Microsoft Skype for Business Deployment Guide

Provisioning for UCMA Connectors

5/6/2025

Provisioning for UCMA Connectors

In version 9.0 of Multimedia Skype for Business, there is:

- One UCMA Connector for Skype for Business using UCMA 5.
- One UCMA Connector for Skype for Business using UCMA 6.

> **Important**
> Support for UCMA 4 is deprecated from release 9.0.

You can provision for UCMA Connectors by either using shell scripts or by using the Skype for Business Topology Builder.

This section contains instructions for provisioning an UCMA Connector application on a trusted application pool with multiple computers, using the Skype for Business Server Management Shell.

See details in Microsoft Developer Network documentation:

- Skype for Business

To provision for UCMA Connectors using shell scripts:

1. Create a **trusted application pool** with the computer(s) where UCMA Connector(s) will be running.
   A. Create a pool with one computer. For example:

```
New-CsTrustedApplicationPool -Identity “trustedpool.skype.lab” -Registrar
Registrar:”pool01.skype.lab” -Site “DalyCity” -ComputerFqdn
“computer1.skype.lab”
```

   B. Add a second computer to the pool. For example:

```
New-CsTrustedApplicationComputer -Identity “computer2.skype.lab” -Pool
“trustedpool.skype.lab”
```

   C. Repeat the above step to add another computer as required.

> **Important**
> On the Skype For Business Front End Pool that is used by Connector, the Meeting Configuration option **PstnCallersBypassLobby** must be enabled. This feature is enabled by default when creating a new Application Pool in Skype For Business so no specific action is required, but this feature should never be

disabled on the Front End Pool used by Connector.

2. Create and enable a new **trusted application** with the service port of the UCMA Connectors and assign this trusted application to the UCMA Connector trusted application pool. For example:

```
New-CsTrustedApplication -ApplicationId “Connector_app” -TrustedApplicationPoolFqdn
“trustedpool.skype.lab” -Port “6001”
```

3. Run the Enable-CsTopology cmdlet to create the appropriate trusted service entries:

```
Enable-CsTopology
```

4. To balance the load among UCMA Connectors, configure **DNS-based load balancing** for the application pool. For example, there are two computers in the application pool `trustedpool.skype.lab`, so the following entries must be present in the DNS:
`computer1 Host(A) 123.1.1.1`
`computer2 Host(A) 123.1.1.2`
`trustedpool Host(A) 123.1.1.1`
`trustedpool Host(A) 123.1.1.2`

   DNS Time to live (TTL) for these entries must be set to `0`.

Important

- Relevant DNS AAAA records are also required for application pools and computers that are used in IPv6 network.
- Because balancing the load between Connectors is based on DNS load balancing, it is not 100% fault-resistant. All Trusted Applications (Connectors) must be running on all computers in the Trusted Application Pool. If some Trusted Applications (Connectors) are not running, call reporting might be delayed. That delay will depend on System Network failure detection, for which any misconfiguration must be corrected as soon as possible.

5. Create **certificates** for the UCMA Connector computers in a trusted application pool. For example:

```
Request-CsCertificate -New -Type default -FriendlyName "trustedpool.skype.lab Pool"
 -CA dc.skype.lab\DC-CA -ComputerFQDN trustedpool.skype.lab -DomainName
 "computer1.skype.lab,computer2.skype.lab"
```

   Each host in the pool must import a copy of this certificate.

Important

For additional information about provisioning for UCMA connectors, consult the Multimedia Connector for Skype for Business Configuration of Microsoft Skype for Business platform White Paper.

Back to Deployment Summary