



TLS Support on Mobility Express

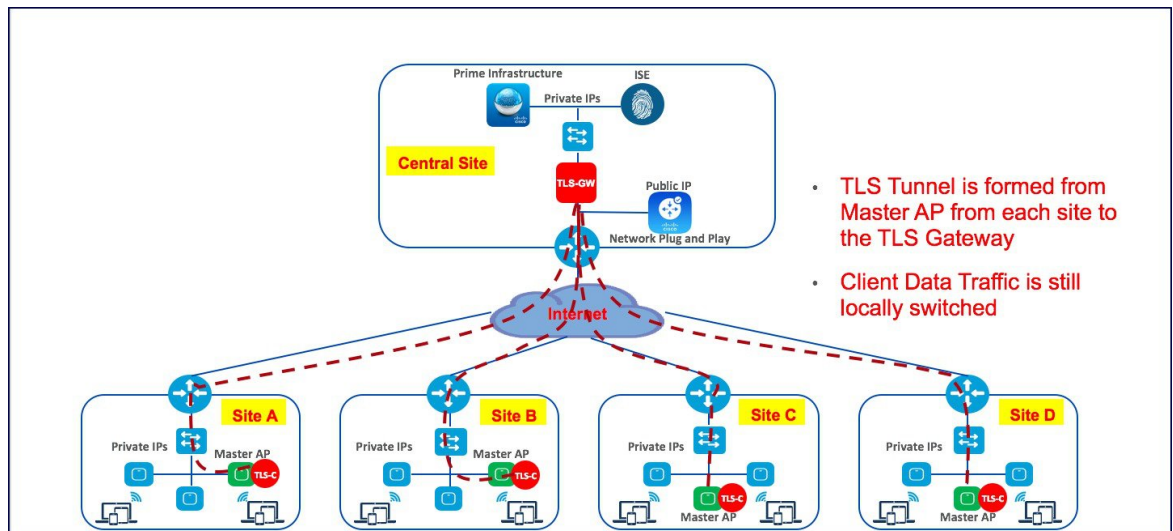
Cisco Mobility Express is a virtual wireless controller function embedded on 802.11ac Wave 2 Access points. With the flexibility of running a wireless LAN controller function on an access point, customers can deploy an Enterprise wireless solution on a single site or multiple sites with up to 100 Access Points at each site. In a multi-site deployment, customers can manage each of the sites using Cisco Prime Infrastructure which would typically be deployed in a central site. However, if the individual sites are connected to the internet via an ISP and are not connected via a dedicated WAN, managing these multi-site deployments can pose a challenge.

To overcome this challenge, starting AireOS Release 8.6, Cisco Mobility Express, customers can now manage the multi-site deployment using Cisco Prime Infrastructure over a TLS Tunnel. In addition to managing these sites, they can also aggregate their DOT1x authentication request to a RADIUS(ISE) which can be deployed along site CPI at the central site.

Please note that only SNMP, RADIUS and SSH traffic flows on the TLS tunnel to the central site and data traffic is still switched locally at individual sites.

TLS Tunnel has two components

1. TLS Client—Starting AireOS Release 8.6, TLS Client has been embedded in the Cisco Mobility Express code and will run on the Master AP
2. TLS Gateway—This is a Virtual Machine which is deployed at the central site to establish the TLS Tunnel. TLS Gateway has two network interfaces
 - a. Public Network—This is the public IP which is reachable from every Master AP. The TLS client establishes a TLS tunnel between Master AP and TLS Gateway using this address.
 - b. Private Network—This the IP address of the private network behind the TLS Gateway where the Cisco Prime Infrastructure, RADIUS and other network devices are deployed.



- [TLS Gateway, on page 2](#)
- [TLS Client, on page 12](#)

TLS Gateway

TLS Gateway is virtual machine and is deployed at the central site.



Note TLS Gateway does not support Cisco Mobility Express platform.

System Requirement for TLS Gateway

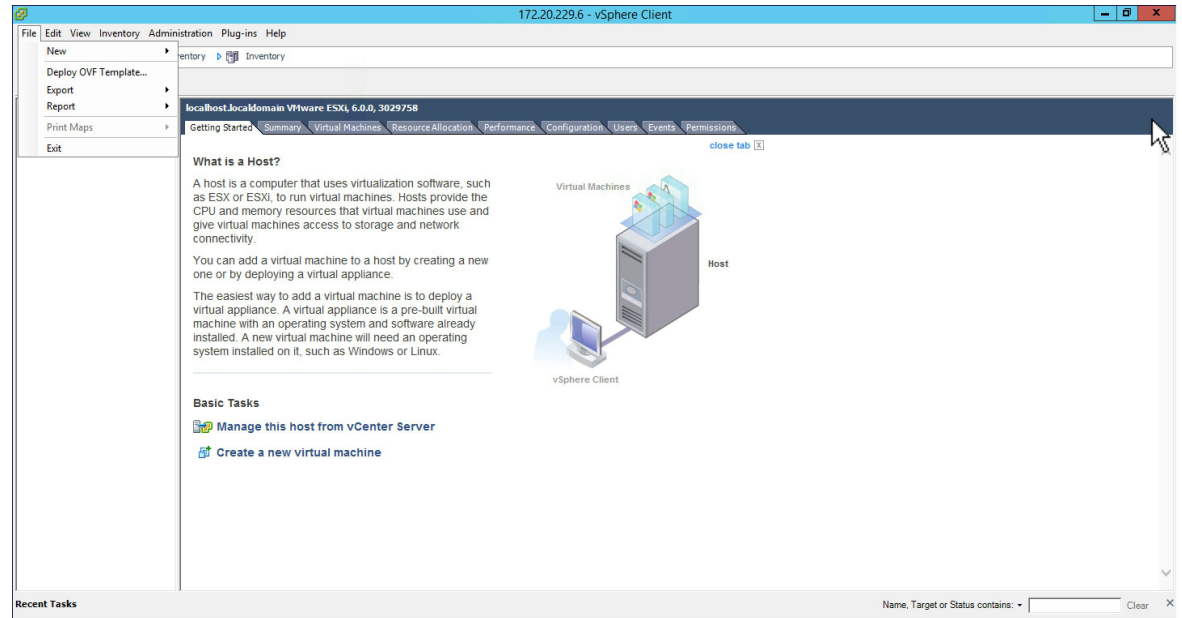
1. Hypervisor: VMware–ESXi 5.5.0/ESXI 6.0
2. VM Resources
 - a. 4 vCPU
 - b. 8GB RAM
 - c. 100 GB Storage
 - d. 2 NICs (One for Public network and one Private network)
3. IP routing requirements
 - a. Routing enabled from TLS-GW Private network towards Prime-infra(SNMP), ISE(Radius), DHCP servers, SSH, Monitoring system and vice-versa
4. TLS-GW public IP should be Reachable from Management IP of ME-AP

Deploying TLS Gateway

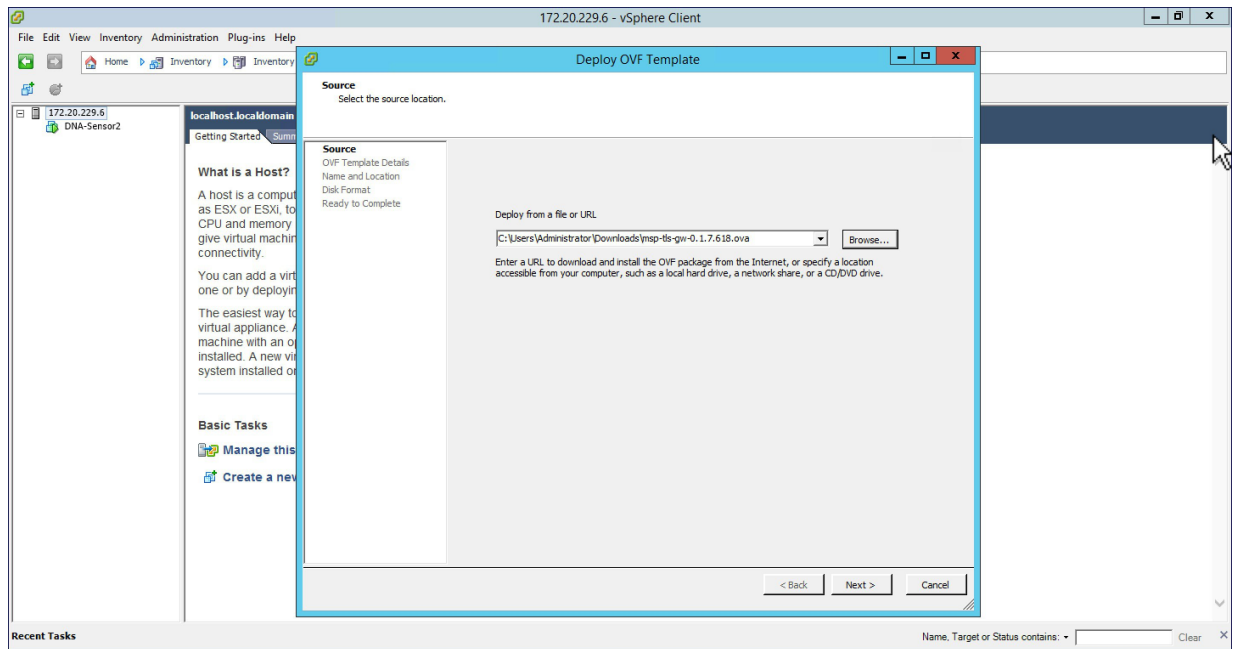
Please follow the steps below to deploy a TLS Gateway at the central site.

Procedure

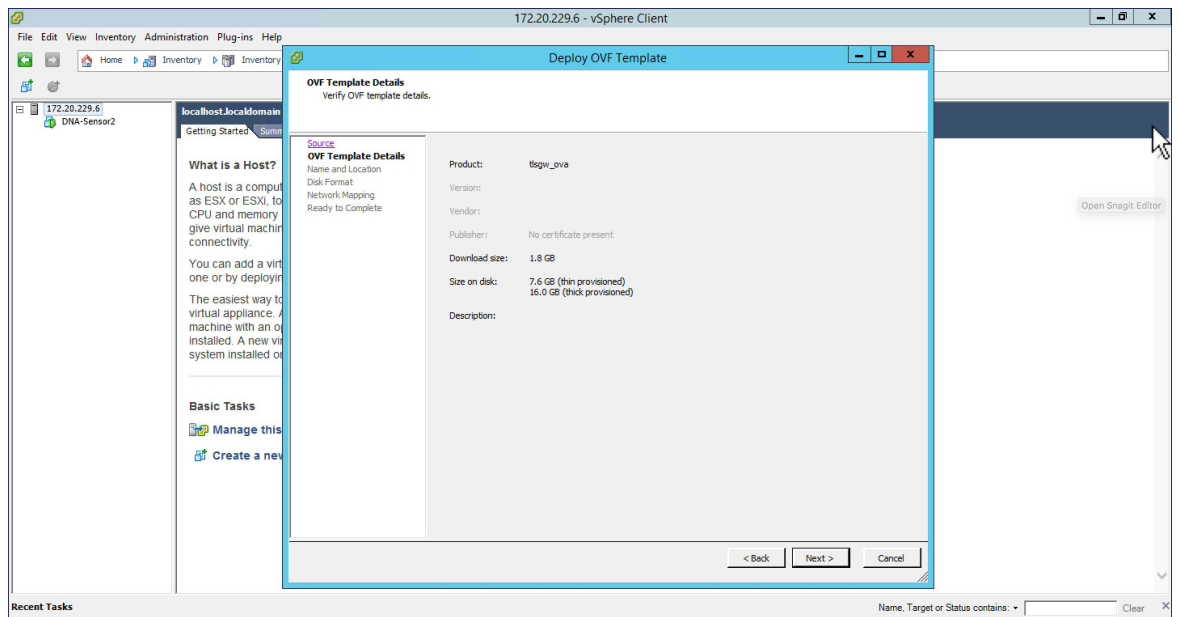
- Step 1** Secure the TLS Gateway OVA File
- Step 2** Navigate to File > Deploy OVF Template on the vSphere Client UI.



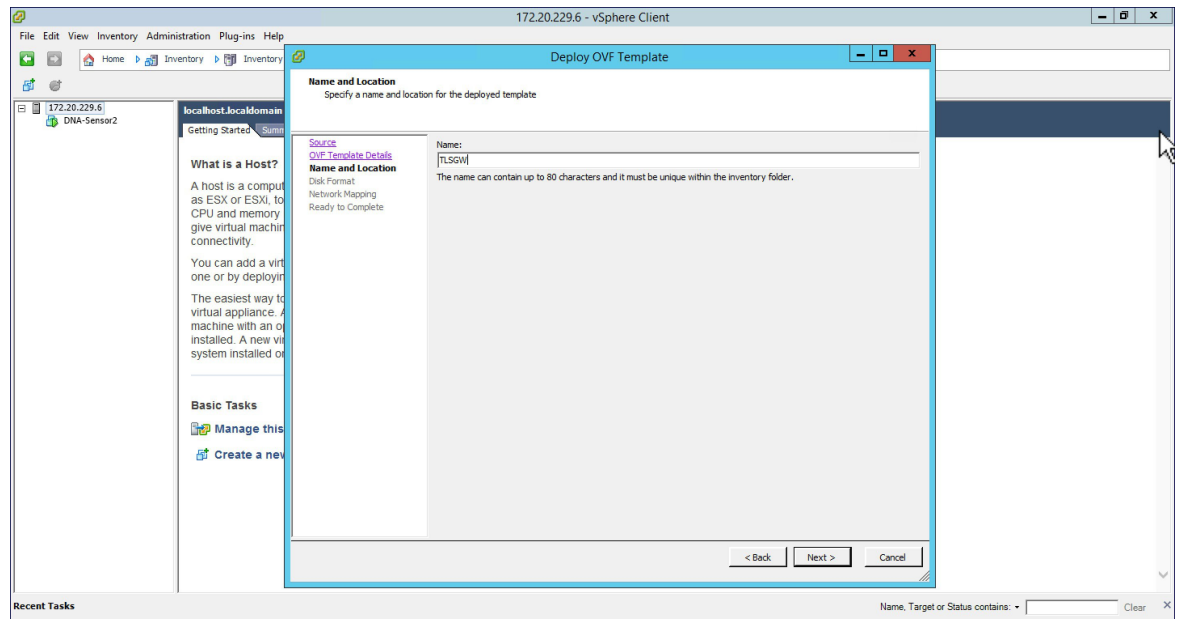
- Step 3** Browse to the TLS Gateway OVA file on your local machine. Click Next.



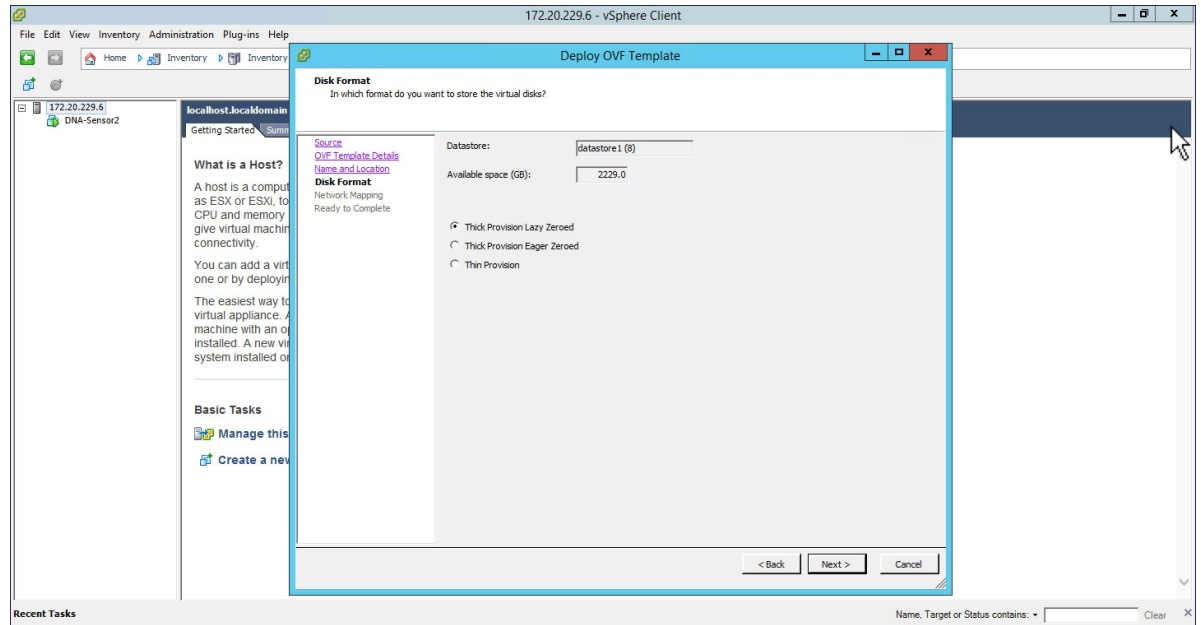
Step 4 Check the OVF Template details and click Next.



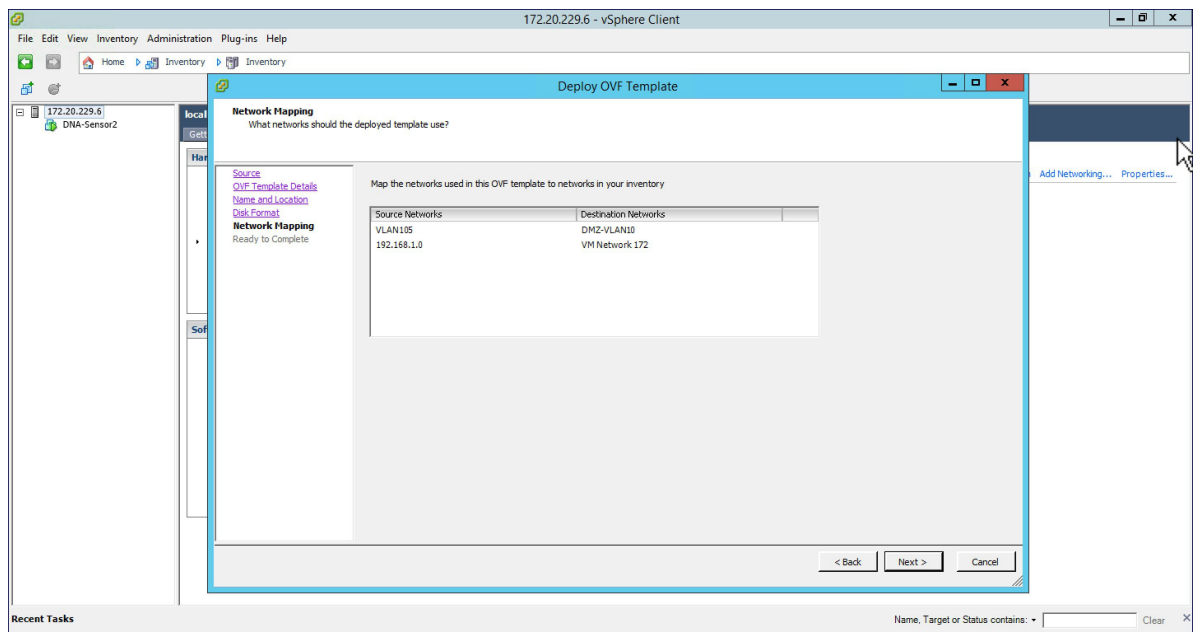
Step 5 Specify the name for the TLS Gateway Virtual Machine.



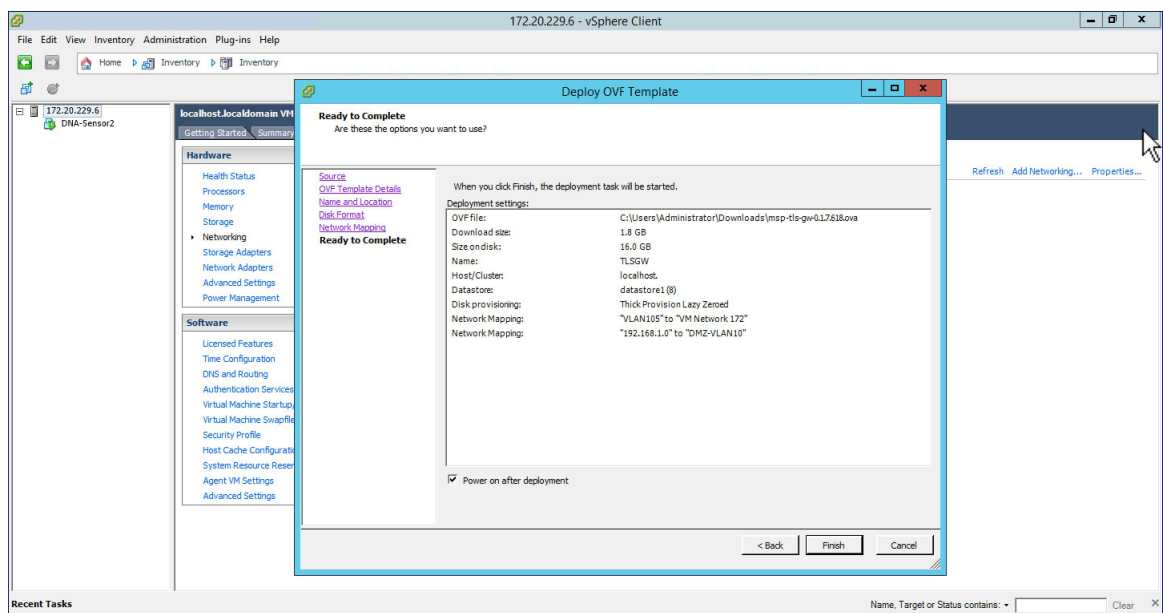
Step 6 For Disk Format, stay with the default and click Next.



Step 7 For Network Mapping, select the Destination Network for the Public Network interface. Click on Next.



Step 8 Verify the Deployment Settings. Enable the 'Power On after deployment' check box and click Finish.



Configuring TLS Gateway

Configuring the TLS Gateway comprises of 3 things:

1. Configure the IP address for Public and Private network interfaces
2. Configure the TLS Gateway configuration file and start the service

3. Configuring the PSK ID-KEY Pair

After the OVA for TLS Gateway is deployed and powered up, follow the steps below to configure the TLS Gateway.

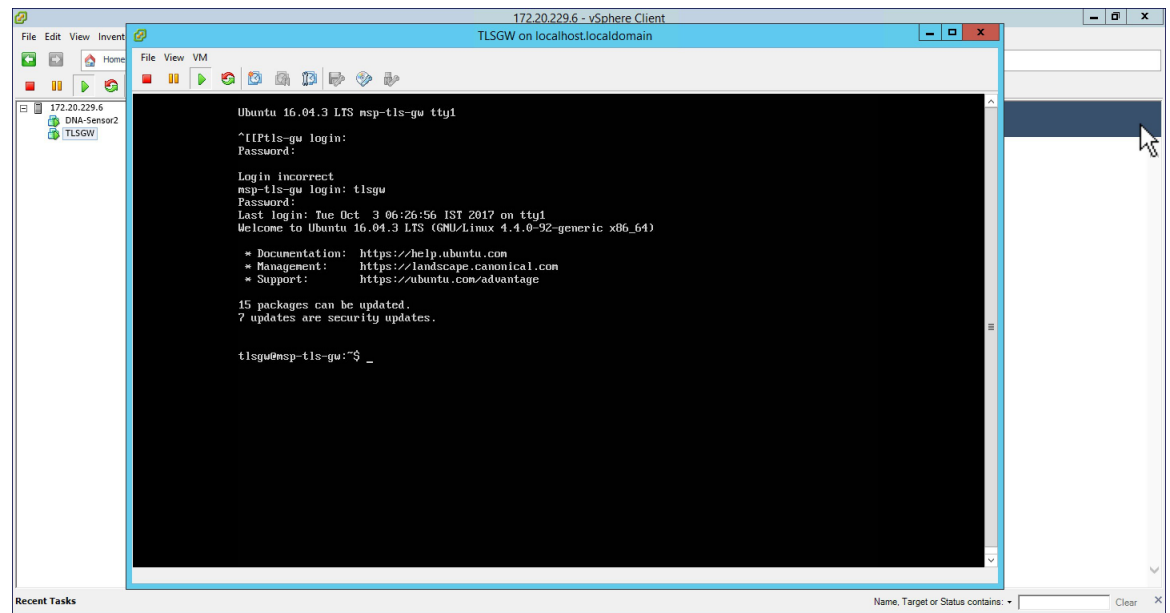
Configuring IP Address for Public and Private network interfaces

Procedure

Step 1 Open a console session to the TLS Gateway VM and login using the following credentials:

username: tlsgw

password: tlsgw



Step 2 Type *ifconfig* to verify the IP address of the Public and Private interfaces as shown below.

Configuring IP Address for Public and Private network interfaces

```

172.20.229.6 - vSphere Client
TLSGW on localhost.localdomain

Ubuntu 16.04.3 LTS msp-tls-gw tty1
msp-tls-gw login: tlgw
Password:
Last login: Wed Nov 15 06:55:52 IST 2017 on tty1
Welcome to Ubuntu 16.04.3 LTS (GNU/Linux 4.4.0-92-generic x86_64)

 * Documentation:  https://help.ubuntu.com
 * Management:    https://landscape.canonical.com
 * Support:       https://ubuntu.com/advantage

15 packages can be updated.
7 updates are security updates.

tlsgw@msp-tls-gw:~$ sudo bash
[sudo] password for tlgw:
root@msp-tls-gw:~# ifconfig
ens160    Link encap:Ethernet  HWaddr 00:0c:29:01:c1:3b
          inet addr:10.10.10.11  Bcast:10.10.10.255  Mask:255.255.255.0
          inet6 addr: fe80::20c:29ff:fe01:c13b/64 Scope:Link
          UP BROADCAST RUNNING MULTICAST  MTU:1500  Metric:1
          RX packets:15 errors:0 dropped:0 overruns:0 frame:0
          TX packets:10 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1000
          RX bytes:864 (864.0 B)  TX bytes:1332 (1.3 KB)

lo        Link encap:Local Loopback
          inet addr:127.0.0.1  Mask:255.0.0.0
          inet6 addr: ::1/128 Scope:Host
          UP LOOPBACK RUNNING  MTU:65536  Metric:1
          RX packets:176 errors:0 dropped:0 overruns:0 frame:0
          TX packets:176 errors:0 dropped:0 overruns:0 carrier:0
          collisions:0 txqueuelen:1
          RX bytes:13392 (13.3 KB)  TX bytes:13392 (13.3 KB)

root@msp-tls-gw:~#

```

Note *ens160* corresponds to the Public network interface and in the above example it has got the IP of **10.10.10.11** from the DHCP server. One can also statically assign the IP address which will be shown the steps ahead. Also, there is no interface for the Private network in the *ifconfig* output above. We can also manually configure this and is shown in the steps ahead.

Step 3 At the **tlsgw@msp-tls-gw:** prompt type **sudo bash** and enter **tlsgw** as the [sudo] password for tlgw.

Step 4 To configure IP address for Public and Private network interface go to **/etc/network** directory by typing **cd /etc/network** at the shell.

Step 5 Open the **interfaces** file using vi editor by typing **vi interfaces** at the shell.

```

172.20.229.6 - vSphere Client
TLSGW on localhost.localdomain

# This file describes the network interfaces available on your system
# and how to activate them. For more information, see interfaces(5).

source /etc/network/interfaces.d/*

# The loopback network interface
auto lo
iface lo inet loopback

# The primary network interface
auto ens160
iface ens160 inet dhcp

# ...

"Interfaces" (readonly) 12L, 300C
1,1 All

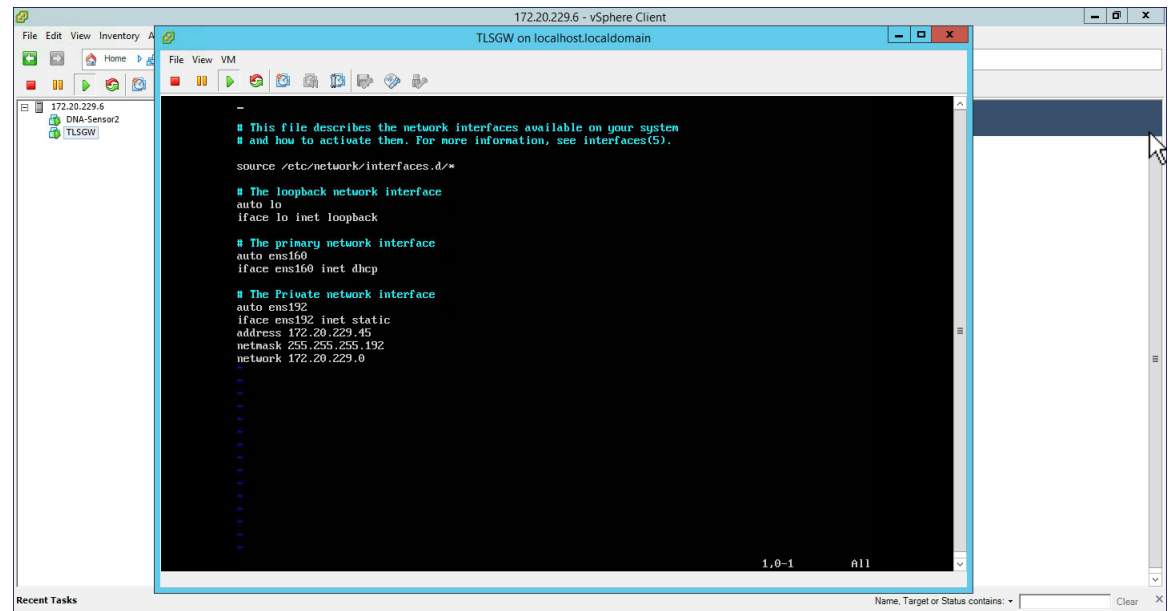
```

Note : **ens160** is Public network interface and is configured for DHCP by default. If you want to statically configure the IP address of Public network interface, replace the **ens160** setting with the following as shown below in the example.

```
auto ens160
iface ens160 inet static
address 10.10.10.11
netmask 255.255.255.0
network 10.10.10.0
```

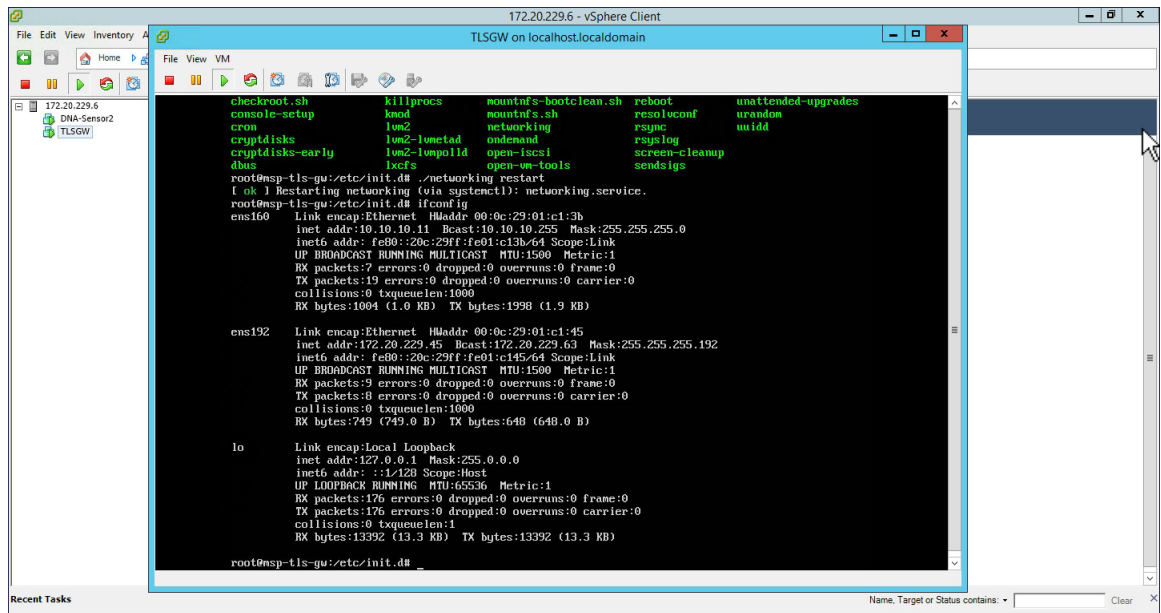
Step 6 To configure the Private network interface IP address, add the following in the **interfaces** file as shown below and save the file.

```
auto ens192
iface ens192 inet static
address 172.20.229.60
netmask 255.255.255.192
network 172.20.229.0
```



Step 7 To restart the network service, go to **/etc/init.d** and type **./networking restart** . Now, do a **ifconfig** and you should see both the Public interface IP address and Private interface IP address. Ping both Public and Private IP address to verify connectivity.

Configure the TLS Gateway configuration file and start the service



Configure the TLS Gateway configuration file and start the service

Procedure

Step 1 : Go to `/opt/cisco/msp-tls-gw/bin/` and edit the `tlsgw_config.txt` with the following:

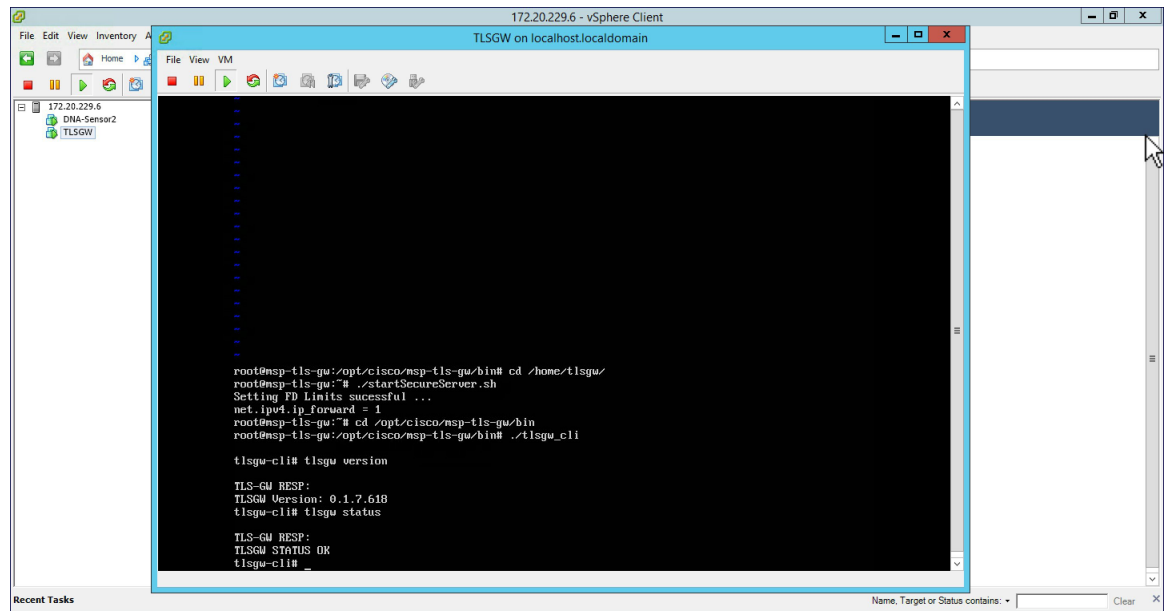
```
server_listening_ipv4_address=10.10.10.11 // Public IP of TLS Gateway
server_listening_port=443 // Port
server_private_ipv4_address=172.20.229.45 // Private IP of TLS Gateway
prefix_subnet=172.20.229.0 // Private IP network of TLS Gateway
prefix_length=26
debug_level=4 // Loglevel for TLS Gateway
dhcp_static_pool_ipv4=20.1.0.0:255.255.0.0 // Local IP pool configured for TLS Client IP
allocation
dpd_interval=60 // Dead Peer Detection timer value for client
rekey_interval=3600 // Rekey timer value for client
retry_interval=20 // Retry timer value for client
```

Note If you are using a DHCP server behind the TLS Gateway, do not configure `dhcp_static_pool_ipv4` in `tlsgw_config.txt` file. This is because broadcast is sent via Private IP of `tls-gw` and if DHCP server exists behind the TLS Gateway, it should assign TLS Client an IP address.

Step 2 Save the file.

Step 3 Go to `/home/tlsgw` and start the TLS Gateway service with script `./startSecureServer.sh`

Step 4 To verify that the TLS Gateway service is running successfully, go to `/opt/cisco/msp-tls-gw/bin/` and run `./tlsgw_cli` as shown below.



Configuring the PSK ID-KEY pair

Configure the Pre Shared Key(PSK) on the TLS Gateway. This will be used by the TLS client on the Master AP to authenticate with the TLS Gateway.



Note

A maximum of 3 PSK ID-KEY pairs can be set for TLGW. PSK-ID can be any character string of length (3-50), PSK password(or key) can be any character string of length (5-256) , Character ':' or 'space' or 'tab' are not allowed for both psk-id and psk-key.

To configure, follow the steps below:

Procedure

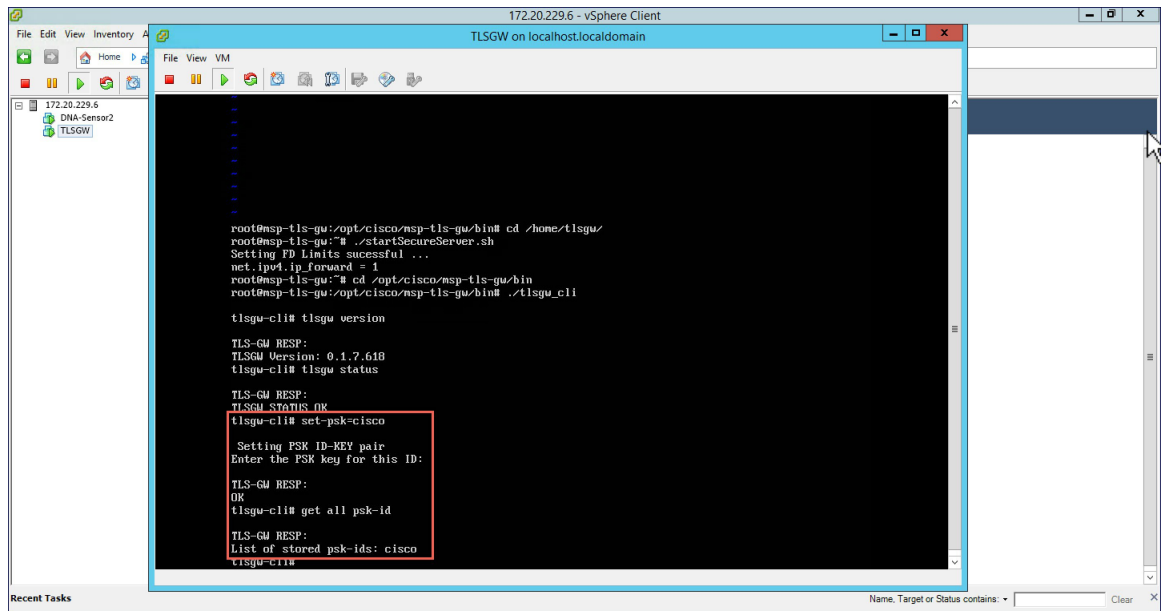
Step 1 : Go to `/opt/cisco/msp-tls-gw/bin/` and run `./tlsgw_cli`

Step 2 Configure the PSK using the following CLI:

```
tlsgw-cli# set-psk=cisco
Setting PSK ID-KEY pair
Enter the PSK key for this ID:
TLS-GW RESP:
OK
```

Step 3 Verify that the PSK ID is configured using the following CLI:

```
tlsgw-cli# get all psk-id
TLS-GW RESP:
List of stored psk-ids: cisco
```



TLS Client

TLS Client is integrated in the AireOS Release 8.6 and is natively present in the code. For TLS client to establish a TLS tunnel with TLS Gateway, Master AP should be able to communicate with the Public IP of the TLS Gateway.

Pre-Requisites for TLS Client

1. Cisco Mobility Express AireOS release 8.6 or higher
2. TLS Gateway Public IP address should be reachable from the Master AP. If TLS Gateway FQDN is used then, TLS_GW FQDN should be configured in the local DNS server, and same DNS server IP should be configuring on ME controller to Resolve the FQDN of TLS Gateway

Configuring TLS Tunnel

There are two ways to configure the TLS Tunnel between TLS Client and TLS Gateway. They are as follows:

Option 1: Zero touch provisioning using Network PnP

During Day 0, one can download the controller configuration from Network PnP. The TLS Tunnel configuration can also be included in the controller configuration file such that after the Master AP downloads the configuration file, reboots, and comes back up, it will automatically establish a TLS Tunnel with the TLS Gateway.

Option 2: Manually configure the TLS Tunnel from WebUI

To configure the TLS Tunnel from the ME WebUI, follow the steps below:

Procedure

- Step 1** Switch to Expert View on the Controller WebUI
- Step 2** Navigate to Services > TLS from the menu on the left
- Step 3** On the TLS Tunnel page, configure the following parameters:
- Enter the TLS Gateway Public IP address or FQDN
 - Enter the port number. Default is 443
 - Enter the PSK ID
 - Enter the PSK Key
 - Enable RADIUS and SNMP

Note RADIUS would be used for ISE and SNMP would be used for Prime Infrastructure.

The screenshot shows the 'TLS Tunnel' configuration page. The left sidebar contains a menu with 'Monitoring', 'Wireless Settings', 'Management', 'Services' (selected), and 'Advanced'. The 'Services' section has a sub-menu with 'TLS' selected. The main content area shows the 'TLS Tunnel' status as 'Disabled'. Below this, there are several configuration fields: 'TLS Tunnel' toggle (disabled), 'TLS Tunnel Uptime Stamp' (Not Available), 'TLS Tunnel Uptime' (Not Available), and 'Failure Reason' (Feature disabled). A 'Refresh' button is present. The 'TLS Gateway FQDN / IP Address' field contains '10.10.10.11'. The 'Port Number' field contains '443'. The 'TLS Pre-Shared Key Identity' field contains 'cisco'. The 'TLS Pre-shared Key' field contains 'cisco'. The 'Show Password' toggle is enabled. Below these fields, the 'RADIUS' and 'SNMP Trap' checkboxes are both checked and highlighted with red boxes. The 'TLS Client Inner IP Address' field is empty. At the bottom, there are 'Apply' and 'Clear' buttons.

Step 4 Click Apply.

Step 5 Finally, enable the TLS Tunnel at the top of the page. If all pre-requisites are met, a tunnel would be created from the Master AP to the Public interface if TLS Gateway.

The screenshot shows the 'TLS Tunnel' configuration page after the settings have been applied. The 'TLS Tunnel' toggle is now enabled and highlighted with a red box. The other configuration fields remain the same as in the previous screenshot. The 'Apply' button is no longer visible, and the 'Clear' button is still present.

