

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.

| Ø | | | | 172.20.229.6 - vSphere Client | | | | _ 0 × |
|------------------------------|--|---|----------------|--|---------------|-----------------|--------------------|--------------------|
| File Edit View Inventory Adr | ministration Plug-ins Help | | | | | | | |
| 🖸 🔯 🔥 Home 🕨 🚮 | Inventory 🕨 🛅 Inventory | 0 | | Deploy OVF Template | L- | | | |
| त्वं व | | OVF Template Details | | | | | | |
| □ 172.20.229.6 | localbert localdomain | Verify OVF template details. | | | | | | |
| DNA-Sensor2 | Getting Starter Sum | | | | | | | |
| | What is a Host? | Source OVF Template Details Name and Location | Product: | tlsgw_ova | | | | h |
| | A host is a comput | Disk Format Network Mapping | Version: | | | | | |
| | as ESX or ESXI, to CPU and memory | Ready to Complete | Vendor: | | | | | Open Snagit Editor |
| | give virtual machin connectivity. | | Publisher: | No certificate present | | | | |
| | You can add a virt | | Download size: | 1.8 GB | | | | |
| | one or by deployin | | Size on disk: | 7.6 GB (thin provisioned) 16.0 GB (thick provisioned) | | | | |
| | The easiest way to virtual appliance. A machine with an o installed. A new vir system installed or | | Description: | | | | | |
| | Basic Tasks | | | | | | | |
| | 🔐 Manage this | | | | | | | |
| | 🗗 Create a nev | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | | | | |
| | | | | | < Back Next > | Cancel | | |
| Recent Tasks | ., . | | | | | Name, Target or | Status contains: • | Clear |

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



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

| 9 | 172.20.229.6 - vSphere Client | _ 0 X |
|---|---|----------------------------|
| File Edit View Inventory Administration Plug-ins Help Image: Second Sec | Deploy OVF Template Disk Format In which format do you want to store the virtual disks? Stored: Orf Template Details Unit and Location Disk Format Hethorit Magning Ready to Complete Complete C Thick Provision Lary Zeroed C Thick Provision Eager Zeroed C Thick Provision | |
| Basic Tasks ြ∰ Manage this ദ്ര† Create a nev | < Back Next > Cancel | |
| Recent Tasks | Name, Targe | or Status contains: Clear |

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

| Ø | 172.20.229.6 - vSphere Client | _ 0 × |
|---|--|---------------------------|
| File Edit View Inventory Administration | Plug-ins Help | |
| Home 🕨 🛃 Inventory 🕨 | Tinventory | |
| ST @ | Deploy OVF Template | |
| C C 17220228.6 DNA-Sensor2 Kar Kar Soft | Debug OV Template Lepidy OV Template Hetwork Happing What networks should the deplayed template use? Map the networks used in this DIF template to networks in your inventory Source OUT Template Deaks Name and Location Def Format Map the networks used in this DIF template to networks in your inventory Source Networks Destruction Networks Dif2 VLAN10 Receive to Complete VLAN105 DH2 VLAN10 192.158.1.0 VM Network 172 | Add Networking Properties |
| | | |
| Recent Tasks | Name, Target or Status contains: • | Clear X |

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

| Ø | | 172.20.229.6 - vSphere Client | _ 🖬 X |
|---|--|--|-----------------------------------|
| File Edit View Inventory Administration Plug-ins Help | | | |
| 🖸 🔯 Home 🕨 👸 Inventory 🕨 🎁 Inventory | | | |
| a a | Ø | Deploy OVF Template | |
| Image: Second | Ready to Complete Are these the options you OVT Template Details Name and Location Disk Format Network Meaning Ready to Complete | Iwant b use? When you dck. Finish, the deployment task will be started. Operforment settings: OVF/Tile: Cl/User1/Administrator/Downloads/msp-tls-gu-0.12638.00 Download state: 1.4 68 Size ondick: 1.6 00 Name: TLSGW Host(Cluster: Iscaling. Disk provisioning: Thick Provision Lasy Zened Network Mapping: "192.168.1.0" to "DMZ-VLANIO" | |
| | | | Ivame, rarget or status contains. |

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

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.



- **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 tlsgw.
- **Step 4** To configure IP address for Public and Private network interface go to */etc/network* directory by typing *cd /etc/interfaces* at the shell.
- **Step 5** Open the *interfaces* file using vi editor by typing *vi interfaces* at the shell.



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 c
 - 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.

| 2 | J | | | | | | | 172.20.229.6 - vSph | ere Client | | | | - 0 × |
|---|----------|----------------------|--------|------|------|--|--|--|--|--|------------------------|-------------|---------|
| 1 | ile Edit | View Inven | tory A | 0 | | | | TLSGW on localhost.locald | omain | | _ 🗆 🗙 | | |
| 1 | - 0 | A Home | P # | File | View | VM | | | | | | | |
| | | | 10 | | | 🕞 😋 🔯 🚳 🔯 l | è 📀 🎶 | | | | | | |
| e | | DNA-Sensor2 TLSGW | | | | <pre>checkroot.sh console-setup cruptdisks cruptdisks-early dbus msp-tls-qu:/et ens160</pre> | killprocs knod lun2 lun2-lunetad lun2-lunetad lun2-lunetad lun2-lunetad lunetas init.da licentig Ethernet Hiadat lo.10.11 Beas red0::20c.237f:15 errors:0 dropp l:0 errors:0 errors:0 errors l:0 errors:0 errors l:0 errors:0 errors l:0 errors:0 errors l:0 errors | nountifs-bootclean.a nountifs.sh networking upen-iacei upen-iacei and the second second networking.sec object:29.01:c1:3h ::10.10.255 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 e0:02:30.257 Mask22 ma | sh reboot resolvconf rsync rsync screen-leanup sendsigs vuice. 55,255,255,0 () er:0 () ::0 ::0 | unattended-upgrades urandom uu idd | | | |
| 1 | | 12 | | | | | | | | | | | ~ |
| R | ecent Ta | sks | | | | | | | | | Name, Target or Status | contains: - | Clear × |
| | _ | | _ | _ | | | | | | | | | |

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 Pear 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.

| File Edit Vew Inventory A Image: Control of the Second | Ø | 172.20.229.6 - vSphere Client | _ 0 × |
|---|--------------------------|---|-------------------------|
| Image: Section of the Very Mit Image: Section of the Very Mit Section of the | File Edit View Inventory | 🖉 TLSGW on localhost.localdomain 📃 🗕 🗖 🗙 | |
| Image: Contract Sector Sect | 🖸 🖾 👌 Home 🕨 🛔 | File View VM | |
| Image: Transformed and the second | | | |
| Image: Control of the set o | | | |
| Image: Tube Image: Tube Image: Tube Tube < | DNA-Sensor2 | | |
| tecent Tasks Name, Target or State contains: • Cterr | TLSGW | | N |
| ront@nsp-tls-gu:?mg:?mg:?mg:?mg:?mg:?mg:?mg:?mg:?mg:?mg | | | hi hi |
| Recent Tasks Name, Target or State contains: • Cter | | | |
| Recent Tasks Name, Target or State contains: • Cter | | | |
| root@nsp-tls-gu:?mpt/cisco/nsp-tls-gu/bimt of /home/tlsgu/ root@nsp-tls-gu:?mt./stortSecureServer.sh Setting PD Linits successful met.ipu4.ip_forward = 1 root@nsp-tls-gu;?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu;?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu:?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu:?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu:?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu:?mt.of.opt/cisco/nsp-tls-gu/bim root@nsp-tls-gu:?mt.of.ofB tlsgu-climtisgu version TLS-GU RESP: TLSGU RESP: TLSGU STATUS OR tlsgu-climt | | | |
| recotfmap-tls-qu:/opt/cisco/map-tls-gu/bimt od /home/tlsgu/ rootfmap-tls-qu:/opt/cisco/map-tls-gu/bimt rootfmap-tls-qu:"to //pt/cisco/map-tls-gu/bimt rootfmap-tls-gu:"to //pt/cisco/map-tls-gu/bimt | | | |
| Recent Tasks Name, Target or State contains: • Cter | | | |
| Recent Tasks Name, Target or State contains. • Cter | | | |
| rootPnsp-tls-gu:?mg.rmg.rls-gu/bint of /home/tlsgu/ rootPnsp-tls-gu:?mg.rmg.rls-gu/bint of /home/tlsgu/ rootPnsp-tls-gu:?mg.rmg.rls-gu/bint rootPnsp-tls-gu:?mg.rls-gu/bint rootPnsp-tls-gu:?mg.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rls-gu/spt.rls-gu/spt.rls-gu/bint rootPnsp-tls-gu/spt.rl | | | |
| Recent Tasks Name, Target or Statu contains: • Cter | | - | |
| root@nsp-tls-gu:?gt/cisco/nsp-tls-gu/bin# cd /home/tlsgu/ root@nsp-tls-gu?fm //startSecureServer.sh Setting:dD Lints wickstdi not.tngtD Lints wickstdi root@nsp-tls-gu?fm //startSecureServer.sh Setting:dt Linguersion TLS-GU RESP: TLSGU Uersion: 0.1.7.618 tlsgu=cli# tlsgu status TLS-GU RESP: TLSGU Uersion Resp: TLSGU UERSI RESP: TLSGU UE | | | = |
| rootemsp-tis-gu:r0ytc:sicormsp-tis-gu/bimt cd /home/tisgu/ rootemsp-tis-gu:" cd,xtartScureServer.sh Setting PD Linits successful met.jup4.jp_foruard = 1 rootemsp-tis-gu/imt cd /opt/ciscormsp-tis-gu/bim rootemsp-tis-gu/imt /lisgu_cli tlsgu-clift tisgu version TLS-GU RESP: TLSGU Version: 0.1.7.618 tlsgu-clift tisgu status TLS-GU RESP: TLSGU Version R tlsgu-clift TLS-GU RESP: TLSGU Version R tlsgu-clift | | а. | = |
| Setting TD Linits successful | | root@nsp-tls-gwi/opt/cisco/nsp-tls-gw/bin# cd /home/tlsgw/ root@nsp-tls-gwi/opt/secures.enver.sh | |
| net.lywi.lp.forward = 1 rootBmsp-tis_u;"it d /opt/cisco/msp-tls_gu/bin rootBmsp-tis_u;"opt/cisco/msp-tls_gu/bin#_/tlsgu_cli tlsgu-clit tlsgu version TLS-GW RESP: TLSGW Uersion: 0.1.7.618 tlsgu-clit tlsgu status TLS-GW RESP: TLSGW Status OK tlsgu-clit Kecent Tasks | | Setting FD Link successful | |
| rootEmsp-tls-gu:/opt/cisco/msp-tls-gu/bin# ./tlsgu_cli tlsgu-cli# tlsgu version TLS-GU RESP: TLS-GU | | net.ipu4.ip_forward = 1 ront@s.ntls=mu:7# cd_cont/cisco/msn-tls=mu/kin | |
| tlsgu-cli# tlsgu version TLS-GU RESP: TLSGU Version: 0.1.7.618 tlsgu-cli# logu status TLS-GU RESP: | | rootemsp-tls-gu:/opt/clsco/msp-tls-gu/bin#/tlsgu_cli | |
| TLS-GU RESP: | | tlsaw-cli# tlsaw version | |
| Recent Tasks Name, Target or Statu contains: • Clear | | | |
| tlsgw-cli#tlsgw status TLS-GW RSSP: TLS-GW RSSP TLS-GW RSSP < | | ILS-WW REST: TLSGW Version: 0.1.7.618 | |
| TLS-GU RESP: TLSGU STATUS OR tlsgu-cli# | | tlsgw-cli# tlsgw status | |
| Image: TLSQU STATUS DR tlsgu-cli# | | TLS-GW RESP: | |
| Recent Tasks Name, Target or Status contains - Clear | | TLSGN STATUS OK | |
| Recent Tasks Name, Target or Statu contains: - Clear | | | |
| | Recent Tasks | Name, Target or Sta | tus contains: - Clear X |

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 TLSGW. 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:
 - a. Enter the TLS Gateway Public IP address or FQDN
 - **b.** Enter the port number. Default is 443
 - c. Enter the PSK ID
 - d. Enter the PSK Key
 - e. Enable RADIUS and SNMP

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

| | U TLS Tunnel Disabled | | |
|-------------------|-------------------------------|------------------|---------|
| 🍄 Monitoring | | | |
| Wireless Settings | TLS Tunnel | | |
| 📩 Management | TLS Tunnel Uptime Stamp | Not Available | |
| 🗲 Services | TLS Tunnel Uptime | Not Available | Refresh |
| U TLS | Failure Reason | Feature disabled | |
| 📥 Advanced | TLS Gateway FQDN / IP Address | 10.10.10.11 | 0 |
| | Port Number | 443 | |
| | TLS Pre-Shared Key Identity | cisco | 0 |
| | TLS Pre-shared Key | cisco | 0 |
| | Show Password | | |
| | RADIUS SNMP Trap | | |
| | TLS Client Inner IP Address | | |
| | | Apply Clear | |

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.

| • | | U TLS Tunnel Disabled | |
|------|-------------------|------------------------------|-----------------------|
| • 3• | Monitoring | | |
| \$ | Wireless Settings | TLS Tuppel | |
| ń. | Management | TLS Tunnel Uptime Stamp | Not Available |
| se ا | Services | TLS Tunnel Uptime | Not Available Refresh |
| | U TLS | Failure Reason | Feature disabled |

I