Skype/Lync Presence - Configuration Best Practices

On this Page

Related Articles

- Managing Node-Level SIP Settings

The instructions in this Best Practice assume the SBC Edge node is running and connected to the WebUI.

Overview - Skype/Lync Presence

This best practice document defines the suggested configuration for both the SBC and Skype/Lync Server in order for Third Party Presence to be published.

Getting Started

The example configuration items are used to configure the SBC Edge for Skype for Business (in order for Third Party Presence to be published):

- Skype/Lync Presence server has the FQDN of **lyncpool.example.com**.
- An analog phone connected to FXS port (phone number 2222) needs presence published when a call is connected/disconnected.
- CAS SG (Phones) defines an Action Set with Transformation Tables to alert the system that presence needs to be published.
- Phone number 2222 is defined in AD as attribute homePhone for a Lync user (msRTCSIP-PrimaryUserAddress = lync1@example.com). It is this relationship that allows the FXS phone at 2222 to publish presence for the Lync user.

Step 1. Configure the Skype/Lync Presence Server

A SIP Server must be configured to point to a Presence Server. A Presence Server runs on a Skype/Lync front-end pool. MTLS is required for communication between the SBC and the Presence Server. Therefore, the transport protocol of the SIP server must be TLS.

Configure Skype/Lync Presence Server as follows:

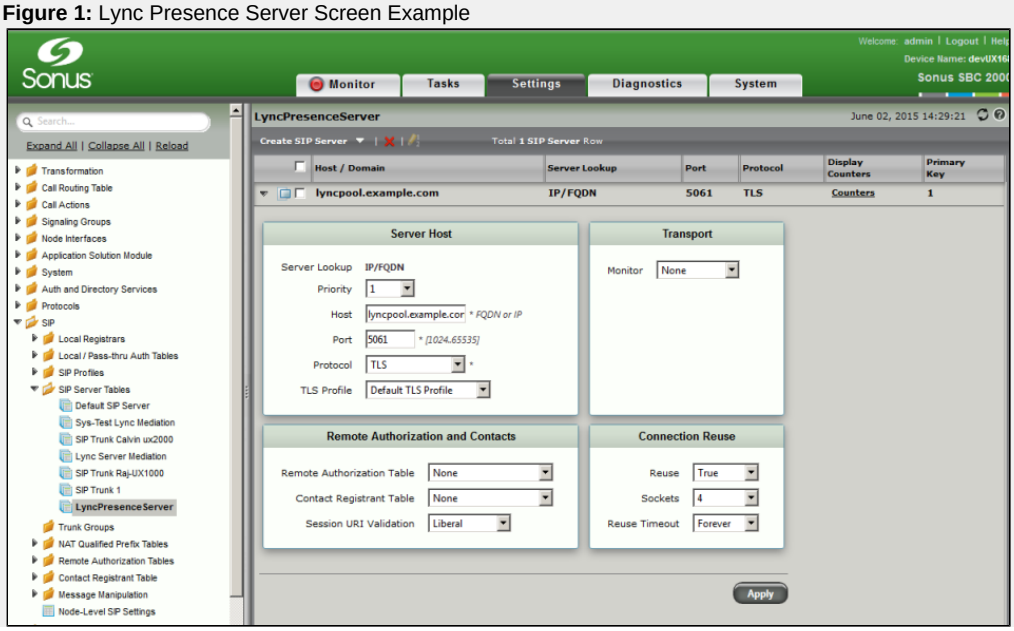
1. In the WebUI, access **SIP > SIP Server Tables.**

2. Create a Lync Presence Server. Use the example below as a guideline for configuration.

3. From the TLS Profile drop down list, select **Default TLS Profile** (ensure the Default TLS profile has the Mutual Authentication parameter set to Enabled; see Creating and Modifying TLS Profiles).

4. In the Port field, enter **5061**.

Figure 1: Lync Presence Server Screen Example



Step 2. Enable Skype/Lync Presence

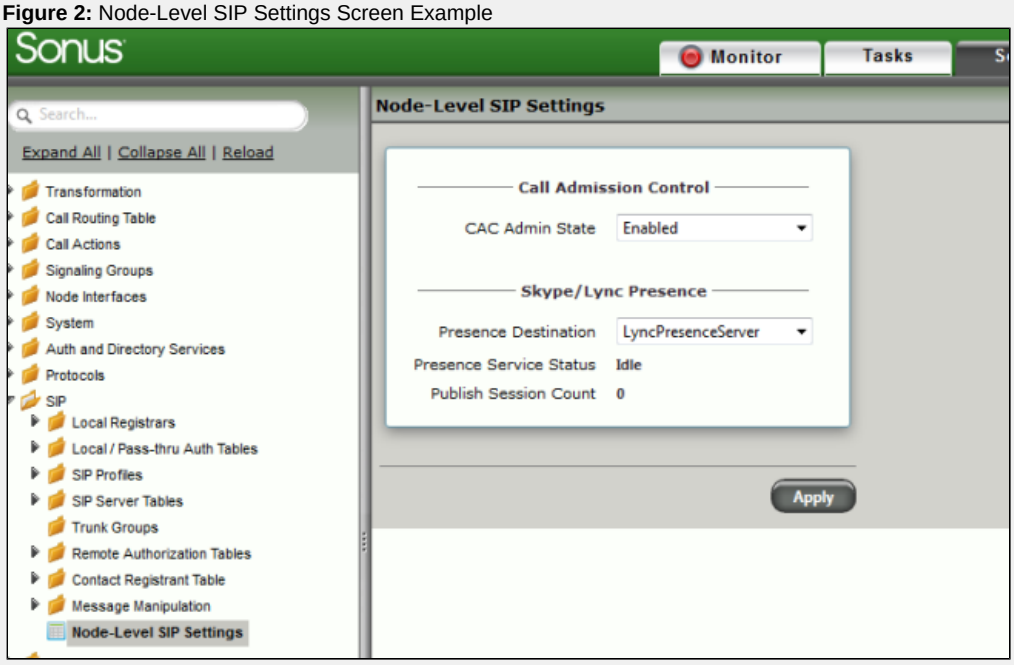
The SIP Server you select for the Presence Destination can be **None** or a SIP Server that has been defined with a transport protocol of TLS.

Enable Skype/Lync Presence as follows:

1. In the WebUI, access **SIP >Node-Level SIP Settings**.

2. From the **Presence Destination** drop-down menu, select a Presence Server (i.e., **Lync Presence Server**). This is the server configured in the previous section.

Figure 2: Node-Level SIP Settings Screen Example



Step 3. Define AD Configuration/Domain Controller for AD Cache Look Up

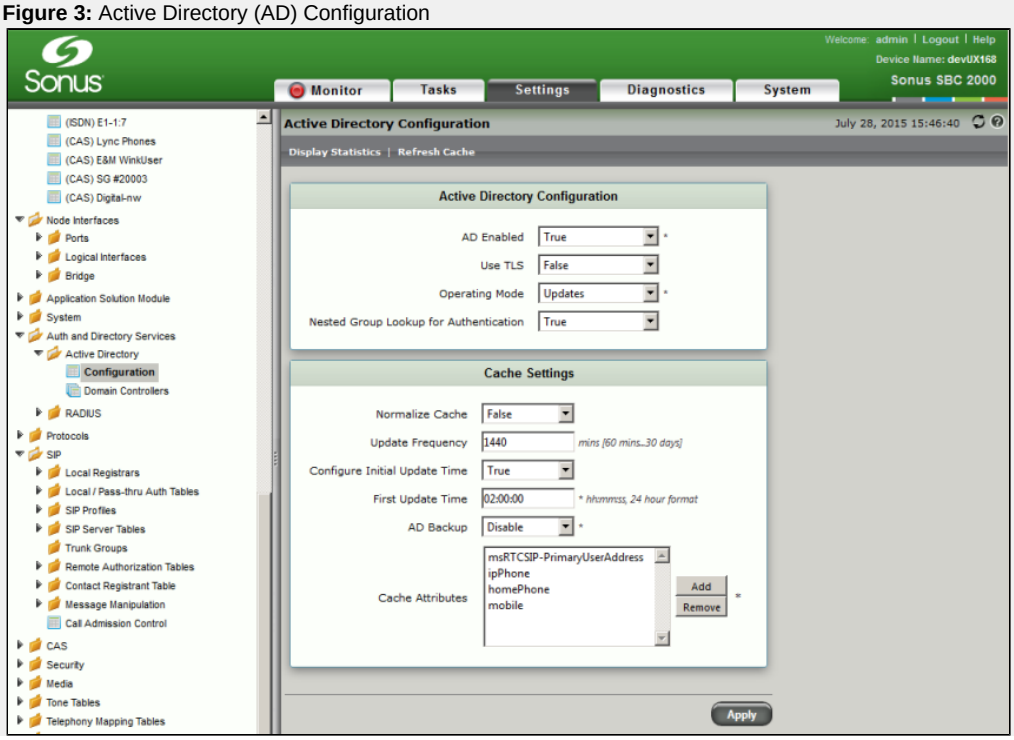
Configure Active Directory (AD)

⚠ Normalize Cache parameter must be set to **False** for the Presence feature to work.

1. In the WebUI, access **Auth and Directory Services >Configuration**.

2. Configure as shown in the example below. For detailed information about Active Directory, see Integrating with Active Directory.

Figure 3: Active Directory (AD) Configuration

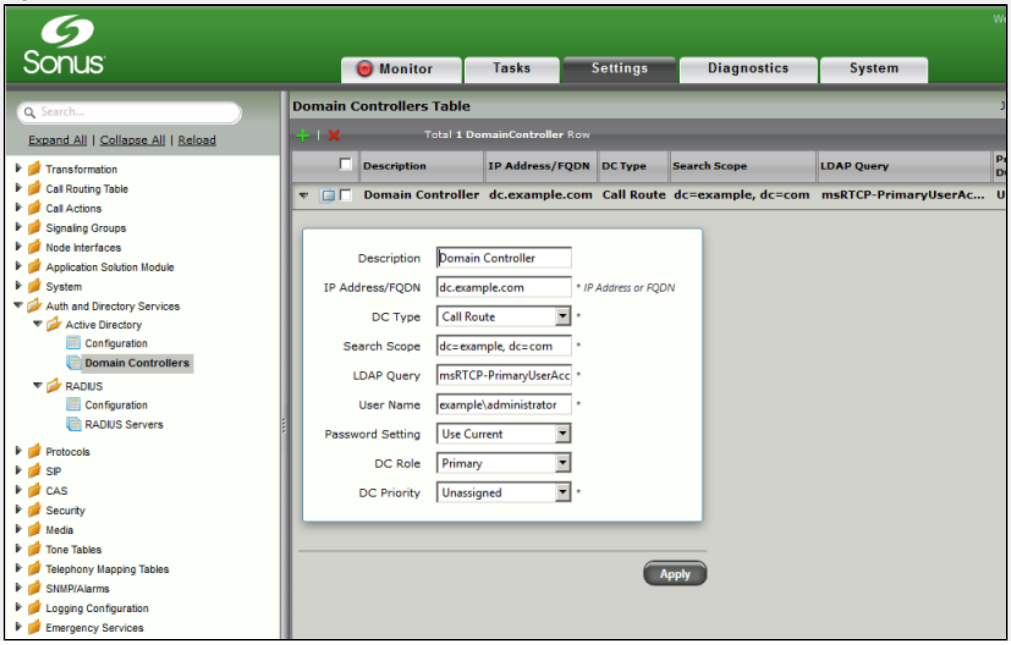


Configure Domain Controller (DC)

Sonus recommends selecting "msRTCSIP-PrimaryUserAddress=*" string as "LDAP Query" to select only Lync enabled AD users.

1. In the WebUI, access **Auth and Directory Services >Domain Controllers**.
2. Add a Domain Controller.
3. Configure as shown in the example below. For detailed information about Domain Controllers, see Adding and Modifying Domain Controllers.

Figure 4: Domain Controllers Table



Step 4. Configure Transformation Entries for Presence

Typically, a non-Lync endpoint desiring its presence to be published, will want the connection of both incoming and outgoing calls to trigger presence. This can be accomplished by defining one Transformation Table with two entries This transformation table will be used by an Action Set (defined in subsequent) Steps.

It is mandatory to have an entry in the Active Directory (AD) that is associated with the non-Lync endpoint; this AD attribute can be any field (ipPhone, homePhone, etc...). Options have been added to the transformation WebUI to make configuring Presence as straightforward as possible. When **Presence - Called Address/Number** is selected for **Input Field Type** (or **Presence - Calling Address/Number**), all of the remaining fields will be filled in with the most typical selections. See the figure below for an example. Note that the Input Field Value and Output Field Value are editable drop down boxes; they present the most likely selections, but also allow the user to overwrite with any value desired.

The example below will do an AD cache look-up for homePhone and match against the Called Address/Number. If there is a match, the msRTCSIP-PrimaryUserAddress of that AD entry will be copied into the **Presence - Called Address/Number** Output Field. It is this called presence value that will be used in the Request URI, To and From headers of the Publish message that announces the presence status. Similar configuration should be defined for the **Presence - Calling Address/Number.** The default value for the **Input Field Value** when the **Input Field Type** is **Presence - Called(ing) Address/Number** will be AD:ipPhone

Input Field Value and Output Field Value are editable list boxes. They present the most likely selections, but also allow you to overwrite the

predefined values.

Create a Transformation entry as follows:

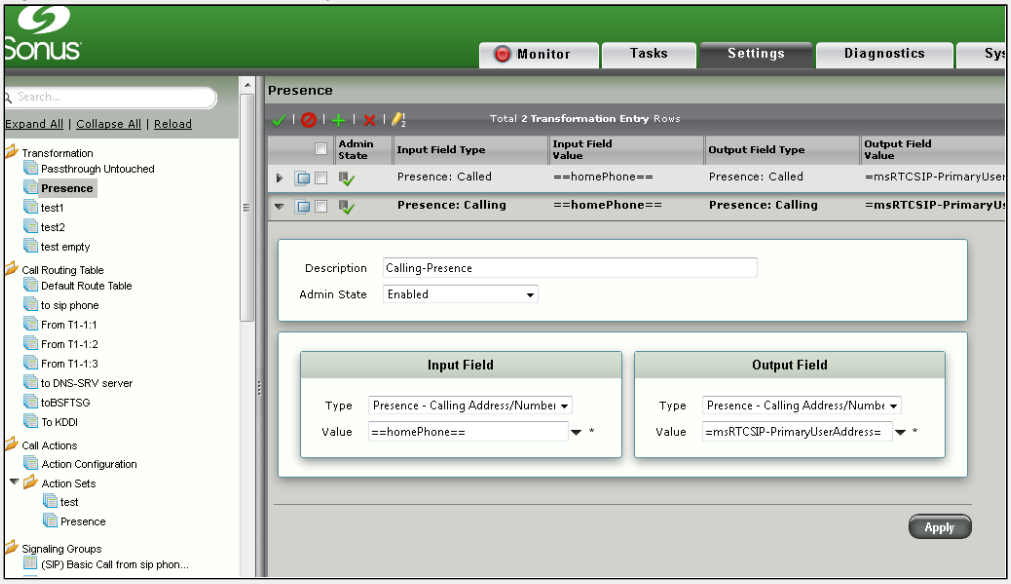
1. In the WebUI, access **Tranformation.**

2. Create an entry for Called/Address Number as shown in the example below. For detailed information about the Transformation table, see Creating and Modifying Entries to Transformation Tables.

3. Create another configuration for Calling Address/Number (Presence).

In the example below, the default value for Input Field's **Value** field is "==homePhone==" when the **Type** field is "Presence Calling Address/Number.

Figure 5: Presence - Called Example



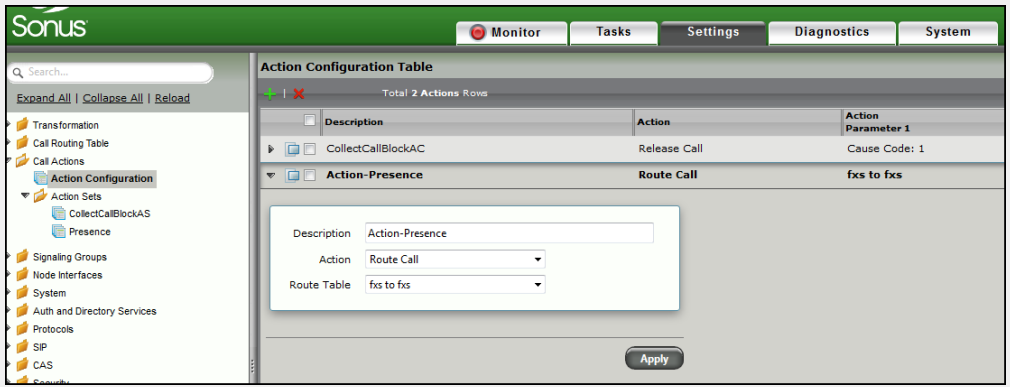
Step 5. Define An Action Configuration

A *Route Call* Action configuration should be defined. This allows routing to take place at the end of the Action set used for Presence.

1. In the WebUI, access **Call Actions > Action Configuration.**

2. Create an entry in the Action Configuration Table as shown in the example below. For detailed information about the Call Actions, see Managing Action Configurations.

Figure 6: Action Configuration Table Screen Example



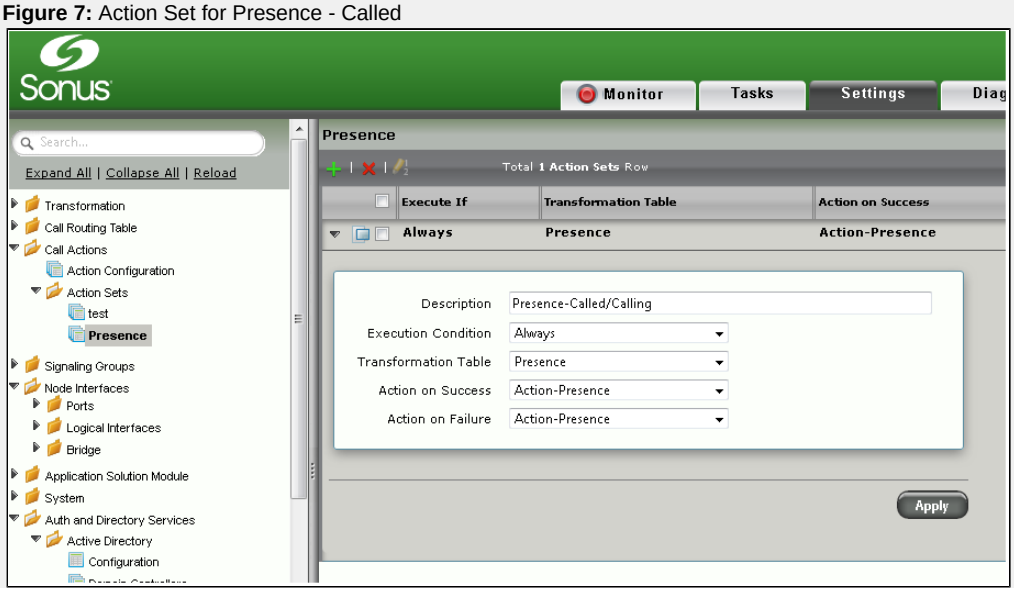
Step 6. Define An Action Set for Presence

The Transformation Entry defined above will be used when defining the single Action Set used for Presence

1. In the WebUI, access **Call Actions > Actions Sets.**

2. Create an Action Set (i.e., **Presence**) as shown in the example below. For detailed information about the Call Actions, see Managing Action Configurations.

Figure 7: Action Set for Presence - Called



Step 7. Attach An Action Set To The Desired Signaling Group(s)

In order for the Action Set to be applied, it must be attached to a Signaling Group.

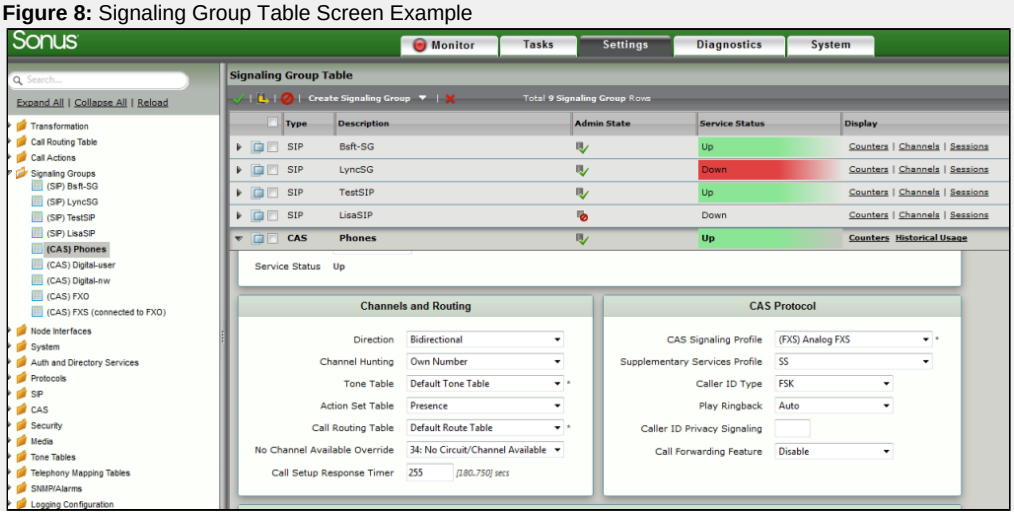
Attach as follows:

1. In the WebUI, access **Signaling Groups.**

2. Select the Signaling Group in which the Actions Set will be attached.

3. In the **Action Set Table** drop down list, select the Action Set (i.e, **Presence**). For detailed information about the Call Actions, see Managing Action Configurations.

Figure 8: Signaling Group Table Screen Example



Configure Lync Server

SBC needs to be configured in Lync Topology as Trusted Application Server/Trusted Application. To configure, execute the following steps using the Lync Server Management Shell.

This topology change requires Lync 2013 Server to be updated to at least version 5.0.8308.866 released on 12/31/2014 as Cumulative Update CU5 HF7.1.

Lync 2013 Server versions earlier than 5.0.8308.866 will not allow the SBC to be configured as Trusted Application Server.

Before executing the steps below make sure that SBC is defined in the PSTN gateway section of the Lync topology.

Obtain The Site ID

Execute Get-CsSite cmdlet to find out the Site Id number

```
Get-CsSite
```

Create A Trusted Application Pool

Execute New-CsTrustedApplicationPool cmdlet to create new pool that will host presence application

```
New-CsTrustedApplicationPool -Identity <Pool FQDN> -Registrar <Registrar FQDN> -Site <Site Id>
```

where:

> *–Identity – FQDN of the SBC providing presence updates to Lync Server*
>
> *–Registrar – FQDN of the Registrar service for the pool*
>
> *–Site – Site Id obtained in Obtain the site ID.*

For example:

```
New-CsTrustedApplicationPool -Identity sbc2000.example.com -Registrar lyncpool.example.com -Site 1
```

Use any Front End or SBA for the Registrar, ideally choosing the most reliable connection to the SBC.

Create A Trusted Application

Execute New-CsTrustedApplication cmdlet to add a presence application to trusted application pool.

```
New-CsTrustedApplication-ApplicationId <String> -TrustedApplicationPoolFqdn <String> -Port <Port
Number>
```

where:

> *–ApplicationId – The name of the application*
>
> *–TrustedApplicationPoolFqdn – The FQDN of the trusted application pool created in Create a Trusted Application Pool.*
>
> *–Port – The port number on which the application will run (5061)*

For example:

```
New-CsTrustedApplication -ApplicationId presence -TrustedApplicationPoolFqdn sbc2000.example.com  -Port
5061
```

⚠ Ensure the port number matches the port number configured in Step 1.

Enable The Lync Server Topology

Execute Enable-CsTopology cmdlet for topology changes to take effect

```
Enable-CsTopology
```