



# Outbound Option Installation

- [Unified CCE Configuration for Outbound Option, on page 1](#)
- [Unified Communications Manager and Gateway Configuration, on page 6](#)
- [Outbound Option Software Installation Steps, on page 14](#)
- [Verification, on page 24](#)

## Unified CCE Configuration for Outbound Option

This section provides procedures for configuring Unified CCE for Outbound Option.

### Unified CCE System Configuration for Outbound Option

The following table lists the steps required to set up your Unified CCE system to handle the optional Outbound Option components.

*Table 1: Configure Unified CCE for Outbound Option*

Step	Task	See
1	Configure the Unified CCE PG.	Configure the PG
2	Configure the Dialer component.	Configure Dialer Component
3	Configure the port map.	Configure Port Map
4	Create a Network VRU.	Create a Network VRU
5	Configure the Media Routing PG.	Configure Media Routing PG (MR PG)
6	Configure a skill group.	Configure Skill Group
7	Create a dialed number.	Create Dialed Number
8	Create a translation route to a VRU.	Unified CCE Documentation
9	Configure system options.	Configure System Options
10	Enable ECC variables.	Enable Expanded Call Variables

Step	Task	See
11	Enable packet capture.	Packet Capture for Troubleshooting

## Configure the PG

### Procedure

---

- Step 1** In ICM Configuration Manager, open **Tools > Explorer Tools > PG Explorer**.
  - Step 2** Click **Retrieve**, and then click **Add PG**.
  - Step 3** Enter the name (for example, **PG1**).
  - Step 4** Select the **Client Type**, either Call Manager, **CUCM**, or **Generic**.
  - Step 5** Click **Add Peripheral**.
  - Step 6** Enter the name (for example, **PG1\_PIM1**).
  - Step 7** On the **Peripheral** tab, check **Enable post routing**.
  - Step 8** Select the **Default Desk Setting** from the drop-down list.
  - Step 9** On the **Routing Client** tab, enter the routing client name (for example, **PIM1\_Voice**).
  - Step 10** Click **Save**.
  - Step 11** Record the assigned Logical Controller ID for later use: \_\_\_\_\_.
  - Step 12** Record the assigned Peripheral ID for later use: \_\_\_\_\_.
- 

## Configure the Dialer Component

You deploy the Dialer as a single redundant pair for each Agent PG with agents who handle Outbound Option calls.

### Procedure

---

- Step 1** Make sure that all CCE services are running.
- Step 2** In the **Unified CCE Configuration Manager**, expand **Outbound Option Option** and double-click **Dialer** to display the **Outbound Option Option Dialer configuration** window.
- Step 3** Click **Retrieve**.
- Step 4** Click **Add** to add a new dialer.
- Step 5** Enter the required information on the **Dialer General Tab**. See the *Configuration Manager Online Help* for details of these fields.
- Step 6** Click **Save**.
- Step 7** Select the **Port Map Selection** tab to display the port map configuration. See the *Configuration Manager Online Help* for details of configuring these mappings.
- Step 8** Click **Add**
- Step 9** Configure a set of ports and their associated extensions.

A Dialer can support 3000 ports. The allowed **Telephony Port** range is from 0 to 2999.

- Step 10** Click **OK**. The port mappings appear on the **Port Map Selection** tab.
- Step 11** Click **Save** to save all the configuration information.

---

**Related Topics**

- [Dialer Port Allocation](#)
- [Install Dialer Component on the PG Virtual Machine](#), on page 20
- [Outbound Option Dialer Component](#)

## Create a Network VRU

Create a Type 2 VRU to use during the Media Routing (MR) PIM setup.

---

**Procedure**

- Step 1** In the **Configuration Manager**, open the **Explorer** tools.
- Step 2** Open the **Network VRU Explorer** tool.
- Step 3** Click **Retrieve**
- Step 4** Click **Add Network VRU**
- Step 5** In the **Network VRU** dialog, enter a **Name** for the VRU.
- Step 6** Set the **Type** drop-down list to Type 2.
- Step 7** Record the VRU name: \_\_\_\_\_.
- Step 8** Click **Save**.



- Note** See the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html> for detailed information about the Unified CCE Configuration Manager tools.
- 

## Configure Media Routing PG (MR PG)

Perform the following steps to configure the MR PG (for example, PG3).

---

**Procedure**

- Step 1** In **Configuration Manager**, open the **Tools > Explorer Tools > PG Explorer**.
- Step 2** Click **Retrieve**, then click **Add PG**.
- Step 3** Enter the **Name** (for example, **PG3\_MR**).
- Step 4** Select a **Client Type** of **Media Routing**.

- Step 5** Click **Add Peripheral**.
- Step 6** Enter the **Name** (for example, **PG3\_MR\_PIM1**).
- Step 7** On the **Peripheral** tab, check **Enable post routing**.
- Step 8** On the **Routing Client** tab, enter the routing client name (for example, **MR\_PIM1\_Voice**).
- Step 9** Set the **Routing Type** dropdown to **None**.
- Step 10** Set the **Default call type** to **None**.
- Step 11** On the **Advanced** tab, select the **Network VRU** from the drop-down list that you created during Unified CCE configuration for Outbound Option.
- Step 12** Click **Save**.
- Step 13** Record the assigned **Logical Controller ID** displayed on the Logical Controller panel for later use:  
\_\_\_\_\_.
- Step 14** Record the assigned **Peripheral ID** displayed on the Peripheral tab, for later use: \_\_\_\_\_.

---

### Related Topics

[Create a Network VRU](#), on page 3

## Configuration for Send to VRU Campaign

Follow these procedures to create and configure the VRU.



**Note** See **Configuring Network VRUs and VRU Scripts** in the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html> for detailed information about the Unified CCE Configuration Manager tools.

---

### Configure Network VRU Type 10

Create a Unified CVP Type 10 VRU.

#### Procedure

---

- Step 1** In the **Configuration Manager**, open the **Explorer** tools.
- Step 2** Open the **Network VRU Explorer** tool.
- Step 3** Click **Retrieve**
- Step 4** Click **Add Network VRU**
- Step 5** In the **Network VRU** dialog, enter a **Name** for the VRU.
- Step 6** Set the **Type** drop-down list to **Type 10**.
- Step 7** Record the VRU name: \_\_\_\_\_.
- Step 8** Click **Save**.
-



**Note** See the *Configuration Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html> for detailed information about the Unified CCE Configuration Manager tools.

## Assign Type 10 Network VRU to VRU-PG

### Procedure

- 
- Step 1** In **Configuration Manager**, open the **Tools > Explorer Tools > PG Explorer**.
  - Step 2** Click **Retrieve**, then click **Add PG**.
  - Step 3** Enter the **Name** (for example, **PG\_VRU**).
  - Step 4** Select a **Client Type** of **VRU**.
  - Step 5** Click **Add Peripheral**.
  - Step 6** Enter the **Name** (for example, **CVP\_PIM**).
  - Step 7** On the **Peripheral** tab, check **Enable post routing**.
  - Step 8** On the **Routing Client** tab, enter the routing client name (for example, **CVP\_PIM\_Voice**).
  - Step 9** Set the **Routing Type** dropdown to **None**.
  - Step 10** Set the **Default call type** to **None**.
  - Step 11** On the **Advanced** tab, select the **Type 10Network VRU** from the drop-down list that you created during Unified CCE configuration for Outbound Option.
  - Step 12** Click **Save**.
  - Step 13** Record the assigned **Logical Controller ID** displayed on the Logical Controller panel for later use: \_\_\_\_\_.
  - Step 14** Record the assigned **Peripheral ID** displayed on the Peripheral tab, for later use: \_\_\_\_\_.
- 

## Configure System Options

### Procedure

- 
- Step 1** In **Unified CCE Configuration Manager**, expand **Outbound Option**, and then select **System Options**.
  - Step 2** Click the **General Options** tab and define the dialing time range to use for all your Outbound Option campaigns, and then click **OK**.

**Note** Remember to select AM or PM for your start and end times.

---

**What to do next**

**Note** If you have previously configured campaigns, you can update them now. Click the **Bulk Update** tab page and define specific dialing time ranges for phone numbers, and then click **Update All Campaigns**.

## Enable Expanded Call Context Variables

Perform the following steps to enable the expanded call context variables.

### Procedure

- 
- Step 1** In the **Configuration Manager**, open **Miscellaneous Tools > System Information**.
  - Step 2** Check **Expanded call context enabled** and save your change.
  - Step 3** In the **List** tools, open the **Expanded Call Variable List** tool and click **Retrieve**.
  - Step 4** Enable all BAxxxx variables (BAAccountNumber, BABuddyName, BACampaign, BADialedListID, BAResponse, BASTatus, and BATimezone).
  - Step 5** Select each variable, and, in the **Attributes** tab, check **Enabled**.
  - Step 6** Click **Save**.
- 

**What to do next**

By default, the solution includes the predefined BAxxxx ECC variables in the "Default" ECC payload. You can also create a custom ECC payload for your Outbound Option call flows. Always remember that you cannot use an ECC variable unless it exists in one of the ECC payloads that you use for a call flow.

## Unified Communications Manager and Gateway Configuration

In the next phase of Outbound Option installation, you set up Unified Communications Manager and its related gateway.

The following table lists the steps that comprise Unified CM setup.

**Table 2: Unified CM Configuration Steps for Deployments with SIP Dialer**

Step Number	Task	Procedure
1	Disable Ring Tone for Dialer Transfer	<a href="#">Disable Ringback During Transfer to Agent for SIP, on page 7</a>
2	Configure SIP Trunks	<a href="#">Configure SIP Trunks, on page 12</a>

## Disable Ringback During Transfer to Agent for SIP

The voice gateway generates a ringback tone to the customer. To prevent the gateway from generating a ringback, apply a SIP normalization script to the Unified Communications Manager SIP trunk.

Apply this SIP normalization script only to the SIP trunk that handles the inbound call from the voice gateway for agent transfer.

- If your deployment uses the same gateway for both PSTN calls and the dialer, complete all steps, 1 to 13, to create a dedicated SIP trunk and apply the normalization script.



---

**Note** The trunk for PSTN calls still needs a 180 RINGING SIP message for inbound calls to trigger the gateway to play ringback to the PSTN.

---

- If your deployment has a dedicated SIP trunk to handle the agent transfer dialer, complete steps 1 to 2 and 8 to 13 to apply the normalization script to your SIP trunk.

### Procedure

---

- Step 1** Navigate to `https://<IP_address>:8443` where `<IP_address>` identifies the Unified Communications Manager server.
- Step 2** Sign in to Unified Communications Manager.
- Step 3** To create a SIP trunk security profile in Unified Communications Manager, select **Communications Manager GUI > System > Security > SIP Trunk Security Profile > [Add New]**.  
The default port is 5060.

Figure 1: SIP Security Profile

**SIP Trunk Security Profile Information**

Name\*

Description

Device Security Mode

Incoming Transport Type\*

Outgoing Transport Type

Enable Digest Authentication

Nonce Validity Time (mins)\*

X.509 Subject Name

Incoming Port\*

Enable Application Level Authorization

Accept Presence Subscription

Accept Out-of-Dialog REFER \*\*

Accept Unsolicited Notification

Accept Replaces Header

Transmit Security Status

SIP V.150 Outbound SDP Offer Filtering\*

284955

**Step 4** Click **Save**.

**Step 5** Create a new SIP trunk and add the new SIP Trunk Security Profile.

Figure 2: Create a New SIP Trunk

**SIP Information**

**Destination**

Destination Address is an SRV

	Destination Address	Destination Address IPv6	Destination Port
1*	<input type="text" value="10.10.10.1"/>	<input type="text"/>	<input type="text" value="5060"/>

MTP Preferred Originating Codec\*

BLF Presence Group\*

SIP Trunk Security Profile\*

347384

**Step 6** Click **Save**.

**Step 7** Click **Reset**.

**Step 8** In **Communications Manager GUI > Devices > Device Settings > SIP Normalization Scripts > [Create New]**, enter the following SIP normalization script into the content field. All other values remain set to default.

```
M = {}
function M.outbound_180_INVITE(msg)
msg:setResponseCode(183, "Session in Progress")
end
return M
```



Figure 3: Add Normalization Script

**SIP Normalization Script Configuration**

Save Delete Reset Add New Import File

Add successful

**SIP Normalization Script Info**

Name\* DialerNormalizationScript

Description

Content\*  

```
M = {}
function M.outbound_180_INVITE(msg)
msg:setResponseCode(183, "Session in Progress")
end
return M
```

Script Execution Error Recovery Action\* Message Rollback Only

System Resource Error Recovery Action\* Disable Script

Memory Threshold\* 50 kilobytes

Lua Instruction Threshold\* 1000 instructions

**Step 9** Click **Save**.

**Step 10** Click **Reset**.

**Step 11** Associate the new normalization script with the SIP trunk.

Figure 4: Associate Script with Trunk

**Normalization Script**

Normalization Script DialerNormalizationScript

Enable Trace

	Parameter Name	Parameter Value
1		

**Step 12** Click **Save**.

**Step 13** Click **Reset**.

## Configuration of Voice Gateways

In an Outbound Option deployment that uses the SIP Dialer, you can have these configuration types:

- The SIP Dialer connects to a SIP Proxy, such as Cisco Unified SIP Proxy. The SIP Proxy, in turn, connects to a voice gateway. A SIP Proxy can connect to more than one voice gateway. A configuration with multiple voice gateways is known as a *server group*.
- Alternately, the SIP Dialer connects directly to a voice gateway without a SIP Proxy. The voice gateway uses a standard dial peer configuration. This setup enables the gateway to know how to direct traffic to agent extensions or to a VRU.

Specify your configuration when you install the Dialer component.

When you configure the voice gateway, you can keep most of the default configuration values. You do set some of the configuration values. If you do not know these values, request the information from your voice network administrator.

- Enable 100rel for Outbound Option. Otherwise, Outbound calls from the SIP Dialer fail. 100rel is enabled globally on the gateway by default. However, if you also route Unified CVP calls with the gateway, you cannot have 100rel enabled globally. In this case, disable 100rel globally with the command `rellxx disable`. Then, enable 100rel on the Outbound dial peer with the example dial-peer command:  

```
voice-class sip rellxx supported "100rel".
```
- The SIP Dialer does not support signaling forward unconditional under voice service voip. When configuring a voice gateway for use with the SIP Dialer, specify signaling forward none.

Telecom carriers sometimes send an ISDN alerting message without a progress indicator. This situation causes the voice gateway to send a SIP 180 Ringing message, instead of a SIP 183 Session In Progress message, to the SIP dialer. The SIP dialer can process provisional messages such as 180, 181, 182, and 183 with or without Session Description Protocol (SDP). When the SIP dialer receives these provisional messages without SDP, the dialer does not perform Call Progress Analysis (CPA) and the Record CPA feature is disabled.

To enable the SIP dialer to perform CPA, add the following configuration to the POTS dial-peer of the voice gateway: `progress_ind alert enable 8`. This code sends a SIP 183 message to the SIP dialer.

Telecom carriers sometimes send an ISDN alerting message without a progress indicator. This situation causes the voice gateway to send a SIP 180 Ringing message, instead of a SIP 183 Session In Progress message, to the SIP dialer. The SIP dialer can process provisional messages such as 180, 181, 182, and 183 with or without Session Description Protocol (SDP). The SIP Dialer processes the CPA information along with the SDP information because the SDP information is part of these provisional messages. But if the dialer receives these provisional messages without SDP, the dialer does not perform Call Progress Analysis (CPA) and the Record CPA feature is disabled. If the next provisional message changes the SDP information, the dialer processes the SDP information.




---

**Note** In a SIP Dialer with Unified CVP VRU deployment, dialer-related call flows do not invoke call-survivability scripts that are enabled on an incoming POTS dial-peer in the Ingress gateway. However, enabling a call-survivability script on an Inbound POTS dial-peer does not negatively affect dialer-related call flows.

---

### Configure Transcoding Profile for Cisco Unified Border Element

The following example shows the transcoding profile for Cisco UBE.



**Note** Transcoding impacts port density.

```
dspfarm profile 4 transcode universal
  codec g729r8
  codec g711ulaw
  codec g711alaw
  codec g729ar8
  codec g729abr8
  maximum sessions 250
  associate application CUBE
!
```

If you use a SIP Proxy, perform the following configuration on the SIP Proxy:

- Enable the SIP Dialer to reach the correct voice gateway for outbound calls.
- Enable the voice gateway to reach all the applicable Unified CM and CVP nodes for calls transferred to an agent, a VRU, or to CVP.
- If your SIP proxy connects to more than one voice gateway, you can optionally load balance between the voice gateways.

For detailed instructions on how to perform SIP Proxy configuration, see the Cisco Unified SIP Proxy documentation website at

[https://www.cisco.com/en/US/partner/products/ps10475/products\\_installation\\_and\\_configuration\\_guides\\_list.html](https://www.cisco.com/en/US/partner/products/ps10475/products_installation_and_configuration_guides_list.html).

## Configure Cisco Unified Border Element

For full details on configuring the Cisco Unified Border Element (Cisco UBE) to support Outbound dialing, see Cisco Unified Border Element Configuration Guide at <https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/tsd-products-support-configure.html>

When configuring Cisco UBE with Outbound Option, ensure that you:

- Configure three dial-peers in the Cisco UBE.

The dial-peers are used for:

- Incoming calls from the dialer.
  - Outgoing calls to the terminating network from the Cisco UBE.
  - Calls to be routed to the Cisco Unified Communications Manager.
- When configuring REFER consumption, issue the following commands in global VoIP configuration mode:
    - **no supplementary-service sip refer**
    - **supplementary-service media-renegotiate**

## Configure Cisco UBE for G.711 A-Law

By default the SIP Dialer always dials out calls using the U-law and A-law codec.

For full details on understanding and configuring codec support, see Cisco Unified Border Element Configuration Guide at <https://www.cisco.com/c/en/us/support/unified-communications/unified-border-element/tsd-products-support-configure.html>



**Note** The Cisco Unified Call Manager enables A-law by default.

To enable the G.711 A-law codec, make the following changes in the Cisco UBE/Egress Gateways.

1. Set the **Outgoing dial peer** codec to "g711alaw".

Specifies that the SDP sent out from Cisco UBE to the customer end point should use the g711alaw codec.

Example:

```
dial-peer voice 2613 voip
destination-pattern 244T
session protocol sipv2
session target ipv4:10.77.58.33
session transport udp
codec g711alaw
no vad
```

2. Set the **Incoming dial peer** codec to "g711alaw"

Specifies that the SDP sent out from Cisco UBE to the Dialer should use g711alaw codec.

Example:

```
dial-peer voice 2614 voip
description sipp_SIP_Incoming_DialPeer_from_dialer
session protocol sipv2
session transport udp
incoming called-number 244T
codec g711alaw
no vad
```

## Configure SIP Trunks

Unified CM is connected to the voice gateway or the SIP Proxy by SIP Trunks, which you configure on Unified CM. Set up route patterns for the Dialer which are appropriate for your dial pattern.

### Procedure

#### Step 1

Configure these trunks as follows:

Option	Description
If you are using a SIP Proxy	<p>Configure two SIP trunks on Unified CM for making the transfer to agents. Configure one trunk between Unified CM and the SIP Proxy. Specify the IP address of the SIP Proxy in the <b>Destination</b> field. Then, configure a second trunk from Unified CM to the voice gateways. Specify the IP address of the voice gateways in the <b>Destination</b> field.</p> <p><b>Note</b> Incoming transport time accepts TCP and UDP. The trunk accepts traffic from the Gateway in TCP or UDP.</p>

Option	Description
If you are not using a SIP Proxy	Configure a SIP trunk on Unified CM from Unified CM to the voice gateway. Specify the IP address of the voice gateway in the <b>Destination</b> field.
If you are using Cisco UBE	Configure a SIP trunk between the Unified CM and Cisco UBE. Specify the IP address of the Cisco UBE in the <b>Destination</b> field.

**Step 2** In Unified CM clusters with more than two nodes, both the voice gateway and Cisco Unified SIP Proxy might connect to each node. To enable those connections, add the SIP trunk to a device pool that points to the Communications Manager Publisher. This configuration ensures that calls go to the agent if a subscriber node fails over. See the following configuration example:

**Example:**

```
dial-peer voice 617 voip
description catch all for refer
destination-pattern 617T
session protocol sipv2
session target ipv4:10.86.227.107 (CUCM Publisher)
codec g711ulaw
!

dial-peer voice 508 voip
description catch all for refer
destination-pattern 508T
session protocol sipv2
session target ipv4:10.86.227.107 (CUCM Publisher)
codec g711ulaw
!
```

**Related Topics**

[Disable Ringback During Transfer to Agent for SIP](#), on page 7

## Configure E1 R2 Signaling

The Outbound Option Dialer may be configured with systems using the E1 R2 signaling protocol. E1 R2 signaling is a channel associated signaling (CAS) international standard that is used with E1 networks in Europe, Latin America, Australia, and Asia. For more information, see [E1 R2 Signaling Theory](#)

The high-level procedure for configuring an E1 R2 controller for use with the Outbound dialer is summarized below. For full configuration details, see [E1 R2 Signaling Configuration and Troubleshooting](#).

**Procedure**

- Step 1** Set up an E1 controller connected to the private automatic branch exchange (PBX) or switch. Ensure that the framing and linecoding of the E1 are properly set for your environment.
- Step 2** For E1 framing, choose either **CRC** or **non-CRC**.
- Step 3** For E1 linecoding, choose either **HDB3** or **AMI**.
- Step 4** For the E1 clock source, choose either **internal** or **line**. Keep in mind that different PBX's may have different requirements for their clock source.

- Step 5**     Configure line signaling.
  - Step 6**     Configure interregister signaling.
  - Step 7**     Customize the configuration with the `cas-custom` command.
- 

### Example E1 R2 Settings

```

controller E1 0/0/0
 framing NO-CRC4
 ds0-group 1 timeslots 1-15,17-31 type r2-digital r2-compelled ani
 cas-custom 1
 country telmex
 category 2
 answer-signal group-b 1
 caller-digits 4
 dnis-digits min 4 max 13
 dnis-complete
 timer interdigit incoming 1000
 groupa-callerid-end

```

## Outbound Option Software Installation Steps

This section discusses the tasks that are associated with installing Outbound Option and related components. Before proceeding, navigate to Logger Side A and Logger Side B and stop all ICM services there. Then perform the steps in the following sections.

### Software Installation and Database Creation

Install the Outbound Option component software and create its database.

If you want to enable Outbound Option High Availability, perform Step 1 on both Logger Side A and Logger Side B.

**Table 3: Software Installation and Database Creation Steps**

Step	Task	See the topic that describes
1	Install the Outbound Option private database on the Logger platform.	How to create an Outbound Option private database.
2	Install the Dialer component on the PG platform.	How to install the Dialer component on the PG.
3	Install the MR PG on the PG platform.	How to install the MR PG on the PG platform.

# Outbound Option for High Availability: Preliminary Two-Way Replication Requirements

If you plan to set up Outbound Option for High Availability two-way replication, there are several preliminary requirements.

## Create an Outbound Option Database on Logger Side A and Side B

If you have enabled Outbound Option on Logger Side A in a previous release, you must:

- Stop all Logger services on Logger Side A.
- Perform a full database backup for the Outbound Option database on Logger Side A and restore it to Logger Side B. Use SQL Server Management Studio (SSMS) to complete this task.

If you have not enabled Outbound Option in a previous release, you must create an Outbound Option database on Logger Side A and Logger Side B. Use the ICMDBA utility to complete this task.



---

**Note** If the database replication fails and it is resolved, the Outbound Option HA must be enabled again. In such a case, you must again synchronize the databases on the Active and Standby sides. Perform a full database backup for the Outbound Option database on Active side and restore it to the Standby side.

---

## Define Logger Public Interface Hostname on Logger Side A and Logger Side B

As you configure Outbound Option for High Availability, you must define the Logger Public Interface Hostname on both sides of the Logger. IP addresses are not allowed.

## Make Campaign Manager and Dialer Registry Setting Customizations on Both Side A and Side B

If you customize any Campaign Manager and Dialer registry settings on one side, you must make the same updates for the registry settings on the other side.

## Stop the Logger Service Before Enabling or Disabling Outbound Option High Availability

Before you enable or disable Outbound Option High Availability, stop the Logger service on the applicable side or sides.

### Related Topics

[Configure the Logger for Outbound Option](#), on page 17

[Create Outbound Option Database](#), on page 15

## Create Outbound Option Database

Before you use Outbound Option, estimate the size for the Outbound Option database.

### Procedure

---

#### Step 1

Collect the following information:

- The size, in bytes, of each customer record in the import file. If the size is less than 128 bytes, use 128. (RecordSize)
- The number of records that are imported. (RecordCount)
- Do the records from new imports replace or append to records that are already in the database?

**Step 2** Estimate the contact table size as follows:

- If imports overwrite existing records: Do not change record count.
- If imports append to existing records: RecordCount = total number of rows kept in a customer table at a time.
- contact-table-size = RecordSize \* RecordCount \* 1.18

**Step 3** Estimate the dialing list table size as follows:

- If imports overwrite existing records: RecordCount = number of rows imported \* 1.5. (50% more rows are inserted into the dialing list than are imported.)
- If imports append existing records: RecordCount = total number of rows kept in customer table at a time \* 1.5
- dialing-list-table-size = rows in dialing list \* 128 bytes \* 4.63

**Step 4** Calculate the database size using this formula:

```
(Number of rows in all DL tables * (size of one row + size of index) ) +
(Number of rows in personal call back table * (size of one row + size of index) ) +
(Number of rows in Contact List table * (size of one row + size of index))
```

**Step 5** Start ICMDBA by entering **ICMDBA** in the Microsoft Windows **Run** dialog box or command window.

**Step 6** Select the **Logger**. Then, select **Database > Create**.

**Step 7** In the **Create Database** window, specify the Outbound Option database type.

**Step 8** Click **Add**. The **Add Device** window appears.

Use this window to create a new data device and log device for the Outbound Option database. Specify the disk drive letter and size in megabytes for each new device.

**Step 9** Click **OK** to create the device.

**Step 10** Click **Create**, and then click **Start**.

**Step 11** Click **Close**.

---

If necessary, you can later edit the device to change storage size, or remove a device, using the **Database > Expand** option.




---

**Caution** You cannot make manual changes to the contents of the Outbound Option database. Do not use triggers in the Outbound Option database. Do not add or modify triggers for the dialing lists or personal callback list. The Dialer\_Detail table in the logger or HDS contains the information that custom applications require. Extract that information from the historical database server (HDS) to a separate server where the custom application can process the data without impacting the HDS.

---





---

**Note** If you have used the ICMDBA tool to create an Outbound Option database on Logger Side B and you later want to uninstall the release, you can manually delete the database. Use SQL Server Management Studio (SSMS) to delete the database. If you have enabled Outbound Option two-way replication, you must disable replication from both Logger Side A and Logger Side B before you can delete the database.

---



---

**Note** When you use the **Append** option to import records to the **Outbound Contact Table**, the size of the Blended Agent (BA) database keeps increasing and it occupies all the available space in the disk. Hence, you must manually purge the **Outbound Contact Table** to create more space on the disk.

---

### What to do next

You must enable autogrowth on the Outbound Option database. For details, refer to the section on verifying database configurations.

### Related Topics

[Outbound Option Database](#)

[Verify Database Configuration](#), on page 27

## Configure the Logger for Outbound Option

Use this procedure to configure the Logger for Outbound Option.

You can (optionally) configure the Logger to enable Outbound Option and Outbound Option High Availability. Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Use the ICMDBA tool to create an outbound database on Side A and Side B; then set up the replication by using Web Setup.

Perform the following procedure on both the Side A and Side B Loggers to configure Outbound Option or Outbound Option High Availability. Both Logger machines must be up and operational.



---

**Important** Before you configure the Logger for Outbound Option High Availability:

- Confirm that an Outbound Option database exists on Logger Side A and Logger Side B.
- 

### Procedure

- 
- Step 1** Open the Web Setup tool.
  - Step 2** Choose **Component Management > Loggers**.
  - Step 3** Choose the Logger that you want to configure, and click **Edit**.
  - Step 4** Click **Next** twice.
  - Step 5** On the Additional Options page, click the **Enable Outbound Option** check box.

- Step 6** Click the **Enable High Availability** check box to enable Outbound Option High Availability on the Logger. Checking this check box enables High Availability two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. Two-way replication requires that you check this check box on the Additional Options page for both Logger Side A and Side B. If you disable two-way replication on one side, you must also disable it on the other side.
- You must enable Outbound Option in order to enable Outbound Option High Availability. Similarly, if you have enabled High Availability, you must disable High Availability (uncheck the **Enable High Availability** check box) before you can disable Outbound Option (uncheck the **Enable Outbound Option** check box).
- Step 7** If you enable High Availability, enter a valid public server hostname address for **Logger Side A** and **Logger Side B**. Entering a server IP address instead of a server name is not allowed.
- Step 8** If you enable High Availability, enter the **Active Directory Account Name** that the opposite side Logger runs under or a security group that includes that account.
- Note** While using Outbound Option High Availability, if you want to change the **Logger Public Interface** or **Active Directory Account Name**, you must disable Outbound Option High Availability using logger setup. Only after disabling Outbound Option HA, change the **Logger Public Interfaces** or **Active Directory Account Name**, then re-enable Outbound Option High Availability to update the new **Logger Public Interface** or **Active Directory Account Name**.
- Step 9** Select the **Syslog** box to enable the Syslog event feed process (cw2kfeed.exe).
- Note** The event feed is processed and sent to the Syslog collector only if the Syslog collector is configured. For more information about the Syslog event feed process, see the *Serviceability Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.
- Step 10** Click **Next**.
- Step 11** Review the Summary page, and click **Finish**.

---

### Related Topics

- [Outbound Option for High Availability: Preliminary Two-Way Replication Requirements](#), on page 15
- [Two-Way Outbound Option Database Replication](#)
- [Upgrade Outbound Option for High Availability in an Existing Deployment](#), on page 19

## Additional Two-Way Outbound Option Database Replication Consideration

Keep in mind the following consideration when setting up two-way replication.

### Import to Active Side

Importing a local file succeeds only if you import it to the active side. To avoid having to identify which side is active, you can use any of the following methods:

- Create a Microsoft Windows file share that is accessible to both sides with the same mapping; for example, `//<machine_name>/drive/file`, viewable from both sides.
- Use Microsoft Windows Distributed File System (DFS). With DFS, you can set up a local drive that DFS updates for you. DFS also makes sure that operations are replicated. For more information, see your Microsoft documentation.

- For campaigns created by using the Outbound API, you can use the Import API to import contacts without identifying the active side. For more information, see the *Cisco Unified Contact Center Enterprise Developer Reference Guide* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-programming-reference-guides-list.html>.

## Upgrade Outbound Option from a Previous Release

### Outbound Option Database

If you are upgrading from a previous CCE release, run the Enhanced Database Migration Tool (EDMT) to upgrade your Outbound Option database. Otherwise, Campaign Manager does not start, and an alarm for an incorrect private database version triggers. See the *Cisco Unified Contact Center Enterprise Installation and Upgrade Guide* at [https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod\\_installation\\_guides\\_list.html](https://www.cisco.com/en/US/products/sw/custcosw/ps1844/prod_installation_guides_list.html) for instructions on running EDMT.

### Do Not Call Data

To support Outbound Option High Availability and replication between Logger Side A and Logger Side B, Do Not Call data now resides in a Do\_Not\_Call database table. Previously, the DoNotCall data was stored in the DoNotCall.restore file on Logger Side A. The DoNotCall.restore file is a text file that contains a comma-delimited list of phone numbers and extensions (if extensions exist).

When you upgrade to the current release and enable Outbound Option (whether or not you enable High Availability), the Do\_Not\_Call table is initially empty, as it is newly created on each Logger side. Populate the Do\_Not\_Call table on Side A and Side B by importing the DoNotCall.restore file, just as you would perform any other import of customer contact information. You do this only once, when you perform an upgrade.

## Upgrade Outbound Option for High Availability in an Existing Deployment

Outbound Option High Availability facilitates two-way replication between the Outbound Option database on Logger Side A and the Outbound Option database on Logger Side B. If you have enabled Outbound Option on Logger Side A in an existing deployment and want to enable Outbound Option High Availability, perform the following steps using SQL Server Management Studio (SSMS).



---

**Note** Note that you need not perform the following procedure if the baA and baB databases are already in synchrony.

---

### Procedure

---

- Step 1** On the Logger Side A server, start SSMS and perform a full database backup of the <customer>\_baA database. (Refer to your SQL Server Management Studio documentation if you require further details about database backup.)
- Step 2** Restore the <customer>\_baA database backup on the Logger Side B server, and rename it as <customer>\_baB.
- a) In SSMS, select **Databases** in the tree in the left pane, and right-click.
  - b) Choose **Restore database**.
  - c) Choose **Device**, and browse to the backed-up <customer>\_baA database file.

- d) Click **Add** to add the database file.
- e) Click **OK**, then click **OK** again.
- f) In the **Database** field, enter <customer>\_baB.
- g) In the tree in the left pane, select **Files**. Note the **Logical File Name** for both the **Rows Data** and **Log** file types.
- h) In the tree in the left pane, select **Options** and check the **Overwrite the existing database (WITH REPLACE)** check box.
- i) Click **OK**.
- j) When the database restore completes with the new name <customer>\_baB, run the following command in a New Query window to rename the **Logical File Name** for both Rows Data and Log:

```
USE master;
GO
ALTER DATABASE <customer>_baB MODIFY FILE ( NAME = <customer>_baA_data0, NEWNAME =
<customer>_baB_data0 );
GO
USE master;
GO
ALTER DATABASE <customer>_baB MODIFY FILE ( NAME = <customer>_baA_log0, NEWNAME =
<customer>_baB_log0 );
GO
```

in which:

- <customer>\_baB is the renamed new database.
- <customer>\_baA\_data0 is the Logical File Name for the Rows Data file type for the database on Side A.
- <customer>\_baB\_data0 is the new Logical File Name for the Rows Data file type for the database on Side B.
- <customer>\_baA\_log0 is the Logical File Name for the Log file type for the database on Side A.
- <customer>\_baB\_log0 is the new Logical File Name for the Log file type for the database on Side B.

---

### Related Topics

[Configure the Logger for Outbound Option](#), on page 17

## Install Dialer Component on the PG Virtual Machine

### Procedure

---

- Step 1** Stop all ICM Services.
- Step 2** On both the Side A and Side B PGs, run Peripheral Gateway Setup. Select **Start > All Programs > Cisco Unified CCE Tools > Peripheral Gateway Setup**.
- Step 3** In the **Cisco Unified ICM/Contact Center Enterprise Components Setup** dialog, select an instance from the left column under **Instances**.
- Step 4** Click **Add** in the **Instance Components** section.

The **ICM Component Selection** dialog opens.

**Step 5** Click **Outbound Option Dialer**.

The **Outbound Option Dialer Properties** dialog opens.

**Step 6** Check **Production mode** and **Auto start at system startup**, unless your Unified ICM support provider specifically tells you otherwise. These options set the Dialer Service startup type to Automatic, so the dialer starts automatically when the machine starts up.

The **SIP (Session Initiation Protocol)** Dialer Type is automatically selected.

**Step 7** Click **Next**.

**Step 8** Supply the following information on this page:

- In the **SIP Dialer Name** field, enter the name of the SIP dialer. For example, **Dialer\_for\_Premium\_Calling\_List**. There's a 32-character limit. The name entered here must match the name that is configured in Configuration Manager.
- For **SIP Server Type**, select either **Cisco voice gateway** or **CUSP/CUBE (Cisco Unified SIP Proxy or Cisco Unified Border Element)**.
- In the **SIP Server** field, enter the hostname or IP address of the Cisco voice gateway.  
**Note** The **SIP Server** hostnames are restricted to a maximum of 16 characters.
- In the **SIP Server Port** field, enter the port number of the SIP Server port. Default is 5060.

Click **Next**.

**Step 9** On the **Outbound Option Dialer Properties** dialog, specify the following information:

- **Campaign Manager server A**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side A Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server B** field. You must supply a value in this field.
- **Campaign Manager server B**—If the Campaign Manager is set up as duplex, enter the hostname or IP address of the machine where the Side B Campaign Manager is located. If the Campaign Manager is set up as simplex, enter the same hostname or IP address in this field and the **Campaign Manager server A** field. You must supply a value in this field.

In simplex mode, make sure not to provide same port number in server Side B and Side A. For more information about port ranges, see the [Port Utilization Guide](#).

- **Enable Secured Connection**— Allows you to establish secured connection between the following:
  - CTI server and dialer
  - MR PIM and dialer

Check the **Enable Secured Connection** check box to enable secured connection.

**Note** Before you enable secured connection between the components, ensure to complete the security certificate management process.

For more information, see the *Security Guide for Cisco Unified ICM/Contact Center Enterprise* at <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-and-configuration-guides-list.html>.

- **CTI server A**—The hostname or IP address of the VM with CTI server-Side A. This server is typically the same VM where the PG is located.
- **CTI server port A**—The port number that the dialer uses to create an interface with CTI server-Side A. Make sure the CTI server port matches with the CG configuration.
- **CTI server B**—The hostname or IP address of the VM with CTI server-Side B. This server is typically the same VM where the PG is located.
- **CTI server port B**—The port number that the dialer uses to create an interface with CTI server-Side B.
- **Heart beat**—The interval between dialer checks for the connection to the CTI server, in milliseconds. The default value is 500.
- **Media routing port**—The port number that the dialer uses to create an interface with the Media Routing PIM on the Media Routing PG. The default is 38001. Make sure that the Media routing port matches that of the MR PG configuration. For example, you can access this registry key:  
Computer\HKEY\_LOCAL\_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\

**Step 10** Click **Next**. A **Summary** screen appears.

**Step 11** Click **Next** to begin the dialer installation.

### Optional - Edit Dialer Registry Value for Auto-Answer

If you enable auto answer in the CallManager with a zip tone, you must disable auto answer in the Dialer or Dialers, if there are more than one. A zip tone is a tone sent to the agent's phone to signal that a customer is about to be connected.

To disable auto answer in the Dialer, after the Dialer process runs for the first time, change the value of the following registry key to 0:

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM\

```

## Modification of Local Static Route File

The SIP Dialer installation process installs an empty template file named DNPHost in the \icm\customerInstanceName\Dialer directory. This file defines the static route mappings of a dialed number wildcard pattern to the IP address or host name with which an agent phone or CTI Route point is registered. For each static route you define, add a row in the following format:

```
wildcard pattern, IP address or host name, description
```

Examples:

```
7?????, 10.86.227.144, transferring outbound calls to agent extensions
86! , 10.86.227.186, for CTI Route Points on CUCM node1
4?????, gambino.cisco.com, transfer to IVR campaign
```

For single gateway deployments, the SIP Dialer reads the static routing info from DNPHost and uses the information to construct the SIP REFER message. If the SIP Dialer supports a voice gateway, the SIP Dialer loads DNPHost, validates the routing entries, and sends an alarm if the file does not exist or is invalid.

See the installed DNPHost file template for additional information about its use.

## Auto Answer Configuration on Agent Phones

The dialer component is preconfigured during installation to auto answer Outbound Option related calls to the Outbound Option agent. However, this default configuration does not provide a zip tone to the agent (which notifies of incoming calls), so agents must monitor the agent application for incoming customer calls.

To enable zip tone, enable auto-answer on the agent's phone configuration in Unified CM. This solution adds about a second onto the transfer time. This solution is identical to the solution that is used for Unified CCE.

For Mobile Agents using the nailed connection, the Unified CM auto answer setting does not provide a zip tone, but contact center enterprise does provide an option for playing a notification tone to the agent using the agent desk settings.

Enabling auto answer in the agent desk settings or in the dialer component in conjunction with the Unified CM can be problematic. Therefore, disable the auto answer option in the dialer component, and enable it either in the agent desk settings or in Unified CM.

## Install MR PG

Perform the following steps to install the MR PG on the Side A platform.

If you are also running a Dialer on Side B, perform the steps on Side B as well.

### Procedure

- 
- Step 1** Run ICM Setup to install a PG that corresponds with the PG you configured (for example, PG3).
- Step 2** In the Peripheral Gateway Properties window, select the MR PG Node ID (for the configured PG; for example, PG3) and the **MediaRouting** Client Type.
- Step 3** Click **Next**.
- Step 4** Add a PIM, **PIM1**.
- Step 5** In the MediaRouting Configuration window, enable the PIM.
- Step 6** Enter the peripheral name and the peripheral ID (recorded at the end of the procedure described in [Configure Media Routing PG \(MR PG\), on page 3](#)) of the MR\_PIM.
- Step 7** Set the Application Hostname fields:
- For simplex deployments, set both of the Application Hostname fields to the computer name of the Outbound Option Dialer.
  - For duplex Sip Dialers with duplex MR PG deployments,
    - Specify the local Dialer HostName in ApplicationHostName1.
    - Specify the remote, duplex Dialer HostName in ApplicationHostName2.
- Step 8** Set the Application Connection Port to the port number used by the Outbound Option Dialer (usually 38001).

- Step 9** Click **Next** until Setup finishes. When Setup finishes, click **Finish**.
- Step 10** Repeat the preceding steps to install the MR PG on the Side B PG platform.
- 

#### What to do next

When you add new PG make sure that PG ID is provided in the Router configuration. Provide the number that is assigned to the PG in the **Enable Peripheral Gateway** field in Web Setup. *See chapter: Installation* in <https://www.cisco.com/c/en/us/support/customer-collaboration/unified-contact-center-enterprise/products-installation-guides-list.html>

#### Related Topics

[Configure the PG](#), on page 2

## Verification

This section provides a series of verification steps to determine if the system has been installed properly. These steps are designed to pinpoint problems that might exist in the setup before actually attempting to deploy the Dialer. If problems occur while using this product, please see this section before contacting Cisco Technical Support (TAC).



---

**Note** This section assumes that the Outbound Option application is installed and at least one Dialer has been configured along with its associated port map. This section also assumes that the Dialer port map has been exported and configured on Unified CM using the BAT tool.

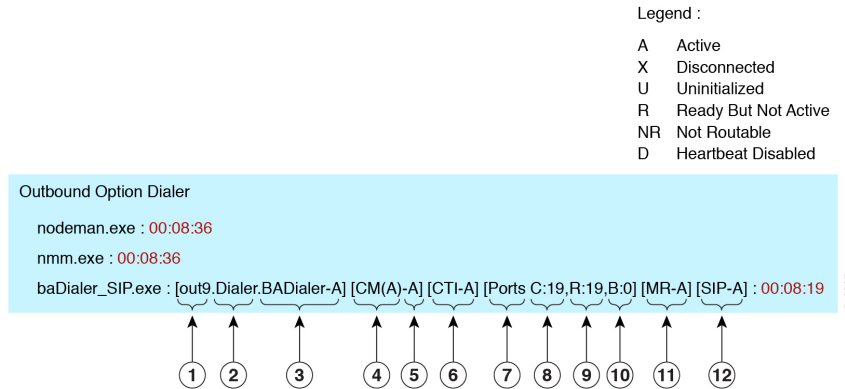
---

## Dialer Component Status

The Dialer component process status provides details about the health of the installation even before any campaign configuration is initiated or before any call is placed. You can view the Dialer component status in the Diagnostic Framework Portico.



Figure 5: SIP Dialer Component Status



1. Customer Instance Name
2. Node Name
3. Process Name
4. Campaign Manager
5. Side Information
6. CTI Server
7. Telephony Port Status
8. Configured Ports
9. Ready Ports
10. Blocked Ports
11. MR PIM
12. SIP Proxy or Voice Gateway

### Customer Instance Name

The customer instance name shows the dialer’s customer instance, node name, and process name. This can be used if TAC asks you to interrogate the system while debugging a problem for a case.

### Campaign Manager

The Campaign Manager shows the Campaign Manager connectivity status. This status is either A for active or X for disconnected. If the Campaign Manager connectivity status is X, the dialer is not connected to the Campaign Manager.

Try pinging from the dialer to the active Campaign Manager by hostname and by IP Address.

- If the ping fails for the IP address, recheck that the IP address is correct and troubleshoot network connectivity.
  - Check to verify whether Outbound Option has been enabled, and the Campaign Manager process is running.
- If the ping is successful for the IP address but not for the DNS hostname, check that the DNS hostname is correct and that it is properly configured in the system’s DNS server.
- If the ping is successful, then recheck the dialer component setup to see if the dialer component setup contains the wrong address or port number for the Logger.
- Check to see if the name of the Dialer configured in Configuration Manager matches the name entered during PG setup.

### CTI Server

The third block shows CTI Server connectivity status. This status is either **A** for active or **X** for disconnected. If the status is **X**, then the dialer cannot connect to either CTI Server on side A or side B.

Try pinging from the dialer to the CTI Server/PG machines by hostname and by IP address.

- If the ping fails for the IP address:
  - Recheck that the IP address is correct, and troubleshoot network connectivity.
  - Check to see whether the CTI Server processes are running.
- If the ping is successful for the IP address but not for the DNS hostname, check that the DNS hostname is correct and whether it is properly configured in the system's DNS server.
- If the ping is successful, then recheck the dialer component set up to see if the dialer component set up contains the wrong address or port number for the CTI Server.
- Check that the PG is online. Check that the PG has been enabled properly in the ICM Router setup.

### Ports

The fourth block shows the state of all dialer ports. The first value, C, shows the total number of configured ports. The second value, R, shows the total number of ready ports. Finally, the third value, B, reports the number of dialer ports that are blocked. (This is runtime activity; it is unusual for ports to be blocked.)

If the number of ports Configured is zero, then the dialer is not receiving port configuration from the Campaign Manager component. Check to verify that ports are configured properly.

If the number of Ready ports is zero, confirm that the PG has been started.

### MR PIM

The next block shows connectivity status with the MR PIM. This status is either **A** for active, **X** for disconnected, or **NR** which means connected but not yet able to route. (The U status is rarely seen and indicates that a particular connectivity object within the dialer has not been created yet.)

- If the MR Status is **X**, check the connectivity by verifying the MR PG address and port configured in the dialer component setup.

If the MR PG status is **NR**, then the Media Routing connection is established. Check to see if the MR PG is online by looking at its status window.

### SIP Dialer

The final block shows connectivity status with the SIP Proxy or Voice Gateway that is connected to the SIP dialer. This status is either **A** for active, **X** for disconnected, or **D** for heartbeat disabled.

## Verify Critical Configuration Steps

In the Dialer Configuration Component, click the Port Map Selection tab and ensure the Dialer is assigned to a Unified CM PG.

## Verify Database Configuration

Perform the following steps in Microsoft SQL Server:

### Procedure

---

- Step 1** Open the SQL Server Management Studio.
  - Step 2** Expand the databases.
  - Step 3** Select the <cust instance\_baA> **Outbound Option** or <cust instance\_baB> **Outbound Option** database. Right click and select **Properties**.
  - Step 4** Select the **Files** page.
  - Step 5** In the database file row, click the button in the **Autogrowth** column. A Change Autogrowth dialog box appear.
  - Step 6** Ensure that the **Enable Autogrowth** box is checked. Click **OK**.
  - Step 7** In the log file row, click the button in the **Autogrowth** column. A Change Autogrowth dialog box appears.
  - Step 8** Ensure that the **Enable Autogrowth** box is checked. Click **OK**.
  - Step 9** Select the **Options** page.
  - Step 10** On the Recovery Model drop-down menu, select **Simple**.
  - Step 11** Click **OK**.
- 

## Verify Router Registry Key

If you are using the Transfer to IVR feature, verify that the following router registry key on Side A and Side B of the Router has a value of 2.

```
HKEY_LOCAL_MACHINE\SOFTWARE\Cisco Systems, Inc.\ICM<customer  
instance>\RouterA/B\Router\  
CurrentVersion\Configuration\Global\SkillGroupCallsInQTimerInterval = 2
```

