Skype for Business Federation

Microsoft IT Showcase Course

Get ready to be what's next.

Microsoft

Agenda

Skype for Business (SfB)/Lync federation

Requirements for federation

Communication

Federation enablement tool

Appendix: Glossary

SfB/Lync federation

Microsoft Federations

What is SfB/Lync federation

What you get from federations

Types of federation – open

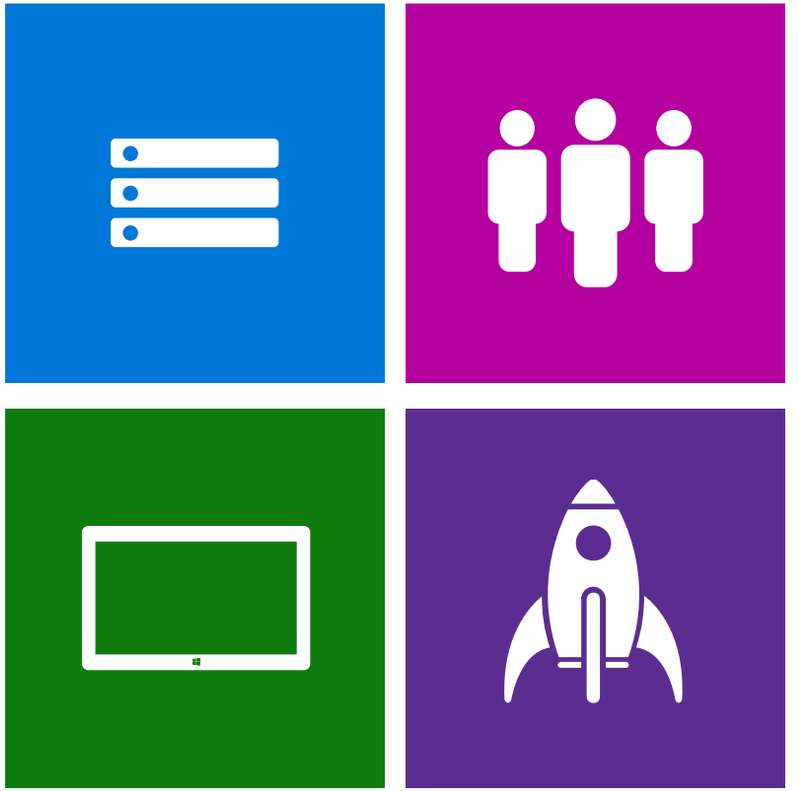
Types of federation – closed

SfB/Lync at Microsoft – Federations

17,000
Federated Domains

What is SfB/Lync federation?

- Allows for collaboration with external companies using SfB/Lync.
- Includes instant messaging (IM) and presence (P). Optionally, includes full audio/video, conferencing, and, application sharing.
- Provides secure communication through transport local area network (LAN) service (TLS) session negotiation.
- Supports on-premises deployment and Office 365 deployment.
- Supports domains using a hosting provider **(enabled by a manual exception process).**



What you get from federations

IM and Presence

- Ability to see the presenece of your customers
- Intitiate direct instant message conversations

Audio

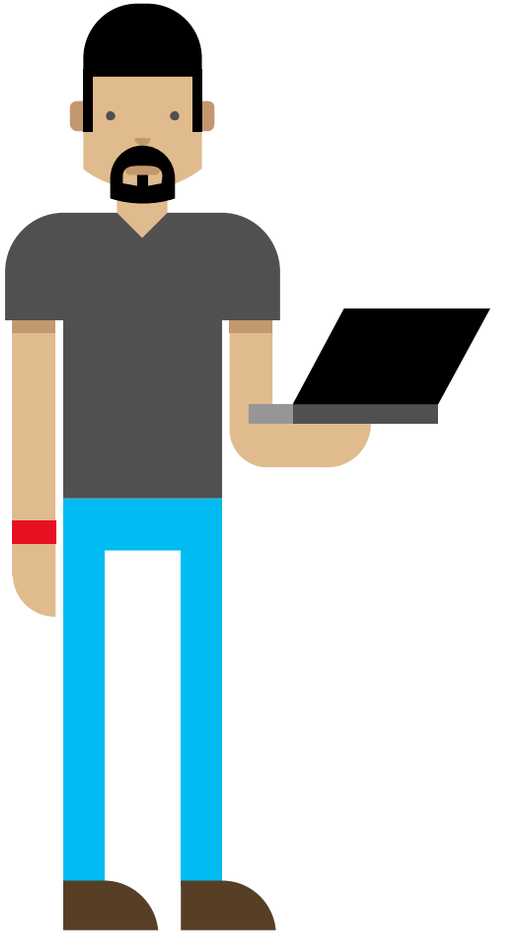
- Simply search for a contact and call with a single click
- On Net call with federated partners/customers or Skype

Video

- If face to face conversations are needed, just add video from the client.

Conferencing

- When there is a need to present data to multiple people, just start a conference with those who you federate with.



Types of federation

Open

- Auto lookup via Domain Name System (DNS) is used for requests
- Not supported by Microsoft IT due to security issues regarding SPIM (Spam IMs)

Note: Microsoft IT only supports closed enhanced federation

Types of federation

Closed

- **Enhanced:** An allow list is used to allow federation with foreign Session Initiation Protocol (SIP) domains. An edge server will look for their server record in DNS to find their edge server. A server certificate is required on both ends for TLS negotiation.
- **Direct:** We specify their edge server fully qualified domain name (FQDN) in the allow list along with the SIP domain.

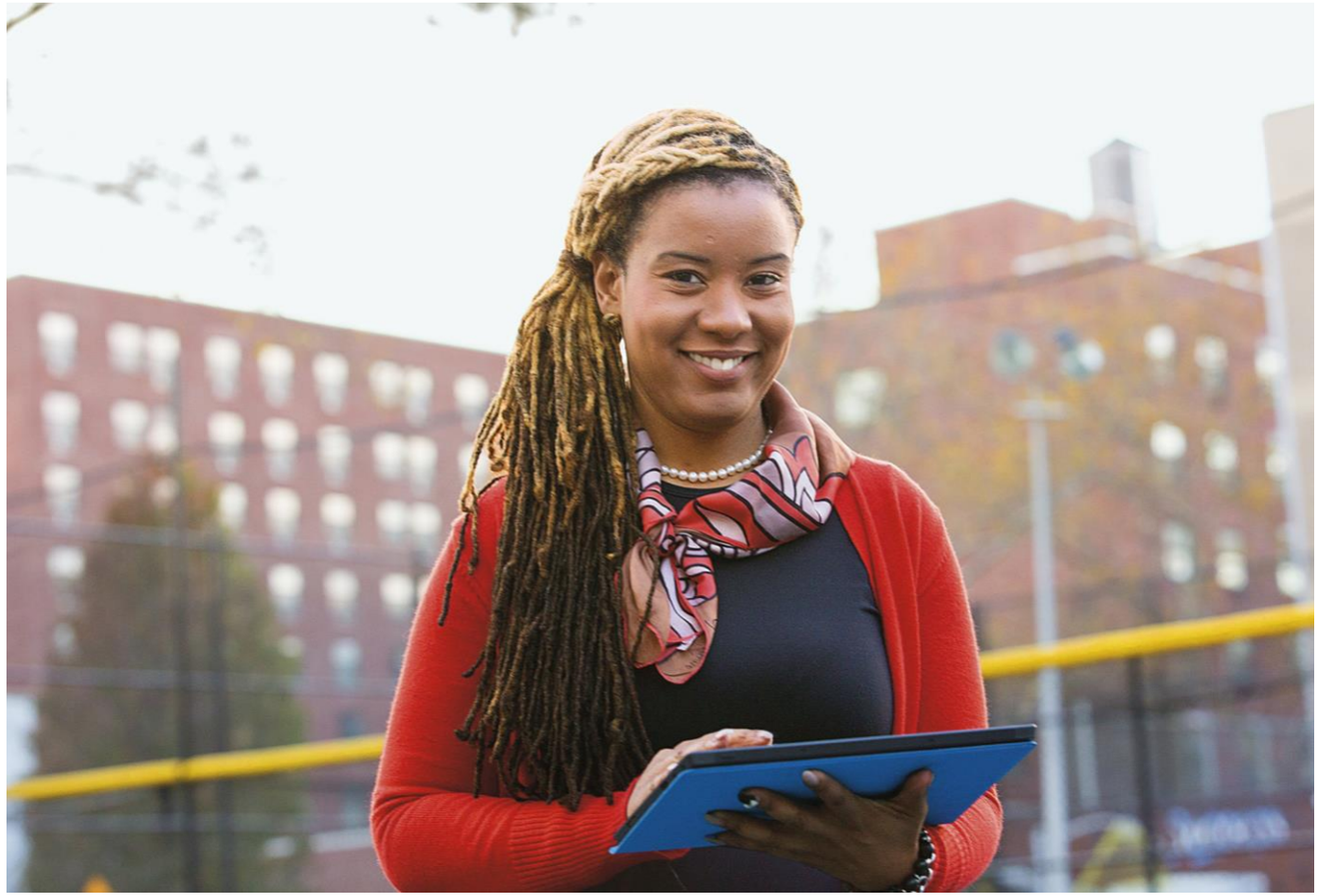
Note: Microsoft IT only supports closed enhanced federation.

Summary

SfB/Lync federation is a service that allows users to communicate with others outside their organization. There are two types of federation:

- Open federation, which is not support by Microsoft IT due to security issues.
- Closed enhanced federation is the only federation supported by Microsoft IT.

Requirements for federation



Requirements for enhanced federation

Requirements for enhanced federation

Firewall

- IM and Presence
  - Transmission control protocol (TCP): 5061 allow-all inbound and outbound
- Audio/Video
  - Outbound (edge to any):
    - Source TCP: 50,000-59,999 → Destination
    - User Datagram Protocol (UDP):3478
    - Source UDP:3478 → UDP:3478
  - Inbound (any to edge):
    - Source Any → Destination TCP:443
    - Source Any → Destination: UDP:3478

For additional information, review the following article:

[Determine external A/V firewall and port requirements for Lync Server 2013]

Requirements for enhanced federation, cont'd.

- Server certificate on edge server
  - Must be from a public certificate provider
  - Secure TLS session negotiation between the edge servers
- Target SIP domain edge server must trust the full chain of authority for Microsoft edge server's certificate
- Microsoft edge server must trust the full chain of authority for target SIP domain edge server's certificate
- Microsoft.com must be on the customer's **Allow** list
  - **Domain:** microsoft.com
  - **Access edge:** sipfed.microsoft.com
- Their SIP domain must be on our **Allow** list

Summary

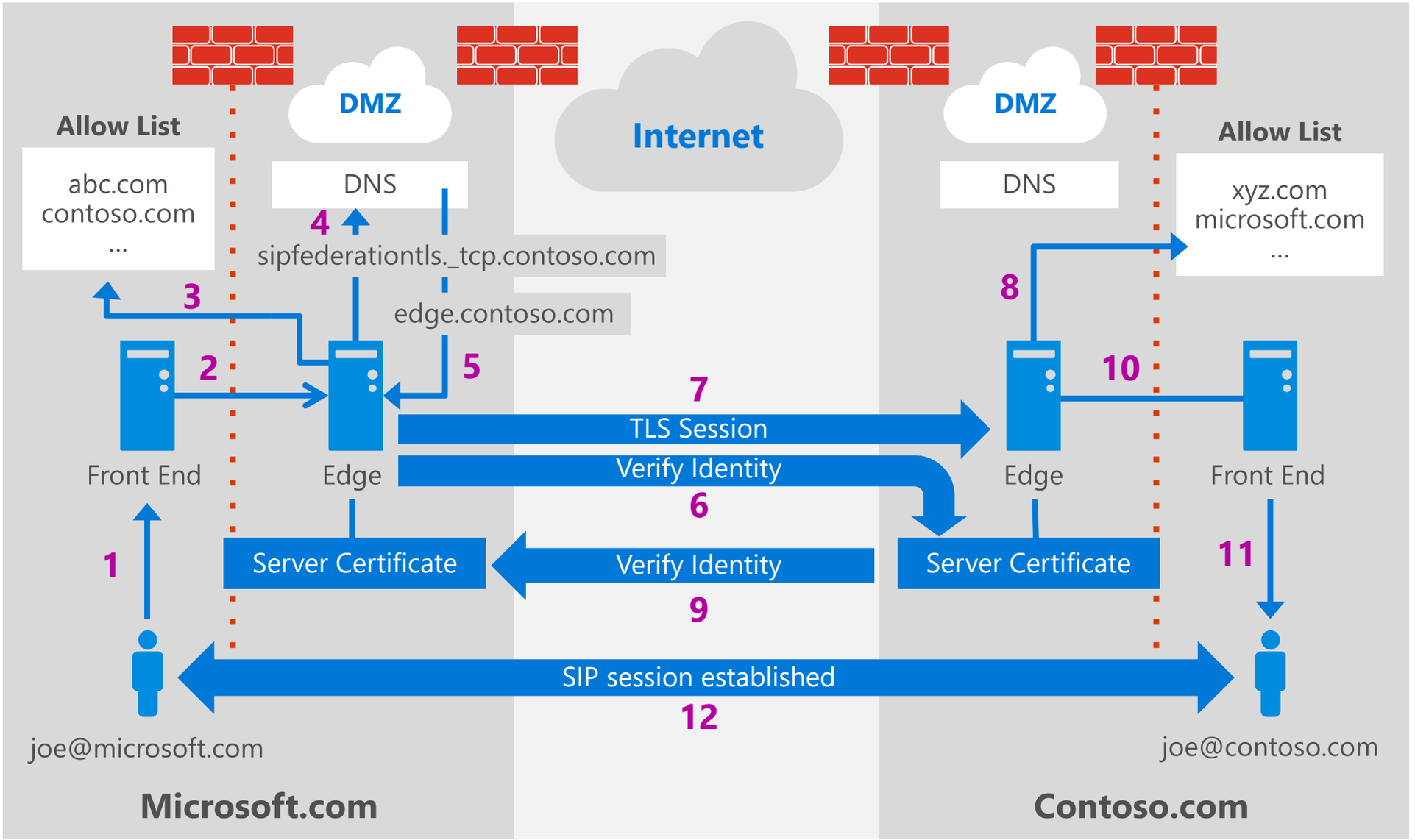
There are a number of requirements that must be met to successfully configure a SfB/Lync closed enhanced federation.

Communication

Federation communication process

Federation communication process

1. A user sends an IM to a federated contact.
2. Front end forwards the communication to edge as a foreign domain.
3. Edge checks the allow list.
4. Edge checks DNS for the SRV record of the federated domain.
5. DNS returns the FQDN of federated edge.
6. Edge checks cert of federated edge to verify identity.
7. Federated edge checks the allow list.
8. Federated edge checks our edge's certificate to verify identity.
9. A TLS session established with federated edge.
10. Federated edge forwards to front end.
11. Front end forwards to endpoint
12. An SIP session is established between endpoints.



Summary

Communication follows a very specific path that begins with a request and includes verification and validation.

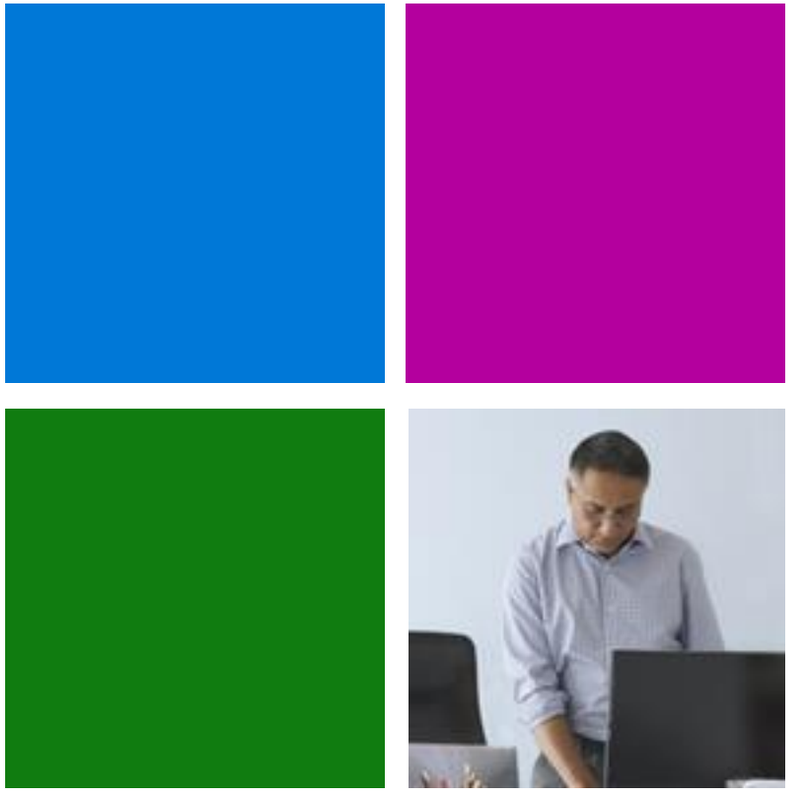
Federation enablement tool

Federation enablement tool

Lessons learned

Federation enablement tool

- **Requires:** Company name, SIP domain, contact @ partner company
- Automatically checks if a TLS session can be negotiated with the target SIP domain edge server.
- Will report back on success or failure on the page and in an email to the requestor including suggested method to resolve failure.
- If successful, the enablement will be fairly immediate. The customer contact's **Presence** info will be visible and you can IM your customer.



Federation enablement tool - lessons learned

- Automates getting SIP domains added to our **Allow** list.
- Initial success rate varies from week to week, this depends on the configuration of the partners edge.
- Vast majority of requests that fail initially are successful on second or third try after a configuration change.

Helpful Links:

- Planning: https://technet.microsoft.com/en-us/library/jj205335.aspx
- Setup: https://technet.microsoft.com/en-us/library/jj204800.aspx
- Managing: https://technet.microsoft.com/en-us/library/gg520966.aspx

Summary

The federation enablement tool helps you identify whether a TLS can be negotiated with a target SIP domain’s edge server, and it reports success or failure. The partner’s configuration is critical to the success of a federation.

Glossary

Federation glossary

Federation glossary

Contoso: A fictitious company that wants to federate with Microsoft.

Domain Name System (DNS): A naming system used on the internet and on private intranets for translating names of host computers into addresses (distributed database system for translating corp in xxx.com format).

Demilitarized zone (DMZ): A partially protected zone on a network that is not fully exposed to the internet but not fully behind the firewall. It is a host computer or computer network that is inserted as a neutral zone between two other computer networks one of both of which are untrusted.

Front end (FE): Front end server.

Fully qualified domain name (FQDN): Full site name of an internet computer system rather than a host name (i.e., www.yammer.com).

Instant messaging (IM): Real-time chat between two or more people.

Federation glossary

Local area network (LAN): A communications network connecting personal computers, workstations, printers and other devices inside a home, office, or facility. The connection uses copper wires or is wireless (WI-FI).

Office 365: Subscription-based Microsoft Office applications, both installed or in the cloud.

On-premises: The company manages the infrastructure to support their respective services (e.g., data centers, servers).

Presence (P): Ability to see the sender/receiver availability – busy, inactive, or away to identify the best mode of communication: mobile, email, or other.

Server (SVR): Shared computer on a local area network.

Session Initiation Protocol (SIP): Set up telephone calls, multimedia conferencing, IM, and other real-time connections

Federation glossary

Transmission Control Protocol (TCP): Transportation layer that is connection oriented with end-to-end protocol that provides sequenced, unduplicated delivery of bytes to a receiver or local user.

Transmission LAN service (TLS): Through the local server provider, allows the ability to send messages, mail and files from one LAN line to another LAN line.

Uniform resource identifier (URI): A unique identifier of a resource on the internet.

Uniform resource locator (URL): An address that can lead you to a file on any computer connected to the internet anywhere in the world.

User Datagram Protocol (UDP): Part of TCP/internet protocol suite. It provides for exchange of datagrams without acknowledgments or guaranteed delivery.