# Configuring the Skype for Business Bridge

# Domains and certificates

The first step in preparing a Skype for Business (S4B) Bridge is to assign it a hostname that other S4B Server deployments can connect to it via SIP federation. This requires configuring DNS records and obtaining a TLS certificate for that hostname, which can be any name of your choosing.

The hostname assigned to a S4B Bridge is also known as its "SIP domain", as it serves as the domain name of the virtual SIP server managed by the bridge for federating with S4B Servers. The rest of this guide refers to a bridge's SIP domain as `<bridge-sipdomain>`.

Once you've chosen a hostname to assign to your bridge, other S4B Servers must be able to resolve that hostname to the bridge's public IP address via DNS. The most straightforward way to achieve this is to obtain public DNS records for `<bridge-sipdomain>`. If obtaining public records is not an option, an S4B Server administrator may configure it with internal records instead (which is outside the scope of this guide).

The DNS records to obtain are as follows:

- `A/AAAA <bridge-sipdomain> <bridge-public-ip-address>`
- `SRV _sipfederationtls._tcp.<bridge-sipdomain> <any-priority> <any-weight> 5061 <bridge-sipdomain>` (optional, but recommended)

You must also obtain a TLS certificate for `<bridge-sipdomain>`. It may be obtained from either a public CSA like Let's Encrypt, or by any PKI scheme shared between the bridge & any S4B Servers it must connect with.

# Basic config

From the Installer's Integrations page, click "Install" under "Skype for Business Bridge".

The most important configuration options are under Advanced > Exposed Services, which is where to set the SIP domain & TLS certificates of the bridge:

- **Skype for Business Bridge Domain:** set this to `<bridge-sipdomain>`
- **SIP:**
  - If your ESS deployment allows for the usage of Host Ports, set "Port" to `5060` and "Port Type" to "Host Port".

    - Otherwise, you must configure a reverse proxy to redirect inbound traffic for port `5060` to the port you choose to assign this setting to.
- **SIPS:** Same as above, but with a port of `5061`.
- **TLS:** Choose "Certificate File" and upload the certificate & private key obtained for `<bridge-sipdomain>`.

# Configuring Skype for Business Server

In order for a S4B Server deployment to connect to your bridge, the deployment must first be configured with an Edge Server to support SIP federation & to explicitly allow federation with the SIP domain of the bridge.

This section describes how to modify an existing S4B Server deployment to federate with the bridge. It assumes that a functional S4B Server deployment has already been prepared; details on how to install a S4B Server deployment from scratch are out-of-scope of this guide.

# Overview

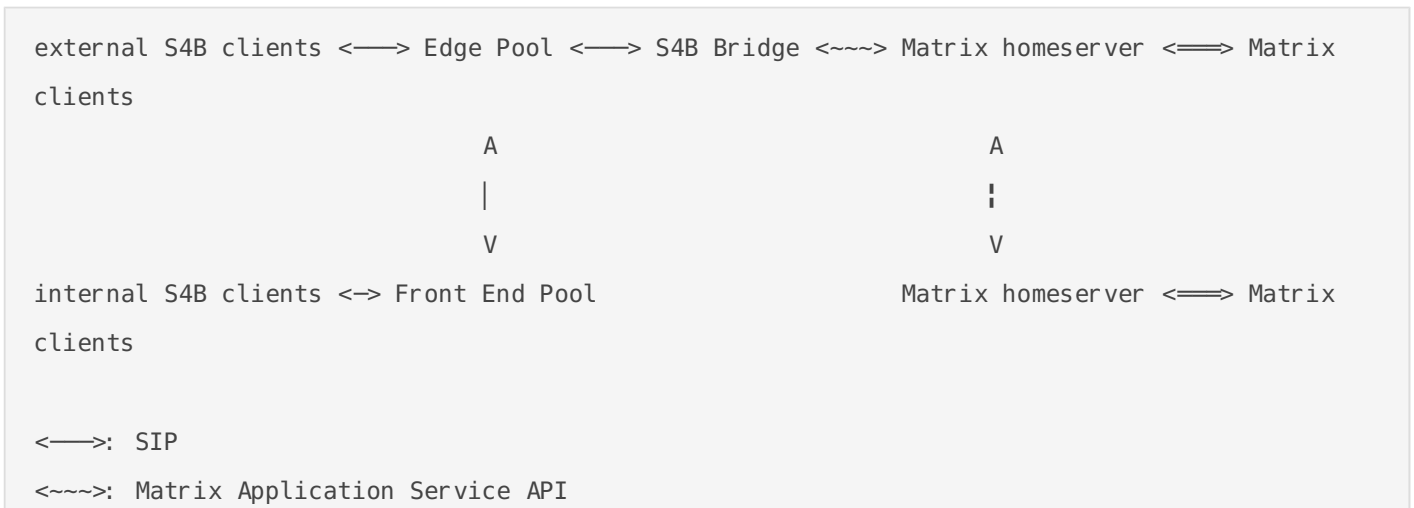
To support SIP federation, a S4B Server deployment uses a pool of one or more **Edge Servers** to relay traffic from external SIP domains to the pool of internal servers that provide the core functionalty of the deployment, known as **Front End Servers**. This design is necessary because Front End Servers are meant to be run within the private network of a deployment, without access to external networks.

Edge Servers are also used as a proxy for allowing native S4B users to log in from outside the deployment's private network. Users who connect in this manner are known as "remote users".

Once equipped with an Edge Server, a S4B Server deployment must then be configured with which external SIP domains it may federate with. By default, traffic from all external SIP domains is blocked.

The S4B Bridge acts as a SIP endpoint with its own SIP domain. Thus, for it to connect to a S4B Server deployment, the deployment must not only be equipped with an Edge Server, but it must set the bridge's SIP domain as an "allowed" domain.

Below is a simple diagram of the network topology of a S4B Server deployment federated with a S4B Bridge:



```
<═══>: Matrix Client-Server API
<------>: Matrix Federation API
```

**This guide covers only the usecase of a single Front End Server and Edge Server.** It is expected that similar instructions apply for multi-server pools, but that has not been tested.

# Prerequisites

A S4B Server deployment must be prepared with least the following components in order for it to be capable of adding an Edge Server:

- A Windows Server host running a Skype for Business 2019 Standard Edition Front End Server
- A Windows Server host acting as a Domain Controller for all hosts in the deployment, and also acting as an internal Certificate Signing Authority (CSA) & DNS server for all hosts
  - If a Domain Controller is not available to act as a CSA, you may use any alternative/custom PKI scheme of your choosing, as long as the root CA certificate is mutually trusted by all hosts.
  - If a Domain Controller is not available to act as a DNS server, custom hostname mappings may instead be applied in the "hosts" file of all hosts, located at `C:\Windows\System32\drivers\etc\hosts`.

Such a deployment will have set some hostnames, which are referred to elsewhere in this guide as follows:

- `<s4b-intdomain>`: The domain name / Primary DNS Suffix of the S4B Server deployment
- `<frnt>.<s4b-intdomain>`: The internal FQDN of the Front End Server, where `<frnt>` is its host name
- `<s4b-sipdomain>`: The default SIP domain of the deployment (visible in the Topology Builder on the Front End Server)

# Deploying the Edge Server

An Edge Server must be deployed on a standalone host within the private network of the S4B Server deployment. **It cannot be collocated on the same host as the Front End Server** (source).

The OS to install on the Edge Server's host must be either Windows Server 2019 or 2016. **Other versions of Windows Server, even newer versions, will not work** (source). It should also be the same version of Windows Server that is installed on the host running the Front End Server. The host must also be outside of the Active Directory domain of the deployment.

Assign the host with a name of your choosing, which will be referred to elsewhere in this guide as `<edge>`. The internal FQDN of the host is therefore `<edge>.<s4b-intdomain>`.

After installing the OS, ensure Internet connectivity and perform Windows Update. Then, use the Server Manager desktop app (which can be found in Windows Search) to install the prerequisites listed by the official S4B

documentation. **Do not install any components needed for a Front End Server**, as they may interfere with Edge Server components. It is also recommended to **not install IIS on the Edge Server**, despite the official documention, as it interferes with VoIP functionality.

Next, install the Skype for Business Administrative Tools. You may use the same installation media that was used for installing the Front End Server. Otherwise, it may be obtained from this download link.

Running the installation media will install two programs, known as the Core Components: the Deployment Wizard and the Management Shell. When using the Deployment Wizard on the Edge Server's host, **do not run any tasks related to Active Directory**, which should have already been run on the Front End Server, and must be run only once for the entire deployment. **It is also unnecessary to install the rest of the Administrative Tools**, such as the Topology Builder, on the Edge Server host.

# Network topology

The network interfaces of hosts within the deployment must be configured such that inbound external SIP traffic is handled solely by one interface of the Edge Server, and that traffic between the Edge and Front End Servers remains within the private network of the deployment.

**The Edge Server needs at least two network interfaces:**

- an external-facing interface for accepting inbound SIP traffic
  - Its default gateway must at least have a route to the IP address of your S4B Bridge instance.
  - If the Edge Server host is behind NAT, inbound traffic must be routed to this interface.
- an internal-facing interface for reaching hosts within the private subnet of the deployment
  - Its DHCP Server must be set to the internal IP address of the deployment's Domain Controller.
  - This interface must not be routable to the public Internet.

Also, the firewall of the Edge Server must at least leave port 5061 open, and have it accessible to either the public Internet, or to the public IP address of your S4B Bridge host.

**The Front End server needs at least one network interface**, and for it to be an internal-facing interface with the same properties of the Edge Server's internal-facing interface. If Internet connectivity is desired (like for facilitating Phone Access & Meeting URLs), add a separate external-facing interface for handling external traffic, instead of making the internal-facing interface publicly routable.

The IP addresses of these interfaces are referred to elsewhere in this guide as follows:

- `<edge-extaddr>`: the address of the Edge Server's external-facing interface
- `<edge-intaddr>`: the address of the Edge Server's internal-facing interface
- `<frnt-intaddr>`: the address of the Front End Server's internal-facing interface

# DNS records

# Internal records

The deployment needs an internal DNS record for the Edge Server's internal-facing interface in order to identify it by name. To add this record, open the DNS Manager on the Domain Controller host, and add an A/AAAA record for `<edge>.<s4b-intdomain>`, the FQDN of the Edge Server host, with the target address set to `<edge-intaddr>`.

# External records

In order for your S4B Bridge to reach your Edge Server, acquire these public DNS records for advertising the SIP domain of your S4B Server deployment:

- `A/AAAA <edge>.<s4b-sipdomain> <edge-extaddr>`
- `CNAME sip.<s4b-sipdomain> <edge>.<s4b-sipdomain>`
- `SRV _sipfederationtls._tcp.<s4b-sipdomain> <any-priority> <any-weight> 5061 <edge>.<s4b-sipdomain>`

# Topology configuration

The topology of your S4B Server deployment may now be updated to include the Edge Server.

On the Front End Server, open the Topology Builder. Choose the option to download the current topology to a file, as this will ensure that you will edit an up-to-date version of the topology in the following steps.

Once the topology is loaded, navigate through the tree list on the left of the window to find the "Edge pools" entry (under "Skype for Business" > "site" > "Skype for Business Server 2019" > "Edge Pools"), right click it, select "New Edge Pool...", and apply the following settings in the wizard that appears:

- Pool FQDN: set to `<edge>.<s4b-intdomain>`
- Enable "This pool has one server"
- Enable federation (port 5061)
- Use a single FQDN and IP address
- Apply IPv4/6 settings so that you will be able to use the Edge Server's internal & external interface addresses later.
- External FQDN: set to `<edge>.<s4b-sipdomain>`
- Leave service ports at their default of 5061, 444, and 443 for Access, Web Conferencing, and A/V Edge Services respectively
- Internal & external IPv4/6 addresses: set these to addresses of the internal & external interfaces you set up earlier. **The internal interface is never 127.0.0.1.**
- Next hop pool & media association: set this to the Front End Server (which should be the only choice)

Next, in the settings for your site (available by right-clicking the tree entry immediately below the top-level "Skype for Business Server" item and choosing "Edit Properties"), enable:

- Apply federation route assignments to all sites
- Enable SIP federation, and choose your Edge Server

All required topology changes have now been set. To apply these changes onto the Front End Server:

- Using the menu bar at the top of the Topology Viewer window, click "Action" > "Topology" > "Publish..." (The progress window may display errors, but these can typically be ignored.)
- Open the Deployment Wizard, click "Install or Update Skype for Business Server System", and execute the "Install Local Configuration Store" step. Choose the option to "retrieve directly from the Central Management Store".
- While still in the Deployment Wizard, execute the "Setup or Remove Skype for Business Server Components" step.

The toplogy must next be published onto the Edge Server. To do so:

- On the Front End Server, open the S4B Management Shell, and export the topology to a file with this command:
  - `Export-CsConfiguration -FileName <path\to\file>`
- Copy that file onto the Edge Server. Ideally export the file to a shared drive so that a manual copy is unnecessary.
- On the Edge Server, open the Deployment Wizard, click "Install or Update Skype for Business Server System", and execute the "Install Local Configuration Store" step. Choose the option to "import from a file (recommended for Edge Servers)", and select the file for the exported topology configuration.
- While still in the Deployment Wizard, execute the "Setup or Remove Skype for Business Server Components" step.

# Certificates

S4B sends/receives all SIP traffic over TLS; thus, the Edge Server needs its own set of certificates, both internal & external to the S4B Server deployment.

To obtain all required certificates, open the Deployment Wizard on the Edge Server, click "Install or Update Skype for Business Server System", and execute the "Request, Install or Assign Certificates" task. This will display the Certificate Wizard, which shows a list of all required certificates, and which services they must contain the domain names of. Only two certificates should be listed: "Edge internal" and "External Edge certificate (public Internet)".

The "Edge internal" certificate should be obtained by sending a certificate signing request to the Domain Controller in your deployment, which acts as an internal Certificate Signing Authority. To do so, click the "Edge internal" entry in the list, then click the Request button on the right edge of the window. This will display a dialog that guides you through the steps of sending the request. Once the request is sent, enter the Domain Controller, accept the request, and then go back to the Edge Server to assign the approved certificate.

In contrast, the "External Edge certificate" must be provided by a Certificate Authority that is trusted by the host running the S4B Bridge. This may be a public CA such as Let's Encrypt, or any custom PKI scheme of your choosing. If using the latter, ensure that the root CA's certificate is installed on both the Edge Server host and the S4B Bridge host.

The "External Edge certificate" must contain these names:

- Subject Name: `<edge>.<s4b-sipdomain>`

- Subject Alternative Names:
  - DNS Name: `<edge>.<s4b-sipdomain>`
  - DNS Name: `sip.<s4b-sipdomain>`

Once the certificate is obtained, use the Certificate Wizard on the Edge Server to assign it.

# Restart to apply changes

Changes to server topology requires restarting system services on both the Front End Server and Edge Server. To do so, open the Management Server on each server, and run these commands:

1. Run `Stop-CsWindowsService` on the Edge Server, and wait for it to complete.
2. Run `Stop-CsWindowsService` on the Front End Server, and wait for it to complete.
3. Run `Start-CsWindowsService` on the Front End Server, and wait for it to complete.
4. Run `Start-CsWindowsService` on the Edge Server, and wait for it to complete.

# Federation settings

With the topology in place, the S4B Server deployment may now be configured to allow federation with your S4B Bridge. Federation settings may be applied on the Front End Server either in the web admin panel at `https://<frnt>.<s4b-intdomain>/macp`, or via Powershell commands in the Management Shell. This section lists each setting that must be applied in the web admin panel, followed by its equivalent Powershell in the Management Shell.

Log into the admin panel using the credentials of your Windows account on the Front End Server, and expand the "Federation and External Access" section on the left sidebar. Then, navigate to the following sections and apply these settings:

- External Access Policy:
  - In either the Global policy or a site-level policy for your S4B site:
    - "Enable communications with federated users"
  - Powershell:
    - To edit the Global policy: `Set-CsExternalAccessPolicy -Identity Global -EnableFederationAccess $True`
    - To create & configure a site-level policy: `New-CsExternalAccessPolicy -Identity Site:<your_site_name> -EnableFederationAccess $True`
- Access Edge Configuration
  - In Global policy (the only option available):
    - "Enable federation and public IM connectivity"
    - *Optional:* "Enable partner domain discovery": Enable this if you would rather have federation be managed dynamically instead of having to explicitly add the SIP domain of your bridge to your S4B Server's allowlist of federated domains. For this to work, you must register a DNS SRV record for your bridge's SIP domain (see the section on bridge domains and certificates). However, adding the bridge's domain to your S4B Server's allowlist is still necessary to prevent the bridge's traffic from being rate-limited.

    - Powershell: `Set-CsAccessEdgeConfiguration -AllowFederatedUsers $True [-EnablePartnerDiscovery $True -DiscoveredPartnerVerificationLevel "AlwaysVerifiable"]`
- SIP Federated Domains
    - add your S4B Bridge's SIP domain as an Allowed Domain:
        - Domain name (or FQDN): `<bridge-sipdomain>`
        - Access Edge service (FQDN):
            - If you registered a DNS SRV record of `_sipfederationtls._tcp.<bridge-sipdomain>`, leave this blank.
            - Otherwise, set this to `<bridge-sipdomain>`.
        - Powershell: `New-CsAllowedDomain -Identity "<bridge-sipdomain>" -Comment "<any-name-of-your-choice>"`

To verify any of these settings in Powershell, replace `New-` or `Set-` in any of the issued commands with `Get-`. To unapply a setting, use `Remove-`.

These changes may take some time before they get applied. When in doubt, restart all services by running `Stop-CsWindowsService` then `Start-CsWindowsService` in the S4B Server Management Shell on both the Front End Server and the Edge Server.

# Contact mapping

# Matrix users in S4B

Once a S4B Server is connected to an instance of the bridge, a Matrix user may be added to a S4B user's contact list as a "Contact Not in My Organization". The S4B desktop client provides this action via the "Add a contact" button, which is on the right edge of the main window just below the contact search bar.

Proceeding will display a prompt to set the IM Address of the contact to be added. Technically, an IM Address is a SIP address without the leading `sip:` scheme.

The IM Address of a Matrix user managed by the bridge is derived from the user's MXID, and has the following mapping:

`@` **`username`** `:` **`matrixdomain`** ? **`username`** `+` **`homeserver`** `@` **`bridge-sipdomain`**

- **`username`**: the "localpart" of the MXID.
- **`matrixdomain`**: the domain name of the Matrix user's homeserver.
- **`bridge-sipdomain`**: the SIP domain of the bridge (which may differ from the homeserver domain).

# S4B users in Matrix

S4B users are represented in Matrix by virtual "ghost" users managed by the bridge. The MXID of a virtual S4B user is derived from the "Bridge > User Prefix" setting (from the bridge's Integrations configuration page in the

Installer) and the IM Address (i.e. the SIP Address) of the virtual user's corresponding S4B user, and has the following mapping:

`username` `@` `s4b-sipdomain` ? `@` `<user-prefix>` `sip=3a` `username` `=40` `s4b-sipdomain` `:` `matrixdomain`

- `<user-prefix>`: the value of "Bridge > User Prefix" from the bridge's configuration. The default value is `_s4b_`.
- `sip=3a`: the URL encoding of the `sip:` scheme of an IM Address (with an escape character of `=` instead of the typical `%`), encoded so as to not conflict with the `:` belonging to the MXID.
  - Note that despite S4B using TLS for all SIP traffic, the IM Addresses of S4B contacts never use the `sips:` scheme.
- `username`: the "localpart" of the IM Address.
- `=40`: the URL encoding of the `@` character of the IM address, encoded so as to not conflict with the `@` belonging to the MXID.
- `s4b-sipdomain`: the SIP domain of the S4B Server.
- `matrixdomain`: the domain name of the homeserver that the bridge is registered with.

Thus, with a `<user-prefix>` of `_s4b_`, the IM Address to MXID mapping is:

`username` `@` `s4b-sipdomain` ? `@_s4b_sip=3a` `username` `=40` `s4b-sipdomain` `:` `matrixdomain`

---

Revision #1
Created 26 October 2023 15:11:10 by Andrew Ferrazzutti
Updated 30 October 2023 20:20:44 by Andrew Ferrazzutti