Jabra GN

WHITE PAPER

NETWORK WHITEPAPER

802.1X AND SCEP ON PANACAST 40 VBS & PANACAST 50 VBS

802.1X + SCEP

802.1X

PanaCast 40 VBS and PanaCast 50 VBS support 802.1X for wired network connections. Both systems utilize TLS (Transport Layer Security) version 1.2 for connections.

The EAP methods that are supported for both PanaCast 40 VBS and PanaCast 50 VBS are EAP-TLS, PEAP-MSCHAPv2, and MD5. Certificates can be added to the device via the Web Console.

HOW TO CONFIGURE

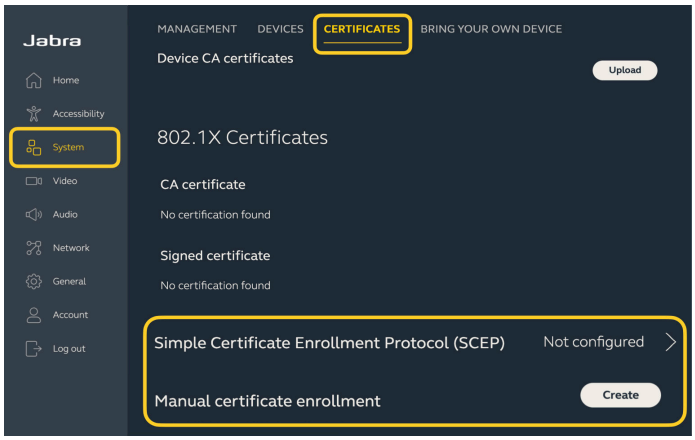
To configure authentication settings for 802.1X, navigate to the device settings from either the touch controller (PanaCast Control or Control IP), or the Web Console by navigating to the device's IP address from a web browser on the same network.

MD5 or MSCHAPv2: These two authentication types are based on username and password. First, select either MD5 or MSCHAPv2 as the 802.1X protocol and then use your username and password.

EAP/TLS: TLS certificates need a certificate signed by an authority to be added to the device. Setting up 802.1X with TLS is a two-step process. First, configure the certificates, and then setup the authentication type. Certificates can either be created manually or automated via SCEP.

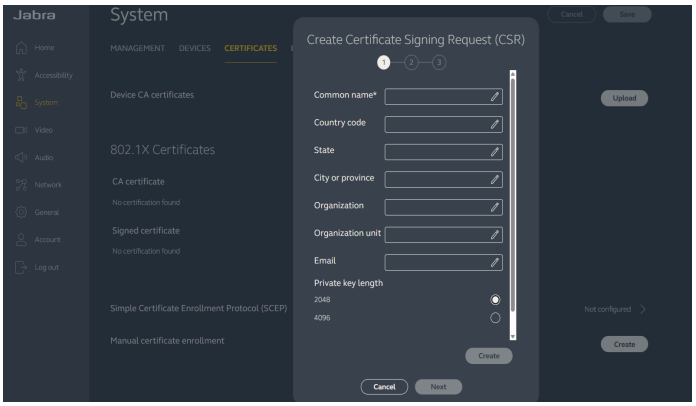
CREATING CERTIFICATES MANUALLY

There are two ways TLS certificates can be added to a device: manual or automatic. From the Web Console, navigate to **System > Certificates** and click **Create** next to **802.1X Manual Certificate Enrollment.**



Next, fill out the fields in the form and click **Create**.

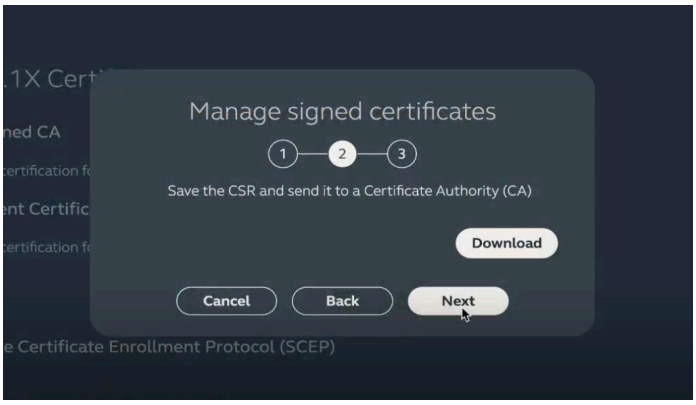
An example of Common Name, Country code, and State would be:
- **Common Name (Required)**: QA1
- **Country code (Optional)**: IT
- **State (Optional)**: Italy



A message may appear that states that any current certificates will be deleted when a new Certificate Signing Request (CSR) is created. Click Confirm if needed. Click **Create** to generate the CSR, then click **Next**.

The following screen will prompt you to save the CSR and send it to a Certificate Authority (CA). Click the **Download** button to obtain the .csr file.

To send a CSR to a Certificate Authority (CA), copy the text from your generated .csr file and submit it through the CA's online portal or use their specific enrollment tools, providing your domain and identity details for validation, after which the CA returns the signed certificate to you for installation.

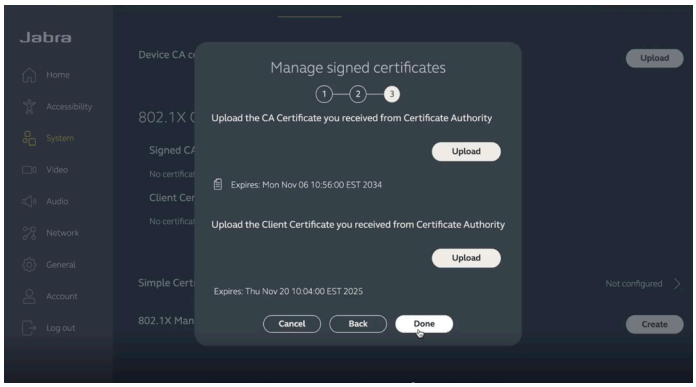


Once you have received the CA certificate, click **Next**.

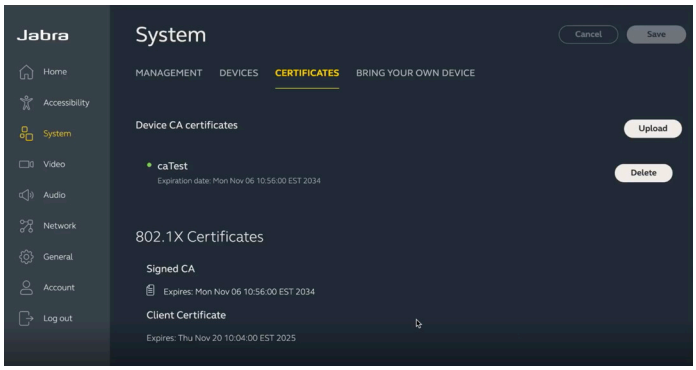
802.1X + SCEP

On the following screen, click the top **Upload** button and select the CA Certificate file to import into the device. There are two certificate formats that are currently supported: **.pem** and **.der**.

Then, click the lower **Upload** button to import the Client Certificate. Expiration dates should appear for both certificates once loaded in the Web Console. Click **Done**.



The certificates should now appear in the Web Console with a green indicator light.



Now that the certificates are configured, you can enable the 802.1X setting by going to the **Network** section. Scroll down to Authentication protocol (802.1X) and click **Configure**. **Toggle on** 802.1X authentication protocol, select **EAP/TLS**, and your uploaded certificates should appear. Click **Save**.

Alternatively, you can upload the certificates from the Web Console and then configure the 802.1X settings directly from the PanaCast Control or Control IP.

Within a few seconds, the device will show as **Connected** to your network. IP address and gateway information will also populate.

SCEP

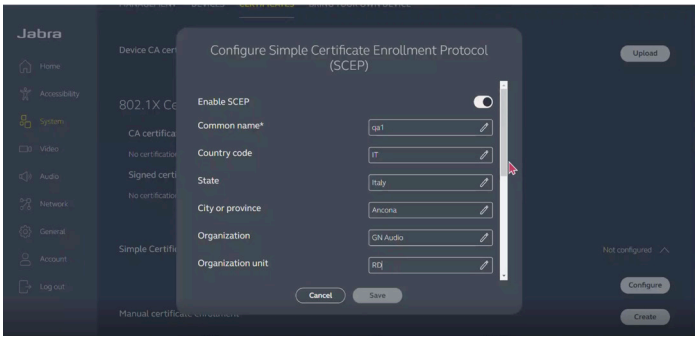
Simple Certificate Enrollment Protocol, or SCEP, is used to streamline the process of issuing digital certificates to network devices, allowing organizations to manage certificates in a secure and scalable way. Using a SCEP server will automatically add the signed certificate and the CA authority file to the video devices.

SCEP support is a software feature that has been added as part of Value Pack 3 service release 1 for PanaCast 50 VBS, as well as upon launch of PanaCast 40 VBS. You can configure certificates from the Web Console.

CREATE AUTOMATIC CERTIFICATES WITH SCEP

When in the Web Console, navigate to **System** in the left-hand navigation menu. Select **Certificates** from the tabs on the top, and locate the 802.1X Certificates section. Next to Simple Certificate Enrollment Protocol (SCEP), expand the section by clicking **Not Configured,** and then click the **Configure** button. **Toggle on** Enable SCEP.

Next, fill out the fields in the form and enter the SCEP server URL from your chosen Certificate Authority provider. The minimum mandatory fields are **Common Name**, **SCEP Server URL**, and **Automatic Renewal Days**.



Once you click Save, the server will then send the certificates to the device, and they will appear on the Web Console automatically. Finally, from either the Web Console or Control IP, navigate to the system settings and select **Network**. Scroll down to Authentication protocol (802.1X) and click **Configure**. **Toggle on** 802.1X authentication protocol, select **EAP/TLS**, and your automatically created certificates should appear. Click **Save**. You may now connect your device to your secure network.