



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 (the controller application could be Cisco Crosswork Infrastructure or 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:

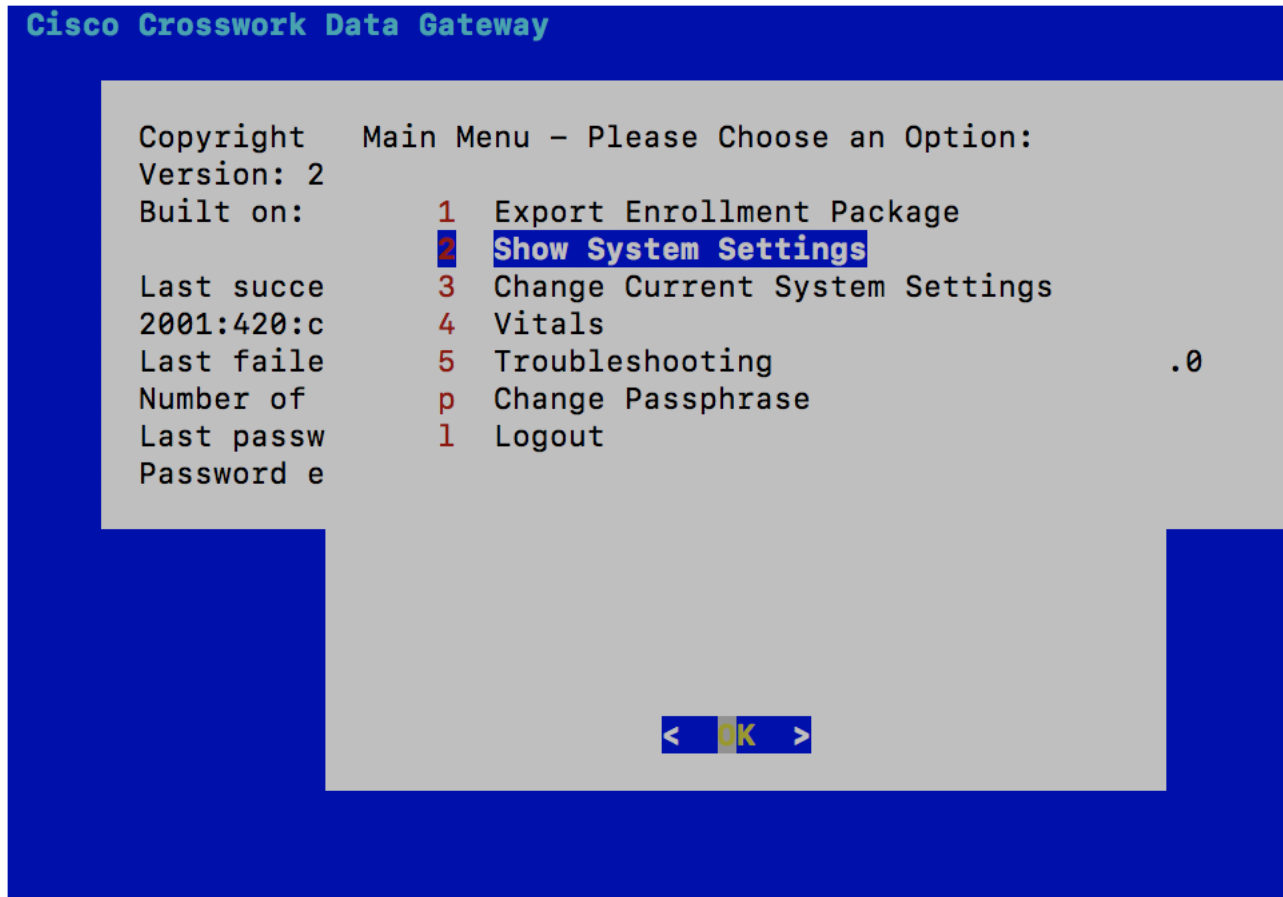
- [Use the Interactive Console, on page 1](#)
- [Manage Crosswork Data Gateway Users, on page 2](#)
- [View Current System Settings, on page 5](#)
- [Change Current System Settings, on page 6](#)
- [View Crosswork Data Gateway Vitals, on page 13](#)
- [Troubleshooting Crosswork Data Gateway VM, on page 14](#)

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 1: Permissions Per Role, on page 3](#).



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 start/shut down Cisco Crosswork Data Gateway, register an application, apply authentication certificates, configure server settings, and perform kernel upgrade.
- **Operator:** The **dg-oper** user is also created by default during the initial VM bring up. Operator can review the state/health of the Cisco Crosswork Data Gateway, retrieve health/error logs, receive error notifications and run connectivity tests between Cisco Crosswork Data Gateway instance and the output destination.



Note

- Both users' credentials are configured 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
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		
Vitals		
Docker Containers	✓	✓
Docker Images		
Controller Reachability		
NTP Reachability		
Route Table		
ARP Table		
Network Connections		
Disk Space Usage		
Linux services		
Troubleshooting		
Ping a Host	✓	✓
Traceroute to a Host	✓	✓
NTP Status	✓	✓
System Uptime	✓	✓
Run show-tech	✓	✓
Remove All Collectors and Reboot VM	✓	×
Reboot VM	✓	×
Test SSH Connection	✓	✓
Export auditd logs	✓	✓
Re-enroll Data Gateway	✓	✓
Enable TAC Shell Access	✓	×

Permissions	Administrator	Operator
Change Passphrase	✓	✓

Change Password

Both administrator 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:

- vNIC Addresses
- NTP
- DNS
- Proxy
- UUID
- Syslog
- Certificates
- First Boot Provisioning Log
- Timezone

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.

Setting Option	Description
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: <ul style="list-style-type: none"> • 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

**Note**

- Crosswork Data Gateway system settings can only be configured by the administrator.

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 16](#). 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 13](#). 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/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/IPv6 subnet in CIDR format.
- Step 6** Click **OK** to save the settings.
-

Configure Syslog



Note For any Syslog server configuration with IPv4/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 address, 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 certificate 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.

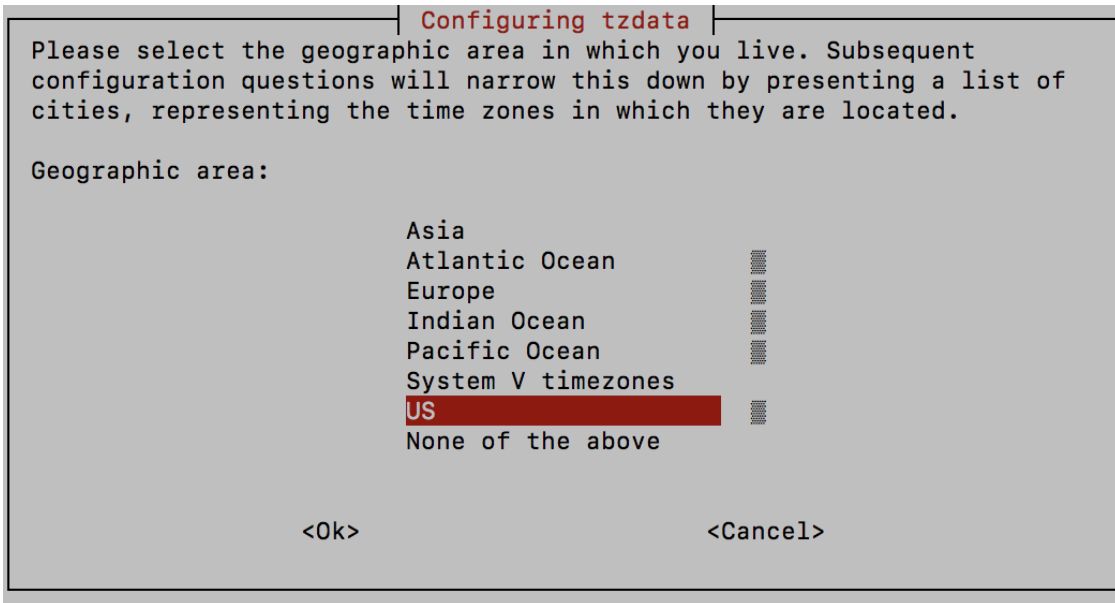
-
- Step 1** From the **Change Current System Settings** menu, select **8 Configure vNIC1 MTU**.
- Step 2** Enter vNIC2 MTU value.
- Step 3** Click **OK** to save the settings.
-

Configure Timezone

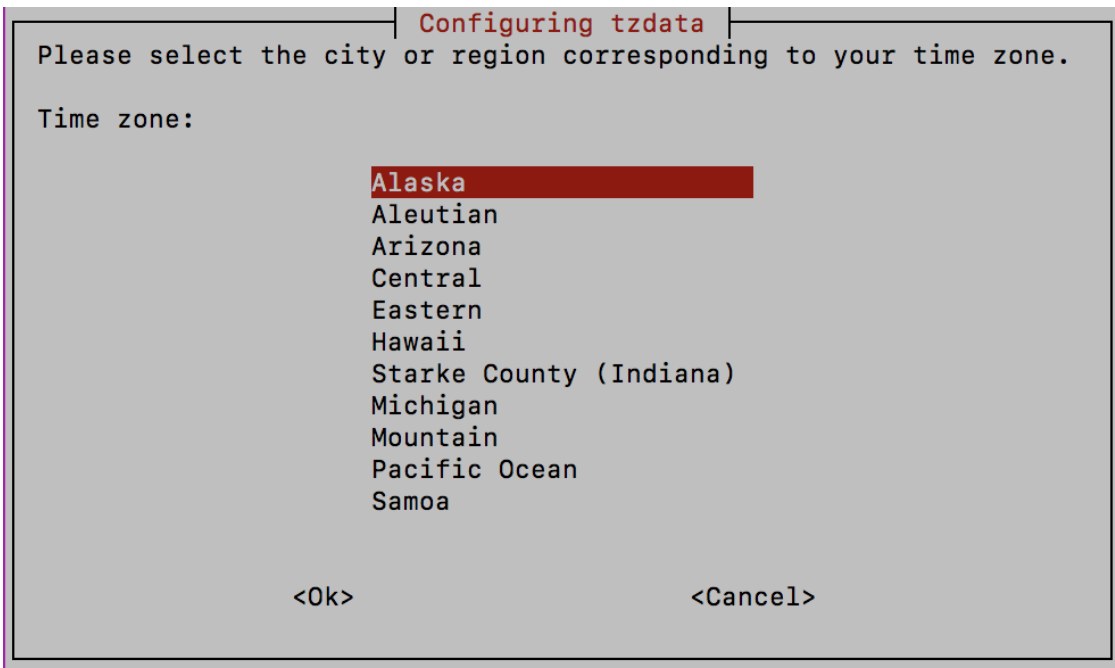
The Crosswork Data Gateway first launches with default timezone as UTC.

Follow the steps to configure timezone:

-
- Step 1** In Crosswork Data Gateway VM interactive menu, select **Change Current System Settings**.
- Step 2** Select **9 Configure Timezone**.
- Step 3** Select the geographic area in which you live.



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



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.

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.

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.

Vital	Description
Docker Containers	Displays the following vitals for the docker containers currently instantiated in the system: <ul style="list-style-type: none"> • Container ID • Image • Name • Command • Created Time • Status • Port
Docker Images	Displays the following details for the docker images currently saved in the system: <ul style="list-style-type: none"> • Repository • Image ID • Created Time • Size • Tag
Controller Reachability	Displays the results of controller reachability test run: <ul style="list-style-type: none"> • Default IPv4 gateway • Default IPv6 gateway • DNS server • Controller • Controller session status

Vital	Description
NTP Reachability	Displays the result of NTP reachability tests: <ul style="list-style-type: none"> • 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: <ul style="list-style-type: none"> • NTP • SSH • Syslog • Docker • Cisco Crosswork Data Gateway Infrastructure containers.

Troubleshooting Crosswork Data Gateway VM

To access **Troubleshooting** menu, select **5 Troubleshooting** from the Main Menu as shown in the following figure:



Note The following figure 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:

- [Ping a Host, on page 15](#)
- [Traceroute to a Host, on page 15](#)
- [Check NTP Status, on page 15](#)
- [Check System Uptime, on page 16](#)

- [Run show-tech, on page 16](#)
- [Reboot Crosswork Data Gateway VM, on page 17](#)
- [Test SSH Connection, on page 16](#)
- [Export auditd Logs, on page 17](#)
- [Enable TAC Shell Access, on page 17](#)

Ping a Host

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

Step 1 From **Troubleshooting** menu, select **1 Ping a Host**.

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

Step 1 From **Troubleshooting** menu, select **2 Traceroute to a Host**.

Step 2 Enter the traceroute destination.

Step 3 Click **OK**.

Check NTP Status

Use this option to check the status of the NTP server.

Step 1 From **Troubleshooting** menu, select **3 NTP Status**.

Step 2 Click **OK**. The cdg displays the NTP server status.

Check System Uptime

Follow the steps to check system uptime since last reboot.

-
- Step 1** From **Troubleshooting** menu, select **4 System Uptime**.
- Step 2** Click **OK**. The Crosswork Data Gateway displays the system uptime.
-

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**.
-

Test SSH Connection

This operation attempts an SSH connection with full debugging enabled on the client side.

1. From **Troubleshooting** menu, select **8 Test SSH**.
2. Enter the following details:
 - Port
 - Host
 - Username
 - Passphrase
3. Click **OK**.

Reboot Crosswork Data Gateway VM



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

Crosswork Data Gateway gives you two options to reboot the VM:

- **Remove All Collectors and Reboot VM:** Select this option from the **Troubleshooting** menu if you want to remove all the collectors (functional images) and reboot VM. This returns the VM to a state just after initial configuration is complete with only infrastructure containers running.
- **Reboot VM:** Select this option from the **Troubleshooting** menu for a normal reboot.

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**.
-

Re-enroll Crosswork Data Gateway

Follow the steps to re-enroll Crosswork Data Gateway:

Before you begin

The existing Crosswork Data Gateway enrollment must be deleted from the controller prior to re-enrolling.

- Step 1** From **Troubleshooting** menu, select **0 Re-enroll Data Gateway**.
- Step 2** Click **Yes** in the below dialog box.
-

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

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

Step 8 Enter the password that you set for the **dg-tac** user.

After entering the password, the system presents the challenge token. The Cisco engineer must sign this token using the SWIMS Aberto tool.

Step 9 Paste the signed response to the challenge token back to the Crosswork Data Gateway VM and press enter to get the shell prompt. 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.

Step 10 Once the troubleshooting is complete, log out of the TAC shell.
