



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

Release 7.1
Revised: April 6, 2011 12:14 pm



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 may also include one or more Web Servers.

- [About RSNA, page 1](#)
- [Prerequisites for RSNA, page 3](#)
- [Restrictions for RSNA, page 3](#)
- [How to Configure RSNA, page 3](#)

About RSNA

- [RSNA](#)
- [RSNA Reserved Meeting Server, page 2](#)

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.

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

The server times must be synchronized 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 the following 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](#), then 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.
- Users choose which server to schedule the meeting on from the Server drop-down box on the Scheduling page. To restrict users from choosing a server other than the Reserved Meeting Server, you may need to disable the Server drop-down box from the scheduling page. This restriction does not apply if the user dials into a local server and uses the TUI to schedule the meeting. In that case the meeting will be scheduled on a local server

Restrictions

Meeting recordings are stored only on the web server that is associated with the schedule home server for the meeting owner. You must know the URL of the web server that you assigned to the meeting owner to access meeting recordings.

Related Topics

- [Configuring the Remote Servers, page 4](#)

Prerequisites for RSNA

- Plan and install your Cisco Unified MeetingPlace systems for RSNA, as described in the following documents:
 - *Planning Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/products_implementation_design_guides_list.html
 - *Installation, Upgrade, and Migration Guide for Cisco Unified MeetingPlace* at http://www.cisco.com/en/US/products/sw/ps5664/ps5669/prod_installation_guides_list.html
- Any 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.
- Single-URL access for Cisco Unified MeetingPlace Web Conferencing is currently not supported.
- 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, page 4](#)
- [Configuring the Remote Servers, page 4](#)
- [How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment, page 5](#)
- [How to Configure User Profiles for RSNA, page 8](#)

Enabling RSNA

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

Before You Begin

Read the following topics:

- [Prerequisites for RSNA, page 3](#)
- [Restrictions for RSNA, page 3](#)

Procedure

- Step 1** Log in to the Administration Center.
- Step 2** Select **System Configuration > Remote Server Configuration**.
- Step 3** Set the [Enable RSNA](#) field to Yes.
- Step 4** Select **Save**.
-

Related Topics

- [Field Reference: Remote Server Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#) module

What To Do Next

Proceed to the [“Configuring the Remote Servers”](#) section on page 4.

Configuring the Remote Servers

Complete this task on each RSNA system.

Before You Begin

Complete the [“Enabling RSNA”](#) section on page 4.

Procedure

- Step 1** Log in to the Administration Center.
- Step 2** Select **System Configuration > Remote Server Configuration**.
- Step 3** Select **Add New**, or select an existing entry.
- Step 4** Configure the fields on the [Add Server Configuration Page](#).
- Step 5** Select **Save**.
- Step 6** Repeat [Step 3](#) through [Step 5](#) to add a server entry for each remote RSNA system.
-

Related Topics

- [Field Reference: Add Server Configuration Page and Edit Server Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#) module
- [Field Reference: Remote Server Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#) module
- [RSNA Reserved Meeting Server, page 2](#)

What To Do Next

Proceed to the [“How to Configure Call Control for RSNA in a Cisco Unified Communications Manager Environment”](#) section on page 5.

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

Complete the following 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, page 5](#)
- [Configuring Cisco Unified Communications Manager: SIP Route Patterns to Remote RSNA Systems, page 7](#)

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

-
- Step 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.
 - Step 2** Log in with your Cisco Unified Communications Manager administrator username and password.
 - Step 3** Select **Device > Trunk**.
 - Step 4** Select **Add New**.

- Step 5** In the Trunk type field, select **SIP Trunk**.
- Step 6** Select **Next**.
- Step 7** Configure the fields described in [Table 1](#).

Table 1 Fields for Adding a SIP Trunk in Cisco Unified Communications Manager 6.1 or a Later Release

Field	Action
Device Name	Enter a unique identifier for this trunk, such as the name or IP address of the <i>remote</i> Cisco Unified MeetingPlace Application Server.
Device Pool AAR Group	The device pool must use a codec that is compatible with the conferencing gateway (or bridge). 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 <i>remote</i> 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. If you did not create a SIP trunk security profile, then select the default Non Secure SIP Trunk Profile .
DTMF Signaling Method	Select No Preference .

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



Tip For field descriptions, select **Help > This Page**.

- Step 9** Select **Save**.
- Step 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”](#) section on page 7.

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](#)” section on page 5.
- 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, then 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

-
- Step 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.
- Step 2** Log in with your Cisco Unified Communications Manager administrator username and password.
- Step 3** Select **Call Routing > SIP Route Pattern**.
- Step 4** Select **Add New**.
- Step 5** Configure the fields described in [Table 2](#).

Table 2 Fields for Adding a SIP Route Pattern in Cisco Unified Communications Manager 6.1 or a Later Release

Field	Action
Pattern Usage	Select IP Address Routing .
Pattern	Enter the IP address of the remote Application Server. 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 ” section on page 5.

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



Tip For field descriptions, select **Help > This Page**.

- Step 7** Select **Save**.

- Step 8** Select **OK** to any pop-up dialog box messages that you see.
- Step 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](#)” section on page 5 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](#)” section on page 8.

How to Configure User Profiles for RSNA

The following fields in each user profile must have the exact same values on both RSNA systems:

- [User ID](#)
- [User password](#)
- [Profile number](#)
- [Profile password](#)
- [Schedule home server](#)

This is typically accomplished by completing the following tasks:

	High-Level Task	Where to Find Instructions
Step 1	Configure the Schedule home server field through user groups.	Configuring the Schedule Home Server Field in User Groups or User Profiles, page 8
Step 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
Step 3	(Optional) Configure Directory Service on <i>one</i> 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
Step 4	If you configured Directory Service on one RSNA system, then configure external AXL authentication on the other (non–Directory Service) system.	Enabling External User Authentication on the Non–Directory Service RSNA System, page 9


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](#)” section on page 5 for each Cisco Unified Communications Manager node that is attached to a Cisco Unified MeetingPlace RSNA system.

Procedure

- Step 1** Log in to the Administration Center.
- Step 2** Select **User Configuration**.
- Step 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.
- Step 4** Select **Edit** or **Add New**, depending on whether you want to configure an existing or a new user group or user profile.
- Step 5** Configure the [Schedule home server](#) field to match the [Home Server number](#) remote server field.
- Step 6** Select **Save**.
- Step 7** Repeat this procedure for all user groups and (if necessary) user profiles.
-

Related Topics

- [Field Reference: Add User Profile Page and Edit User Profile Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#) module
- [How to Configure User Profiles for RSNA](#), page 8

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 log 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”](#) section on page 8.

Procedure

- Step 1** On the non–Directory Service system, log in to the Cisco Unified MeetingPlace Administration Center.
- Step 2** Select **User Configuration > Directory Service > Directory Service Configuration**.
- Step 3** Configure the following fields, using the exact same values that you entered on the Directory Service–configured system:
- [AXL username](#)
 - [AXL password](#)
 - [AXL confirm password](#)
 - [AXL URL](#)

- Step 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, then select **Cancel** and return to [Step 2](#).
 - If you think you accidentally modified *and saved* any of the other fields, then 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**.
- Step 5** Select **Save**.
-

Related Topics

- [Field Reference: Directory Service Configuration Page](#) in the [Administration Center Page References for Cisco Unified MeetingPlace](#) module
- [How to Configure User Profiles for RSNA, page 8](#)