TELNET
WORLDWIDE

Microsoft Teams Direct Routing Help Guide

Website Identity Authentication and Encryption

SSL Certificates

SSL stands for Secure Sockets Layer and is a security protocol that creates an encrypted link between a server and a browser. An SSL Cert. is a file presented by a web server that guarantees to your end users that their connection is authentic, and is used in the encryption process in tandem with an SSL key.

Private Keys

A private key is generated by your SSL certificate provider and is used to secure the communications between a client and a server.

SSL Certificate Validation

SSL Certificates are obtained through a Certificate Authority (CA), who validates that the organization requesting the SSL Certificate actually owns the domain in question. There are a few ways this can be validated:

1. **Email Validation**
   a. Requesting party provides domain for which they are ordering the certificate
   b. CA emails one of the email addresses specified in the WHOIS registry
   c. Requesting party follows process outlined in the email to validate the certificate
2. **CNAME Validation**
   a. Requesting party purchases the certificate and selects CNAME Validation at the end of the process
   b. Requesting party creates a new CNAME record from your DNS provider, as specified by the CA

CA Certificates

*also known as a Root CA Cert

Your certificate authority will also need to provide you with a CA certificate. The CA certificate is signed by the certificate authority and is used to authenticate that your SSL certificate truly did come from a trusted CA. This certificate is usually available from the same portal where you purchased your SSL certificate.

Where to Get an SSL and CA Certificate

You can get an SSL Certificate from any of the following links:

https://app.zerossl.com/signup/basic
www.cloudflare.com/ssl/
www.godaddy.com/web-security/ssl-certificate
https://sectigo.com/ssl-certificates-tls

A Note About FQDNs

An FQDN is a Fully Qualified Domain Name, and is used to find a unique resource on a domain. If your company's name is example.com and you wanted to stand up a new TelNet Worldwide SBC as part of the Microsoft Teams Direct Routing package, you might stand up a new server with telnetsbc.example.com.

Types of SSL Certificates

Wildcard SSL Certificates

Wildcard SSL Certificates can be used on multiple servers under the same domain.

- **Example:** example1.example.com and example2.example.com could some use the same certificate
- **Note:** If you have a Wildcard Certificate with a wildcard in the Common Name/System Name and or only a wildcard in the Subject Alternative Name, it will work, but is NOT supported.

Single Domain Certificates

Single Domain Certificates are only for one server.

- **Example:** example1.example.com would have a different SSL Certificate than example2.example.com