**Main page:** Cisco Unified MeetingPlace, Release 8.0

**Up one level:** Configuration

**Note:** In this document, a "system" refers to a complete Cisco Unified MeetingPlace site installation, which includes one active Application Server and one active Media Server. The system might also include one or more Web Servers.

- About RSNA
- Prerequisites for RSNA
- Restrictions for RSNA
- How to Configure RSNA

# Contents

# About RSNA



## RSNA

The Reservationless Single Number Access (RSNA) feature allows multiple Cisco Unified MeetingPlace systems to appear as one system to the user community. Any user who hosts (as a profiled user) or attends (as a profiled user or as a guest) a reservationless meeting can join the meeting by dialing the access phone number of the Cisco Unified MeetingPlace system that is local to that user, regardless of which system is hosting the meeting. Users are then redirected to the system that is hosting the meeting.

## Dial Prefixes

Dial prefixes are applied to transfer addresses when call transfers are routed through Cisco IOS voice gateways. Cisco Unified MeetingPlace uses the first applicable method in Table: Options for Configuring Dial Prefixes to determine the dial prefix for each remote server.

**Table: Options for Configuring Dial Prefixes**

| Method | | How and When to Use This Method |
|---|---|---|
| 1 | Extended dial prefix | Use this option to control the type of codec used when performing call transfers between particular Cisco Unified MeetingPlace systems.<br><br>You configure the Routing Unit Number and Routing Codec fields with non-default values for each remote server. The system uses the configured values to create a four-digit dial prefix *UUCC*, where:<br>• *UU* is the Routing Unit Number (with a leading 0 if necessary)<br>• *CC* represents the codec<br><br>The codec digits are:<br>• G.711U-01<br>• G.711A-02<br>• G.729-03<br>• G.729a-04<br>• G.729b-05<br>• G.722-06<br>• ILBC-07<br><br>**Note:** On the Cisco IOS voice gateway, make sure that you specify the same codec in the dial peer configuration.<br><br>**Note:** The Cisco Unified MeetingPlace Application Server supports 711a, 711u, 722, 729a, 729b, ILBC codecs when configured to use the hardware Media Server. The server supports 711a, 711u, 722, 729a when configured to use the Express Media Server.<br><br>See the Example Configuration for Extended Dial Prefix. |
| 2 | Common dial prefix | Use this option when you want all Cisco Unified MeetingPlace systems to use the same dial prefix and the same codec for all call transfers.<br><br>You configure the Dial prefix field on the Remote Server Configuration Page so that the field is not blank. The system uses the configured Dial prefix for all remote servers. To enable the Dial prefix field, the Routing Codec field must be set to None. |

| | | |
|---|---|---|
| | | Consult your telephony administrator to determine the Dial prefix required by your routing plan. Cisco IOS-based routing typically requires a 4-character dial prefix, while Cisco Unified Communications Manager-based routing does not require a dial prefix at all.<br><br>**Note:** If you configure the Dial prefix, each RSNA systems must be configured to use the same dial prefix.<br><br>See the Example Configuration for Common Dial Prefix. |
| 3 | Default dial prefix | For simplicity, we recommend that you use this option.<br><br>You leave these fields with the default values:<br>• Dial prefix-blank<br>• Routing Unit Number-0<br>• Routing Codec-None<br><br>The system generates a 13-character dial prefix by combining the following:<br>• 12-digit IP address in the SIP Agent Address 1 remote server field<br>• The character "x"<br><br>For example, if the transfer IP address is 172.27.1.1, the generated dial prefix is 172027001001x. |

**Related Topics**

- Configuring Call Control for RSNA Using Cisco IOS Voice Gateways
- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module

## RSNA Reserved Meeting Server

The RSNA Reserved Meeting Server feature allows a single Application Server to host reserved meetings within an RSNA-based network. Typically, all meeting reservations are on the one designated Reserved Meeting Server. When users attend meetings by accessing their local server, if their local server does not recognize the meeting ID, it transfers the user to the Reserved Meeting Server.

**Note:** You must synchronize the server times between the local Application Server and the Reserved Meeting Server.

The local server attempts to transfer calls to the Reserved Meeting Server if all of these conditions are true:

- The Reserved Meeting Server feature has been configured on the local server:

The local server must be configured with a remote server record in which the Reserved Meeting Server check box is checked.

If you want any user profiles to identify the remote Reserved Meeting Server as the Schedule home server, create a duplicate remote server record in which you do the following:

- Do NOT check the Reserved Meeting Server check box.
- Enter a Home Server number in the range 0 to 999.
- Make sure that all other fields are identical between the duplicate records for the Reserved Meeting Server.

- The meeting ID that the user entered does not match the meeting ID of any meetings scheduled around that time on the local server.
- The meeting ID that the user entered does not match any user profile, active or not.
- The user confirms the meeting ID.

In addition, consider the following behavior of the RSNA Reserved Meeting Server feature:

- This feature does not prevent meetings from being scheduled locally and will not warn or transfer a user who attempts to schedule a meeting locally.
- If a meeting is scheduled on a server other than the Reserved Meeting Server, this feature will not facilitate attendance of that meeting.
- A locally scheduled meeting always takes precedence over a remote one. This rule applies even if a local meeting recently ended and the user hears that meeting is over.
- If the meeting does not exist on the remote system, the system prompts the user for a meeting ID after the transfer.

**Related Topics**

- Configuring the Remote Servers

# Prerequisites for RSNA

- Plan and install your Cisco Unified MeetingPlace systems for RSNA as described in the following:
  - *Planning Guide for Cisco Unified MeetingPlace* at http://docwiki.cisco.com/wiki/Cisco_Unified_MeetingPlace%2C_Release_8.0_--_Planning_Your_Deploy
  - Quick Start for Installing and Configuring Cisco Unified MeetingPlace Release 8.0 module
- Participating voice gateways and endpoints that directly access Cisco Unified MeetingPlace must support SIP and the SIP REFER method of transferring calls as specified in RFC 3515.

**Related Topics**

- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module

# Restrictions for RSNA

- Only two RSNA systems (sites) are currently supported.
  - Both RSNA systems must use the same Type of media server setting; for example, they must both be set either to Express Media Server or to Hardware Media Server.

    - Both RSNA systems must use the same type of connectivity; for example, with connectivity through Cisco Unified Communications Manager or through Cisco Unified Border Element (CUBE) connected node.
- RSNA is not supported with web conferencing integrations (Cisco WebEx and IBM Lotus Sametime).
- Meeting recordings are stored only on the Web Server that is associated with the Schedule home server for the meeting owner. To access meeting recordings, the users must know the URL of the Web Server that you assigned to the meeting owner.
- The system cannot strongly authenticate users by password when they are transferred between servers. This causes the following restrictions for profiled users who are transferred into a meeting:
    - Recorded names are not permanently stored on the system.
    - When leaving the meeting, the users are treated as unidentified.

#### Related Topics

- Configuring Reservationless Single Number Access (RSNA) for Cisco Unified MeetingPlace module

# How to Configure RSNA

- Enabling RSNA
- Configuring the Remote Servers
- How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment
- Configuring Call Control for RSNA Using Cisco IOS Voice Gateways
- How to Configure User Profiles for RSNA

## Enabling RSNA

Complete this task on each Cisco Unified MeetingPlace system for which you want to enable RSNA.

#### Before You Begin

Read these topics:

- Prerequisites for RSNA
- Restrictions for RSNA

#### Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Remote Server Configuration**.
3. Set the Enable RSNA field to **Yes**.
4. Select **Save**.

#### Related Topics

- Table: Field Reference: Remote Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (R - S pages)

#### What To Do Next

Proceed to the Configuring the Remote Servers.

## Configuring the Remote Servers

Complete this task on each RSNA system.

#### Before You Begin

- Complete the Enabling RSNA.
- Read the Dial Prefixes.

#### Procedure

1. Sign in to the Administration Center.
2. Select **System Configuration > Remote Server Configuration**.
3. Select **Add New**, or select an existing entry.
4. Configure the fields on the Add Server Configuration Page.
5. Select **Save**.
6. Repeat Step 3 through Step 5 to add a server entry for each remote RSNA system.
7. (Optional) Complete these steps to configure a Common dial prefix to apply to all call transfers.

   **Note:** If you configure the Dial prefix, all RSNA systems must use the same dial prefix. For simplicity, we recommend that you instead configure each RSNA system to use the Default dial prefix. For details, see the Dial Prefixes.

   1. Click **Remote Server Configuration**.
   2. Configure the Dial prefix field.
   3. Click **Save**.

#### Related Topics

- Table: Field Reference: Add Server Configuration Page and Edit Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (A - C pages)
- Table: Field Reference: Remote Server Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (R - S pages)
- RSNA Reserved Meeting Server

#### What To Do Next

Proceed to one of these topics:

- How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment
- Configuring Call Control for RSNA Using Cisco IOS Voice Gateways

## How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment

Complete these tasks, in the order shown, on each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

- Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System
- Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems

### Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System

In this task, you connect the local Cisco Unified Communications Manager to each remote Cisco Unified MeetingPlace RSNA system.

#### Before You Begin

- Configure non-RSNA call-control for each Cisco Unified MeetingPlace system as described in the Configuring Call Control for Cisco Unified MeetingPlace module.
- We recommend that you create a SIP trunk security profile in Cisco Unified Communications Manager specifically for Cisco Unified MeetingPlace.

  See Configuring a SIP Trunk Security Profile in Cisco Unified Communications Manager for Cisco Unified MeetingPlace in the Integrating Cisco Unified MeetingPlace with Cisco Unified Communications Manager module.

- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

#### Procedure

1. Go to **http://***ccm-server***/**, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Device > Trunk**.
4. Select **Add New**.
5. In the Trunk type field, select **SIP Trunk**.
6. Select **Next**.

7. Configure the fields described in Table: Fields for Adding a SIP Trunk in Cisco Unified Communications Manager Release 6.1 (or Later).

**Table: Fields for Adding a SIP Trunk in Cisco Unified Communications Manager Release 6.1 (or Later)**

| Field | Action |
|---|---|
| Device Name | Enter a unique identifier for this trunk, such as the name or IP address of the *remote* Cisco Unified MeetingPlace Application Server. |
| Device Pool<br><br>AAR Group | The device pool must use a codec that is compatible with the conferencing gateway (or bridge).<br><br>For security and toll fraud prevention, use a device pool and an automatic alternate routing (AAR) group that will block any undesired phone numbers from being dialed out. |
| Media Termination Point Required | Uncheck this check box. |
| Destination Address | The DNS hostname or IP address of the *remote* Cisco Unified MeetingPlace server. |
| Destination Port | Keep the default value of **5060**. |
| SIP Trunk Security Profile | Select the SIP trunk security profile that you created specifically for Cisco Unified MeetingPlace.<br><br>If you did not create a SIP trunk security profile, select the default **Non Secure SIP Trunk Profile**. |
| DTMF Signaling Method | Select **No Preference**. |

8. Configure all other required fields appropriately for your current deployment.

   **Tip:** For field descriptions, select **Help > This Page**.
9. Select **Save**.
10. Repeat this task to add a SIP trunk to each remote Cisco Unified MeetingPlace RSNA system.

#### What to Do Next

Proceed to the Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems.

### Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems

In this task, you enable the local Cisco Unified Communications Manager to route calls to each remote Cisco Unified MeetingPlace RSNA system.

**Before You Begin**

- Complete the Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System.
- You perform this task in the Cisco Unified Communications Manager Administration pages. Because the pages and menus vary by release, you should check the Cisco Unified Communications Manager Administration online help for step-by-step instructions that are specific to your release.

**Restriction**

By associating a SIP route pattern to a SIP trunk, you can no longer put the SIP trunk in a route group. If, for some reason, you need to put the SIP trunk in a route group, create duplicate SIP trunks. Specifically, for each SIP trunk that is associated with a SIP route pattern, create an identical SIP trunk that is *not* associated with a SIP route pattern.

**Procedure**

1. Go to **http://***ccm-server***/**, where *ccm-server* is the fully-qualified domain name or IP address of the Cisco Unified Communications Manager server.
2. Sign in to Cisco Unified Communications Manager Administration.
3. Select **Call Routing > SIP Route Pattern**.
4. Select **Add New**.
5. Configure the fields described in Table: Fields for Adding a SIP Route Pattern in Cisco Unified Communications Manager Release 6.1 (or Later).

**Table: Fields for Adding a SIP Route Pattern in Cisco Unified Communications Manager Release 6.1 (or Later)**

| Field | Action |
|---|---|
| Pattern Usage | Select **IP Address Routing**. |
| Pattern | Enter the IP address of the remote Application Server.<br><br>**Note:** This value must match the SIP Agent Address 1 field that was configured on the local Cisco Unified MeetingPlace system to identify the remote system. |
| SIP Trunk | Select the SIP trunk that you configured in the Configuring Cisco Unified Communications Manager: SIP Trunk to Remote RSNA System. |

6. Configure all other required fields appropriately for your current deployment.

   **Tip:** For field descriptions, select **Help > This Page**.
7. Select **Save**.
8. Select **OK** to any pop-up dialog box messages that you see.
9. Repeat this task to add a SIP route pattern to each remote Cisco Unified MeetingPlace RSNA system.

**What to Do Next**

Repeat the tasks in the How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment for each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

Then proceed to the How to Configure User Profiles for RSNA.

## Configuring Call Control for RSNA Using Cisco IOS Voice Gateways

Use this procedure to configure dial peers on voice gateways to route call transfers to the remote Cisco Unified MeetingPlace systems.

**Before You Begin**

- Configure non-RSNA call control for each Cisco Unified MeetingPlace system as described in the Configuring Call Control for Cisco Unified MeetingPlace module.
- You perform this task in the Cisco IOS command-line interface (CLI) of the router. For more information about the Cisco IOS commands used in this procedure, see the *Cisco IOS Commands Master List* for your Cisco IOS software major release.

**Procedure**

1. On the Cisco IOS voice gateway for the remote Cisco Unified MeetingPlace system, enter privileged EXEC mode or any other security level set by a system administrator. Enter your password if prompted.
   `Router#` **`enable`**
2. Enter global configuration mode.
   `Router#` **`configure terminal`**
3. Enter dial peer voice configuration mode and define a remote voice over IP (VoIP) dial peer.
   `Router(config)#` **`dial-peer voice`** *`number`* **`voip`**
   The *number* is one or more digits that identify the dial peer. Valid entries are from 1 to 2147483647.
4. (Optional) Provide a comment or description to help you remember what is attached to this interface.
   `Router(config-dialpeer)#` **`description`** *`string`*
5. Route calls to the remote system:
   `Router(config-dialpeer)#` **`destination-pattern`** *`digits`*
   - For Cisco Unified MeetingPlace Release 8.0, the destination pattern must match the dial prefix for the remote server. See the Dial Prefixes.
   - For the Extended RSNA Prefix feature, the dial-peer destination pattern must match the Extended Prefix string on the originating Cisco Unified MeetingPlace Application Server for the server being transferred to.
6. Configure the dial peer to use SIP.
   `Router(config-dialpeer)#` **`session protocol sipv2`**
7. Configure any IP address.
   `Router(config-dialpeer)#` **`session target ipv4:`***`ip-address`*
   The target IP address is ignored, but it is passed as part of the SIP REFER command. When the voice gateway receives a SIP REFER request with the string matching the RSNA dial

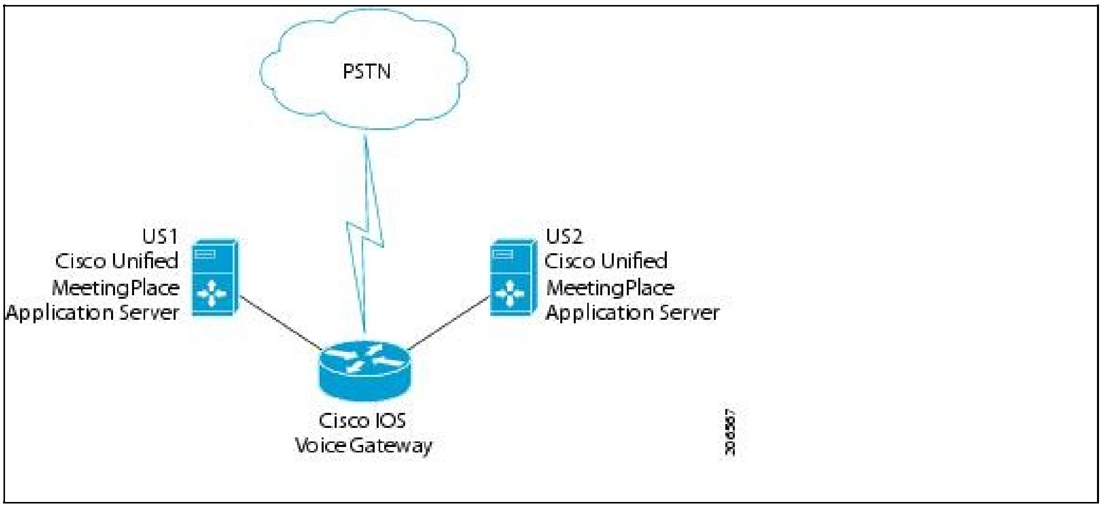
peer, the voice gateway forwards the call to the target Cisco Unified MeetingPlace Application Server.

8. Configure the router to forward dual tone multifrequency (DTMF) tones by using Real-Time Transport Protocol (RTP) with the Named Telephone Event (NTE) payload type.
   `Router(config-dialpeer)#` **`dtmf-relay rtp-nte`**
9. Configure the codec to use when transferring calls.
   `Router(config-dialpeer)#` **`codec`** `[`**`g711ulaw`** `|` **`g711alaw`** `|` **`g729 | g722-64 | ilbc`**`]`
10. Disable voice activity detection (VAD) for the calls using this dial peer.
   `Router(config-dialpeer)# [`**`no`**`]` **`vad`**
11. Exit the current mode.
   `Router(config-dialpeer)#` **`exit`**
12. Repeat this procedure on each Cisco IOS voice gateway that is attached to an RSNA system.

**Example Configuration for Extended Dial Prefix**

The example in Figure: Direct Connection Between a PSTN Gateway and the Application Server using Extended Dial Prefixes shows a topology with two Cisco Unified MeetingPlace Application Servers in the United States. In this scenario, calls that are transferred between the U.S. servers (US1 and US2) use the G.711 codec.

**Figure: Direct Connection Between a PSTN Gateway and the Application Server using Extended Dial Prefixes**




On the Application Servers in this example, configuring the Routing Codec field on the Application Server results in the extended prefix values shown in Table: Extended Prefix Values.

**Table: Extended Prefix Values**

| Server | Extended Prefix |
|---|---|
| US1 | 0101 |
| US2 | 0201 |

Note that the actual codec used when transferring calls depends on the dial-peer configuration on the gateway, not on the value of the Routing Codec field. Any codec (other than None) can be chosen for the Routing Codec field to generate the extended prefix. However, the codec you choose for a given server should be consistent across both of the Application Servers to generate the same extended prefix for that server.

Given these prefix values, the U.S. voice gateway would be configured with dial peers that match the extended prefixes:

```
 !
dial-peer voice 210 voip
description rsna_refer_to_us1
destination-pattern 0101
session protocol sipv2
session target ipv4:10.10.10.1
dtmf-relay rtp-nte
codec g711ulaw
no vad
 !
dial-peer voice 220 voip
description rsna_refer_to_us2
destination-pattern 0201
session protocol sipv2
session target ipv4:10.10.10.2
dtmf-relay rtp-nte
codec g711ulaw
no vad
 !
```

**Example Configuration for Common Dial Prefix**

The example in Figure: Direct Connection Between a PSTN Gateway and the Application Server using Common Dial Prefix shows a multi-node RSNA topology with a direct connection between a PSTN gateway and the Application Server. In this scenario, calls that are transferred between servers using a common dial prefix.

**Figure: Direct Connection Between a PSTN Gateway and the Application Server using Common Dial Prefix**

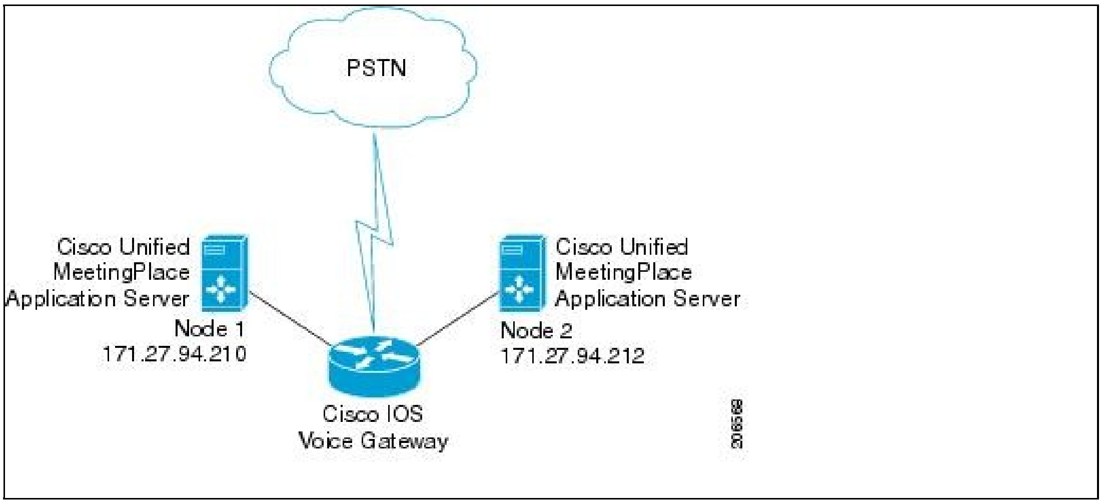



Table: Cisco Unified MeetingPlace Application Server Configuration shows the configuration for Node 1 and Node 2.

**Table: Cisco Unified MeetingPlace Application Server Configuration**

| Node 1 Configuration | Node 2 Configuration |
|---|---|
| **Remote Server Configuration** | **Remote Server Configuration** |
| Name: Node 2 | Name: Node 1 |
| Home server number: 2 | Home server number: 1 |
| SIP agent address 1: 171.27.94.212 | SIP agent address 1: 171.27.94.210 |
| **RSNA Configuration** | **RSNA Configuration** |
| Enable RSNA: Yes | Enable RSNA: Yes |
| Dial prefix: 2420 | Dial prefix: 2420 |

The Cisco IOS voice gateway has this configuration:

**Incoming dial peer:**

```
 !
dial-peer voice 1 pots
description T1 CAS from PSTN
incoming called-number 9550931
direct-inward-dial
```

```
forward-digits all
 !
```

**Outgoing dial peers**

```
 !
dial-peer voice 100 voip
description to_AppServer_Node_1
destination-pattern 9550931
session protocol sipv2
session target ipv4:171.27.94.210
dtmf-relay rtp-nte
codec g711ulaw
no vad
 !
dial-peer voice 200 voip
description to_AppServer_Node_2
destination-pattern 9550931
session protocol sipv2
session target ipv4:171.27.94.212
dtmf-relay rtp-nte
codec g711ulaw
no vad
 !
```

**RSNA SIP REFER dial peer**

```
 !
dial-peer voice 900 voip
description RSAN configure for SIP REFER
huntstop
```

```
destination-pattern 2420

session protocol sipv2

session target ipv4:1.1.1.1

dtmf-relay rtp-nte

codec g711ulaw

no vad

 !

Dial peer hunt sequence

dial-peer hunt 1
```

#### Troubleshooting Tip

You can use the **debug ccsip messages** Cisco IOS command to look at SIP REFER messages.

#### Related Topics

- Configuring Access Phone Numbers and Notification Labels module
- Configuring Direct Inward Dial for Cisco Unified MeetingPlace module

#### What to Do Next

Proceed to How to Configure User Profiles for RSNA.

## How to Configure User Profiles for RSNA

These fields in each user profile must have the exact same values on the RSNA systems:

- User ID
- User password
- Profile number
- Profile PIN
- Schedule home server

This is typically accomplished by completing these tasks:

| | High-Level Task | Where to Find Instructions |
|---|---|---|
| 1 | Configure the Schedule home server field through user groups. | Configuring the Schedule Home Server Field in User Groups or User Profiles |
| 2 | Synchronize the user database between the two sites. | Configuring User Database Replication for Two Sites in the Configuring Cisco |

| | | |
|---|---|---|
| | | Unified MeetingPlace Directory Service module |
| 3 | (Optional) Configure Directory Service on *one* RSNA system to synchronize Cisco Unified MeetingPlace user profiles with Cisco Unified Communications Manager and configure external AXL authentication. | Configuring Cisco Unified MeetingPlace Directory Service module |
| 4 | If you configured Directory Service on one RSNA system, configure external AXL authentication on the other (non-Directory Service) system. | Enabling External User Authentication on the Non-Directory Service RSNA System |

### Configuring the Schedule Home Server Field in User Groups or User Profiles

Complete this task on each RSNA system.

#### Before You Begin

Complete the tasks in the How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment for each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

#### Procedure

1. Sign in to the Administration Center.
2. Select **User Configuration**.
3. Select **User Groups** or **User Profiles**, depending on whether you want to configure a user group or an individual user profile.

    **Tip:** Because Directory Service does not synchronize this particular configuration, we recommend that you configure user groups and allow the user profiles to inherit the group default values.
4. Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.
5. Configure the Schedule home server field to match the Home Server number remote server field.
6. Select **Save**.
7. Repeat this procedure for all user groups and (if necessary) user profiles.

#### Related Topics

- Table: Field Reference: Add User Profile Page and Edit User Profile Page in the Administration Center Page References for Cisco Unified MeetingPlace (A - C pages)
- How to Configure User Profiles for RSNA

#### What To Do Next

Proceed to Configuring User Database Replication for Two Sites in the Configuring Cisco Unified MeetingPlace Directory Service module.

### Enabling External User Authentication on the Non-Directory Service RSNA System

By performing this task, you enable Directory Service users to sign in to either RSNA system. Note that the same Cisco Unified Communications Manager server is used for authentication.

#### Before You Begin

Complete Step 1 through Step 3 in the How to Configure User Profiles for RSNA.

#### Procedure

1. On the non-Directory Service system, sign in to the Cisco Unified MeetingPlace Administration Center.
2. Select **User Configuration > Directory Service > Directory Service Configuration**.
3. Configure these fields, using the exact same values that you entered on the Directory Service-configured system:
    - AXL user ID
    - AXL password
    - AXL confirm password
    - AXL URL
4. Do not modify any of the other fields on the Directory Service Configuration Page.
    - If you think you accidentally modified any of the other fields, select **Cancel** and return to Step 2.
    - If you think you accidentally modified *and saved* any of the other fields, do the following:
        - Make sure that Perform full sync with Cisco Unified Communications Manager is **unchecked**.
        - Make sure that Hostname for Active Directory Service either matches the value configured on the Directory Service-configured system or is left **blank**.
5. Select **Save**.

#### Related Topics

- Table: Field Reference: Directory Service Configuration Page in the Administration Center Page References for Cisco Unified MeetingPlace (D - G pages)
- How to Configure User Profiles for RSNA