Using TLS

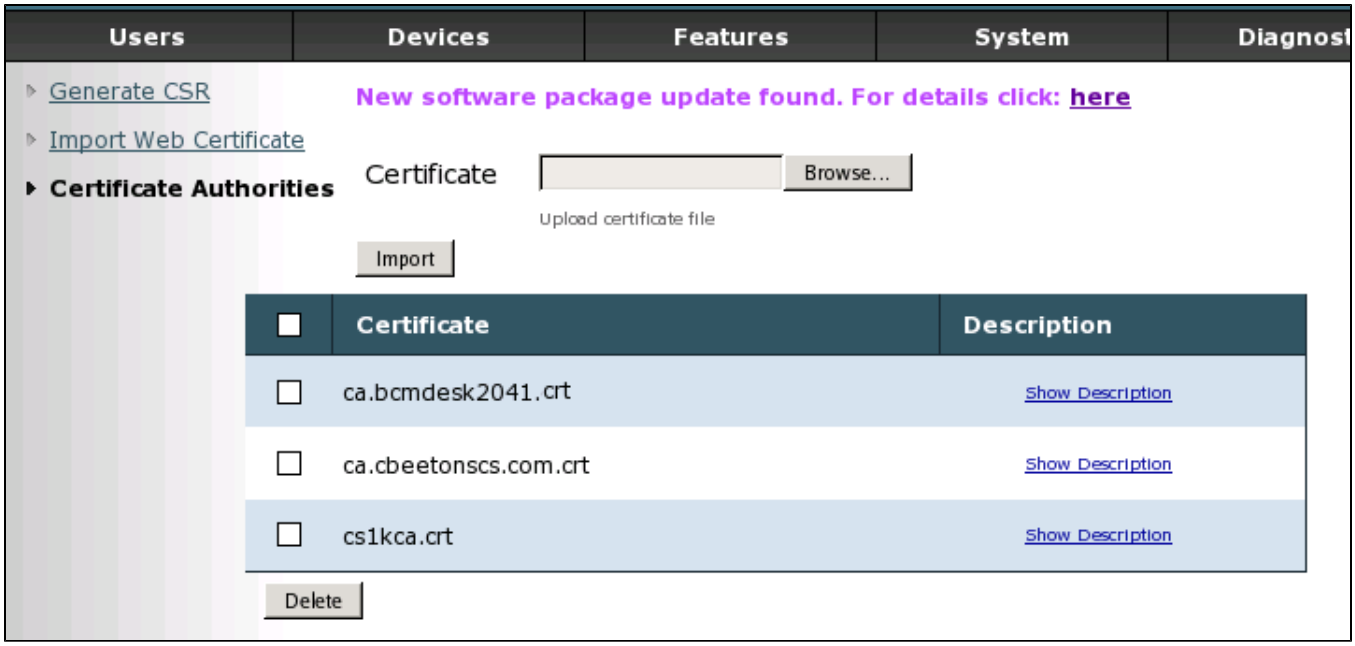
In 4.2, it is possible to use TLS for connections through a sipXbridge gateway. This provides encryption and authentication for the external connection between sipXecs and other systems which support TLS. It is also possible to assign permissions to remote TLS peers, so that users of those systems can access internal resources which require permissions.

Export sipXecs Certificate Authority

In order for TLS to work, the two systems will exchange certificates, and each system must be able to validate the other's certificate. Since sipXecs certificates are self-signed by our own Certificate Authority, you must install our CA certificate on the other system. The CA certificate can be saved by clicking on it on the Certificate Authorities panel under System -> Certificates. Install this certificate on the remote system following whatever procedure it requires.

Import remote Certificate Authority

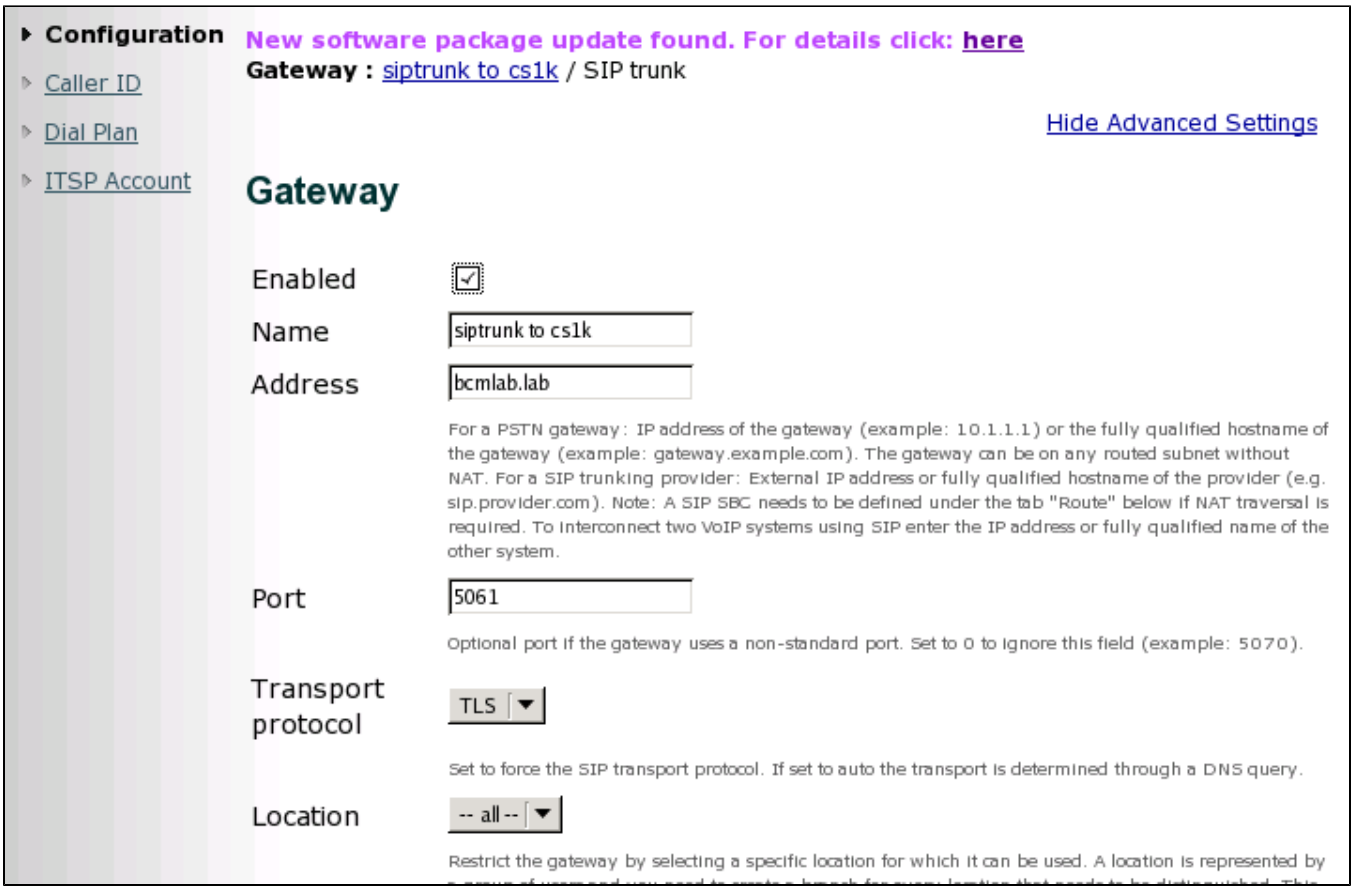
Similarly, the remote system's CA certificate must be imported into sipXecs. This is done on the Certificate Authorities panel under System -> Certificates. It may be necessary to restart the bridge as indicated on the screen but as this will be done after the next step, the message can be ignored here.



Configure TLS ports

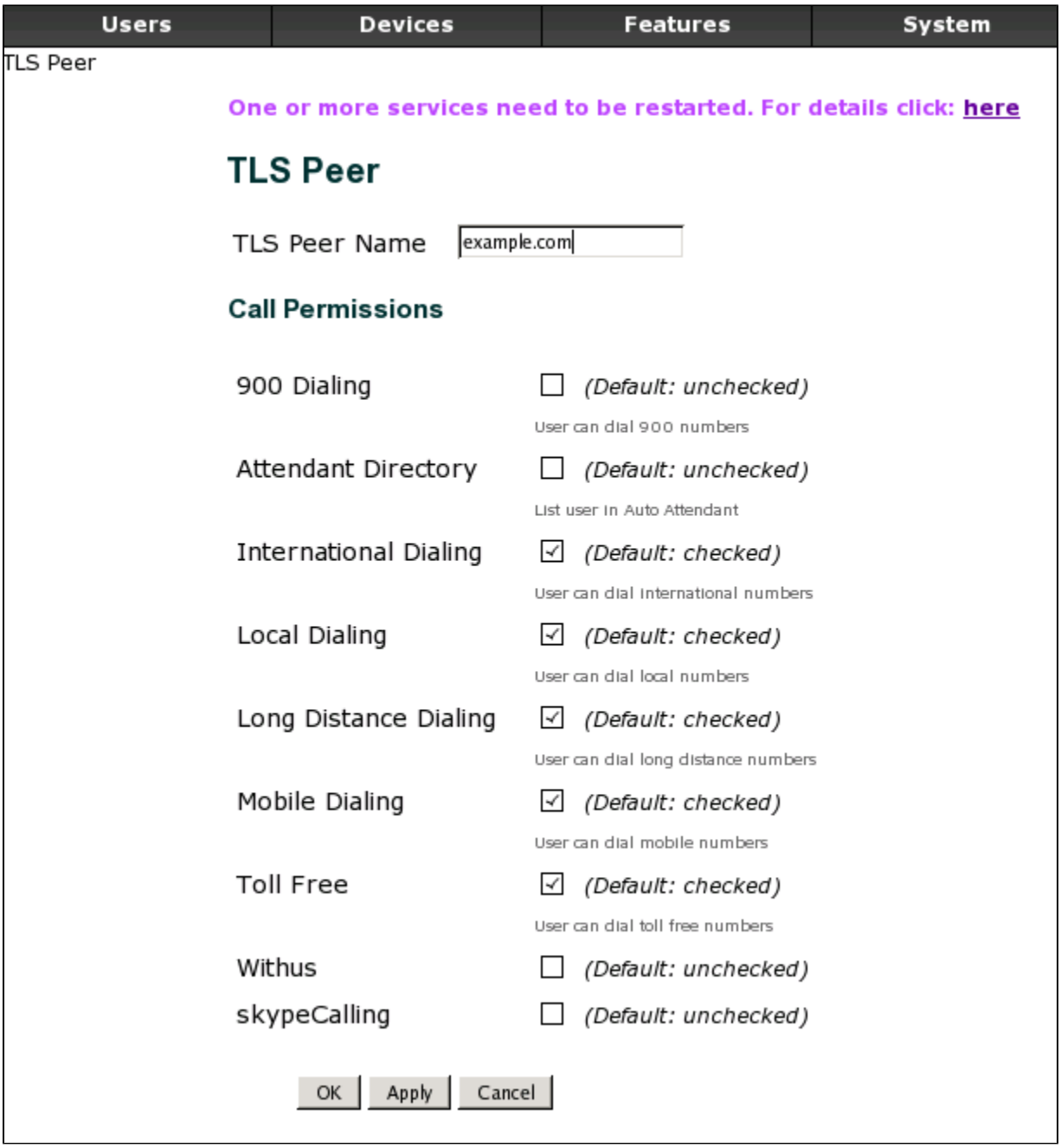
Now set the Gateway transport to TLS and change the port to match the remote TLS port (often 5061; for sipXecs to sipXecs, use 5081). It is necessary to restart the bridge as indicated on the screen.

Note that the remote system may need to be configured to send to port 5081 (the TLS port of a sipXbridge gateway).



Configure TLS Peer permissions (if desired)

An additional advantage of using TLS for remote gateways is that users of the remote system can be mapped to a sipXecs user, and may then use resources which require permissions (e.g. ITSP gateways, etc). To enable this mapping, add a TLS Peer under the Users menu, using as the TLS Peer Name the identity which the remote system presents in the SubjAltName field of its certificate (usually the SIP Domain or FQDN of the remote system). You can then specify permissions to be applied when any users from that system dial.



If no matching TLS Peer is configured, then a warning message will be logged in sipxbridge.log, containing the list of identities which were in the certificate: "No matching TLS Peer found for <list of identities in the certificate>.

Note that for this to work, the certificate sent by the remote system must implement draft-ietf-sip-domain-certs-04.txt , which recommends that the SIP domain identity be conveyed as a SubjAltName extension of type uniformResourceIdentitier .

Troubleshooting TLS connections

If the remote system's CA certificate is not installed, then a TLS connection will not be established and calls will be rejected with a failure response indicating the low level problem (e.g. "503 ValidatorException: unable to find valid certification path to requested target" or "SipException: PKIXCertPathBuilderImpl could not build a valid CertPath" (the exact message depends on the JVM being used).

If the remote certificate identity (from the SubjAltName field) does not match the remote system's address, then a TLS connection will not be established and calls will be rejected with reason 5xx "Certificate identity does not match requested domain". In this case, an alarm will be raised stating "The configuration requires the identity '<expected remote identity>', but the remote certificate contains only the following identities: <list of identities in the certificate>". sipXecs requires that remote systems support draft-ietf-sip-domain-certs-04.txt, which recommends that the SIP domain identity be conveyed as a SubjAltName extension of type uniformResourceIdentitier, and that that identity must match the domain to which the request is being sent.