories to the /etc/pki/ca-trust/sources/anchors/ directory, as shown.

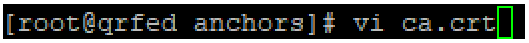
    - command: cd /etc/pki/ca-trust/sources/anchors/



```
[root@qrfed new.certs]# cd /etc/pki/ca-trust/source/anchors/
```

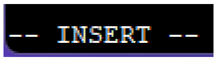
22. Create a new root ca file within the directory.

    - command: vi ca.crt



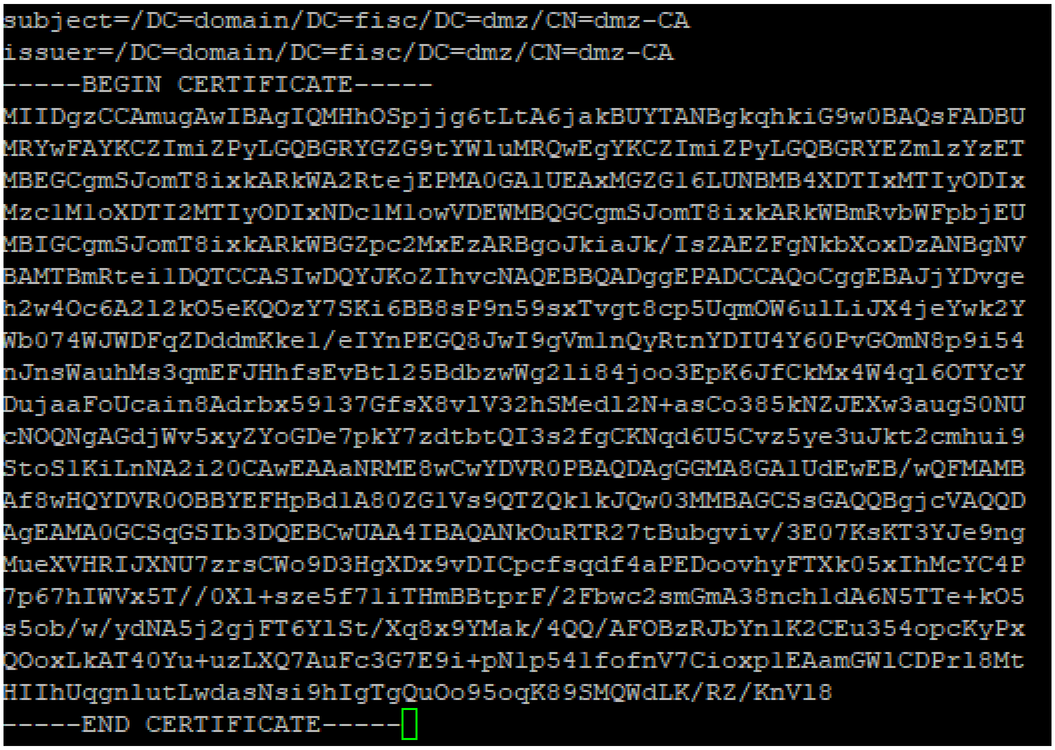
```
[root@qrfed anchors]# vi ca.crt
```

23. Type i key, to enter insert mode.



```
-- INSERT --
```

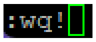
24. Copy and paste the contents from the text file for the root ca public key into the file, as shown.



```
subject=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
issuer=/DC=domain/DC=fisc/DC=dmz/CN=dmz-CA
-----BEGIN CERTIFICATE-----
MIIDgzCCAmugAwIBAgIQMHhOSpjjg6tLtA6jakBUYTANBgkqhkiG9w0BAQsFADBU
MRYwFAYKCZImiZPyLGQBGRYGZG9tYW1uMRQwEgYKCZImiZPyLGQBGRYEZmlzYzET
MBEGCgmSJomT8ixkARkWA2RtejEPMA0GA1UEAxMGZG16LUNBMB4XDTIxMTIyODIx
MzclMloXDTI2MTIyODIxNDclMlowVDEWMBQGCgmSJomT8ixkARkWBmRvbWFpbjEU
MBIGCgmSJomT8ixkARkWBGZpc2MxEzARBgoJkiaJk/IsZAEZFgNkbXoxDzANBgNV
BAMTBmRteilDQTCCASIwDQYJKoZIhvcNAQEBBQADggEPADCCAQoCggEBAJjYDvge
h2w4Oc6A2l2kO5eKQOzY7SKi6BB8sP9n59sxTvgt8cp5UqmOW6ulLiJX4jeYwk2Y
Wb074WJWDFqZDddmKke1/eIYnPEGQ8JwI9gVmlnQyRtnYDIU4Y60PvGOmN8p9i54
nJnsWauhMs3qmEFJHhfsEvBtl25BdbzwWg2li84joo3EpK6JfCkMx4W4ql6OTYcY
DujaaFoUcain8Adrbx59137GfsX8vlV32hSMedl2N+asCo385kNZJEXw3augS0NU
cNOQNgAGdjWv5xyZYoGDe7pkY7zdtbtQI3s2fgCKNqd6U5Cvz5ye3uJkt2cmhui9
StoSlKiLnNA2i20CAwEAAaNRME8wCwYDVR0PBAQDAgGGMA8GA1UdEwEB/wQFMAMB
Af8wHQYDVR0OBBYEFHpBdlA80ZGlVs9QTZQklkJQw03MMBAGCSsGAQQBgjcVAQQD
AgEAMA0GCSqGSIb3DQEBCwUAA4IBAQANkOuRTR27tBubgviv/3E07KsKT3YJe9ng
MueXVHRIJXNU7zrsCWo9D3HgXDx9vDICpcfsqdf4aPEDoovhyFTXk05xIhMcYC4P
7p67hIWVx5T//0Xl+sze5f7liTHmBBtprF/2Fbwc2smGmA38nchldA6N5TTe+kO5
s5ob/w/ydNA5j2gjFT6YlSt/Xq8x9YMak/4QQ/AFOBzRJbYnlK2CEu354opcKyPx
QOoxLkAT40Yu+uzLXQ7AuFc3G7E9i+pNlp54lfofnV7CioxplEAamGWlCDPrl8Mt
HIIhUqgnlutLwdasNsi9hIgTgQuOo95oqK89SMQWdLK/RZ/KnV18
-----END CERTIFICATE-----
```

25. Press the esc key to exit editing mode, as shown.

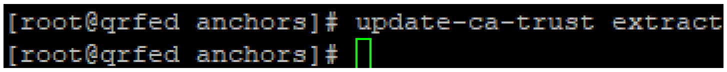
26. Save and exit the file.
    - command: :wq!



```
:wq!
```

27. Update the root cert bundle, adding the customer CA to the master file, as shown.

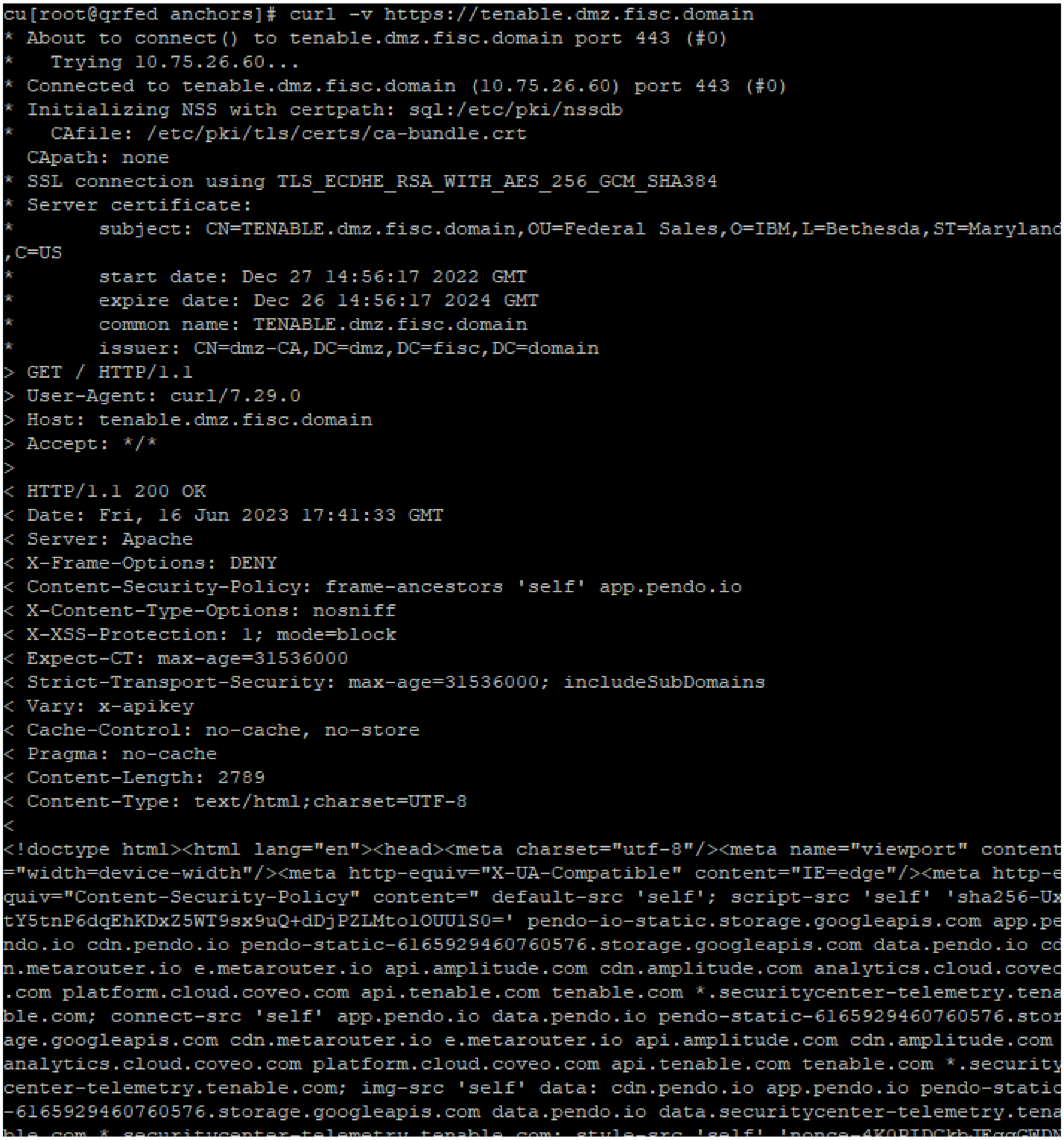
    - command: update-ca-trust extract



```
[root@qrfed anchors]# update-ca-trust extract
[root@qrfed anchors]#
```

28. Test that the root certificate was properly added. Attempt to reach another site within the customer environment which was signed by that root CA. A response similar to the one below should be seen. There should be no errors in the output.

    - command: curl -v https://tenable.dmz.fisc.domain



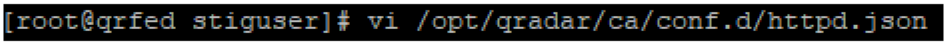
```
cu[root@qrfed anchors]# curl -v https://tenable.dmz.fisc.domain
* About to connect() to tenable.dmz.fisc.domain port 443 (#0)
*   Trying 10.75.26.60...
* Connected to tenable.dmz.fisc.domain (10.75.26.60) port 443 (#0)
* Initializing NSS with certpath: sql:/etc/pki/nssdb
*   CAfile: /etc/pki/tls/certs/ca-bundle.crt
  CApath: none
* SSL connection using TLS_ECDHE_RSA_WITH_AES_256_GCM_SHA384
* Server certificate:
*       subject: CN=TENABLE.dmz.fisc.domain,OU=Federal Sales,O=IBM,L=Bethesda,ST=Maryland
,C=US
*       start date: Dec 27 14:56:17 2022 GMT
*       expire date: Dec 26 14:56:17 2024 GMT
*       common name: TENABLE.dmz.fisc.domain
*       issuer: CN=dmz-CA,DC=dmz,DC=fisc,DC=domain
> GET / HTTP/1.1
> User-Agent: curl/7.29.0
> Host: tenable.dmz.fisc.domain
> Accept: */*
>
< HTTP/1.1 200 OK
< Date: Fri, 16 Jun 2023 17:41:33 GMT
< Server: Apache
< X-Frame-Options: DENY
< Content-Security-Policy: frame-ancestors 'self' app.pendo.io
< X-Content-Type-Options: nosniff
< X-XSS-Protection: 1; mode=block
< Expect-CT: max-age=31536000
< Strict-Transport-Security: max-age=31536000; includeSubDomains
< Vary: x-apikey
< Cache-Control: no-cache, no-store
< Pragma: no-cache
< Content-Length: 2789
< Content-Type: text/html;charset=UTF-8
<
<!doctype html><html lang="en"><head><meta charset="utf-8"/><meta name="viewport" content
="width=device-width"/><meta http-equiv="X-UA-Compatible" content="IE=edge"/><meta http-e
quiv="Content-Security-Policy" content=" default-src 'self'; script-src 'self' 'sha256-Ux
tY5tnP6dqEhKDxZ5WT9sx9uQ+dDjPZLMtolOUUlS0=' pendo-io-static.storage.googleapis.com app.pe
ndo.io cdn.pendo.io pendo-static-6165929460760576.storage.googleapis.com data.pendo.io cd
n.metarouter.io e.metarouter.io api.amplitude.com cdn.amplitude.com analytics.cloud.coveo
.com platform.cloud.coveo.com api.tenable.com tenable.com *.securitycenter-telemetry.tena
ble.com; connect-src 'self' app.pendo.io data.pendo.io pendo-static-6165929460760576.stor
age.googleapis.com cdn.metarouter.io e.metarouter.io api.amplitude.com cdn.amplitude.com
analytics.cloud.coveo.com platform.cloud.coveo.com api.tenable.com tenable.com *.security
center-telemetry.tenable.com; img-src 'self' data: cdn.pendo.io app.pendo.io pendo-static
-6165929460760576.storage.googleapis.com data.pendo.io data.securitycenter-telemetry.tena
ble.com *.securitycenter-telemetry.tenable.com; style-src 'self' 'nonce-4K0RIDCkbJFggGWDN
```

29. If the previous step was successful, you may proceed to the final section “Implement QRadar Certificate”.

Implement QRadar Certificate

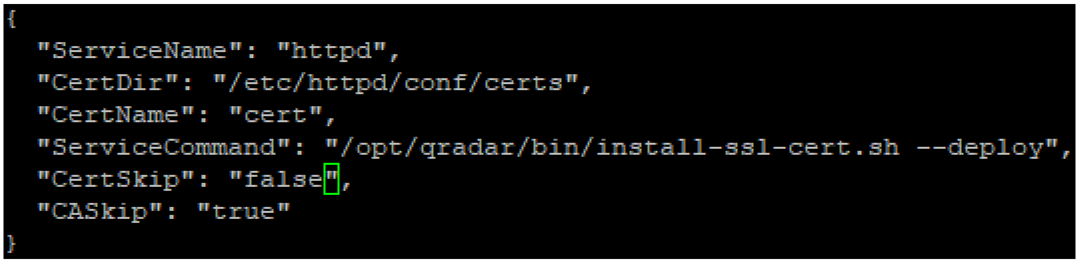
1. Disable CA framework from monitoring and automatically replacing the soon to be implemented certificate. Edit /opt/qradar/ca/conf.d/httpd.json.

   - command: vi /opt/qradar/ca/conf.d/httpd.json



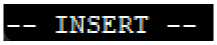
```
[root@qrfed stiguser]# vi /opt/qradar/ca/conf.d/httpd.json
```

2. The file will open, use the down arrow key, naviagate down to “CertSkip”.



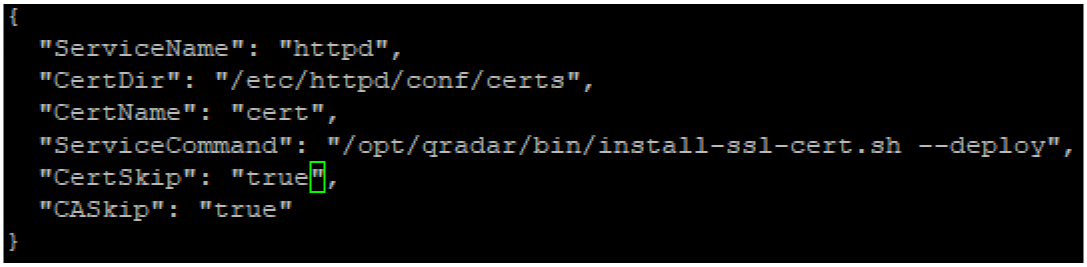
```
{
  "ServiceName": "httpd",
  "CertDir": "/etc/httpd/conf/certs",
  "CertName": "cert",
  "ServiceCommand": "/opt/qradar/bin/install-ssl-cert.sh --deploy",
  "CertSkip": "false",
  "CASkip": "true"
}
```

3. Type the i key, this will insert into editing mode, as shown.



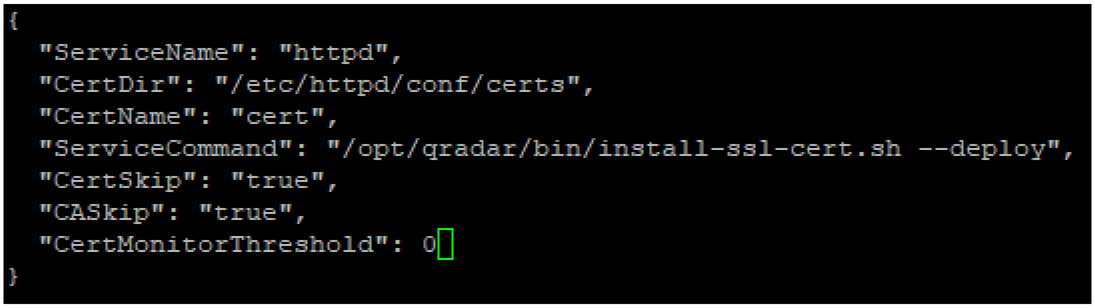
```
-- INSERT --
```

4. Change the “CertSkip”: “false” to “CertSkip”: “true”, as shown.



```
{
  "ServiceName": "httpd",
  "CertDir": "/etc/httpd/conf/certs",
  "CertName": "cert",
  "ServiceCommand": "/opt/qradar/bin/install-ssl-cert.sh --deploy",
  "CertSkip": "true",
  "CASkip": "true"
}
```

5. Scroll to “CASkip”: “true” and add a comma (,) after the “true”. Then add the “CertMonitorThreshold”: 0, as shown.



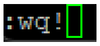
```
{
  "ServiceName": "httpd",
  "CertDir": "/etc/httpd/conf/certs",
  "CertName": "cert",
  "ServiceCommand": "/opt/qradar/bin/install-ssl-cert.sh --deploy",
  "CertSkip": "true",
  "CASkip": "true",
  "CertMonitorThreshold": 0
}
```

6. Pres the esc key, to exit editing mode.

```
~
```

7. Save and exit the file.

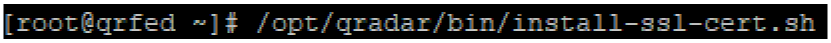
   - Command: :wq!



```
:wq!
```

8. Use the QRadar Console ssl script to import the certificate and key, as shown.

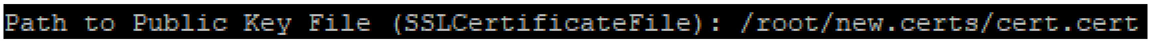
   - command: /opt/qradar/bin/install-ssl-cert.sh



```
[root@qrfed ~]# /opt/qradar/bin/install-ssl-cert.sh
```

9. The script will run and it will first ask you for the new QRadar certificate path.

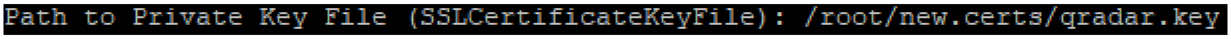
   - Enter: /root/new.certs/cert.cert



```
Path to Public Key File (SSLCertificateFile): /root/new.certs/cert.cert
```

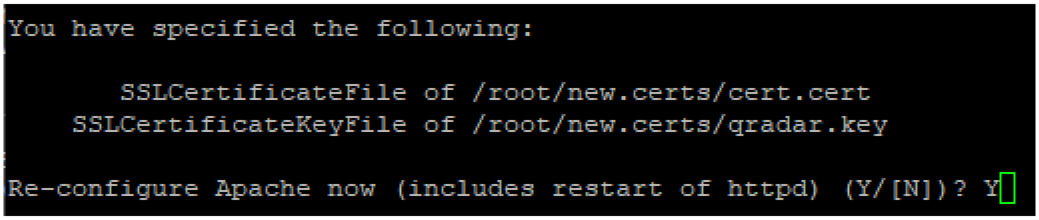
10. Next you will be prompted for the qradar key which was used to generate the CSR.

   - Enter: /root/new.certs/qradar.key



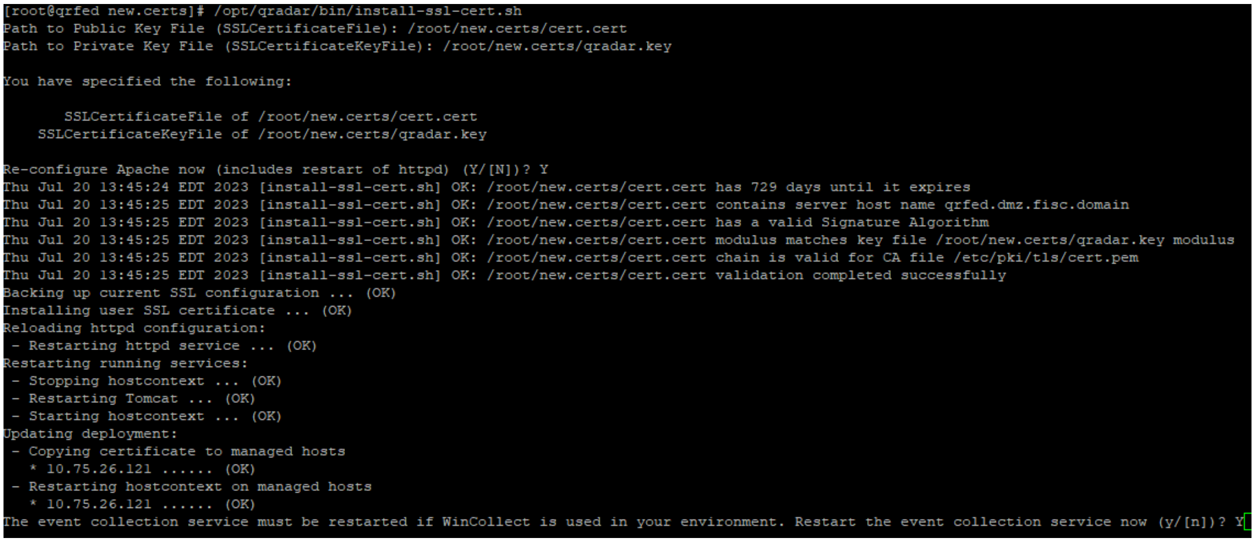
```
Path to Private Key File (SSLCertificateKeyFile): /root/new.certs/qradar.key
```

11. Enter Y and hit enter, as shown at the following prompt:



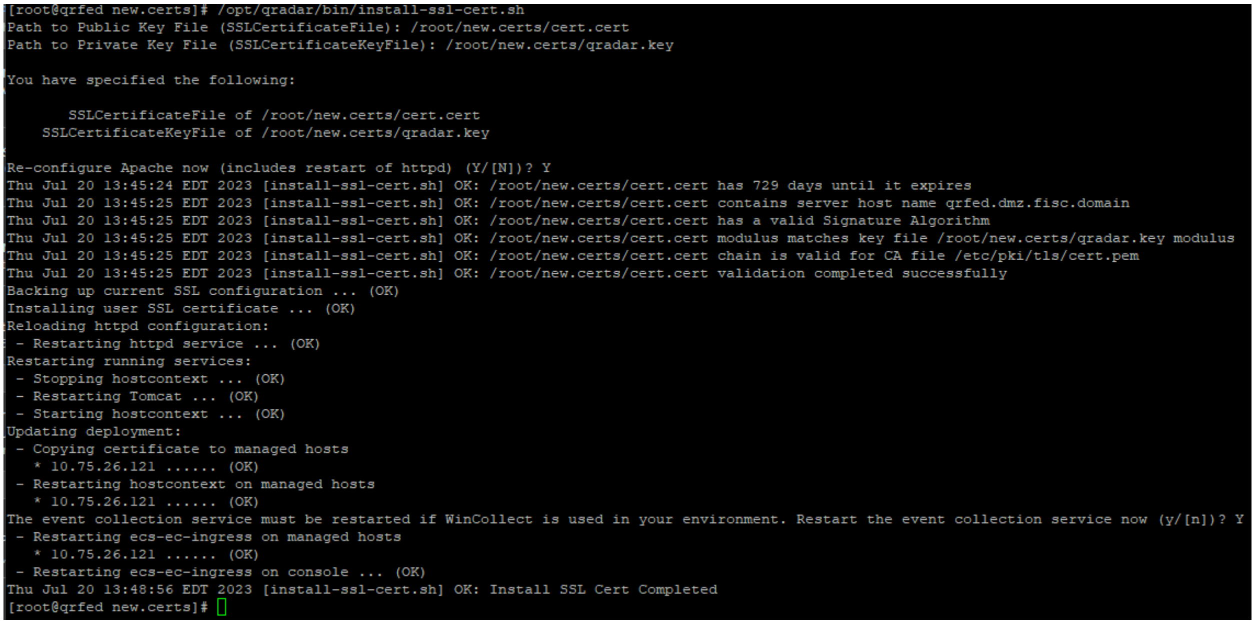
```
You have specified the following:

       SSLCertificateFile of /root/new.certs/cert.cert
    SSLCertificateKeyFile of /root/new.certs/qradar.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? Y
```

12. After entering Y, the script will begin to install the certificates. You will be asked if you want to restart WinCollect service type Y and hit enter:



```
[root@qrfed new.certs]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/new.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/new.certs/qradar.key

You have specified the following:

       SSLCertificateFile of /root/new.certs/cert.cert
    SSLCertificateKeyFile of /root/new.certs/qradar.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? Y
Thu Jul 20 13:45:24 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert has 729 days until it expires
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert contains server host name qrfed.dmz.fisc.domain
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert has a valid Signature Algorithm
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert modulus matches key file /root/new.certs/qradar.key modulus
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert chain is valid for CA file /etc/pki/tls/cert.pem
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert validation completed successfully
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
 - Restarting httpd service ... (OK)
Restarting running services:
 - Stopping hostcontext ... (OK)
 - Restarting Tomcat ... (OK)
 - Starting hostcontext ... (OK)
Updating deployment:
 - Copying certificate to managed hosts
   * 10.75.26.121 ...... (OK)
 - Restarting hostcontext on managed hosts
   * 10.75.26.121 ...... (OK)
The event collection service must be restarted if WinCollect is used in your environment. Restart the event collection service now (y/[n])? Y
```

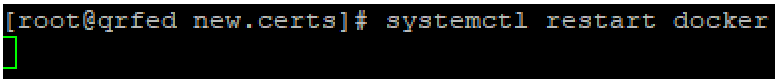
13. Verify the TLS certs were successfully installed via the final “OK: Install SSL Cert Completed” message is presented:



```
[root@qrfed new.certs]# /opt/qradar/bin/install-ssl-cert.sh
Path to Public Key File (SSLCertificateFile): /root/new.certs/cert.cert
Path to Private Key File (SSLCertificateKeyFile): /root/new.certs/qradar.key

You have specified the following:

       SSLCertificateFile of /root/new.certs/cert.cert
    SSLCertificateKeyFile of /root/new.certs/qradar.key

Re-configure Apache now (includes restart of httpd) (Y/[N])? Y
Thu Jul 20 13:45:24 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert has 729 days until it expires
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert contains server host name qrfed.dmz.fisc.domain
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert has a valid Signature Algorithm
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert modulus matches key file /root/new.certs/qradar.key modulus
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert chain is valid for CA file /etc/pki/tls/cert.pem
Thu Jul 20 13:45:25 EDT 2023 [install-ssl-cert.sh] OK: /root/new.certs/cert.cert validation completed successfully
Backing up current SSL configuration ... (OK)
Installing user SSL certificate ... (OK)
Reloading httpd configuration:
 - Restarting httpd service ... (OK)
Restarting running services:
 - Stopping hostcontext ... (OK)
 - Restarting Tomcat ... (OK)
 - Starting hostcontext ... (OK)
Updating deployment:
 - Copying certificate to managed hosts
   * 10.75.26.121 ...... (OK)
 - Restarting hostcontext on managed hosts
   * 10.75.26.121 ...... (OK)
The event collection service must be restarted if WinCollect is used in your environment. Restart the event collection service now (y/[n])? Y
 - Restarting ecs-ec-ingress on managed hosts
   * 10.75.26.121 ...... (OK)
 - Restarting ecs-ec-ingress on console ... (OK)
Thu Jul 20 13:48:56 EDT 2023 [install-ssl-cert.sh] OK: Install SSL Cert Completed
[root@qrfed new.certs]#
```

14. Finally, restart docker on which ever host is running all apps. This can either be the Console or App Host.

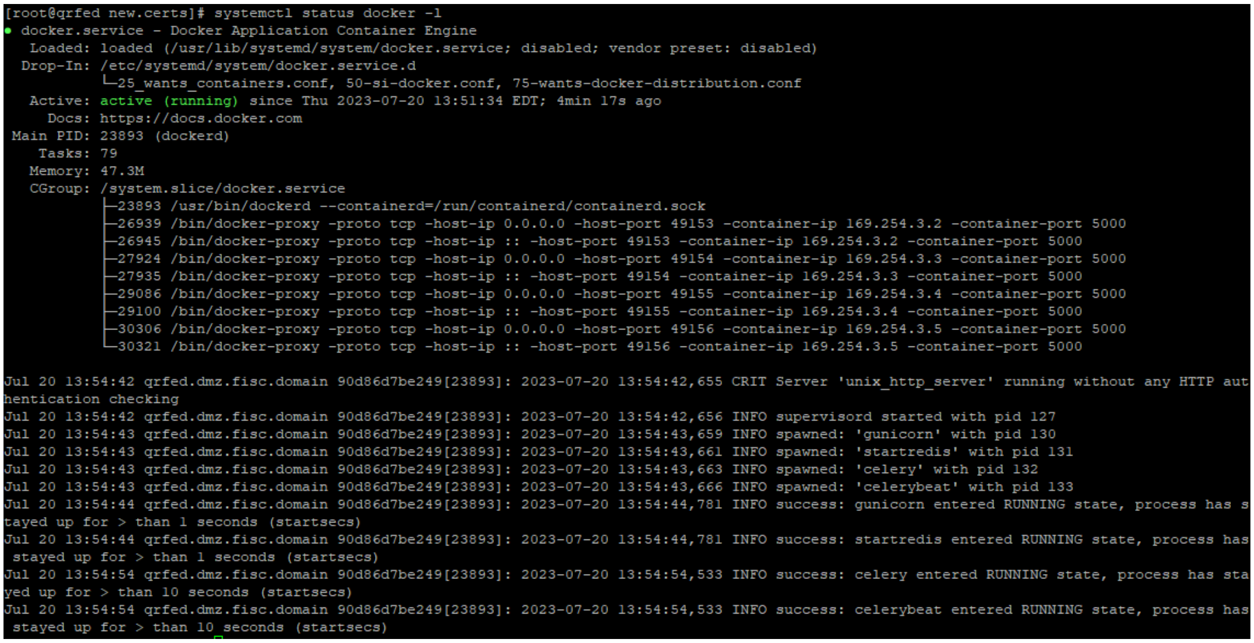
    - command: systemctl restart docker



```
[root@qrfed new.certs]# systemctl restart docker
```

15. Verify docker is up and running before proceeding to the next section.

    - command: systemctl status docker -l



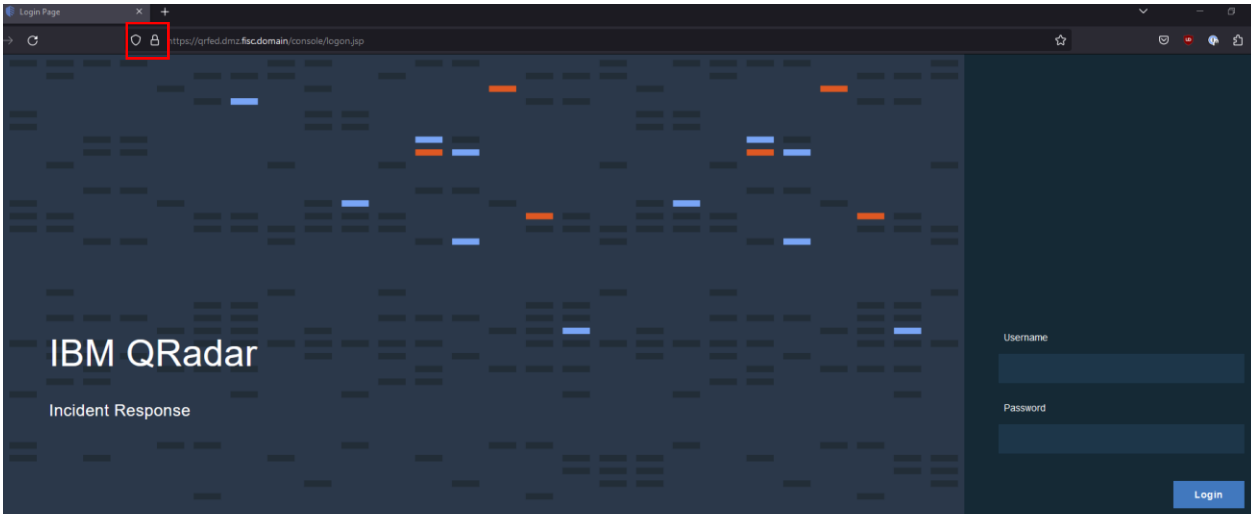
```
[root@qrfed new.certs]# systemctl status docker -l
● docker.service - Docker Application Container Engine
   Loaded: loaded (/usr/lib/systemd/system/docker.service; disabled; vendor preset: disabled)
  Drop-In: /etc/systemd/system/docker.service.d
           └─25_wants_containers.conf, 50-si-docker.conf, 75-wants-docker-distribution.conf
   Active: active (running) since Thu 2023-07-20 13:51:34 EDT; 4min 17s ago
     Docs: https://docs.docker.com
 Main PID: 23893 (dockerd)
    Tasks: 79
   Memory: 47.3M
   CGroup: /system.slice/docker.service
           ├─23893 /usr/bin/dockerd --containerd=/run/containerd/containerd.sock
           ├─26939 /bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 49153 -container-ip 169.254.3.2 -container-port 5000
           ├─26945 /bin/docker-proxy -proto tcp -host-ip :: -host-port 49153 -container-ip 169.254.3.2 -container-port 5000
           ├─27924 /bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 49154 -container-ip 169.254.3.3 -container-port 5000
           ├─27935 /bin/docker-proxy -proto tcp -host-ip :: -host-port 49154 -container-ip 169.254.3.3 -container-port 5000
           ├─29086 /bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 49155 -container-ip 169.254.3.4 -container-port 5000
           ├─29100 /bin/docker-proxy -proto tcp -host-ip :: -host-port 49155 -container-ip 169.254.3.4 -container-port 5000
           ├─30306 /bin/docker-proxy -proto tcp -host-ip 0.0.0.0 -host-port 49156 -container-ip 169.254.3.5 -container-port 5000
           └─30321 /bin/docker-proxy -proto tcp -host-ip :: -host-port 49156 -container-ip 169.254.3.5 -container-port 5000

Jul 20 13:54:42 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:42,655 CRIT Server 'unix_http_server' running without any HTTP aut
hentication checking
Jul 20 13:54:42 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:42,656 INFO supervisord started with pid 127
Jul 20 13:54:43 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:43,659 INFO spawned: 'gunicorn' with pid 130
Jul 20 13:54:43 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:43,661 INFO spawned: 'startredis' with pid 131
Jul 20 13:54:43 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:43,663 INFO spawned: 'celery' with pid 132
Jul 20 13:54:43 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:43,666 INFO spawned: 'celerybeat' with pid 133
Jul 20 13:54:44 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:44,781 INFO success: gunicorn entered RUNNING state, process has s
tayed up for > than 1 seconds (startsecs)
Jul 20 13:54:44 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:44,781 INFO success: startredis entered RUNNING state, process has
 stayed up for > than 1 seconds (startsecs)
Jul 20 13:54:54 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:54,533 INFO success: celery entered RUNNING state, process has sta
yed up for > than 10 seconds (startsecs)
Jul 20 13:54:54 qrfed.dmz.fisc.domain 90d86d7be249[23893]: 2023-07-20 13:54:54,533 INFO success: celerybeat entered RUNNING state, process has
 stayed up for > than 10 seconds (startsecs)
```

Verify TLS Encrypted Web Page

1. Open preferred web browser

2. In the URL address bar, enter the web address of the QRadar instance. Look for the lock in the top left corner as shown:

   Example: https://qrfed.dmz.fisc.domain



3. If the secure lock does not show in the browser as shown in step 2, then ensure that the Root CA certificate is in the browser trusted root certificates.