imagicle

Configuration for Microsoft Skype for Business Presence

Architecture

Imagicle Presence Service connects directly to Microsoft Lync / SfB Frontend Service through Microsoft UCMA API.

Requirements

- Imagicle presence service is compatibile with Microsoft Lync 2010 server and above (Skype for Business server).
- Connection to Microsoft Lync / SfB requires Windows Server 2008 R2 64 bit or better (32 bit not supported).

Configuration Task List

The main configuration steps are:

1. Choose the EndPoint type
2. Configure Microsoft Lync/Skype for Business Server
3. Configure Imagicle AppSuite Server
4. Configure Imagicle Presence Service

Choose EndPoint Type

An UCMA application can connect to Microsoft Lync / SfB in three different modes, that have different requirements. Here they are, ordered from the quicker to setup to the slower:

- User End Point without Secure TLS Connection
- User End Point with Secure TLS Connection
- Trusted Application End Point (manually provisioned)

User End Point without Secure TLS Connection

In this mode, Imagicle Presence Service impersonates a standard Microsoft Lync / SfB user to queries for other users' presence.
Hence, a Microsoft Lync / SfB user is required to be created specifically.
This mode doesn't require the Imagicle Application Suite to be been joined to the Microsoft Lync / SfB Server domain.
This mode uses a non-secure SIP connection.

User End Point with Secure TLS Connection

It's like *User End Point without Secure TLS Connection*, except that a secure TLS SIP connection to Microsoft Lync / SfB Server is used. So you need to install a Web Server certificate from the network Certification Authority (see below).

Trusted Application End Point (manually provisioned)

In this mode, Imagicle Presence Service does not represent an individual user, hence it is not required to create a dedicated Microsoft Lync / SfB user. A secure TLS SIP connection to Microsoft Lync / SfB Server is used. You need to to install a Web Server certificate from the network Certification Authority (see below). On the other hand, it's mandatory to join the Imagicle Application Suite to the Microsoft Lync / SfB Server domain.

Microsoft Lync / SfB Configuration

User End Point without Secure TLS Connection

The configuration task list is:

1. Create an ad-hoc user on Active Directory
2. Enable user on Microsoft Lync / SfB Server
3. Enable non secure standard SIP port on Microsoft Lync / SfB Server:
   On a Microsoft Lync / SfB Server node, open "Lync / SfB Server Management Shell" and execute the command:

   ```
   Set-CsRegistrar "registrar:fqdn-registrar.domain" -SipServerTcpPort 5060
   ```
4. Ensure that port 5060 of Microsoft Lync / SfB Front End Server is reachable via TCP from the Imagicle Application Suite server

User End Point with Secure TLS Connection

The configuration task list is:

1. Create a dedicated user on Active Directory
2. Enable the user on Microsoft Lync / SfB Server

Application End Point (manually provisioned)

A trusted application requires an entry in the Microsoft Lync / SfB Server topology document that specifies the computers on which the application runs. The main steps to configure Microsoft Lync / SfB Server are:

1. Create a Trusted Application Pool for Imagicle Server
2. Create a Trusted Application for Imagicle Presence Service
3. Enable modification to the topology

On a Microsoft Lync / SfB Server node open the "Lync / SfB Server Management Shell" and execute all commands explained in this section.

Create a Trusted Application Pool for Imagicle Server

First of all, the Imagicle Server must be configured as a Trusted Application Pool server within Microsoft Lync / SfB topology. You can skip this step if you have already configured a Trusted Application Pool to activate Queue Manager Enteprise integration.
To check whether a Trusted Application Pool already exists for Imagicle server, execute command:

```
Get-CsTrustedApplicationPool -Identity fqdn-ImagicleApplicationServer
```

If you get an error, the Trusted Application Pool does not exist. You can create it executing the following command (pay attention to adjust the FQDN of Front End node):

```
New-CsTrustedApplicationPool -Identity fqdn-ImagicleApplicationServer -Site site-ImagicleApplicationServer -registra
```

Create a Trusted Application for Imagicle Presence Service

To configure Imaigcle Presence Service as a Trusted Application within Microsoft Lync / SfB, execute the following command:

```
New-CSTrustedApplication -ApplicationId ImagicleLyncConnector -TrustedApplicationPoolFqdn fqdn-ImagicleApplicationSe
```

This will return a result similar to:

```
Identity: fqdn-ImagicleApplicationServer/urn:application:imagiclelyncconnector
ComputerGruus: {fqdn-ImagicleApplicationServer sip:fqdn-ImagicleApplicationServer@youtdomain..uu;opaque=srvr:imagicl
ServiceGruu: sip:fqdn-ImagicleApplicationServer@yourdomain..uu;opaque=srvr:imagiclelyncconnector:atifA-VpOFO2x9rrBUE
Protocol: Mtls
ApplicationId: urn:application:imagiclelyncconnector
TrustedApplicationPoolFqdn: fqdn-ImagicleApplicationServer
Port: 14001
LegacyApplicationName: imagiclelyncconnector
```

Copy the **ServiceGruu** paste into a temporary text file - this will be required later, in step "Presence Service Configuration".

Enable modification to the topology

To apply all above modifications, execute command:

```
Enable-CsTopology
```

Imagicle Server Configuration

Imagicle server needs to be configured once, through these steps:

1. Instal UCMA Runtime 3.0
2. Join Active Directory Domain (only when using Trusted Application End Point)
3. Install Web server Certificate (only when using a secure SIP connection)

Install UCMA Runtime 3.0

Imagicle Presence Service with Microsoft Lync / SfB integration needs Microsoft UCMA **version 3.0** runtime to run. You must download it from www.imagicle.com/go/UCMA and install it on Imagicle Application Server.

Note: Microsoft UCMA version 3.0 is compatible with Microsoft Lync 2010, 2013 and SfB 2015.

Note: while Presence integration requires UCMA 3.0, QME integration with Microsoft Lync / SfB requires UCMA 4.0, that does not replace UCMA 3.0. So, if you plan to use both QME and Presence, you have to install first UCMA 4.0 Runtime, then UCMA 3.0 Runtime.

Join Active Directory Domain

If you have planned to configure Presence integration as Trusted Application End Point, Imagicle Server must be joined to the Microsoft Lync / SfB Server domain.

Install a Web server Certificate

If you have planned to configure Presence integration to use secure connection to Microsoft Lync / SfB Front End Server (i.e. if you have choosed either *User End Point with Secure TLS* or *Trusted Application*), you have to get a Web Server certificate from the network Certification Authority and install it as a computer certificate on the Application Suite server.

Certificate enrollment

1. Log in to the Imagicle Application Server as an administrator with permission to *Enroll for a Web Server Certificate* (e.g. a Domain Administrator)..
2. Click the **Start** button, then **Run**, type **cmd.exe**, right click over **Command Prompt** and click on **Run as administrator**
3. In the Command prompt shell, type **mmc.exe**.
4. Open the **File** menu and select **Add/Remove snap-in**.
5. In the Add or Remove Snap-ins window, select **Certificates**, and click **Add**.
6. Choose **Computer Account**, and click Next.
7. Choose **Local Computer**, and then Finish.
8. Click OK on the Add or Remove Snap-ins window.
9. Expand **Certificates**.
10. Expand **Trusted Root Certification Authorities** and click **Certificates**. Make sure the root certificate is present for the Enterprise Certificate Authority in the domain.
11. Right-click Personal and select All Tasks, then **Request New Certificate**.
12. Click Next.
13. If prompted to select a Certificate Enrollment Policy, select one under the category of Configured by your administrator. Click Next.
14. Select **Web Server** (If Web server is unavailable see the WebServer certificate section), and click the link for *More information is required to enroll for this certificate*. Click here to configure settings.
15. Click the **Subject** tab.
16. For Microsoft Lync Server 2010/2013/SfB:
    1. Under the Subject Name section, change the **Type** to Common Name, and change the **Value** of the Fully Qualified Domain Name of the Microsoft Lync / SfB Server Pool (e.g. sfb.mydomain.com), and then click **Add**.
    2. Under the **Alternative Name** Section, change the Type to **DNS**, and change the **Value** to the Fully Qualified Domain Name of the Microsoft Lync / SfB Server Pool (e.g. sfb.mydomain.com), and then click **Add**.
    3. Again, under the Alternative Name Section, leave the Type specified as DNS, and change the **Value** to the Fully Qualified Domain Name of the server hosting the Imagicle Application Suite (e.g. ias.mydomain.com).
    4. Click Add.
17. Click the General tab.
18. Type **OCSConnector** for the Friendly Name, then click Apply, and OK.
19. On the Certificate Enrollment window, click Enroll.
20. Verify that the **STATUS** is Succeeded, and click Finish.

WebServer certificate

If there is no available WebServer certificate, you have to create it.

1. On the CA computer, click **Start**, type **certtmpl.msc**, and then press ENTER.
2. In the contents pane, right-click the **Web Server** template, and then click **Properties**.
3. Click the **Security** tab, and then click **Add**.
4. Click **Object Types**
5. Flag **Computers** checkbox
6. In **Enter the object names to select**, type the name of Imagicle Application Suite Server, and then click **OK**.
7. In **Permissions**, click **Enroll** under **Allow**, and then click **OK**.

Imagicle Presence Service Configuration

Please configure the users properties as described in the Imagicle Presence Service configuration section of this guide.

Login into Imagicle Application Suite web portal with global administrative privilege. Go to *Administration*, *Presence* web page, select *Configuration* tab and then:

- **Enable rich presence services (Microsoft Lync / SfB based)** by flagging the checkbox
- Select the End Point of your choiche

User End Point Configuration

Fill all the following fields:

- **Microsoft Lync / SfB Server Address:** FQDN of Microsoft Lync / SfB Front End server
- **Use TLS:** flag if connection with Microsoft Lync / SfB Server is Secure SIP (needs a valid certificate released by the network Authority - see above)

Credentials

Fill the following fields with credentials of the ad-hoc created user (see paragraph "*Microsoft Lync /SfB Configuration - User End Point*"):

- **Username:** enter the username of the ad hoc created monitoring user
- **URI:** enter the sip address of the ad hoc created user, in the format user@mydomain.com.
  E.g. imagicle.presence@imagicle.com
- **Password:** enter the password of the ad hoc created monitoring user
- **Domain:** enter the domain of the presence server e.g. IMAGICLE.COM

Application End Point Configuration

- **Microsoft Lync / SfB Server Address:** enter FQDN of Microsoft Lync / SfB Front End server
- **Application Contact URI:** enter an existing Lync / SfB SIP URI (e.g. Lync / SfB_administrator@yourdomain.com)
- **Application Gruu:** enter the **ServiceGruu** value returned by New-CSTrustedApplication command
- **Certificate Name**: enter the Friendly Name of the certificate installed on Imagicle server
- **Application Host**: check that matches value used for **Identity** parameter in **New-CsTrustedApplicationPool** command
- **Application Port**: check that matches the **Port** value returned by **New-CSTrustedApplication** command