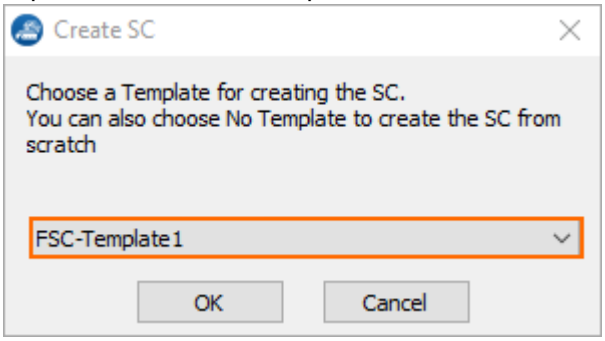
Secure Connector Setup and Configuration

https://campus.barracuda.com/doc/91128302/

To deploy a Secure Connector, configure the Secure Connector device via the SCA Editor in the Control Center, or add a Secure Connector Configuration using a configuration template. Configuration settings configured via a template are automatically used and cannot be configured on a per-device basis. For more information, see Configure a Secure Connector via Templates. To configure a Secure Connector via the SCA Editor, perform the following steps.

Step 1. Add a Secure Connector Configuration

1. Go to ***your cluster*** **> Cluster Settings > Secure Connector Editor**.
2. Click **Lock**.
3. Click **Add SC**.
4. (optional) Select a template.

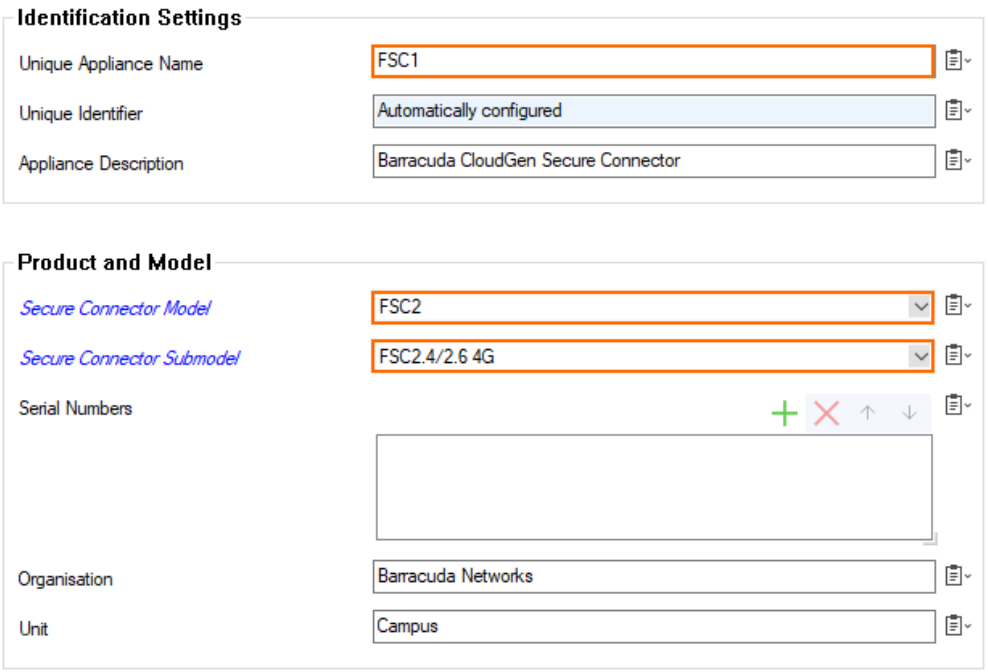


5. Click **OK**. The **Create SC** window opens.

Step 2. Configure the Settings for the Secure Connector

Configure Identification Settings

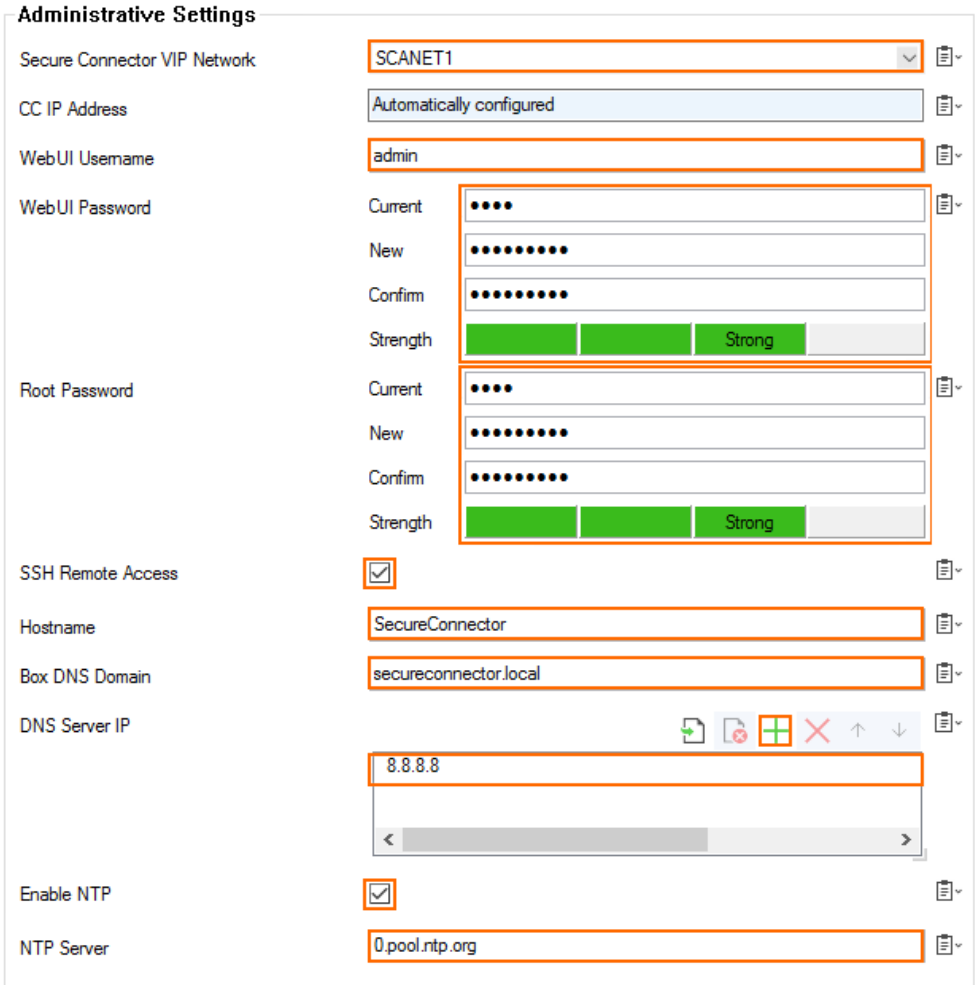
1. Enter a **Unique Appliance Name** for the Secure Connector. The name is final and cannot be changed later.
   The **Unique Identifier** is a string containing the range, cluster, and unique appliance name.
2. (optional) Enter a description for the Secure Connector.
3. From the **Secure Connector Model** drop-down list, select the hardware version. E.g., **FSC2**.
4. From The **Secure Connector Submodel** drop-down list, select the applicable submodel. E.g., **FSC2.4/2.6 4G**.



5. Click **+** to add the serial number of the Secure Connectors allowed to connect with this configuration.
6. (optional) Enter your company details and specify the location and time zone of the Secure Connector unit.

Configure Administrative Settings

1. In the left menu, click **Administrative Settings**.
2. Select the Secure Connector data network from the **Secure Connector VIP Network** drop-down list. The Secure Connector is automatically assigned to the Access Controller associated with the Secure Connector network.
3. Set the **WebUI Username/Password** for the web interface of the Secure Connector.
4. Enter the **Root Password** for the Secure Connector. The default root password is: `ngf1r3wall`
   The default password is intended for initial access only. You must change the password once you are logged into the Secure Connector. For more information, see How to Change the Root Password and Management ACL.
5. Select the **SSH Remote Access** check box to enable SSH. You must also create an Secure Connector management rule to be able to log in via SSH. For more information, see How to Create Secure Connector Firewall Management Rules.
6. Enter the **Hostname** used for the Secure Connector. You can use the same hostname for all Secure Connectors.
7. In the **Box DNS Domain** field, enter the domain for the Secure Connector.
8. Next to **DNS Server IP**, click **+** to enter the IP addresses for the DNS servers.
9. Select the **Enable NTP** check box to synchronize the time with an NTP server.
10. Enter the FQDN or IP address for the **NTP Server** located near your location. Default: `0.pool.ntp.org`



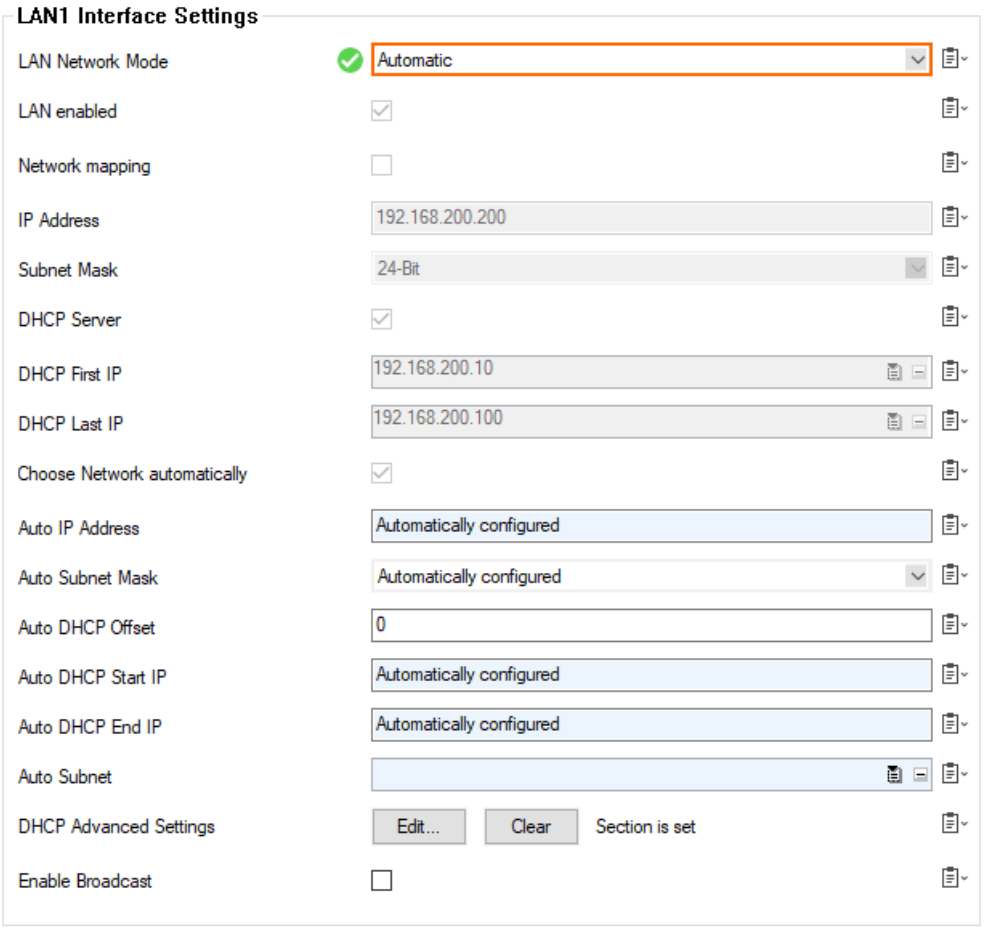
Configure WAN Settings

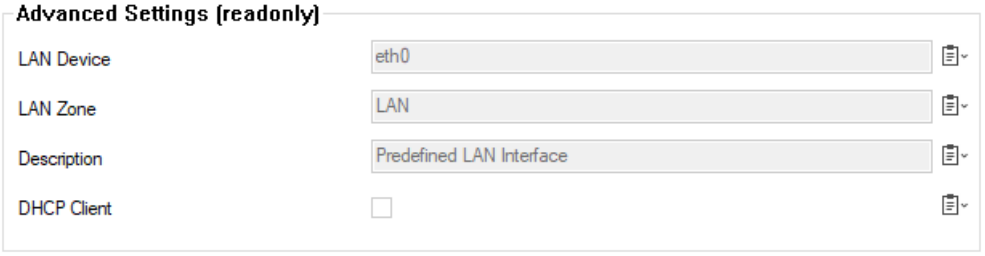
1. In the left menu, click **WAN Settings**.
2. From the **WAN Network Mode** drop-down list, select **Manual** or **DHCP Client**.
3. Configure the WAN connection for the WAN port. For more information, see Secure Connector WAN Connections.

Configure LAN Settings

1. In the left menu, click **LAN Settings**.
2. Select the **LAN Network Mode**:
   - **Manual** – The network must be entered manually. Devices behind the Secure Connector require a static IP address.
   - **Manual (Mapped)** – The network is entered manually. Devices behind the Secure Connector require a static IP address. The static network is mapped to an automatically assigned subnet out of the Secure Connector data network.
   - **DHCP-Server** – The network is entered manually. Devices behind the Secure Connector receive an IP address from the DHCP server on the Secure Connector.
   - **DHCP-Server (Mapped)** – The network is entered manually. Devices behind the Secure

Connector receive an IP address from the DHCP server on the Secure Connector. The network is mapped to an automatically assigned subnet out of the Secure Connector data network.
- **Automatic** – The network assigned to the Secure Connector is assigned automatically by the Control Center.





Configure Wi-Fi Settings (SC1, SC2.1, SC2.3, SC2.5, SC2.7)

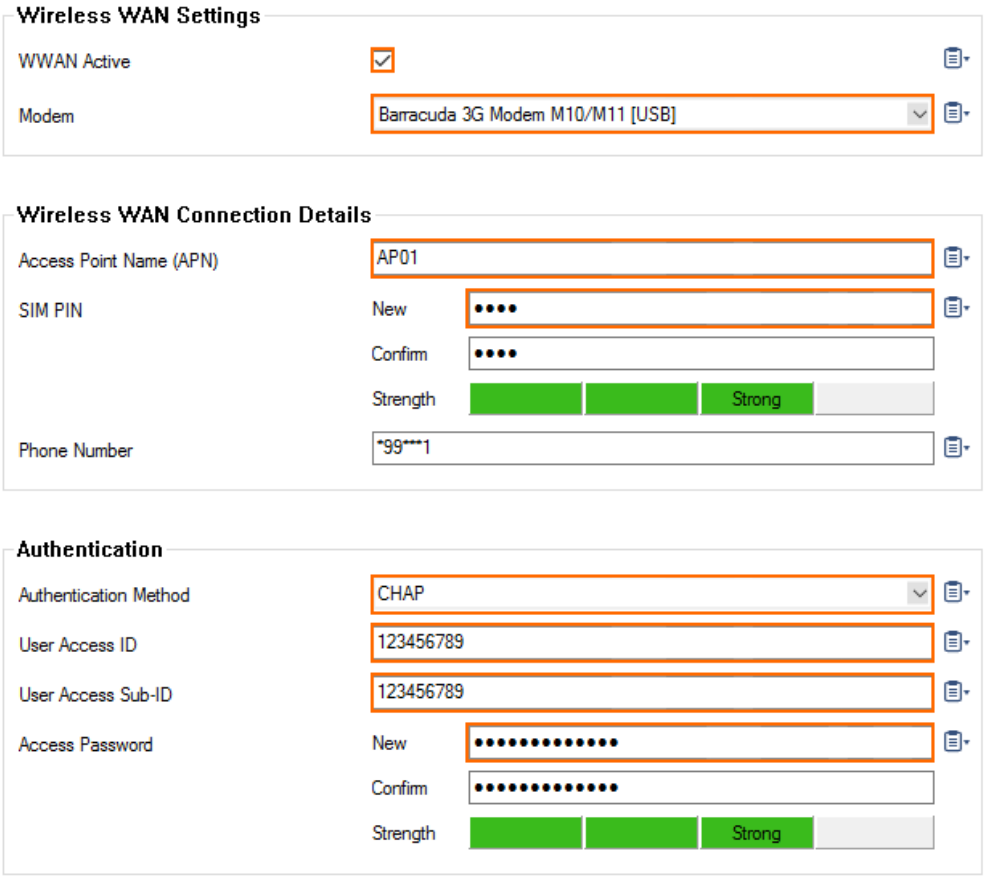
1. In the left menu, click **Wi-Fi Settings**.
2. Select the **Wi-Fi Mode**:
   - **Access Point Mapped** – Manual Wi-Fi network configuration mapped to a Secure Connector data network assigned by the Control Center.
   - **Access Point Manual** – Manual Wi-Fi network configuration.

- **Access Point Automatic** – The Control Center automatically assigns a data network to the Wi-Fi network of the SC.
- **Wi-Fi Client** – Select to use the Wi-Fi interface as a WAN interface.

For more information, see Secure Connector Wi-Fi Access Point or Secure Connector WAN Connections.

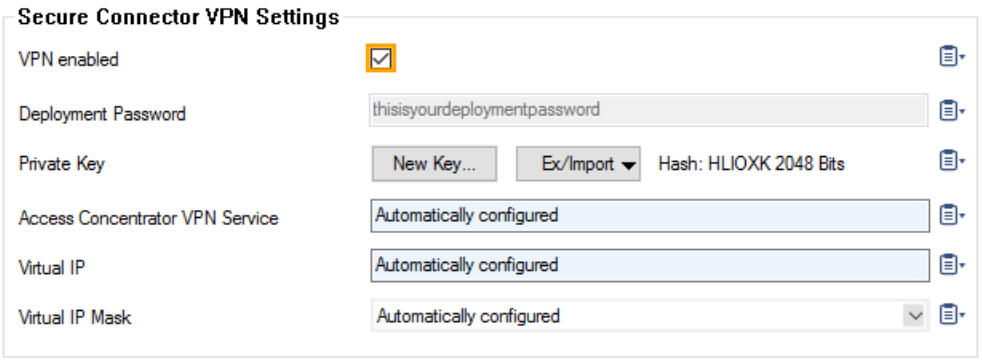
Configure Wireless WAN Settings (SC2.2, SC2.3, SC2.4, SC2.5, SC2.6, SC2.7)

1. In the left menu, click **Wireless WAN Settings**.
2. Select the **WWAN Active** check box.
3. Select the **Modem**.
4. Enter the name of the WWAN access point you wish to connect to.
5. If applicable, enter the unlocking PIN code for your SIM card.
6. Enter the **Phone Number** number without the trailing hash (#).
7. Select the **Authentication Method**.
8. Enter the **User Access ID** assigned by your WWAN service provider.
9. (optional) Enter the **User Access Sub-ID** assigned by your WWAN service provider.
10. Enter the **Access Password** assigned by your WWAN service provider.

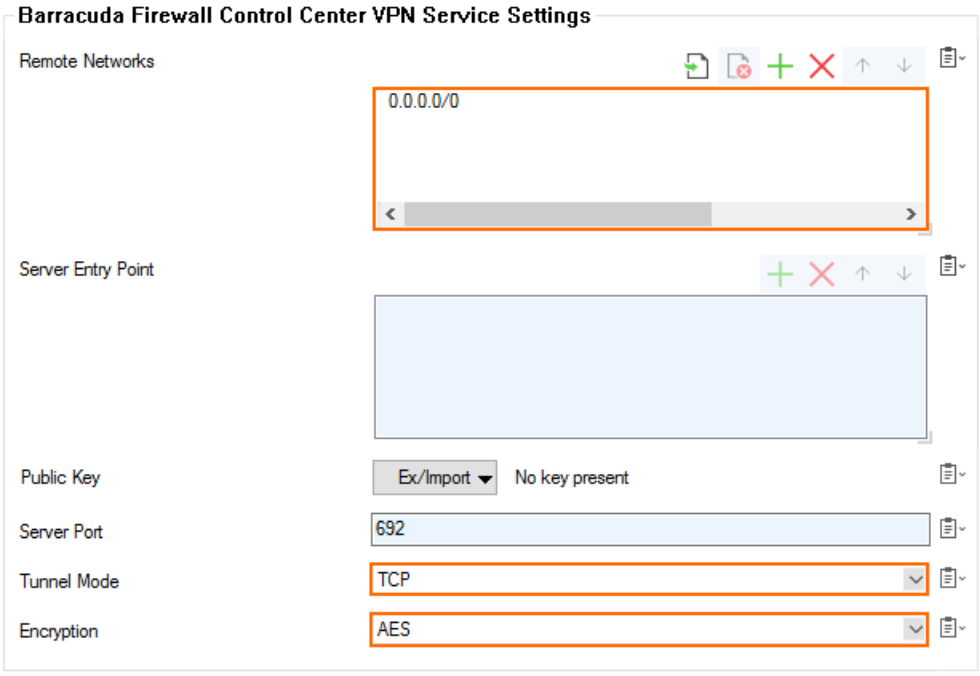


Configure VPN Settings

1. In the left menu, click **VPN Settings**.
2. Select the **VPN enabled** check box.
3. Click **New Key** and select the **Key Length** to generate the private certificate.
4. Click **Edit** and fill in the certificate information.
5. (Manual network only) – Enter the VIP IP address in the **Virtual IP** field. If automatically assigned, this is the first IP address in the Secure Connector subnet assigned to the unit.



6. Next to **Remote Networks**, click **+** to add the networks routed through the VPN tunnel. To send everything through the tunnel and to offer Internet access, enter `0.0.0.0/0`.
   The **Server Port** is the **Entry Port** configured for the Access Controller. The **VPN Access Controller Public Key** is automatically filled in when the configuration is saved.
7. From the **Tunnel Mode** drop-down list, select the transport protocol. Select **TCP** (default) for more reliability and **UDP** for high performance.
8. Select the **Encryption** algorithm used.



Configure Routing Settings

1. In the left menu, click **Routing Settings**.

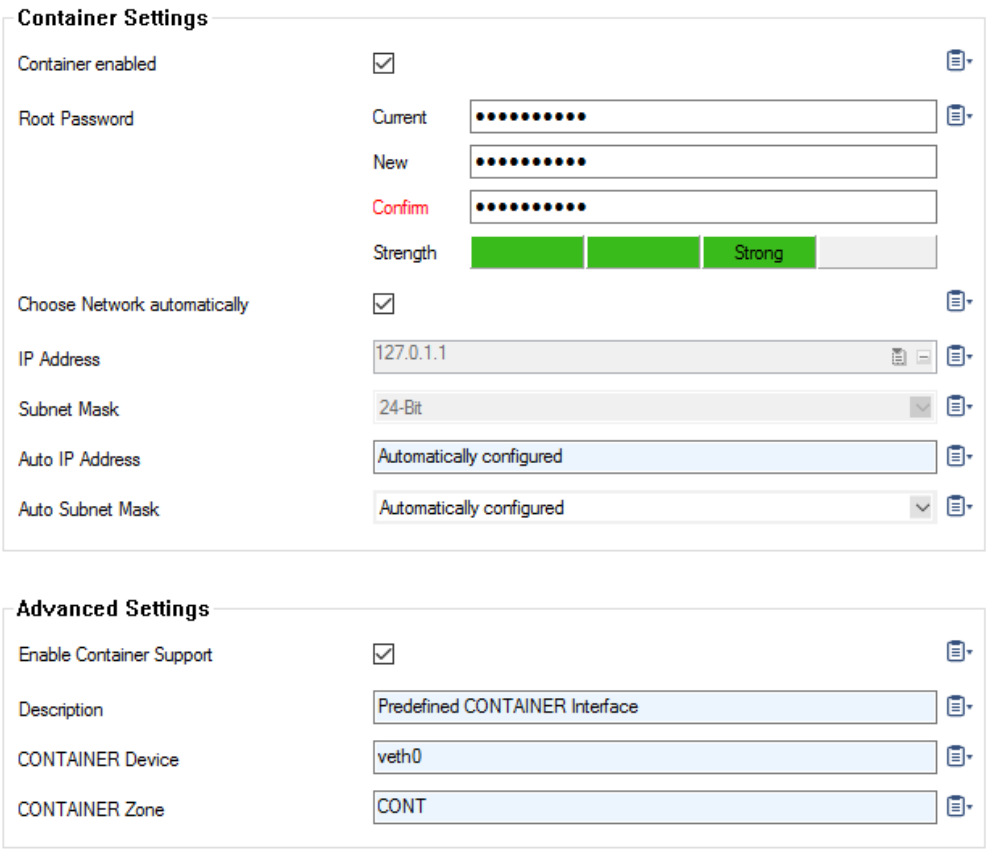
2. Click **+** to add **System Routes**. For more information, see Secure Connector Routing.

Configure Firewall Settings

1. In the left menu, click **Firewall Settings**.
2. Configure the **Firewall Settings**. For more information, see Secure Connector Firewall.

Configure Container Settings

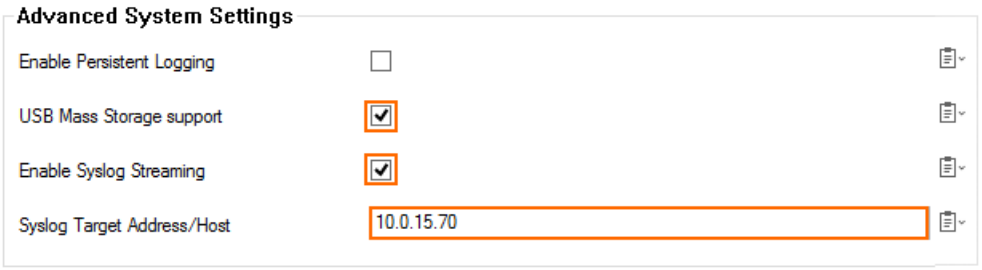
1. In the left menu, click **Container Settings**.
2. Select the **Container enabled** check box.
3. Enter the **Root Password** for container support on the Secure Connector.



For more information, see Secure Connector Container.

Configure Advanced Settings

1. In the left menu, click **Advanced**:
2. Configure **Logging**. For more information, see Secure Connector Logging.
3. Select **USB Mass Storage support** to use the Secure Connector as a mass storage device on your desktop computer. This allows you to copy configuration files directly to the Secure Connector.



4. To configure syslog streaming, see Secure Connector Logging.
5. Click **OK**.
6. Click **Activate**.

Configure Custom Script

In some cases, you may want to trigger the execution of a script during network activation. This can be done by adding the script text into an edit field and enabling the execution.

1. In the left menu, click **Advanced**.
2. Click **Enable Custom Script** to enable execution of the script.
3. For **Add Custom Script**, add your script code into the edit field.

4. Click **Send Changes**.
5. Click **Activate**.

Figures

1. sc_01.png
2. sc_id_settings.png
3. adm_settings.png
4. lan_settings01.png
5. wap_conf01.png
6. sc_vpn.png
7. vpn_ac01.png
8. container_settings.png
9. sc_advanced_settings.png
10. SC_add_custom_script.png