



DIGI INTERNATIONAL
9350 Excelsior Blvd, Suite 700
Hopkins, MN 55343
952-912-3444 / 877-912-3444
www.digi.com

PCI compliance procedures

1. Install and maintain a firewall configuration to protect cardholder data

1.1. Stateful packet inspection

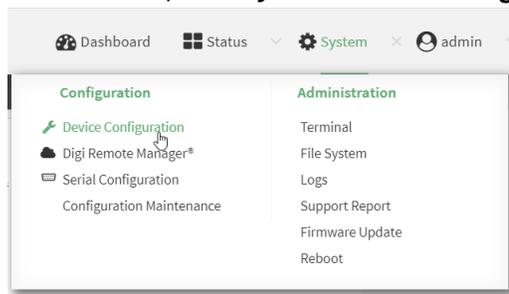
Firewall with stateful packet inspection is enabled by default.

1.2. NAT

NAT is enabled by default on the **External** firewall zone.

To enable NAT on any firewall zone:

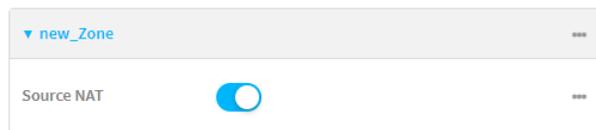
1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Firewall > Zones**.
4. Create a new zone or select an existing zone.



5. Enable **Source NAT**.



6. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> add firewall zone new_Zone
(config firewall zone new_Zone)> src_nat true
(config firewall zone new_Zone)> save
Configuration saved.
>
```

1.3. DMZ

Digi devices with more than one Ethernet port or with Wi-Fi capabilities can be configured to enable DMZ functionality. Each Ethernet port or Wi-Fi access point can be on a separate and distinct network.

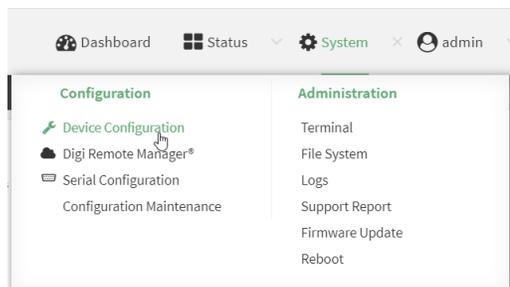
For example, multiple networks can be created, with one Ethernet port set to passthrough mode for point-of-sale (POS) traffic. A device connected to this Ethernet port will receive its IP address directly from an internet connection. Other Ethernet ports can be configured to operate in "router" mode, creating one or more LANs that isolate internal and public traffic from the POS network.

1.3.1. Example configuration

In the following example configuration, a Digi device with multiple Ethernet ports and Wi-Fi SSIDs (such as a TX64 or TX54) is configured to:

- A private network consisting of both an Ethernet device and a Wi-Fi access point.
- A separate public network consisting of both an Ethernet device and a Wi-Fi access point.
- An Ethernet port in passthrough mode for point-of-sale (POS) traffic.

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Configure access points:
 - a. Click **Network > Wi-Fi > Access points**.
 - b. Create an access point or select an existing one.

Add

- c. Select the appropriate **Radio** (for dual-Wi-Fi models), and enter the **SSID** and **Pre-shared key**.

The screenshot shows the configuration page for a private access point. The title is 'private_AP'. The settings are as follows:

- Enable:
- Radio: Wi-Fi1 radio
- SSID: private_SSID
- SSID broadcast:
- Encryption: WPA2 Personal (PSK)
- Pre-shared key: [masked with dots]
- Group rekey interval: 10m

At the bottom, there is an 'Add' button with the text 'Wi-Fi access point' and a plus sign icon.

- d. Repeat for the public access point.

The screenshot shows the configuration page for a public access point. The title is 'public_AP'. The settings are as follows:

- Enable:
- Radio: Wi-Fi2 radio
- SSID: public_SSID
- SSID broadcast:
- Encryption: WPA2 Personal (PSK)
- Pre-shared key: [masked with dots]
- Group rekey interval: 10m

4. Configure bridges:

- e. Disable the default bridge:

- i. Click **Network > Bridges > LAN1**.
- ii. Click **Enable** to disable the bridge.
- iii. Create two new bridges: **private_bridge** and **public_bridge**.

The screenshot shows an input field for adding a new bridge. The text 'private_bridge' is entered into the field, and there is a plus sign icon to the right of the field.

- iv. For **private_bridge**, click to expand **Device**.
- v. Click **Add Device**.
- vi. Select the **ETH2** Ethernet device.
- vii. Click **Add Device** again.

viii. Select the **private_AP** Wi-Fi access point.



ix. Repeat for **public_bridge**, selecting the **ETH3** and Ethernet device and the **public_AP** Wi-Fi access point.



5. Configure VLANs:

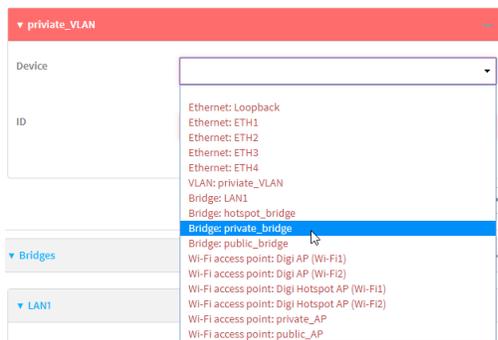
a. Create two new VLANs: **private_VLAN** and **public_VLAN**:

i. Click to expand **Network > Virtual LAN**.

ii. Add the VLANs.



iii. For **private_VLAN**, for Device, select **private_bridge**.



iv. For **public_VLAN**, select **public_bridge**.

NOTE: Make sure that the VLANs' IDs are set to different values.

6. Configure the firewall:

a. Create a **guest_Zone** Firewall zone for the public network:

- i. Click to expand **Firewall > Zone**.
- ii. Add the zone.

Add +

b. Create a packet filter that only allows traffic from the **guest_Zone** to access the **External** zone, thereby blocking all other traffic coming from the **guest_Zone**:

- i. Click to expand **Firewall > Packet filtering**.
- ii. Click **+** to add a packet filter.
- iii. Type a **Label** for the packet filter.
- iv. For **Source** zone, select **guest_Zone**.
- v. For **Destination** zone, select **External**.

7. Configure the LANs:

a. Click to expand **Network > Interfaces**.

b. Add two new interfaces, **private_LAN** and **public_LAN**.

Add +

c. Click to expand **private_LAN**.

- i. For **Zone**, select **Internal**.
- ii. For **Device**, select **private_bridge**.
- iii. Click to expand **IPv4**.
- iv. For **Address**, enter the IP address and subnet mask of the LAN network.

The screenshot shows the configuration page for the 'private_LAN' interface. It is divided into two main sections: 'private_LAN' and 'IPv4'. In the 'private_LAN' section, the 'Enable' toggle is turned on. The 'Interface type' is set to 'Ethernet', the 'Zone' is set to 'Internal', and the 'Device' is set to 'Bridge: private_bridge'. In the 'IPv4' section, the 'Enable' toggle is also turned on. The 'Type' is set to 'Static IP address'. The 'Metric' is 0, 'Weight' is 10, 'Management priority' is 0, and 'MTU' is 1500. The 'Address' field contains '10.10.10.1/24'.

- d. Click to expand **public_LAN**.
 - i. For Zone, select **guest_Zone**.
 - ii. For **Device**, select **public_bridge**.
 - iii. Click to expand **IPv4**.
 - iv. For **Address**, enter the IP address and subnet mask of the LAN network.

- e. Reconfigure the default LAN as a DMZ for the POS network:
 - i. Click to expand **Network > Interface > LAN1**.
 - ii. For **Interface** type, select **IP Passthrough**.
 - iii. For **Device**, select **Ethernet: ETH1**.
 - iv. Click to expand **Source interfaces**.
 - v. For **Interface**, select **WAN1**.
 - vi. Click **+** to add another interface.

Add interface **+**

- vii. Select **WWAN1**.

8. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

1. Log into the Admin CLI as a user with Admin access and enter configuration mode:

```
> config
(config)>
```

2. Configure Wi-Fi access points:

```
(config)> add network wifi ap private_AP
(config network wifi ap private_AP)> radio wifi1
(config network wifi ap private_AP)> ssid private_SSID
(config network wifi ap private_AP)> encryption key_psk2 passcode1
(config network wifi ap public_AP)> add .. public_AP
(config network wifi ap public_AP)> radio wifi2
(config network wifi ap public_AP)> ssid public_SSID
(config network wifi ap public_AP)> encryption key_psk2 passcode2
```

3. Configure network bridges:

```
(config network wifi ap public_AP)> ...
(config)> network bridge lan1 enable false
(config)> add network bridge private_bridge
(config network bridge private_bridge)> add device end /network/device/eth2
(config network bridge private_bridge)> add device end /network/wifi/ap/private_AP
(config network bridge private_bridge)> add .. public_bridge
(config network bridge public_bridge)> add device end /network/device/eth3
(config network bridge public_bridge)> add device end /network/wifi/ap/public_AP
```

4. Configure VLANs:

```
(config network bridge public_bridge)> ...
(config)> add network vlan private_VLAN
(config network vlan private_VLAN)> device /network/bridge/private_bridge
(config network vlan private_VLAN)> id 0
(config network vlan private_VLAN)> add .. public_VLAN
(config network vlan public_VLAN)> device /network/bridge/public_bridge
(config network vlan public_VLAN)> id 1
```

5. Configure the firewall:

```
(config network vlan public_VLAN)> ...
(config)> add firewall zone guest_Zone
(config firewall zone guest_Zone)> ...
(config)> add firewall filter end
(config firewall filter 2)> label guest_Filter
(config firewall filter 2)> src_zone guest_Zone
(config firewall filter 2)> dst_zone external
```

6. Configure the LANs:

```
(config firewall filter 2)> ...
(config)> add network interface private_LAN
(config network interface private_LAN)> zone internal
(config network interface private_LAN)> device /network/bridge/private_bridge
(config network interface private_LAN)> ipv4 address 10.10.10.1/24
(config network interface private_LAN)> add .. public_LAN
(config network interface public_LAN)> zone guest_Zone
(config network interface public_LAN)> device /network/bridge/public_bridge
(config network interface public_LAN)> ipv4 address 10.10.11.1/24
(config network interface public_LAN)> .. lan1
(config network interface lan1)> type passthrough
(config network interface lan1)> device /network/device/eth1
(config network interface lan1)> add passthrough src end wan1
(config network interface lan1)> add passthrough src end wwan1
```

7. Save the configuration:

```
(config network interface lan1)> save
Configuration saved.
>
```

1.4. Further locking down the router entry points

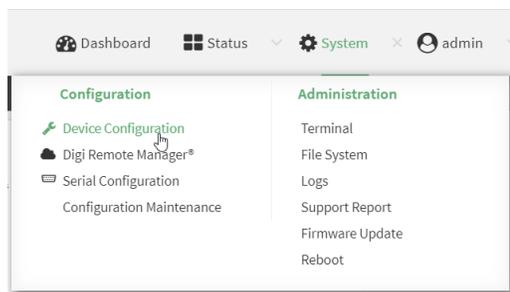
Router entry points can be locked down further by using access control list configuration and firewall rules.

1.4.1. Universal Plug and Play (UPnP)

Universal Plug and Play (UPnP) is disabled by default.

1.4.2. Disable pings to the WAN interface

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Firewall > Custom rules**.
4. **Enable** the rule.
5. For **Rules**, input the following text:

```
iptables -I INPUT -p icmp -m set --match-set zone-external src,src -j DROP
```

6. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> firewall custom enable true
(config)> firewall custom rules "iptables -I INPUT -p icmp -m set --match-set zone-external
src,src -j DROP"
(config)> save
Configuration saved.
>
```

1.4.3. Disable remote administration

Remote administration is disabled by default through the access control list for the **web_admin** and **ssh** services.

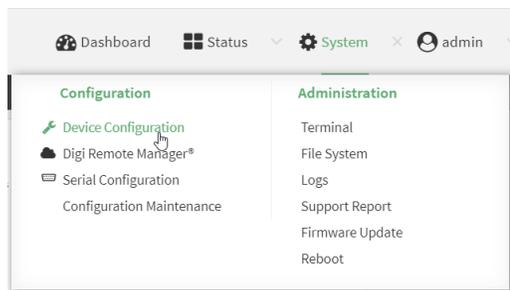
1.4.4. Disable shell access

By default, user accounts that are members of an authentication group with Admin access have access to the Admin CLI, a secure command line interface that allows the user to configure and monitor the device without having access to the underlying operating system.

By default, no user accounts have access to the interactive shell of the underlying operating system. However, the default configuration allows users to be provided access to the interactive shell of the device's operating system.

You can disable the ability for users to be provided access to the interactive shell:

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Authentication**.
4. Click to disable **Allow shell (Warning)**.



NOTE: After disabling the **Allow shell** option, re-enabling the feature will erase the device's configuration and reboot the device.

5. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

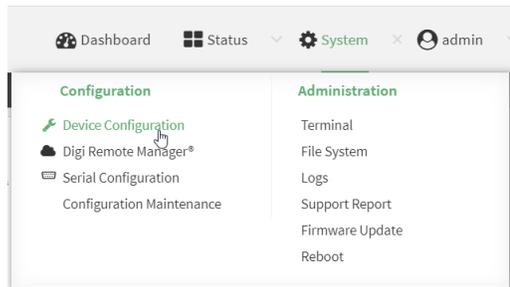
Command line

```
> config
(config)> auth allow_shell enable false
(config)> save
Configuration saved.
>
```

1.4.5. MAC filtering

You can either blacklist MAC addresses, which prevents devices from accessing the interface, or whitelist MAC addresses, which gives devices exclusive access to the interface.

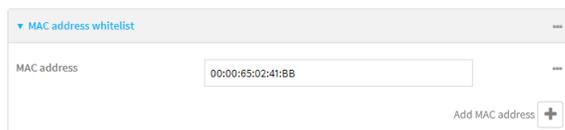
1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Network > Interfaces**.
4. Click to expand the appropriate interface.
5. Click either **MAC address blacklist** or **MAC address whitelist**.
6. Click **+** to add a MAC address.

Add MAC address **+**

7. For **MAC address**, type the MAC address.



8. Click **+** to add additional MAC addresses to the blacklist or whitelist.
9. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> add network interface wan1 mac_blacklist end 00:00:65:02:41:BB
(config)> add network interface wan1 mac_blacklist end 00:00:65:02:41:BC
(config)> save
Configuration saved.
>
```

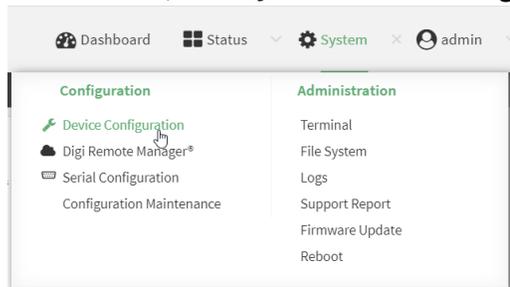
2. Do not use vendor-supplied defaults for system passwords and other security parameters

2.1. Default password for **admin** account

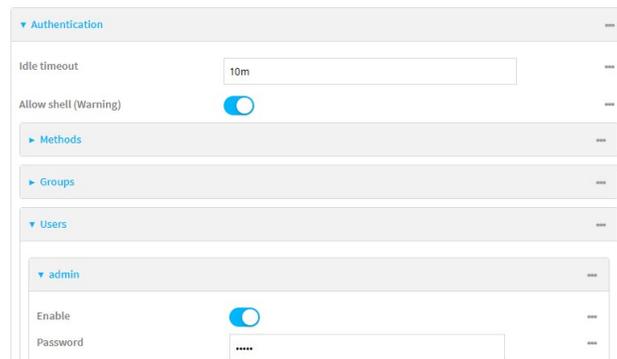
All newly-manufactured Digi devices have a unique default password for the **admin** account. This password must be changed before any configuration changes can be saved.

To change the unique password for the **admin** account:

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Authentication > Users > admin**.
4. For **Password**, type the new password.



5. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> auth user admin password new_password
(config)> save
Configuration saved.
>
```

2.2. User authentication using RADIUS or TACACS+

You can configure your Digi device to use a remote RADIUS or TACACS+ server for user authentication. Multiple authentication methods can be configured, including both remote server and local user authentication. Methods are attempted in the order that they are listed. If local user authentication is not allowed and the remote servers are not accessible, users will not be able to log into the device until the remote server is accessible.

2.2.1. Configure the RADIUS or TACACS+ server

Example FreeRADIUS Configuration

With FreeRADIUS, users are defined in the **users** file in your FreeRADIUS installation. To define users:

1. Open the FreeRadius user file in a text editor. For example:

```
$ sudo gedit /etc/freeradius/3.0/users
```

2. Add users to the file using the following format:

```
user1 Cleartext-Password := "user1"
      Unix-FTP-Group-Names := "admin"
user2 Cleartext-Password := "user2"
      Unix-FTP-Group-Names := "serial"
```

The value of the Unix-FTP-Group-Names attribute must correspond to an authentication group configured on your Digi device.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

```
$ sudo freeradius -CX
```

This should return a message that completes similar to:

```
...  
Configuration appears to be OK
```

5. Restart the FreeRADIUS server:

```
$ sudo freeradius /etc/init.d/freeradius restart
```

Example TACACS+ Configuration

With TACACS+, users are defined in the server configuration file. On Ubuntu, the default location and filename for the server configuration file is **/etc/tacacs+/tac_plus.conf**.

1. Open the TACACS+ server configuration file in a text editor. For example:

```
$ sudo gedit /etc/tacacs+/tac_plus.conf
```

2. Add users to the file using the following format:

```
user = user1 {  
    name = "User1 for TX54"  
    pap = cleartext password1  
    service = system {  
        groupname = admin,serial  
    }  
}  
user = user2 {  
    name = "User2 for TX54"  
    pap = cleartext password2  
    service = system {  
        groupname = serial  
    }  
}
```

The value of the groupname attribute must correspond to an authentication group configured on your Digi device.

3. Save and close the file.
4. Verify that your changes did not introduce any syntax errors:

```
$ sudo tac_plus -C /etc/tacacs+/tac_plus.conf -P
```

If successful, this command will echo the configuration file to standard out. If the command encounters any syntax errors, a message similar to this will display:

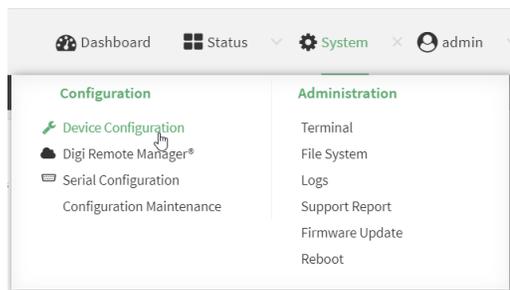
```
Error: Unrecognised token on line 1
```

5. Restart the TACACS+ server:

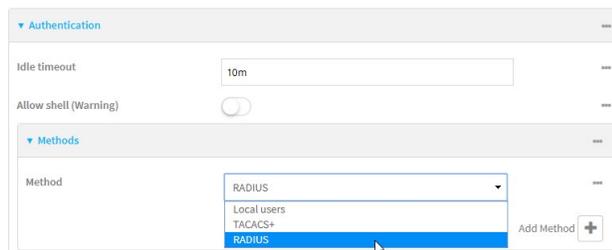
```
$ sudo /etc/init.d/tacacs_plus restart
```

2.2.2. Configure the Digi device for RADIUS or TACACS+ support

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Configure the authentication methods:
 - a. Click **Authentication > Methods**.
 - b. For **Method**, select either **TACACS+** or **RADIUS**.

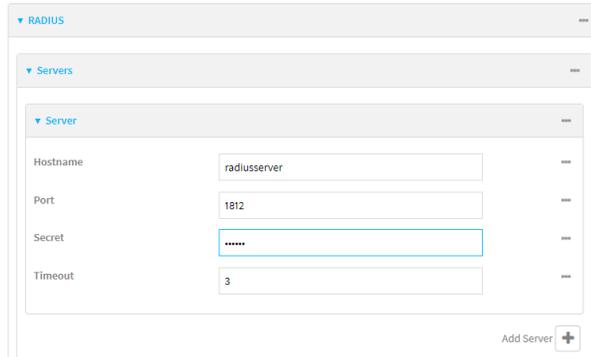


- c. (Optional) Click **+** to add additional authentication methods.

Add Method 

4. Configure RADIUS or TACACS+ support:
 - a. Click **Authentication > RADIUS or TACACS+**.
 - b. Click to expand **Servers**.
 - c. Click **+** to add a remote authentication server.

- d. For **Hostname**, type the hostname or IP address of the RADIUS server.
- e. For **Secret**, type the server's shared secret.



The screenshot shows a web interface for configuring RADIUS servers. It has a hierarchical menu on the left with 'RADIUS' expanded to 'Servers' and then 'Server'. The main area contains a form with the following fields: 'Hostname' with the value 'radiusserver', 'Port' with '1812', 'Secret' with a masked value '.....', and 'Timeout' with '3'. An 'Add Server' button with a plus sign is located at the bottom right of the form.

- f. Click **+** to add additional remote authentication servers. The device attempts to connect to the servers in the order they are listed.
5. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

1. Log into the Admin CLI as a user with Admin access and enter configuration mode:

```
> config
(config)>
```

2. Configure the authentication method:

- a. To use only remote server authentication, delete the default local authentication:

- i. Determine the index number of the authentication method:

```
(config)> show auth method
0 local
```

- ii. Delete the authentication method:

```
(config)> del auth method 0
```

b. Add the remote server authentication method:

- To add the RADIUS remote server authentication method:

```
(config)> add auth method end radius
```

- To add the TACACS+ remote server authentication method:

```
(config)> add auth method end tacacs+
```

3. Configure the RADIUS or TACACS+ support:

- Configure RADIUS server support:

```
(config)> add auth radius server end
(config auth radius server 0)> hostname radiusServer
(config auth radius server 0)> secret radius_secret
(config auth radius server 0)> add .. auth radius server end
(config auth radius server 1)> hostname backupRadiusServer
(config auth radius server 0)> secret radius_secret1
```

- Configure TACACS+ server support:

```
(config)> add auth tacacs+ server end
(config auth tacacs+ server 0)> hostname tacacsServer
(config auth tacacs+ server 0)> secret tacacs_secret
(config auth tacacs+ server 0)> add .. auth tacacs+ server end
(config auth tacacs+ server 1)> hostname backupTacacsServer
(config auth tacacs+ server 0)> secret tacacs_secret1
```

4. Save the configuration:

```
(config network interface lan1)> save
Configuration saved.
>
```

3. Track and monitor access to the Digi device

3.1. System and event logs

Messages about attempts to connect to the device are in the **System** log and are similar to:

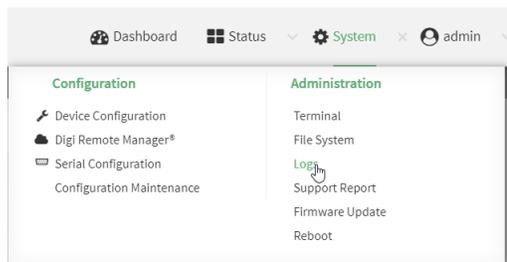
```
Apr 16 14:42:38 TX64 Apr 16 14:42:38 0040FF800120 us:
name=admin~service=sshd~state=opened~remote=192.168.0.100~tty=ssh
Apr 16 14:43:24 TX64 stunnel: LOG5[279]: Service [service.web_admin] accepted connection
from ::ffff:192.168.3.107:51039
```

Messages about firmware version, system uptime, and related information are in the **Events** log:

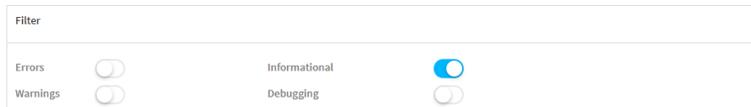
```
Apr 16 13:38:40 status firmware version=20.2.162.90 mac=000000000000 serial=TX64-
000000 uptime=10 days, 16 hours, 41 minutes, 3 seconds sku=WR64-A121
```

3.1.1. View system and event logs

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Administration**, click **Logs**.



3. (Optional) Filter the System log for informational messages. Messages about attempts to access the device are logged as informational messages.
 - a. Under **System Logs**, for **Filter**, click to deselect **Errors** and **Warnings**.



- b. To limit the output to events related to accessing the device:
 - i. In the search box, type **service**.



Command line

To view the system log from the Admin CLI:

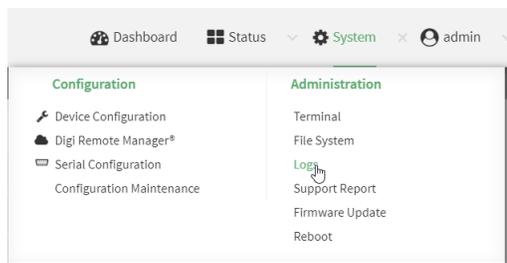
```
> show log
Apr 16 15:49:56 TX64 mm: interface_wwan2 SIM failover: SIM slot switch successful
Apr 16 15:49:56 TX64 netifd: Interface 'interface_wwan2' is now down
Apr 16 15:49:56 TX64 netifd: Interface 'interface_wwan2' is setting up now
```

To filter the output to informational messages:

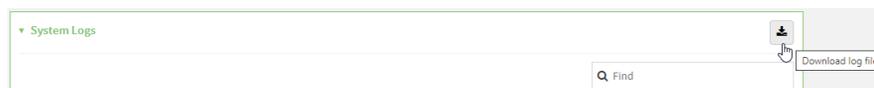
```
> show log filter info
Apr 16 15:54:58 TX64 firewalld[777]: reloading status
Apr 16 15:55:39 TX64 kernel: DROP (filter): IN=eth1 OUT=
MAC=01:00:5e:00:00:01:00:40:ff:80:23:b0:08:00 SRC=0.0.0.0 DST=224.0.0.1 LEN=32 TOS=0x00
PREC=0xC0 TTL=1 ID=0 DF PROTO=2
```

3.1.2. Download system and event logs

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Administration**, click **Logs**.



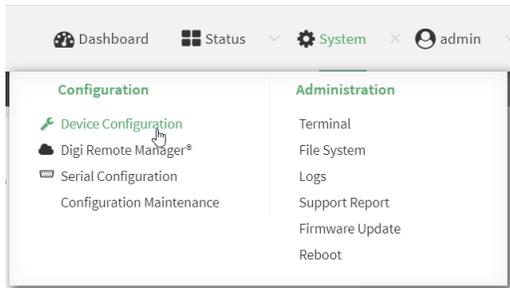
3. Click  to download a local copy of the log file.



3.1.3. Configure an external log server

You can also configure Digi devices to send log messages to a remote log server.

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **System > Log > Server list**.
4. Click **+** to add a remote log server.



5. For **Server**, type the hostname or IP address of the server.
6. (Optional) Select the types of messages to be sent to the server.
7. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

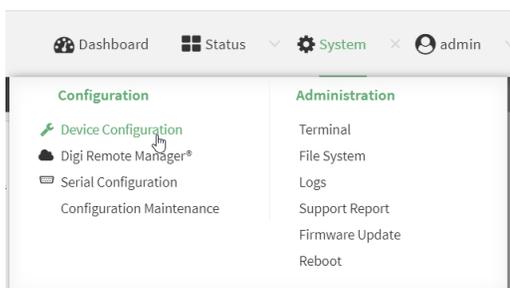
Command line

```
> config
(config)> add system log remote end
(config system log remote 0)> server logserverhostname
(config system log remote 0)> save
Configuration saved.
>
```

3.1.4. Configure the type of events to be logged

By default, all event types are logged. You can omit certain events from the log, and also configure the interval in which events are logged.

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **System > Log > Event categories**.

4. Click to expand a category to configure the event logging for that category. For example, to configure event logging for firmware-related events:
 - a. Click to expand **Firmware**.



- b. Click **Enable error events** to disable, or click **Enable status events** to disable.
 - c. For **Status interval**, change the default amount of time between periodic status events.
 - d. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

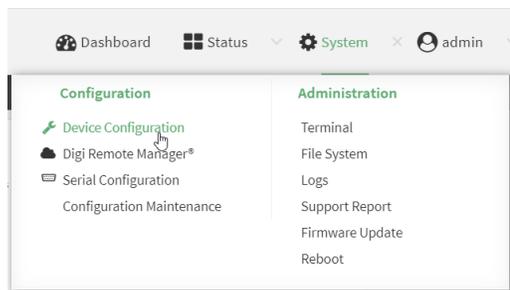
Command line

```
> config
(config)> system log event firmware
(config system log event firmware)> show
error true
status true
status_interval 30m
(config system log event firmware)> status false
(config system log event firmware)> status_interval 10m
(config system log event firmware)> save
Configuration saved.
>
```

3.1.5. Time synchronization

By default, Digi devices synchronize their time with the Digi NTP server, time.devicecloud.com. You can change the NTP server used by the device, or add additional servers. You can also change the device's time zone.

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **System > Time**.

4. For **Timezone**, select the appropriate time zone for the device.
5. Click to expand **NTP servers**.
6. (Optional) For Server, type the hostname or IP address of an alternate NTP server.
7. Click **+** to add additional NTP servers.

Add Server 

8. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> system time timezone ?
...
Pacific/Saipan
Pacific/Tahiti
Pacific/Tarawa
Pacific/Tongatapu
Pacific/Wake
Pacific/Wallis
UTC
Default value: UTC
Current value: UTC

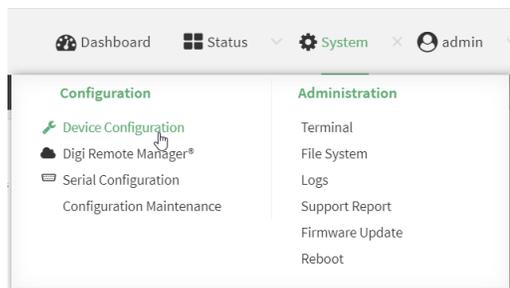
(config)> system time timezone America/Chicago
(config)> system time ntp server 0 time-a-wwv.nist.gov
(config)> add system time ntp server end time-b-wwv.nist.gov
(config)> save
Configuration saved.
>
```

3.2. SNMP support

Digi devices support Simple Network Management Protocol version 3 (SNMPv3). By default, support is not enabled.

To enable and configure SNMPv3:

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Service > SNMP**.
4. **Enable** SNMP.
5. Type the **Username** used to connect to the SNMP agent.
6. Type the **Password** used to connect to the SNMP agent.
7. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

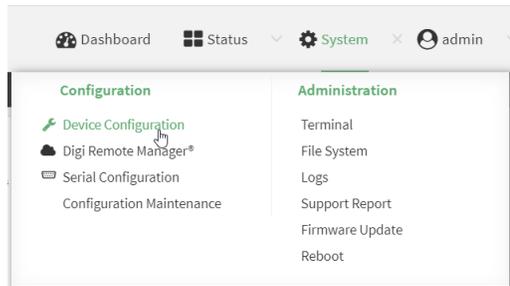
Command line

```
> config
(config)> service snmp enable true
(config)> service snmp username snmp-name
(config)> service snmp password snmp-password
(config)> save
Configuration saved.
>
```

4. SSL certificates for web-based management

By default, Digi devices use an automatically generated, self-signed certificate. You can configure the WebUI to use a certificate signed by a Certificate Authority (CA).

1. Log into the WebUI as a user with full Admin access rights.
2. On the menu, click **System**. Under **Configuration**, click **Device Configuration**.



3. Click **Service > Web administration**.
4. For **SSL certificate**, paste the contents of the certificate and private key in PEM format.
5. Click **Apply** to save the configuration and apply the change.

The **Apply** button is located at the top of the WebUI page. You may need to scroll to the top of the page to locate it.

Command line

```
> config
(config)> service web_admin cert <paste content of certificate and private key in PEM
format>
(config)> save
Configuration saved.
>
```