UC Connector Deployment Guide

Enabling Secure Communication

12/20/2025

Enabling Secure Communication

UC Connector supports the Kerberos protocol for establishing secure connections—using simple Transport Layer Security (TLS) or Mutual Transport Layer Security (MTLS)—between the UC Connector application and Microsoft Lync/Skype for Business Front End Server. Kerberos is required for integrations with the Front End Server to act as a client. MTLS is required to push presence status to Lync / Skype for Business.

About TLS/Kerberos Security

Kerberos is a secure method for authenticating a request for a service in a computer network. If configured for TLS/Kerberos secure communication, when UC Connector registers with Microsoft Lync / Skype for Business (by sending a SIP REGISTER request), the server will use Kerberos authentication procedures to send sip `401 Unauthorized` or sip `407 proxy authentication required` in the following cases:

- UCC is using regular TCP connection, and the UC Connector host IP address has not been added to the Trusted Host list.
- UCC is configured to use TLS connection.

To configure TLS/Kerberos, see the Kerberos information in the *UC Connector 8.0.3 Lync Integration Deployment Guide*, Security Procedures.

About MTLS

If configured for Mutual Transport Layer Security (MTLS), a shared trusted Certificate Authority (CA) on both the UC Connector host and the Lync deployment are used to establish secure communication. The certificates prove the identity of each server to the other.

To configure MTLS, see the *UC Connector 8.0.3 Lync Integration Deployment Guide*, Security Procedures.