Configure Crosswork Data Gateway VM

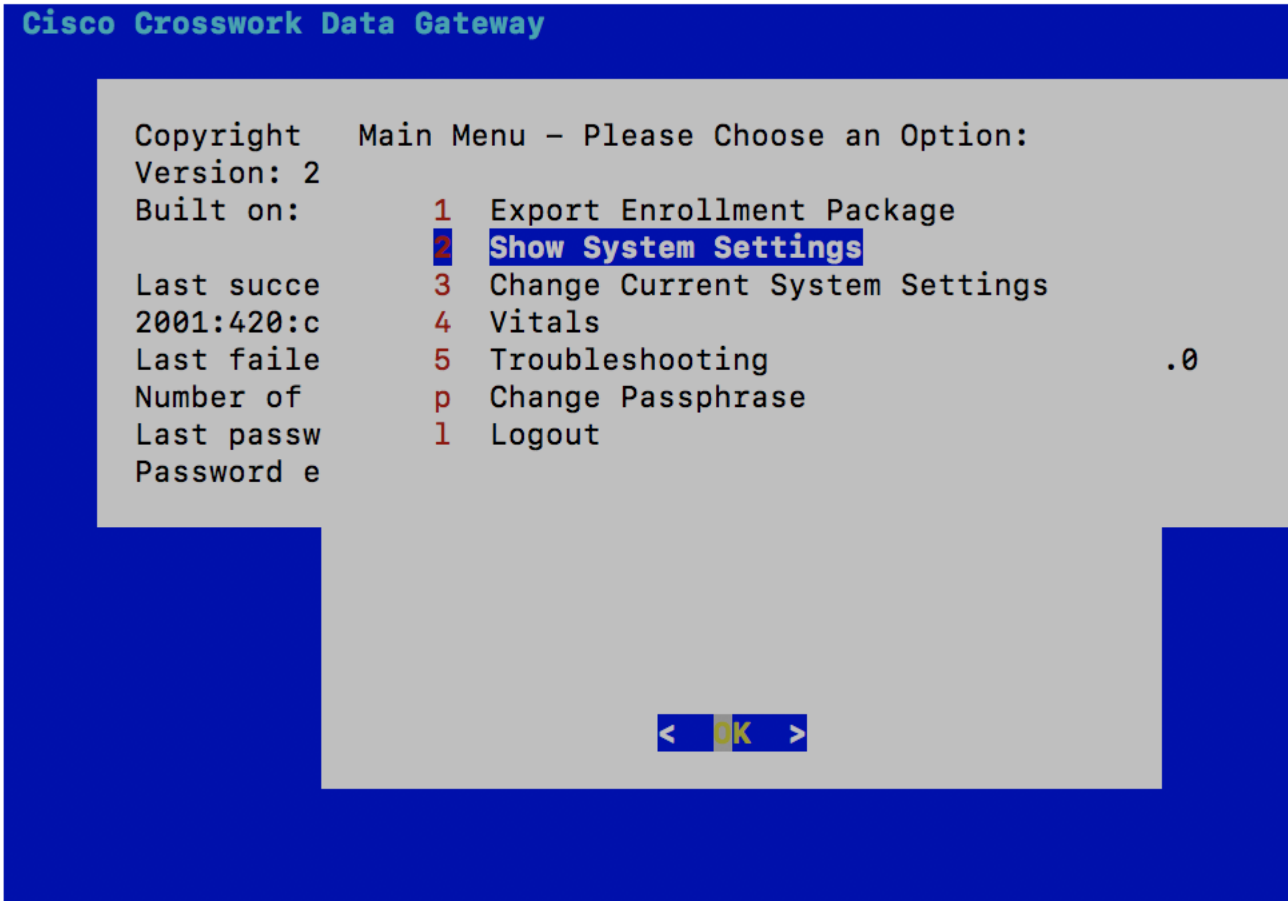
A Cisco Crosswork Data Gateway instance is created as a standalone VM and can be geographically separate from the controller application (Crosswork Cloud). This VM is capable of connecting to the controller application which will enable data collection from the network.

This chapter contains the following topics:

Use the Interactive Console

Cisco Crosswork Data Gateway launches an interactive console upon successful login. The interactive console displays the **Main Menu** as shown in the following figure:

Note The Main Menu shown here corresponds to **dg-admin** user. It is different for **dg-oper** user as the operator does not have same privileges as the administrator. See Table Table 1: Permissions Per Role, on page 3.



```
Cisco Crosswork Data Gateway

  Copyright   Main Menu - Please Choose an Option:
  Version: 2
  Built on:      1  Export Enrollment Package
                 2  Show System Settings
  Last succe     3  Change Current System Settings
  2001:420:c     4  Vitals
  Last faile     5  Troubleshooting                    .0
  Number of      p  Change Passphrase
  Last passw     l  Logout
  Password e

                        <  OK  >
```

The Main Menu presents the following options:

1. Export Enrollment Package

2. Show System Settings

3. Change Current System Settings

4. Vitals

5. Troubleshooting

p. Change Passphrase

l. Logout

Manage Crosswork Data Gateway Users

This section contains the following topics:

- Supported User Roles, on page 3
- Change Password, on page 5

Supported User Roles

Cisco Crosswork Data Gateway supports only two users with the following user roles:

- **Administrator**: One default **dg-admin** user with administrator role is created when Cisco Crosswork Data Gateway is brought up for the first time. This user cannot be deleted and has both read and write privileges such as starting and shutting down the Cisco Crosswork Data Gateway VM, registering an application, applying authentication certificates, configuring server settings, and performing a kernel upgrade.
- **Operator**: The **dg-oper** user is also created by default during the initial VM bring up. This user can review the health of the Cisco Crosswork Data Gateway, retrieve error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.

Note

- User credentials are configured for both the user accounts during Cisco Crosswork Data Gateway installation.
- Users are locally authenticated.

The following table shows the permissions available to each role:

Table 1: Permissions Per Role

Permissions	Administrator	Operator
Export Enrollment Package	✓	✓
Show system settings		
vNIC Addresses NTP DNS Proxy UUID Syslog Certificates First Boot Provisioning Log Timezone	✓	✓
Change Current System Settings		

Permissions	Administrator	Operator
Configure NTP Configure DNS Configure Control Proxy Configure Static Routes Configure Syslog Create new SSH keys Import Certificate Configure vNIC2 MTU Configure Timezone Configure Password Requirements Configure Simultaneous Login Limits Configure Idle Timeout	✓	✕
Vitals		
Docker Containers Docker Images Controller Reachability NTP Reachability Route Table ARP Table Network Connections Disk Space Usage Linux services NTP Status System Uptime	✓	✓
Troubleshooting		
Run Diagnostic Commands	✓	✓
Run show-tech	✓	✓
Export auditd logs	✓	✓
Enable TAC Shell Access	✓	✕
Change Passphrase	✓	✓

Change Password

Both adminstrator and operator users can change their own passphrases but not each others'.

Follow these steps to change your passphrase:

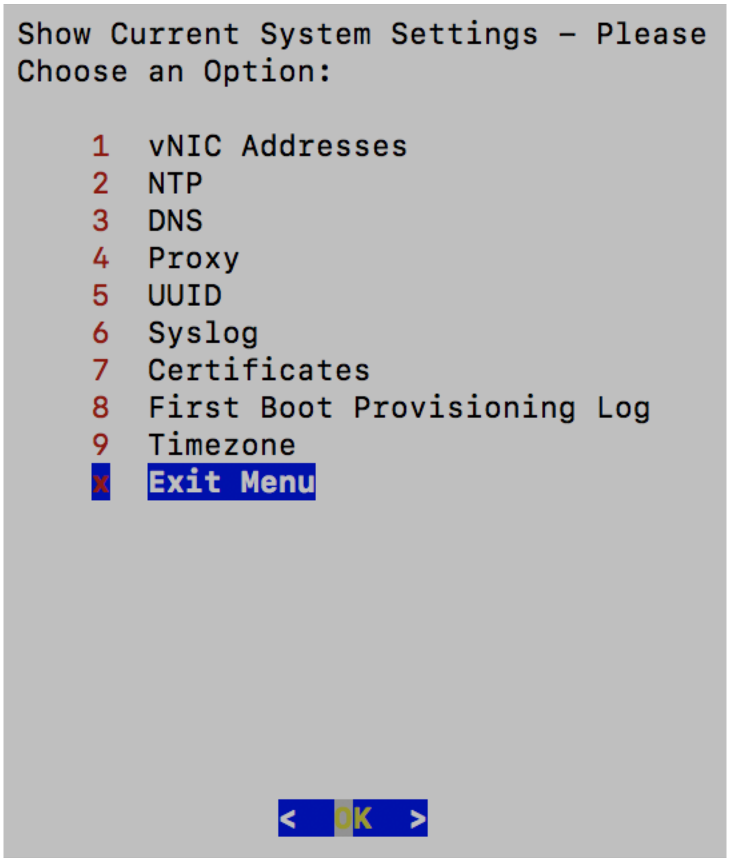
Step 1 From the Main Menu, select **p Change Passphrase** and click **OK**.

Step 2 Input your current password and press Enter.

Step 3 Enter new password and press Enter. Re-type the new password and press Enter.

View Current System Settings

Crosswork Data Gateway allows you to view the following settings:



```
Show Current System Settings - Please
Choose an Option:

     1   vNIC Addresses
     2   NTP
     3   DNS
     4   Proxy
     5   UUID
     6   Syslog
     7   Certificates
     8   First Boot Provisioning Log
     9   Timezone
     x   Exit Menu

               <  OK  >
```

Follow these steps to view the current system settings:

Step 1 From the Main Menu, select **2 Show System Settings**, as shown in the following figure:

Step 2 Click **OK**. The **Show Current System Settings** menu opens.

Step 3 Select the setting you want to view.

Setting Option	Description
1 vNIC Addresses	Displays the vNIC configuration, including address information.
2 NTP	Displays currently configured NTP server details.
3 DNS	Displays DNS server details.
4 Proxy	Displays proxy server details (if any configured).
5 UUID	Displays the system UUID.
6 Syslog	Displays the Syslog forwarding configuration. If no Syslog forwarding is configured, this will display only "# Forwarding configuration follows" on screen.
7 Certificates	Provides options to view the following certificate files: • Crosswork Data Gateway signing certificate file • Controller signing certificate file • Controller SSL/TLS certificate file • Syslog certificate file • Collector certificate file
8 First Boot Provisioning Log	Displays the content of the first boot log file.
9 Timezone	Displays the current timezone setting.

Change Current System Settings

Crosswork Data Gateway allows you to configure the following settings:

- NTP.
- DNS.
- Control proxy.
- Static routes.
- Syslog.
- SSH keys.
- Certificate.
- vNIC2 MTU.

- Timezone.
- Password requirements.
- Simlutaneous login limits.
- Idle timeout.
- Configure auditd.

Note

- Crosswork Data Gateway system settings can only be configured by the administrator.
- In settings options where you require to use SCP, if you are not using the default SCP port 22, you can specify the port as a part of the SCP command. For example,

  ```
  -P55 user@host:path/to/file
  ```

  where 55 is a custom port.

Configure NTP

It is important that NTP time be synchronized with the controller application and its Crosswork Data Gateway instances. If not, then session handshake doesn't happen and functional images are not downloaded. In such cases, error message clock time not matched and sync failed is logged in controller-gateway.log. To access log files, see Run show-tech, on page 20. You can use Controller Reachability and NTP Reachability options from **Main Menu** > **Vitals** to check NTP reachability for the controller application as well as the Crosswork Data Gateway. See View Crosswork Data Gateway Vitals, on page 14. If NTP has been set incorrectly,you will see error Session not established.

When configuring Crosswork Data Gateway to use authentication via a keys file, the chrony.keys file must be formatted in a specific way as documented at https://chrony.tuxfamily.org/doc/3.5/chrony.conf.html#keyfile. For sites that use ntpd and are configured to use a ntp.keys file, it is possible to convert from ntp.keys to chrony.keys using the tool https://github.com/mlichvar/ntp2chrony/blob/master/ntp2chrony/ntp2chrony.py. The tool converts ntpd configuration into a chrony compatible format, but only the keys file is required to be imported into Crosswork Data Gateway.

Follow the steps to configure NTP settings:

Step 1 From the **Change Current System Settings** Menu, select **1 Configure NTP**.

Step 2 Enter the following details for the new NTP server:

- Server list, space delimited
- Use NTP authentication?
- Key list, space delimited and must match in number with server list
- Key file URI to SCP to the VM
- Key file passphrase to SCP to the VM

Step 3 Click **OK** to save the settings.

Configure DNS

Step 1 From the **Change Current System Settings** menu, select **2 Configure DNS** and click **OK**.

Step 2 Enter the new DNS server address(es) and domain.

Step 3 Click **OK** to save the settings.

Configure Control Proxy

If you have not configured a proxy server during installation, avail this option to set up a proxy sever:

Step 1 From the **Change Current System Settings** menu, select **3 Configure Control Proxy** and click **OK**.

Step 2 Click **Yes** for the following dialog if you wish to proceed. Click **cancel** otherwise.

Step 3 Enter the new Proxy server details:

- Server URL
- Bypass addresses
- Proxy username
- Proxy passphrase

Step 4 Click **OK** to save the settings.

Configure Static Routes

The static routes are configured when Crosswork Data Gateway receives add/delete requests from the collectors. The **Configure Static Routes** option from the main menu can be used for troubleshooting purpose.

Note Static routes configured using this option are lost when the Crosswork Data Gateway reboots.

Add Static Routes

Follow the steps to add static routes:

Step 1 From the **Change Current System Settings** menu, select **4 Configure Static Routes**.

Step 2 To add a static route, select **a Add**.

Step 3 Select the interface for which you want to add a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format when prompted.

Step 6 Click **OK** to save the settings.

Delete Static Routes

Follow the steps to delete a static route:

Step 1 From the **Change Current System Settings** Menu, select **4 Configure Static Routes**.

Step 2 To delete a static route, select **d Delete**.

Step 3 Select the interface for which you want to delete a static route.

Step 4 Select the IP version.

Step 5 Enter IPv4 or IPv6 subnet in CIDR format.

Step 6 Click **OK** to save the settings.

Configure Syslog

Note For any Syslog server configuration with IPv4 or IPv6 support for different Linux distributions, please refer your system administrator and configuration guides.

Follow the steps to configure Syslog:

Step 1 From the **Change Current System Settings** Menu, select **5 Configure Syslog**.

Step 2 Enter the new values for the following syslog attributes:.

- Server address: IPv4 or IPv6 address of a syslog server accessible from the management interface. If you are using an IPv6 addres, it must be surrounded by square brackets ([1::1]).
- Port: Port number of the syslog server
- Protocol: Use UDP, TCP, or RELP when sending syslog.
- Use Syslog over TLS?: Use TLS to encrypt syslog traffic.
- TLS Peer Name: Syslog server's hostname exactly as entered in the server certificate SubjectAltName or subject common name.
- Syslog Root Certificate File URI: PEM formatted root cert of syslog server retrieved using SCP.
- Syslog Certificate File Passphrase: Password of SCP user to retrieve Syslog certificate chain.

Step 3 Click **OK** to save the settings.

Create New SSH Keys

Creating new SSH keys will remove the current keys.

Follow the steps to create new SSH keys:

Step 1 From the **Change Current System Settings** Menu, select **6 Create new SSH keys**.

Step 2 Click **OK**. Crosswork Data Gateway launches an auto-configuration process that generates new SSH keys.

Import Certificate

Updating any certificate other than Controller Signing Certificate causes a collector restart.

Crosswork Data Gateway allows you to import the following certificates:

- Controller signing certificate file
- Controller SSL/TLS certificate file
- Syslog certficate file
- Proxy certificate file

Step 1 From the **Change Current System Settings** Menu, select **7 Import Certificate**.

Step 2 Select the certificate you want to import.

Step 3 Enter SCP URI for the selected certificate file.

Step 4 Enter passphrase for the SCP URI and click **OK**.

Configure vNIC2 MTU

You can change vNIC2 MTU only if you are using 3 NICs.

If your interface supports jumbo frames, the MTU value lies in the range of 60-9000, inclusive. For interfaces that do not support jumbo frames, the valid range is 60-1500, inclusive. Setting an invalid MTU causes Crosswork Data Gateway to revert the change back to the currently configured value. Please verify with your hardware documentation to confirm what the valid range is. An error will be logged into kern.log for MTU change errors which can be viewed after running showtech.

Step 1 From the **Change Current System Settings** menu, select **8 Configure vNIC1 MTU**.

Step 2 Enter vNIC2 MTU value.

Step 3 Click **OK** to save the settings.

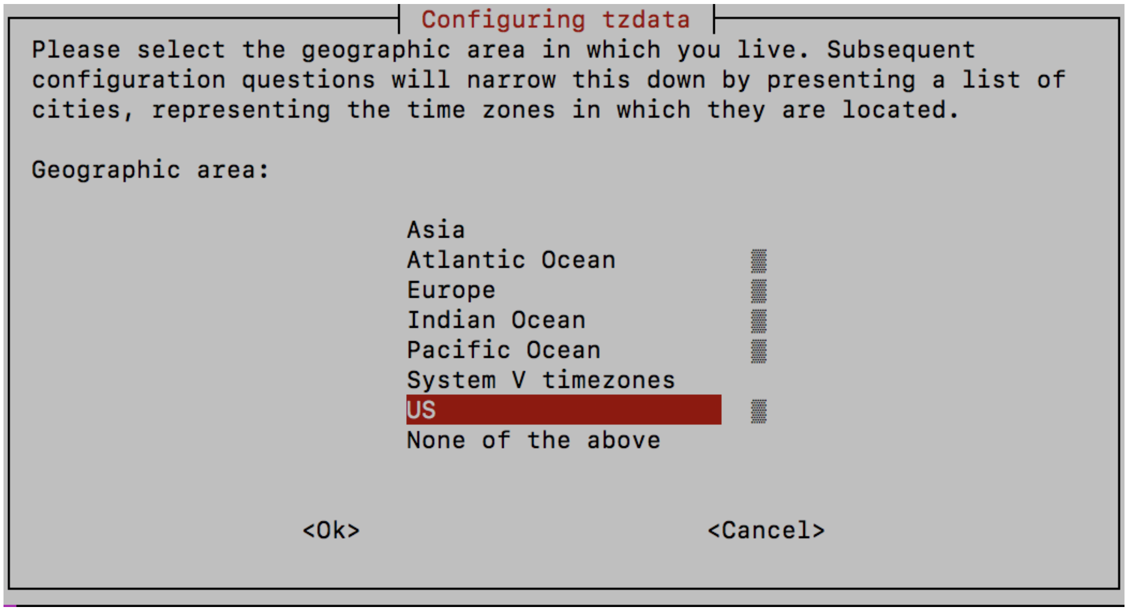
Configure Timezone of the Crosswork Data Gateway VM

The Crosswork Data Gateway VM first launches with default timezone as UTC. Update the timezone with your geographical area so that all Crosswork Data Gateway processes (including the showtech logs) reflect the timestamp corresponding to the location you have chosen.

Step 1 In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.

Step 2 Select **9 Timezone**.

Step 3 Select the geographic area in which you live.



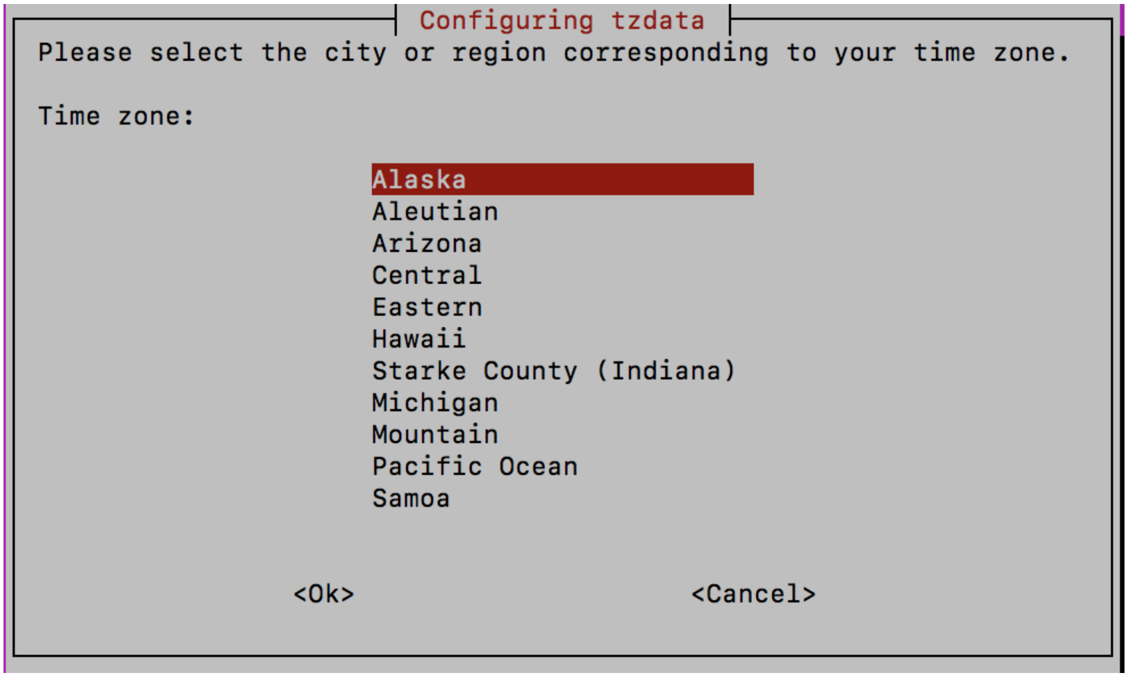
```
                          Configuring tzdata
Please select the geographic area in which you live. Subsequent
configuration questions will narrow this down by presenting a list of
cities, representing the time zones in which they are located.

Geographic area:

                         Asia
                         Atlantic Ocean
                         Europe
                         Indian Ocean
                         Pacific Ocean
                         System V timezones
                         US
                         None of the above


                  <Ok>                        <Cancel>
```

Step 4 Select the city or region corresponding to your timezone.



```
┤ Configuring tzdata ├
Please select the city or region corresponding to your time zone.

Time zone:

                    Alaska
                    Aleutian
                    Arizona
                    Central
                    Eastern
                    Hawaii
                    Starke County (Indiana)
                    Michigan
                    Mountain
                    Pacific Ocean
                    Samoa


               <Ok>                   <Cancel>
```

Step 5 Select **OK** to save the settings.

Step 6 Reboot the Crosswork Data Gateway VM so that all processes pick up the new timezone.

Step 7 Log out of the Crosswork Data Gateway VM.

Configure Password Requirements

You can configure the following password requirements:

- Password Strength
- Password History
- Password expiration
- Login Failures

Step 1 From **Change Current System Settings** menu, select **0 Configure Password Requirements**.

Step 2 Select the password requirement you want to change.

Set the options you want to change:

- **Password Strength**
  - Min Number of Classes
  - Min Length
  - Min Changed Characters

    - Max Digit Credit
    - Max Upper Case Letter Credit
    - Max Lower Case Letter Credit
    - Max Other Character Credit
    - Max Monotonic Sequence
    - Max Same Consecutive Characters
    - Max Same Class Consecutive Characters

- **Password History**
    - Change Retries
    - History Depth
- **Password expiration**
    - Min Days
    - Max Days
    - Warn Days
- **Login Failures**
    - Login Failures
    - Initial Block Time (sec)
    - Address Cache Time (sec)

Step 3 Click **OK** to save the settings.

Configure Simultaneous Login Limits

By default, Crosswork Data Gateway supports 10 simultaneous sessions for the **dg-admin** and **dg-oper** user on each VM. To change this:

Step 1 From the **Change Current System Settings** menu, select **a Configure Simultaneous Login Limits**.

Step 2 In the window that appears, enter the number of simultaneous sessions for the **dg-admin** and **dg-oper** user.

Step 3 Select **Ok** to save your changes.

Configure Idle Timeout

Step 1 From the **Change Current System Settings** menu, select **b Configure Idle Timeout**.

Step 2 Enter the new value of idle timeout in the window that appears.

Step 3 Enter **Ok** to save your changes.

Configure Remote Auditd Server

Use this procedure to configure the auditd daemon export to a remote server.

Step 1 From the **Change Current System Settings** menu, select **c Configure auditd**.

Step 2 Enter the following details:

- Remote auditd server address.
- Remote auditd server port.

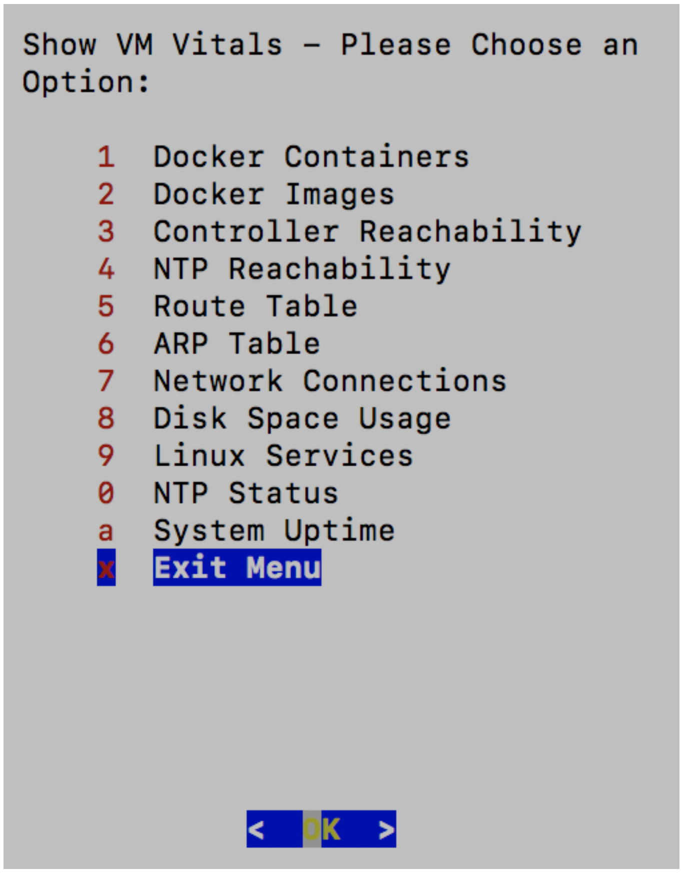
Step 3 Select **OK** to save your changes.

View Crosswork Data Gateway Vitals

Follow these steps to view Cisco Crosswork Data Gateway vitals:

Step 1 From the Main Menu, select **4 Vitals**.

Step 2 From the **Show VM Vitals** menu, select the vital you want to view.



```
Show VM Vitals - Please Choose an
Option:

     1   Docker Containers
     2   Docker Images
     3   Controller Reachability
     4   NTP Reachability
     5   Route Table
     6   ARP Table
     7   Network Connections
     8   Disk Space Usage
     9   Linux Services
     0   NTP Status
     a   System Uptime
     x   Exit Menu


            <  OK  >
```

Vital	Description
Docker Containers	Displays the following vitals for the Docker containers currently instantiated in the system: • Container ID • Image • Name • Command • Created Time • Status • Port

Vital	Description
Docker Images	Displays the following details for the Docker images currently saved in the system: • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status
NTP Reachability	Displays the result of NTP reachability tests: • NTP server resolution • Ping • NTP Status • Current system time
Route Table	Displays IPv4 and IPv6 routing tables.
ARP Table	Displays ARP tables.
Network Connections	Displays the current network connections and listening ports.
Disk Space Usage	Displays the current disk space usage for all partitions.
Linux Services	Displays the status of the following Linux services: • NTP • SSH • Syslog • Docker • Cisco Crosswork Data Gateway Infrastructure containers.
Check NTP Status	Displays the NTP server status.

Vital	Description
Check System Uptime	Displays the system uptime.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu.

Note The image shows the Troubleshooting Menu corresponding to **dg-admin** user. Few of these options are not available to **dg-oper** user. See Table Table 1: Permissions Per Role, on page 3.

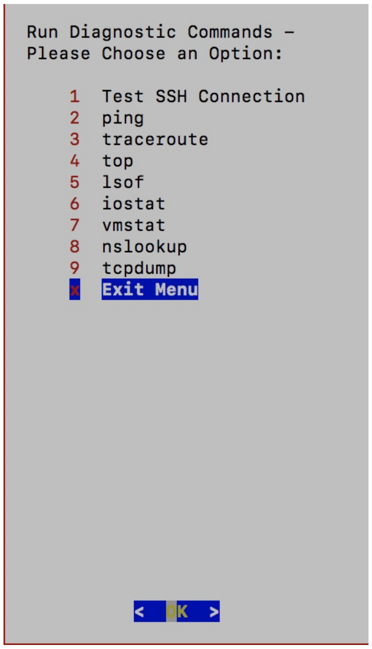
The **Troubleshooting** menu that provides you the following options:

- Run Diagnostic Commands, on page 17
- Run show-tech, on page 20
- Shutdown the Crosswork Data Gateway VM, on page 20
- Export auditd Logs, on page 20
- Enable TAC Shell Access, on page 21

Run Diagnostic Commands

The **Run Diagnostics** menu provides you the following options in the console:

Figure 1: Run Diagnostics Menu



```
Run Diagnostic Commands –
Please Choose an Option:

    1  Test SSH Connection
    2  ping
    3  traceroute
    4  top
    5  lsof
    6  iostat
    7  vmstat
    8  nslookup
    9  tcpdump
    x  Exit Menu

             <  OK  >
```

Ping a Host

Crosswork Data Gateway provides you ping utility that can be used to check reachability to any IP address.

Step 1 From **Run Diagnostics** menu, select **2 ping**.

Step 2 Enter the following information:

- Number of pings
- Destination hostname or IP
- Source port (UDP, TCP, TCP Connect)
- Destination port (UDP, TCP, TCP Connect)

Step 3 Click **OK**.

Traceroute to a Host

Crosswork Data Gateway provides **traceroute** option to help troubleshoot latency issues. Using this option provides you a rough time estimate for the Crosswork Data Gateway to reach the destination.

Step 1 From **Run Diagnostics** menu, select **3 traceroute**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Command Options to Troubleshoot

Crosswork Data Gateway provides several commands for troubleshooting.

Step 1 Navigate to **5 Troubleshooting** > **1 Run Diagnostics**.

Step 2 Select the command and other option or filters for each of the commands:

- **4 top**
- **5 lsof**
- **6 iostat**
- **7 vmstat**
- **8 nsolookup**

Step 3 Click **Ok**.

Once you have selected all the options, Crosswork Data Gateway clears the screen and runs the command with the specified options.

Download tcpdump

Crosswork Data Gateway provides the tcpdump option that allows you to capture and analyze network traffic.

Note This task can only be performed by a **dg-admin** user.

Step 1 Go to **5 Troubleshooting** > **Run Diagnostics** > **9 tcpdump**.

Step 2 Select an interface to run the tcpdump utility. Select the **All** option to run it for all interfaces.

Step 3 Select the appropriate checkbox to view the packet information on the screen or save the captured packets to a file.

Step 4 Enter the following details and click **Ok**.

- Packet count limit
- Collection time limit
- File size limit
- Filter expression

Depending on the option you choose, Crosswork Data Gateway displays the packet capture information on the screen or saves it to a file. Once the tcpdump utility reaches the specified limit, Crosswork Data Gateway compresses the file and prompts for the SCP credentials to transfer the file to a remote host. The compressesd file is deleted once the transfer is complete or if you've decided to cancel the file transfer before completion.

Run show-tech

Crosswork Data Gateway provides the option **show_tech** to export its log files to a user-defined SCP destination.

The collected data includes the following:

- Logs of all the Data Gateway components running on Docker containers
- VM Vitals

It creates a tarball in the directory where it is executed. The output is a tarball named `DG-<CDG version>-<CDG host name>-year-month-day--hour-minute-second.tar.xz.enc`.

The execution of this command may take several minutes depending on the state of Crosswork Data Gateway.

Step 1 From **Troubleshooting** menu, select **5 Show-tech** and click **OK**.

Step 2 Enter the destination to save the tarball containing logs and vitals.

Step 3 Enter your SCP passphrase and click **OK**.

The showtech file downloads in an encrypted format.

Note Depending on how long the system was in use, it may take several minutes to download the showtech file.

Step 4 After the download is complete run the following command to decrypt it:

Note In order to decrpyt the file, you must use OpenSSL version 1.1.1i. Use the command `openssl version` to check the openssl version on your system.

To decrypt the file on a MAC, you must install OpenSSL 1.1.1+. This is because LibreSSL's `openssl` command does not support all the switches supported by OpenSSL's `openssl` command.

```
openssl enc -d -AES-256-CBC -pbkdf2 -md sha512 -iter 100000 -in <showtech file> -out <decrypted
filename> -pass pass:<password>
```

Shutdown the Crosswork Data Gateway VM

From the **Troubleshooting** Menu, select **5 Shutdown VM** to power off the Crosswork Data Gateway VM.

Export auditd Logs

Follow the steps to export auditd logs:

Step 1 From **Troubleshooting**, select **9 Export audit Logs**.

Step 2 Enter a passphrase for auditd log tarball encryption.

Step 3 Click **OK**.

Remove Rotated Log Files

Use this procedure to removes all rotated log files (*.gz or *.xz) in the `/var/log` and `/opt/dg/log` folders.

Step 1 From **Troubleshooting** menu, select **8 Remove Rotated Log files**.

Step 2 Select **Yes** in the dialog that appears to save your changes.

Enable TAC Shell Access

The TAC Shell Access function allows a Cisco engineer to directly log in to the Ubuntu shell via multifactor authentication, using a reserved user named **dg-tac**.

Initially, the **dg-tac** user account is locked and password is expired to prevent the user from getting a shell prompt. Once enabled, the dg-tac user is active until the next calendar day, 12:00 a.m UTC (midnight UTC), which is less than 24 hours.

The steps to enable the **dg-tac** user are as follows:

Note Enabling this access requires you to communicate actively with the Cisco engineer.

Before you begin

Ensure that the Cisco engineer who is working with you has access to the SWIMS Aberto tool.

Step 1 Log in to the Data Gateway VM as the **dg-admin** user.

Step 2 From the main menu, select **5 Troubleshooting**.

Step 3 From the **Troubleshooting** menu, select **t Enable TAC Shell Access**.

A dialog appears, warning that the **dg-tac** user login requires a password that you set and a response to a challenge token from TAC. At this point, you may answer **No** to stop the enable process or **Yes** to continue.

Step 4 If you continue, the system prompts for a new password to use and shows the day when the account disables itself.

Step 5 Enter a password to unlock the account in the console menu.

Step 6 Log out of the Crosswork Data Gateway.

Step 7 Follow these steps if the Crosswork Data Gateway VM can be accessed by the Cisco engineer directly. Move to **Step 8** otherwise.

a) Share the password that you had set in Step 5 for the **dg-tac** user with the Cisco engineer who is working with you.

b) The Cisco engineer logs in as the **dg-tac** user Via SSH with the password you had set.

After entering the password, the system presents the challenge token. The Cisco engineer signs the challenge token using the SWIMS Aberto tool and pastes the signed response to the challenge token back at the Crosswork Data Gateway VM.

c) The Cisco engineer logs in successfully as the **dg-tac** user and completes the troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

d) After troubleshooting is complete, the Cisco engineer logs out of the TAC shell.

Step 8 If Crosswork Data Gateway VM cannot be accessed directly by the Cisco engineer, start a meeting with the Cisco engineer with desktop sharing enabled.

a) Log in as the **dg-tac** user Via SSH using the following command:

```
ssh dg-tac@<DG hostname or IP>
```

b) Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. Share this token with the Cisco engineer who will then sign the token using the SWIMS Aberto tool and share the response with you.

c) Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt.

d) Share your desktop or follow the Cisco engineer's instructions for troubleshooting.

There is a 15-minute idle timeout period for the **dg-tac** user. If logged out, the Cisco engineer needs to sign a new challenge to log in again.

e) Log out of the TAC shell after troubleshooting is complete.

Audit TAC Shell Events

Timestamp information of the following list of TAC shell events is logged to the **tac_shell.log** file. The Tac shell events are also sent to the Crosswork Cloud controller.

- TAC shell enabled
- TAC shell disabled
- dg-tac login
- dg-tac log out

If the Data Gateway is unable to connect to the Crosswork Cloud controller, the TAC shell events are logged in the `/opt/dg/data/controller-gateway/audit/pending` folder. Once the Crosswork Cloud controller is reachable, these events are sent within 5 minutes.

The **tac_shell.log** file is available in the showtech bundle of the Crosswork Data Gateway VM.