ClickShare Network Integration

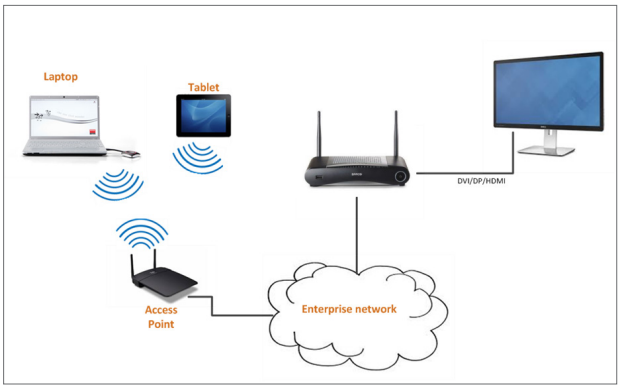
Application note

1 Introduction

"ClickShare Network Integration" aims at deploying ClickShare in larger organizations without interfering with the existing wireless network infrastructure. In a default stand-alone setup, the ClickShare Base Unit creates its own wireless access point (AP) which the ClickShare Buttons use to connect. These so-called "rogue" APs can become a nuisance in larger installations. Next to that, meeting participants who are sharing content from mobile devices have to switch networks to connect with the ClickShare Base Unit.

This is where ClickShare Network Integration comes in. Once fully configured and enabled, the built-in AP of the Base Unit is disabled. The Button or the mobile devices can then connect to a wireless access point that is part of the corporate network. At this point, the Base Unit needs to be connected to the corporate network via the wired Ethernet interface so that the Buttons and mobile devices can share their content on the Base Unit.

In the following sections of this application note, we discuss how all of this can be set up, and we explain a bit more about the inner details.



2 Security Modes

There are 2 security modes supported by the Button to connect to the corporate network:

- The first one, which applies to a typical corporate network setup, is **WPA2-Enterprise with 802.1X**.
- As we also want to support smaller organizations, which might have a more traditional Wi-Fi setup, there is also support for WPA2-PSK, also known as **WPA2-Personal**.

Both modes are based on Wi-Fi Protected Access (WPA). In this document, we talk about WPA2 – an improved version of the original WPA standard – which adds AES encryption to improve security.

2.1 WPA2-Enterprise with 802.1X

WPA2-Enterprise relies on a server (using RADIUS) to authenticate each individual client on the network. To do this, authentication 802.1x is used (also known as port-based Network Access Control). 802.1x encapsulates the Extensible Authentication Protocol (EAP) for use on local area networks. This is also known as "EAP over LAN" or EAPoL. Using RADIUS, these EAPoL messages are routed through the network in order to authenticate the client device on the network – which, in the case of ClickShare, are the Buttons.

The 802.11i (WPA2) standard defines a number of required EAP methods. However, not all of them are used extensively in the field, and some other ones (which are not in the standard) are used much more often. Therefore, we have selected the most widely used EAP methods. The list of EAP methods supported in the ClickShare system is:

- EAP-TLS
- PEAP
- EAP-TTLS

More details on each of them, plus setup instructions, can be found further down in this application note.

3 Considerations

When you choose to integrate the ClickShare system into your corporate network, there are a few things to consider up front. First of all, make sure that all your Base Units can be connected to your network via the wired Ethernet interface. Also, take into account the amount of bandwidth that each Button needs to stream the captured screen content to the Base Unit – this is usually somewhere between 5 and 15 Mbps. So, prevent bottlenecks in your network (e.g. 100 Mbps switches) that could potentially degrade your ClickShare experience due to a lack of bandwidth.

4 Prerequisites

Before rolling out ClickShare Network Integration, make sure your infrastructure meets the following prerequisites.

4.1 Network

Once you enable the corporate network, the internal Wi-Fi access point of the ClickShare Base Unit is disabled. Make sure your Base Unit is connected to the corporate network via its wired Ethernet interface.

4.2 Firewall

To ensure that you can successfully share content via the ClickShare Button, or from mobile devices, to the Base Unit, make sure the following ports are open on your network:

Sender		CSE-200 Base Unit
ClickShare Button	TCP	6541-6545
	UDP	514
ClickShare Presenter	TCP	6541-6545
	UDP	5353
WebUI	TCP UDP	80; 443
REST API	TCP UDP	4000; 4001
Airplay	TCP UDP	4100-4200; 7000; 7100; 47000 4100-4200; 5353

4.3 VLAN

A lot of corporate networks are divided into multiple VLANs – for example, to separate BYOD (Bring Your Own Device) traffic from the "core" corporate network. Take this into consideration when integrating ClickShare into your network. ClickShare Buttons connecting to your wireless infrastructure should be able to connect to the Base Units. Furthermore, if you want to use the mobile apps, these should also be able to reach the Base Units. It is advisable to put all ClickShare Units into a separate VLAN so they are easily manageable.

4.4 DNS

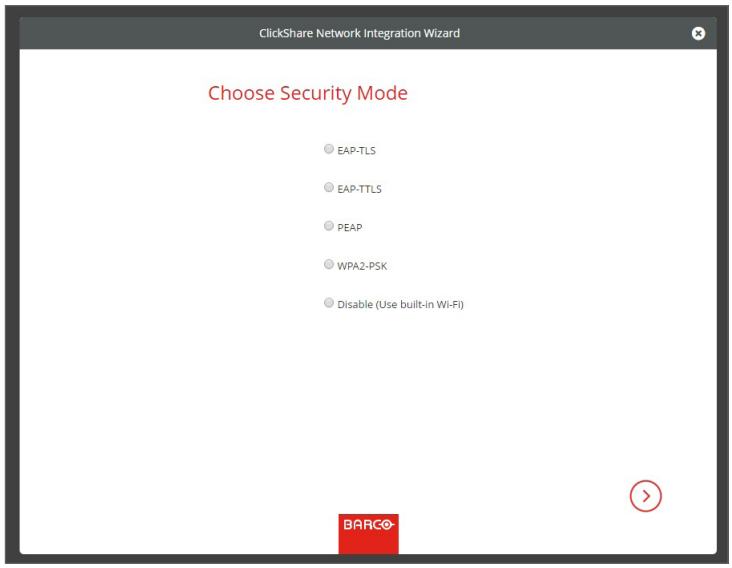
For the Buttons to be able to stream their content to the Base Unit, they must be able to resolve the Base Unit's hostname within the network. If no DNS is available Buttons will fall back to the IP of the Base Unit at the moment of USB pairing. Because of this we strongly advise to reserve IP addresses in your DHCP server for each Base Unit to prevent issues when the hostname is not resolvable.

4.4 NTP

When using EAP-TLS, you must also configure NTP on the Base Unit. This can be done via the Base Unit WebUI. The Base Unit must have the correct time to handle the certificates required for EAP-TLS. Preferably, you should use an NTP server with high availability on the local corporate network. Be advised that, when using an NTP server on the internet, the Base Unit cannot connect through a proxy server.

5 Setup

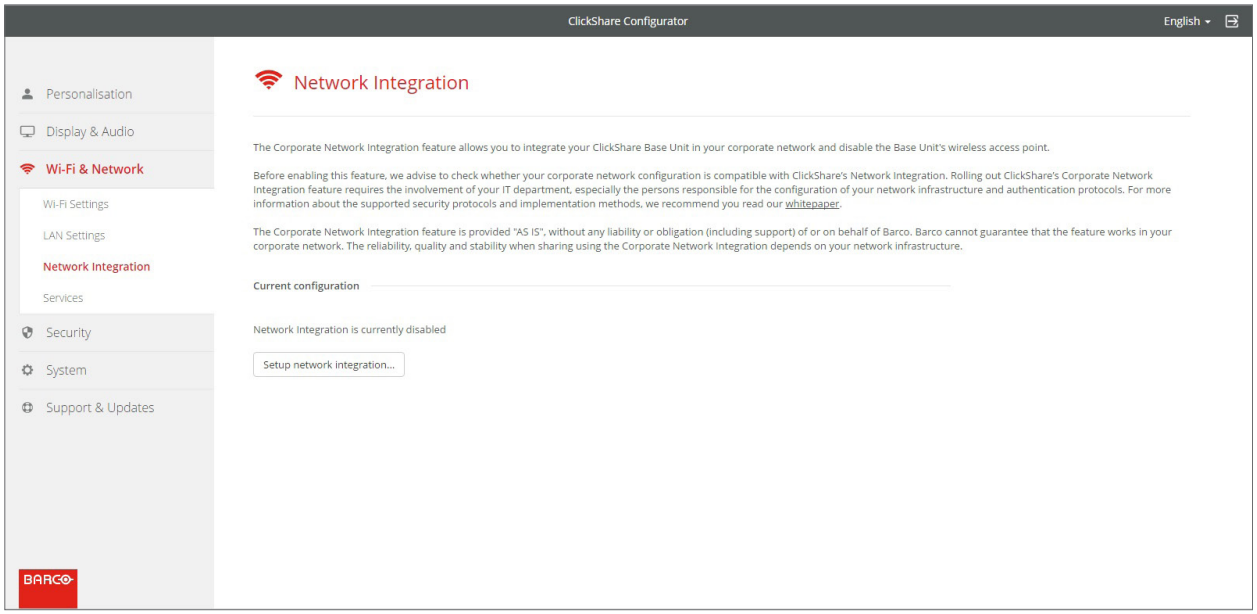
To facilitate the setup, we have opted for a wizard in the ClickShare WebUI. This wizard will guide you through the process according to the security mode you select. Further down, you will find an overview and explanation of each supported security mode and the input that is required to get everything integrated and working.



5.1 Before you start

Before enabling this feature, we advise to check whether your corporate network configuration is compatible with ClickShare's Network Integration. Rolling out ClickShare's Corporate Network Integration feature requires the involvement of your IT department, especially the persons responsible for the configuration of your network infrastructure and authentication protocols.

The Corporate Network Integration feature is provided "AS IS", without any liability or obligation (including support) of or on behalf of Barco. Barco cannot guarantee that the feature works in your corporate network. The reliability, quality and stability when sharing using the Corporate Network Integration depends on your network infrastructure.



5.2 Security methods

The next 4 sections describe each of the supported security methods in further detail. Please refer to the one that applies to your environment.

5.3 Post Setup

Please note that you must re-pair all of the ClickShare Buttons after completing the setup wizard. Before re-pairing, the old standalone mode is still active on the Base Unit and you will be unable to share.

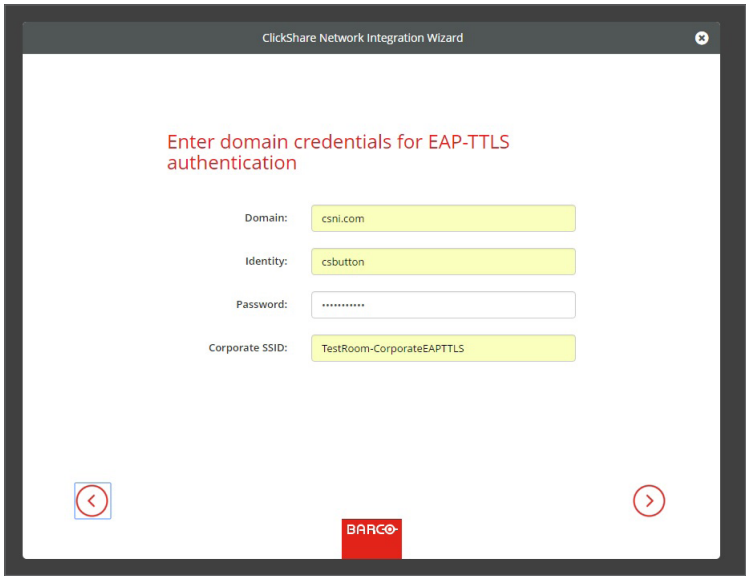
5.4 Apps

Once integrated into the network, any mobile device connected to the corporate network will be able to share content with any Base Unit on the network. (If so desired, you can prohibit sharing from mobile devices via the Base Unit's WebUI.) We advise to enable passcode authentication for mobile devices. This option can be found on the 'Wi-Fi & Network > Services' page of the WebUI.

6 EAP-TLS

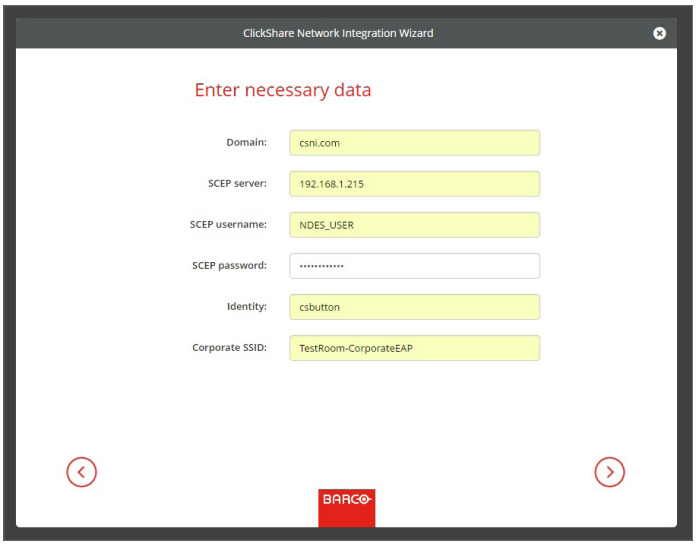
EAP-TLS (Transport Layer Security) is an EAP method based on certificates, which allows mutual authentication between client and server. It requires a PKI (Public Key Infrastructure) to distribute server and client certificates. (If this is too big of a hurdle for your organization, EAP-TTLS and PEAP provide good alternatives.) Even though an X.509 client certificate is not strictly required by the standard, it is mandatory in most implementations, including ours.

When implemented using client certificates, EAP-TLS is considered to be one of the most secure EAP methods. The only minor disadvantage, compared to PEAP and EAP-TTLS, is that the user's identity is transmitted in the clear before the actual TLS handshake is performed. EAP-TLS is supported via SCEP or manual certificate upload.



6.1 SCEP

The Simple Certificate Enrolment Protocol (SCEP) enables issuing and revoking certificates in a scalable way. We have included SCEP support to allow for quicker and smoother integration of the ClickShare Base Unit and Buttons into the corporate network. Because most companies use Microsoft Windows Server and its active directory (AD) to manage users and devices, our SCEP implementation is specifically targeted at the Network Device Enrolment Service (NDES), which is part of Windows Server 2008 R2 and 2012. At this time, no other SCEP server implementations are supported.



6.1.1 NDES

The Network Device Enrolment Service is Microsoft's server implementation of the SCEP protocol. If you want to enable EAP-TLS using SCEP, make sure NDES is enabled, configured and running on your Windows Server. For more details about setting up NDES, please visit the Microsoft website[1].

SCEP uses a so-called "challenge password" to authenticate the enrollment request. For NDES, this challenge can be retrieved from your server at: http(s)://[your-server-hostname]/CertSrv/mscep_admin. When you enter the necessary credentials into the setup wizard, the Base Unit automatically retrieves this challenge from the web page and uses it in the enrollment request – thereby fully automating the process.

6.1.2 Provide certificates manually

If your current setup doesn't support SCEP, or if you prefer not to use it but you still want to benefit from the mutual authentication EAP-TLS offers, you can also upload the necessary certificates manually.

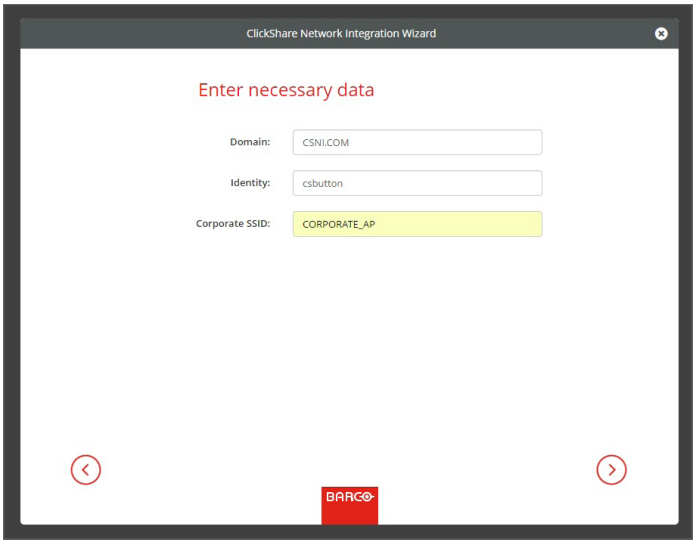
- SCEP Server IP / Hostname
- SCEP Username
- SCEP Password
- Domain
- Identity
- Corporate SSID

For a detailed explanation of each setting, please go to section 10: 'Configuration details'.

[1] NDES White Paper: http://social.technet.microsoft.com/wiki/contents/articles/9063.network-device-enrollment-service-ndes-in-active-directory-certificate-services-ad-cs-en-us.aspx

6.2 Provide certificates manually

If your current setup doesn't support SCEP, or if you prefer not to use it but you still want to benefit from the mutual authentication EAP-TLS offers, you can also upload the necessary certificates manually.



6.2.1 Client Certificate

The client certificate you provide should be signed by the authoritative root CA in your domain and should be linked to the user you specify in the Identity field. Also, make sure that the client certificate you provide contains the private key – this is necessary to set up the TLS connection successfully. The client certificate should be a so called device or machine certificate and not a user certificate.

6.2.2 CA Certificate

The CA certificate is the certificate of the authoritative root CA in your domain that is used in setting up the EAP-TLS connection. During the wizard, the Base Unit ensures that it can validate the chain of trust between the Client and the CA certificates you provide.

6.2.2 Input

To successfully set up an EAP-TLS configuration using SCEP, the following data is required:

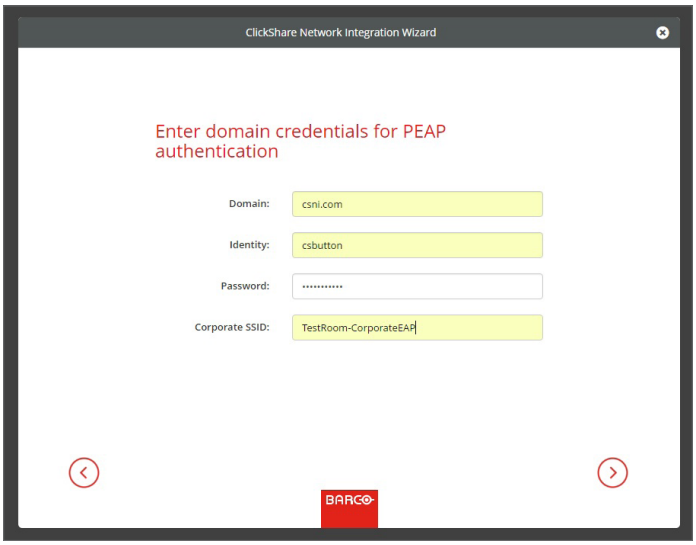
- Client Certificate
- CA Certificate
- Domain
- Identity
- Corporate SSID

For a detailed explanation of each setting, please go to section 10: 'Configuration details'.

7 PEAP

PEAP (Protected Extensible Authentication Protocol) is an EAP implementation co-developed by Cisco Systems, Microsoft and RSA Security. It sets up a secure TLS tunnel using the server's CA certificate, after which actual user authentication takes place within the tunnel. This way of working enables to use the security of TLS while authenticating the user, but without the need for a PKI.

The standard does not mandate which method is to be used to authenticate within the tunnel. But in this application note, with regard to PEAP, we are referring to PEAPv0 with EAP-MSCHAPv2 as the inner authentication method. This is one of the two certified PEAP implementations in the WPA and WPA2 standards – and by far the most common and widespread implementation of PEAP.



7.1 Input

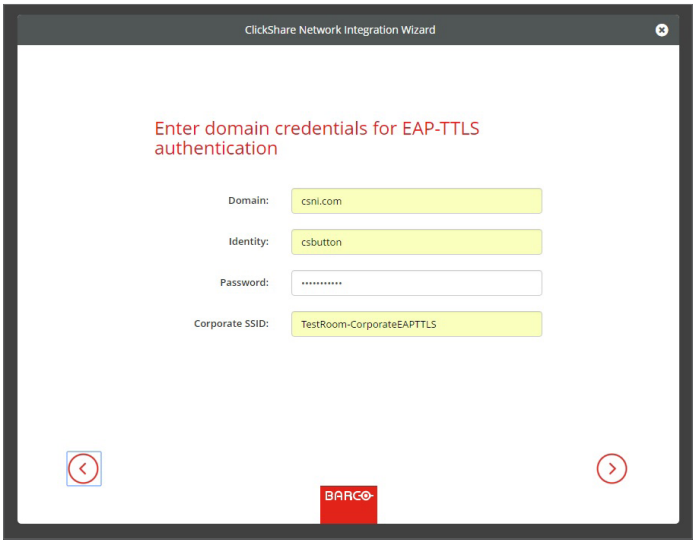
- Domain
- Identity
- Password
- Corporate SSID

For a detailed explanation of each setting, please go to section 10: 'Configuration details'.

8 EAP-TTLS

EAP-TTLS (Tunneled Transport Layer Security) is an EAP implementation by Juniper[2] networks. It is designed to provide authentication that is as strong as EAP-TLS, but it does not require issuing a certificate to each user. Instead, only the authentication servers are issued certificates. User authentication is performed by password, but the password credentials are transported in a securely encrypted tunnel based on the server certificates. User authentication is performed against the same security database that is already in use on the corporate LAN: for example, SQL or LDAP databases, or token systems.

Because EAP-TTLS is usually implemented in corporate environments without a client certificate, we have not included support for this. If you prefer to use client certificates per user, we suggest using EAP-TLS instead.



8.1 Input

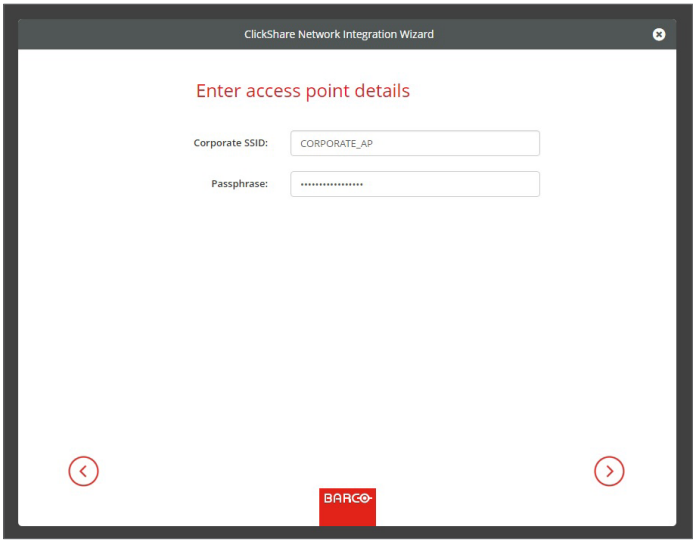
- Domain
- Identity
- Password
- Corporate SSID

For a detailed explanation of each setting, please go to section 10: 'Configuration details'.

[2] https://www.juniper.net/techpubs/software/aaa_802/sbrc/sbrc70/sw-sbrc-admin/html/EAP-024.html

9 WPA-PSK

WPA2-PSK does not distinguish between individual users – there is 1 password (PSK – Pre-Shared Key) for all clients connecting to the wireless infrastructure. This makes setup very straightforward. Once connected, all data transmitted between client and AP is encrypted using a 256-bit key.



9.1 Input

- Corporate SSID
- Pre-Shared Key

For a detailed explanation of each setting, please go to section 10: 'Configuration details'.

10 Configuration details

You can use this section as a quick reference guide – it describes the different settings you can encounter in the setup wizard in more detail.

10.1 SCEP Server URL / Hostname

This is the IP or hostname of the Windows Server in your network running the NDES service. Since Internet Information Services (IIS) supports both HTTP and HTTPS, specify which of the two you want to use. If not specified, we default to HTTP.

Examples: http://myserver or https://10.192.5.1 or server.mycompany.com (will use http)

10.2 SCEP Username

This is a user in your Active Directory which has the required permission to access the NDES service and request the challenge password. To confirm this, the user should be part of the CA Administrators group (in the case of a stand-alone CA) or have enroll permissions on the configured certificate templates.

10.3 SCEP Password

This is the password of the User Account used as SCEP Username. The password is never stored on the Base Unit – it is kept in memory just long enough to request the Challenge Password from the server, and then it is immediately removed from memory.

10.4 Domain
The company domain for which you are enrolling should match the one defined in your Active Directory.

10.5 Identity
The identity of the user account in the Active Directory, which the ClickShare Buttons use to connect to the corporate network. When using

10.6 Password
The corresponding password for the identity that you are using to authenticate on the corporate network. Per Base Unit, every Button uses the same identity and password to connect to the corporate network.

10.7 Corporate SSID
The SSID of your corporate wireless infrastructure to which the ClickShare Buttons connect.

10.8 Client Certificate
When we talk about client certificates we specifically mean the so called device or machine certificates not a user certificate.
We support 2 formats for uploading a client certificate:

- PKCS#12 (.pfx) – An archive file format for storing multiple cryptography objects.
- Privacy Enhanced Mail (.pem) – A Base64 encoded DER certificate stored between 2 tags: "-----BEGIN CERTIFICATE-----" and "-----END CERTIFICATE-----".

When the provided PKCS#12 file also contains the necessary CA certificate, the Base Unit extracts it and verifies the chain of trust, so that you do not have to provide the CA certificate separately.

10.9 CA Certificate
We support the common .crt file extension, which can contain a Base64 encoded DER certificate.

10.10 Pre-Shared Key
The key used in WPA2-PSK to authenticate onto the wireless infrastructure. This can be a string of 64 hexadecimal digits or a passphrase of 8 to 63 printable ASCII characters.

11 Troubleshooting
Even though the Base Unit does its best to validate the provided configuration input, it is still possible that the Button will not be able to connect to your corporate network. There are several potential root causes for this, including but not limited to: incorrect SSID, SSID not available, incorrect EAP Identity / Password, firewall settings, VLAN configuration, ...

To receive feedback from the Button when it is trying to connect to your corporate network, please look at the ClickShare Client log. This log can be enabled by pressing the Shift key when starting the Client executable. Look for the lines "EDSUSBDongleConnection::mpParseDongleMessages". An error code and a short summary of the issue should be logged.
An example of this line could be the one below:

> EDSUSBDongleConnection::mpParseDongleMessages - error message Selected interface 'wlan0';bssid=00:0e:8e:3a:a8:efssid=ClickShare-CorporateCSC-1;id=0;mode=station;pairwise_cipher=CCMP;group_cipher=CCMP;key_mgmt=WPA2-PSK;wpa_state=COMPLETED;ip_address=192.168.2.2;address=00:23:a7:3a:17:bd;#012

To check if a button could reach the Base Unit please connect a PC in the same way a Button would connect (same user name, pw, certificates) and ping the Base Unit's hostname, you can find the hostname in the Based Units WebUI. If the ping fails try pinging the IP adjust your network setup so pinging the hostname is successful.

We strongly advise to reserve IP addresses in your DHCP server for each Base Unit to prevent issues when the hostname is not resolvable.