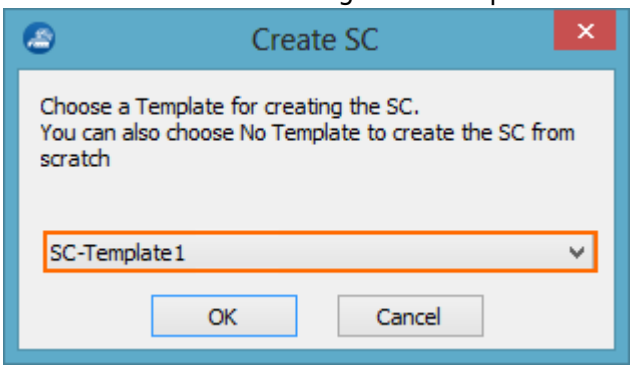
How to Add a Secure Connector Configuration

https://campus.barracuda.com/doc/46895049/

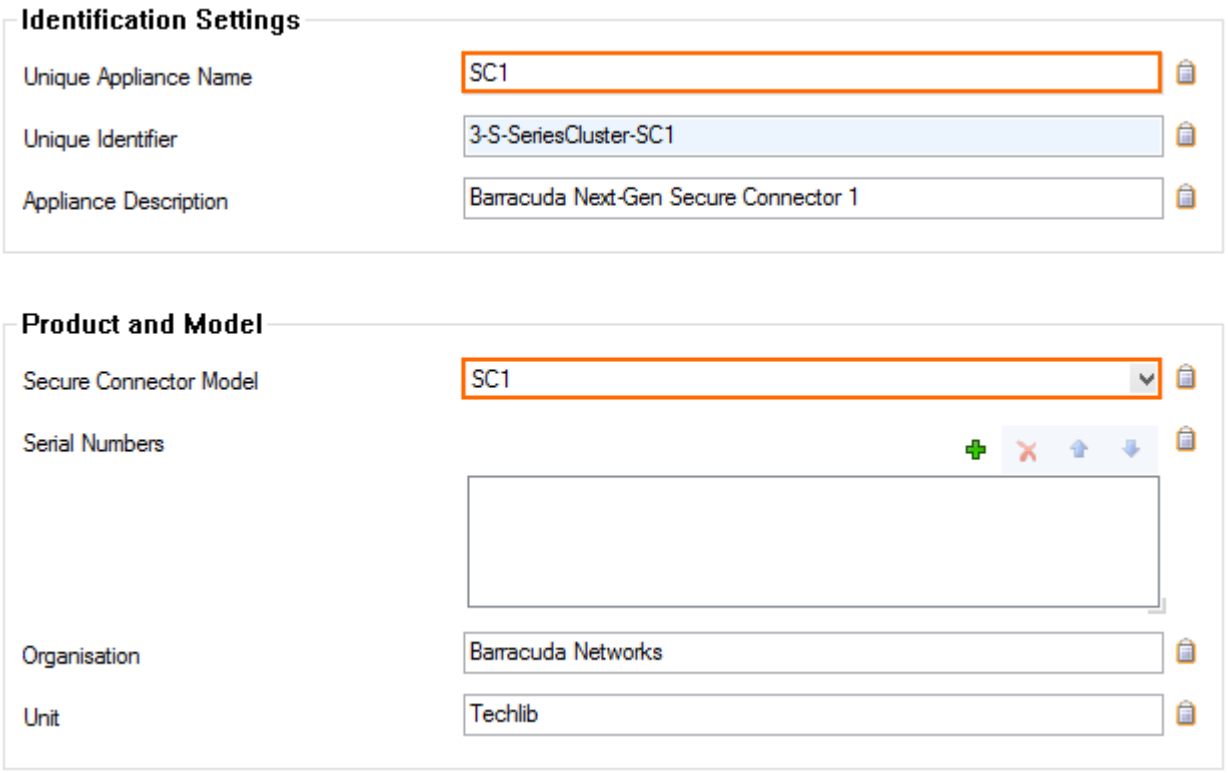
NextGen Secure Connectors are configured and managed by the NextGen Control Center using the Secure Connector Editor. You can either create the configuration as a template and then assign it to the SC device, or directly configure the SC. For more information, see How to Create and Apply SC Templates.

Add a Secure Connector configuration

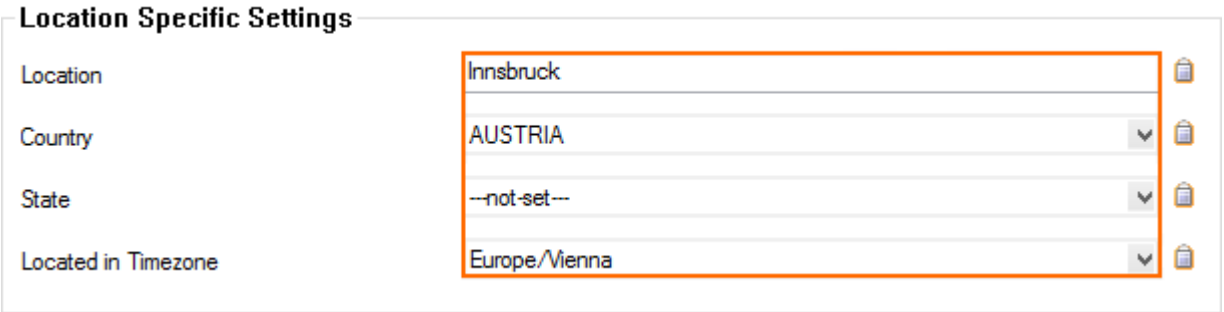
1. Log in to your Control Center.
2. Go to ***your Cluster*** **> Cluster Settings > Secure Connector Editor**.
3. Click **Lock**.
4. Click **Add SC**. The **Create SC** window opens.
5. (optional) Select a template. Configuration settings configured via template are automatically used and cannot be configured on a per-device basis.



6. Configure the **Identification Settings**:
   - **Unique Appliance Name** – Enter a unique name for the SC. The name is final and cannot be changed later.
   - (automatic) **Unique Identifier** – The identifier is a string containing the range, cluster, and unique appliance name.
   - (optional) **Appliance Description**
7. Configure the **Product and Model**:
   - **Secure Connector Model** – Select the hardware version. E.g., **SC1**.
   - (optional) **Serial Numbers** – Click **+** to add the serial number of the SCs allowed to connect with this configuration.
   - (optional) **Organization**
   - (optional) **Unit**

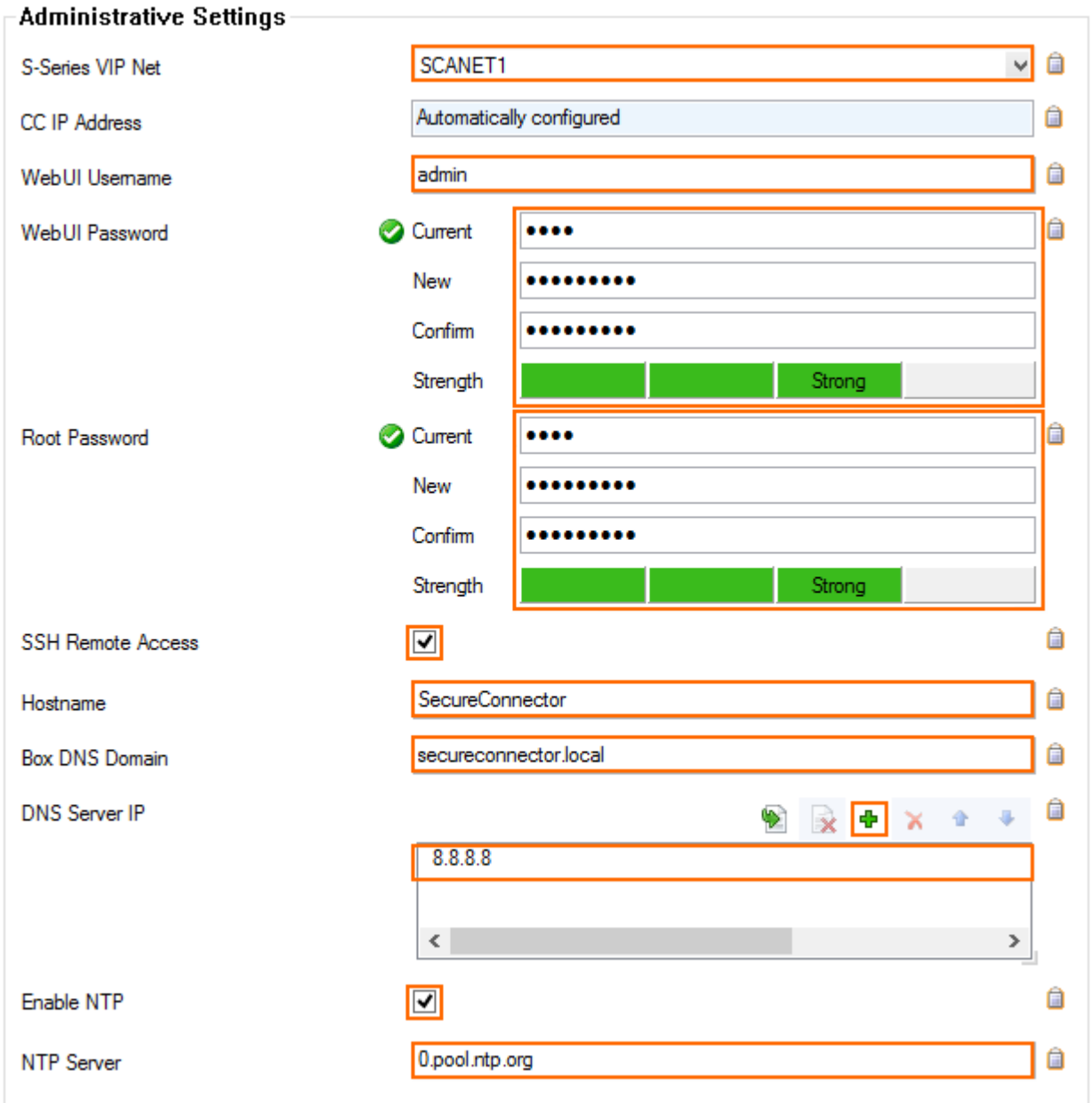


8. Configure the **Location Specific Settings**:
   - (optional) **Location** – Enter the location.
   - (optional) **Country** – Select the country.
   - (optional) **State** – If applicable, select the state.
   - **Located in Timezone** – Select the SC time zone.

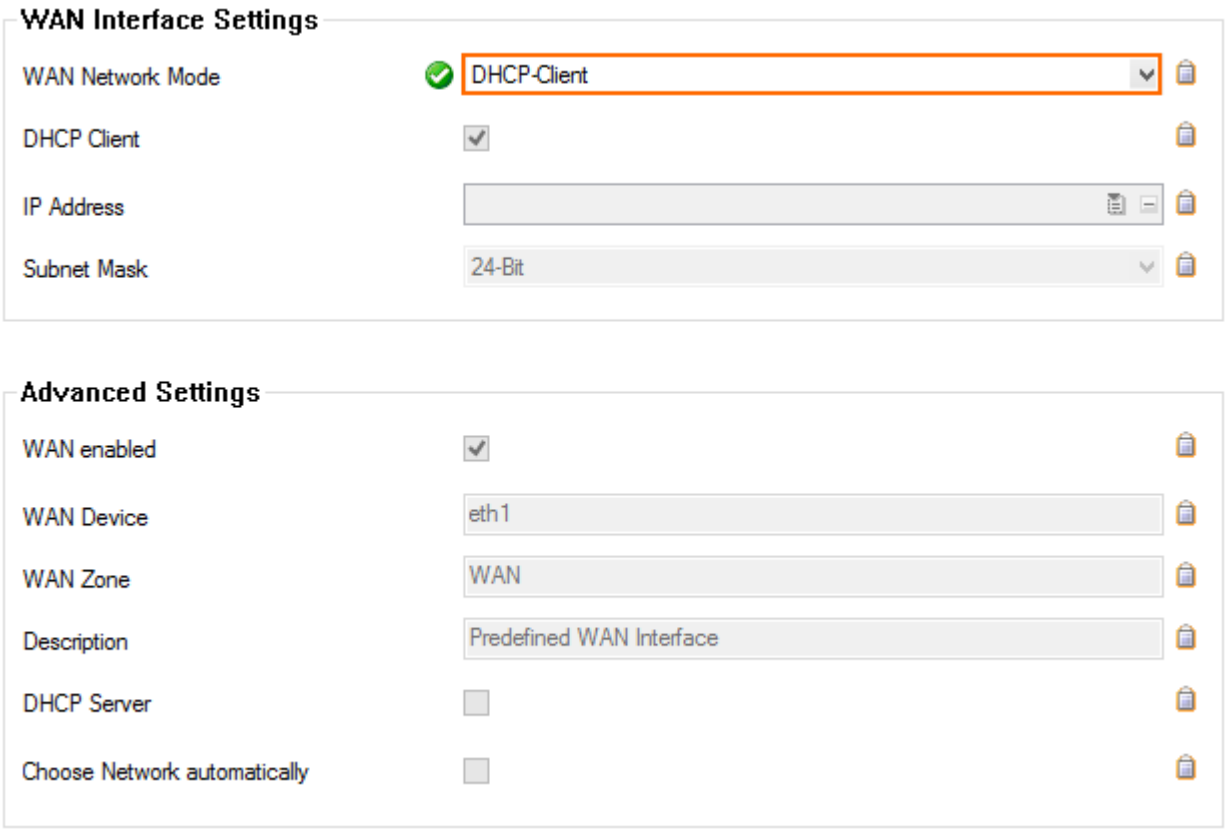


9. In the left menu, click **Administrative Settings** and configure:
   - **S-Series VIP Net** – Select the SC Network. The SC is automatically assigned to the SAC associated with the SC network.
   - **WebUI Username** and **WebUI Password** – Set the username and password for the web interface of the SC.
   - **Root Password** – Enter the root password. The default root password is: `ngf1r3wall`
   - **SSH Remote Access** – Select the check box to enable SSH. You must also create an SC management rule to be able to log in via SSH. For more information, see How to Create SC Firewall Management Rules.
   - **Hostname** – Enter the hostname used for the SC. You can use the same hostname for all SCs.

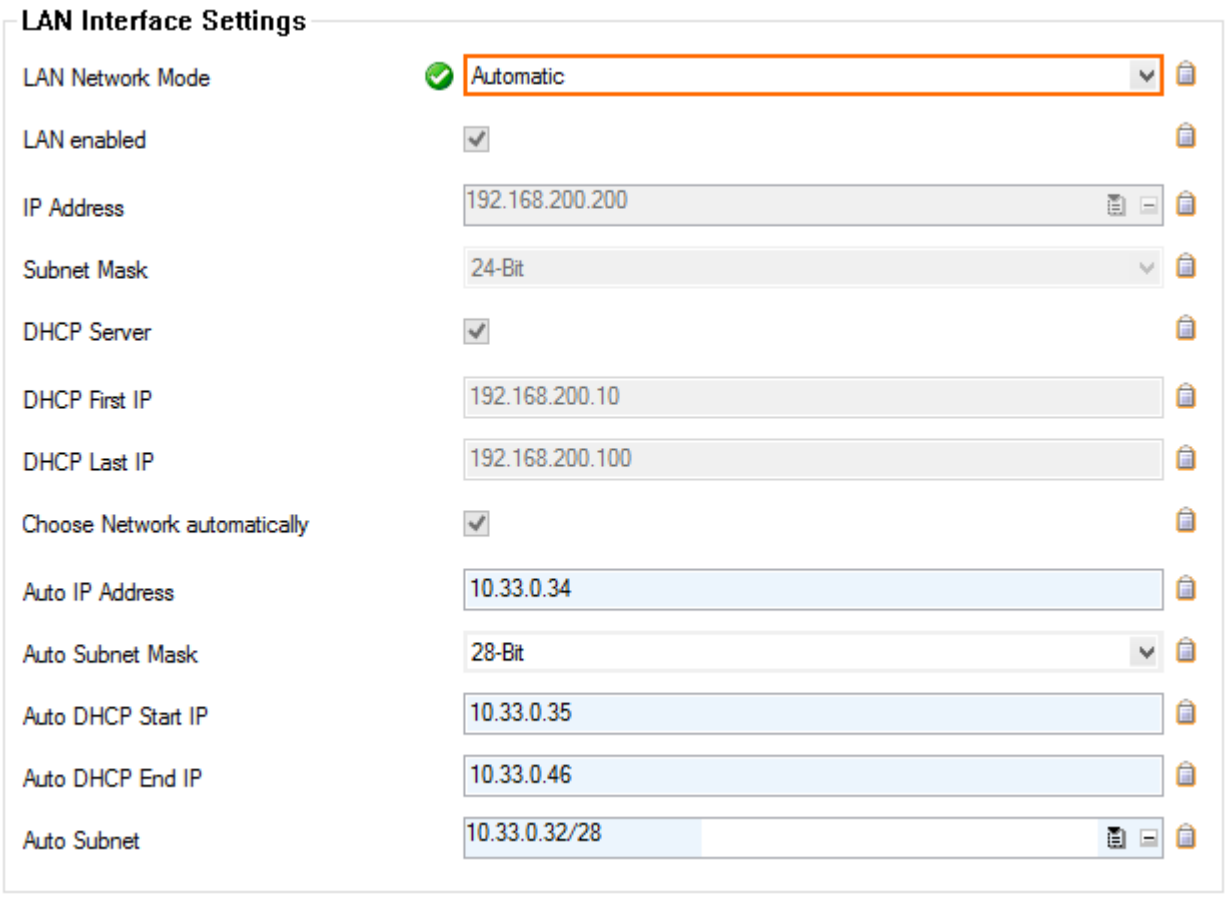
- **Box DNS Domain** – Enter the domain for the SC.
- **DNS Server IP** – Click **+** to enter the IP addresses for the DNS servers.
- **Enable NTP** – Select the check box to synchronize the time with an NTP server.
- **NTP Server IP** – Enter the FQDN or IP address for the NTP server located near your location. Default: `0.pool.ntp.org`



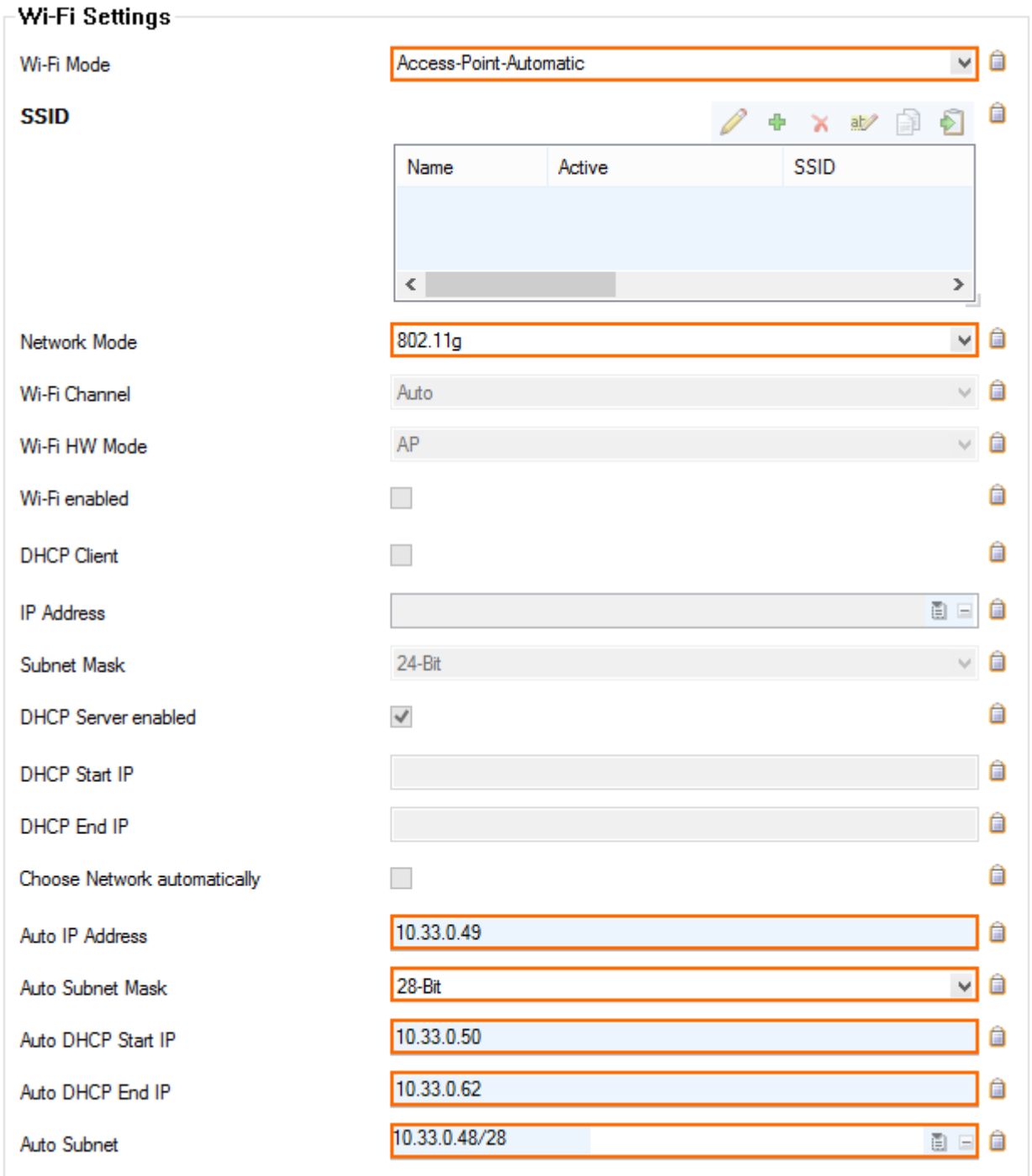
10. In the left menu, click **WAN Settings**.
11. Configure the WAN connection for the WAN port. For more information, see SC WAN Connections.



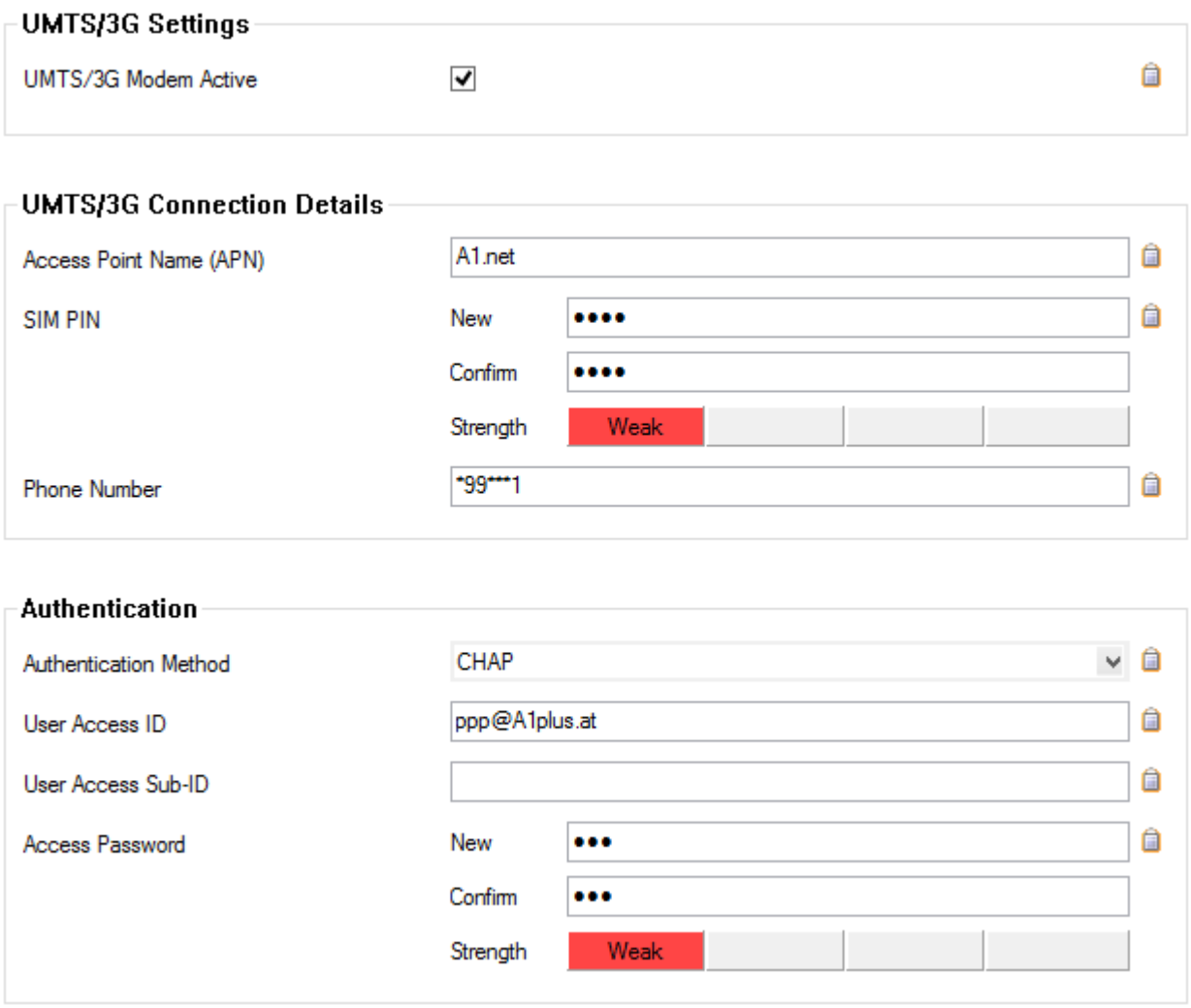
12. In the left menu, click **LAN Settings**.
13. Select the **LAN Network Mode**:
    In the left menu, click **LAN Settings**:
    - **Automatic** (default) – The SC is automatically assigned a subnet from the SC network with the pool size specified in the SC network configuration.
    - **Manual** – Define the IP address and all other SC network settings manually. You can also enable the DHCP server for the network.



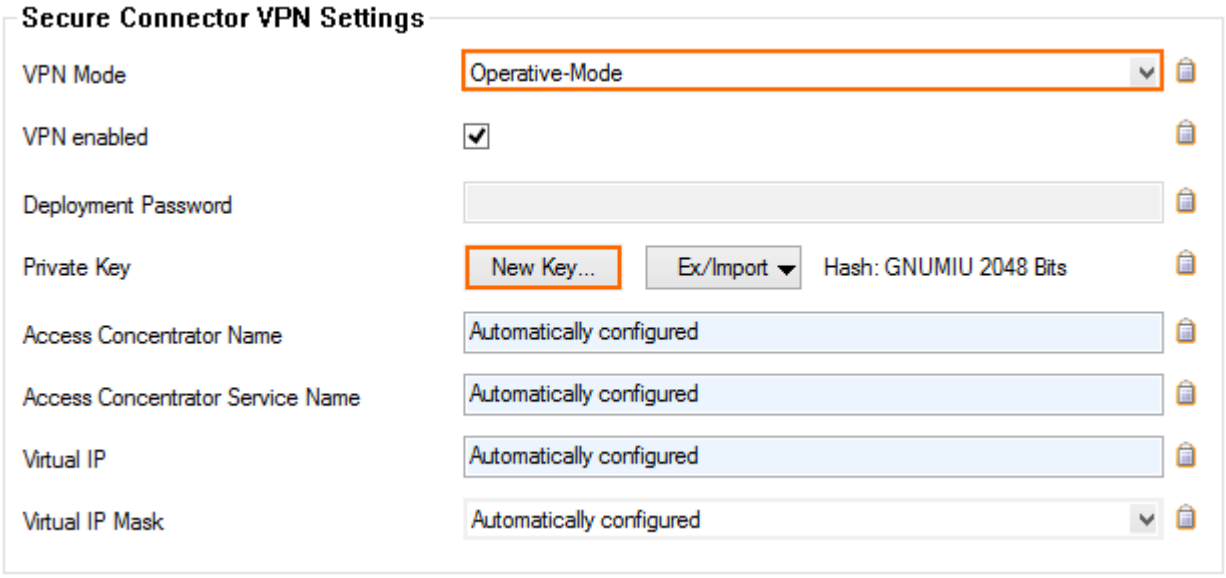
14. In the left menu, click **Wi-Fi Settings**.
15. Configure the **Wi-Fi Settings**:
    - **Access Point** – Configure the **Wi-Fi Settings**. For more information, see SC Wi-Fi Access Point.
    - **Wi-Fi Client** – To use the Wi-Fi interface as a WAN interface, see SC WAN Connections.



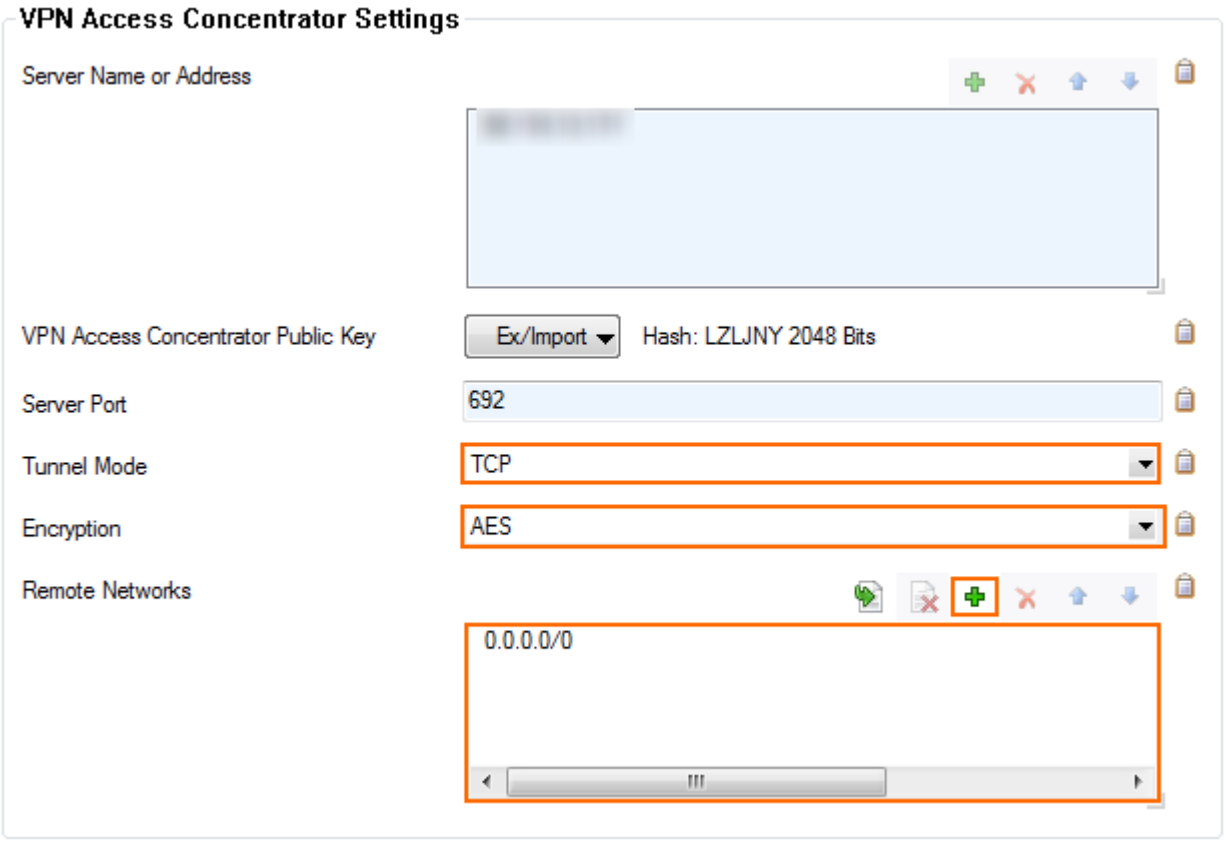
16. In the left menu, click **UMTS/3G Modem Settings**.
17. Configure the **UMTS/3G Modem Settings**:
    - **UMTS/3g Modem Active** – Select the check box to enable the USB modem.
    - **UMTS 3G Connection Details** – Enter the connection details of your mobile provider.
    - **Authentication** – Enter the authentication settings supplied by your mobile provider.



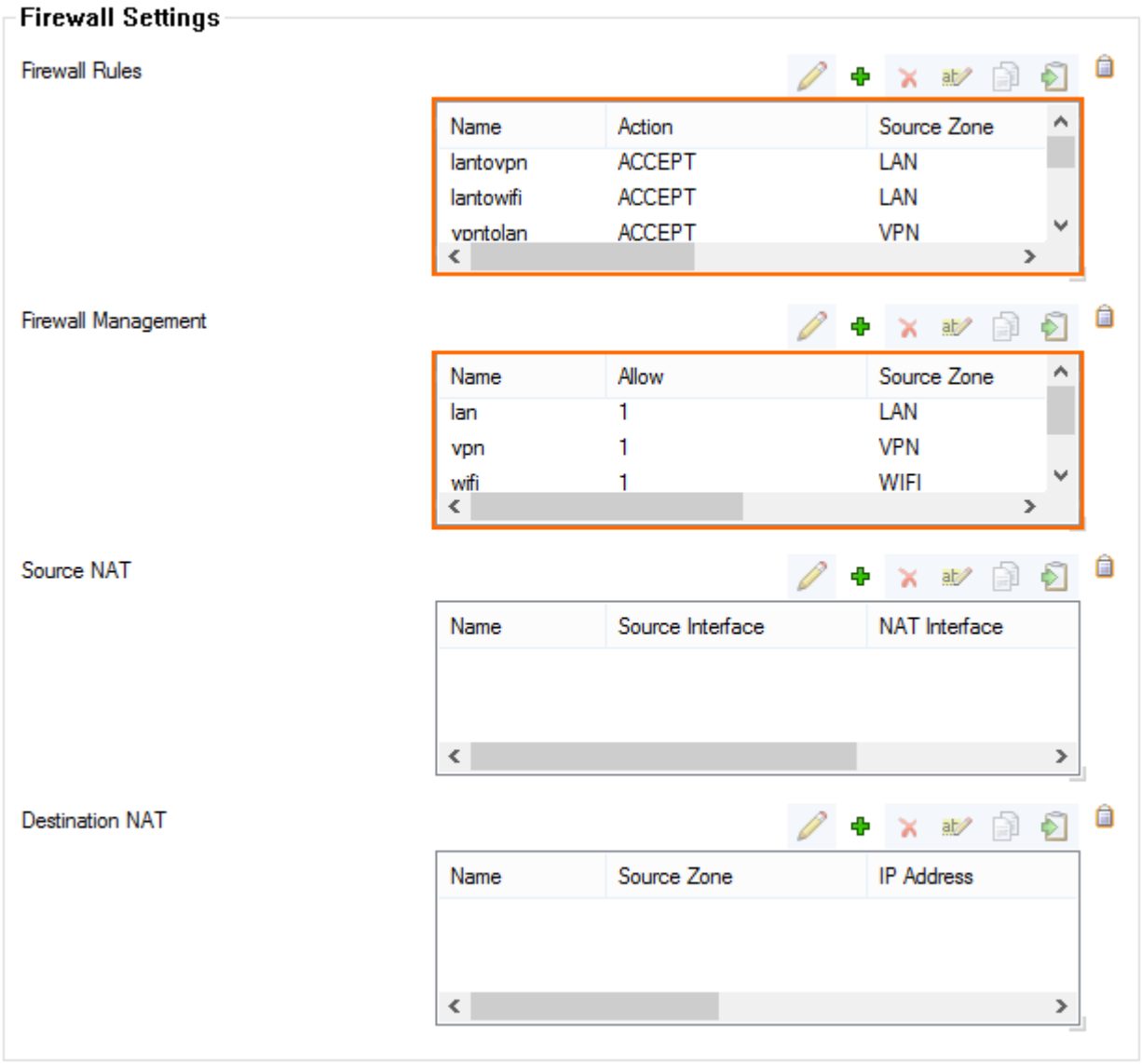
18. Configure the **Secure Connector VPN Settings**:
    - **VPN Mode**:
        - **Operative Mode** (default) – Use certificates to authenticate to the SAC.
        - **Deployment Mode** – Use a passphrase to authenticate to the SAC.
    - **VPN enabled** – Select the check box.
    - (Deployment mode only) **Deployment Password** – Enter the passphrase used to authenticate when connecting to the SAC.
    - **Private Key** – Click **New Key** and select the **Key Length** to generate the private certificate.
    - (manual network only) **Virtual IP** – Enter the VIP IP address. If automatically assigned, this is the first IP address in the SC subnet assigned to the unit.



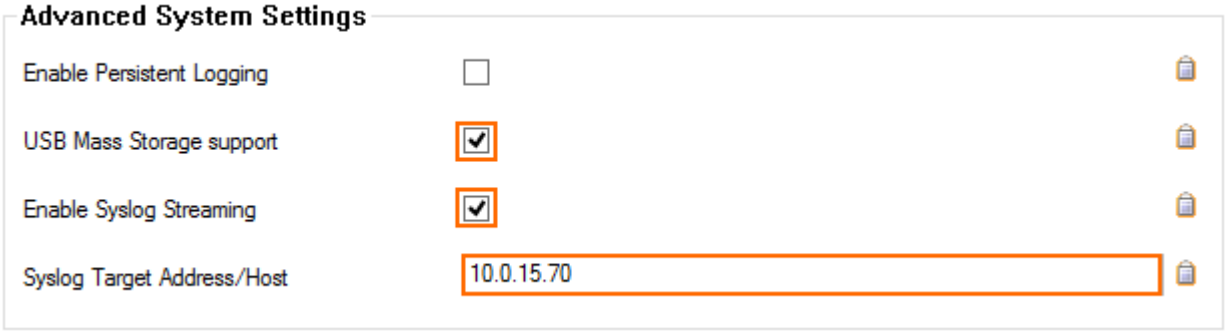
19. Configure the **VPN Access Concentrator Settings**:
    - **(automatic) Server Name or Address** – This is automatically filled in with the **Point of Entry** configured for the SAC when the configuration is saved.
    - **(automatic) VPN Access Concentrator Public Key** – The key is automatically filled in when the configuration is saved.
    - **(automatic) Server Port** – This is the **Entry Port** configured for the SAC.
    - **Tunnel Mode** – Select the transport protocol. Select **TCP** (default) for more reliability and **UDP** for high performance.
    - **Encryption** – Select the encryption algorithm used.
    - **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`.



20. In the left menu, click **Routing Settings**.
21. Click **+** to add **System Routes**. For more information, see SC Routing.
22. (optional) In the **Link Selection** section, configure the failover policies if you are using more than one WAN connection. For more information, see FSC Link Selection.
23. In the left menu, click **Firewall Settings**.
24. Configure the **Firewall Settings**. For more information, see SC Firewall.



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



28. To configure syslog streaming, see SC Syslog Streaming.
29. Click **OK**.

30. Click **Activate**.

Next steps

To deploy a SC using this configuration, see:

- SC Deployment via SC Configuration File
- SC Deployment via VPN Deployment Mode

Figures

1. tmp_select.png
2. id_settings.png
3. loc_settings.png
4. adm_settings.png
5. wan_settings.png
6. lan_settings.png
7. wifi_settings.png
8. umts_settings.png
9. sc_vpn_settings.png
10. vpn_ac_settings.png
11. acfw_settings.png
12. sc_advanced_settings.png