



Cisco Meeting Server

Deployments with Third Party Call Control

January 02, 2019

Contents

Change History	3
1 Introduction	4
1.1 How to Use this Guide	4
1.1.1 Commands	6
1.1.2 Terminology	6
2 Configuring a SIP Trunk to an Avaya CM	7
2.1 Configuration Summary	7
2.2 Cisco Meeting Server Configuration	7
2.3 Avaya CM Configuration	8
3 Configuring a Polycom DMA for the Cisco Meeting Server	13
3.1 Setting up the External SIP Peer	13
3.2 Creating the Dial Rule	15
Cisco Legal Information	18
Cisco Trademark	19

Change History

Date	Change Summary
January 02, 2019	No change for version 2.5. Removed version from title.
July 24, 2018	No change for Cisco Meeting Server 2.4
May 8, 2017	No change.
December 20, 2016	No change.
August 03, 2016	Rebranded for Cisco Meeting Server 2.0

1 Introduction

The Cisco Meeting Server software can be hosted on specific servers based on Cisco Unified Computing Server (UCS) technology as well as on the Acano X-Series hardware, or on a specification-based VM server. Cisco Meeting Server is referred to as the Meeting Server throughout this document.

Note: The term Meeting Server in this document means either a Cisco Meeting Server 1000, an Acano X-Series Server or the software running on a virtual host.

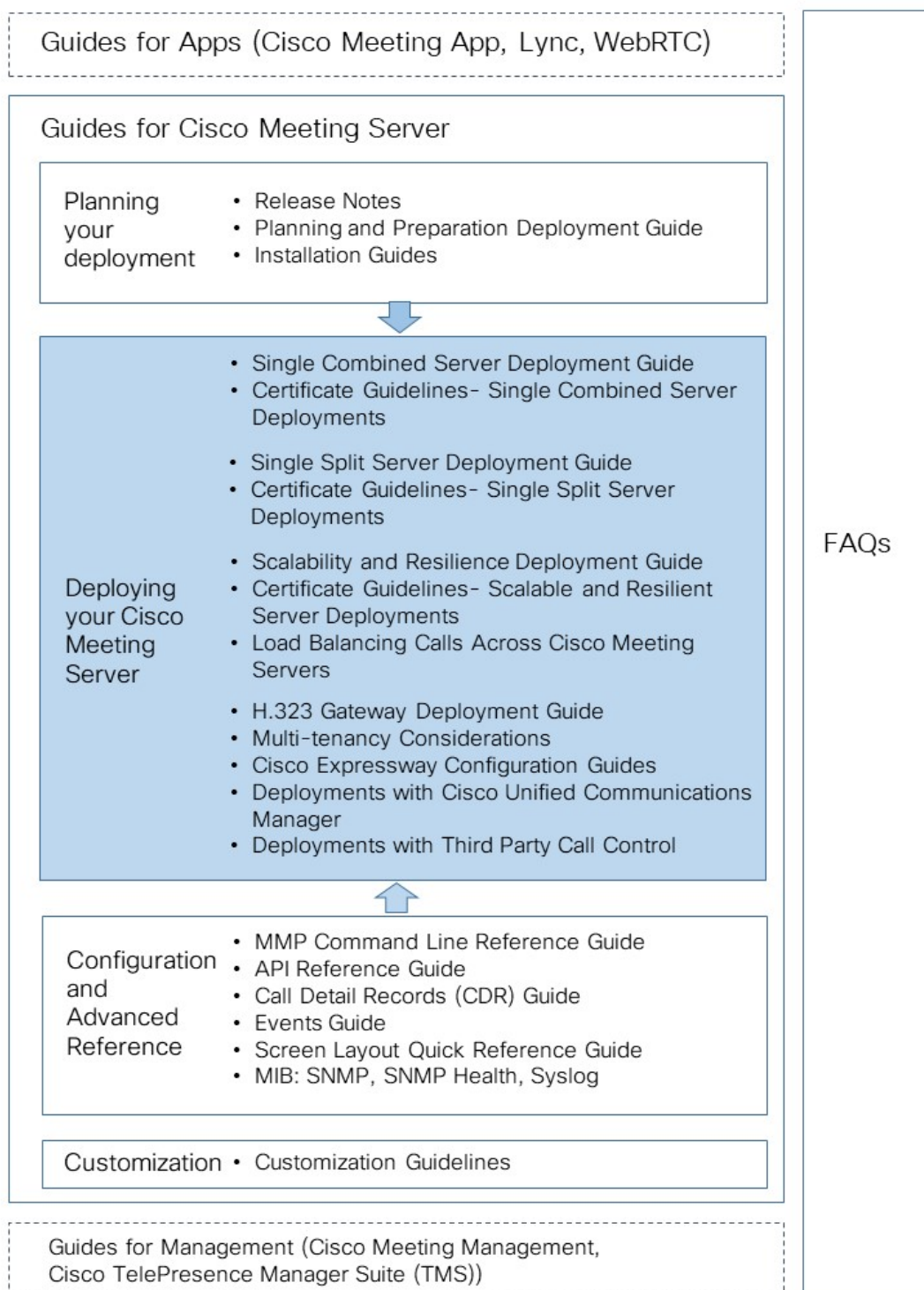
This document provides examples of how to configure the Meeting Server to work with third party call control devices from Avaya and Polycom. The examples may need to be adapted according to your specific deployment. These instructions apply equally to all Meeting Server deployment topologies (single server and scaled/resilient deployments).

A separate guide details how to deploy the Meeting Server with Cisco Unified Communications Manager, see [Cisco Meeting Server with Cisco Unified Communications Manager Deployment Guide](#).

1.1 How to Use this Guide

This guide is part of the documentation set (shown in Figure 1) for the Meeting Server.

Figure 1: Cisco Meeting Server documentation set



1.1.1 Commands

In this document, commands are shown in **black** and must be entered as given – replacing any parameters in <> brackets with your appropriate values. Examples are shown in **blue** and must be adapted to your deployment.

1.1.2 Terminology

Throughout this document the conferencing types mentioned are those as defined in Table 1.

Table 1: Conferencing Types

Conference type	Description
Rendezvous (also known as personal CMR)	Pre-defined, permanently available addresses that allow conferencing without previous scheduling. The host shares the address with other users, who can call in to that address at any time.
Ad hoc	Instant or escalated conferencing, for example manually escalated from a point-to-point call to a multiparty call with three or more participants.
Scheduled	Pre-booked conferences with a start and end time.

2 Configuring a SIP Trunk to an Avaya CM

This appendix provides an example of setting up a SIP trunk between the Cisco Meeting Server and the Avaya Communications Manager (Avaya CM) and may need to be adapted.

Note: If you are not your organization's Avaya CM administrator, then Cisco strongly advises you to seek the advice of your local administrator on the best way to implement the equivalent on your server's configuration.

Note: Avaya CM is an Avaya PBX, so calls will be audio only, however, the Cisco Meeting Server does not impose this restriction on interoperability with Avaya: therefore a call defined to be type 'avaya' in the Meeting Server does not imply that the call is audio-only.

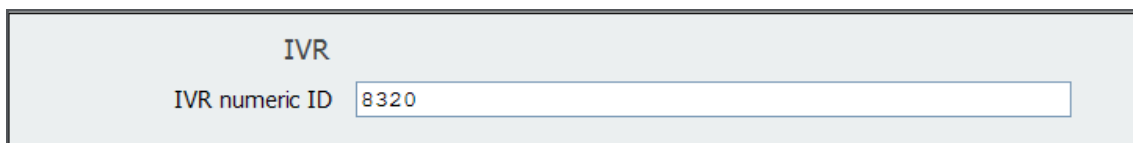
2.1 Configuration Summary

This example deployment assumes that:

- This audio connection between Avaya CM and the Meeting Server is accessed via dialing a prefix 49
- The assigned IVR digits for the Meeting Server are 8320; that is a user from the Avaya environment will dial 498320 to access the Meeting Server IVR
- A DID extension 5328 to route to this same number and allow for PSTN dial-in to the Meeting Server
- Avaya Software Version: CM6 R016x.00.1.510.1 Update: 19940

2.2 Cisco Meeting Server Configuration

1. Log in to the Web Admin Interface and go to **Configuration > General**.
2. For IVR Numeric ID, enter 8320.



The screenshot shows a configuration window titled "IVR". Inside the window, there is a label "IVR numeric ID" followed by a text input field containing the value "8320".

These digits will be passed from the Avaya CM to the Meeting Server, and then routed to the Meeting Server IVR.

3. Click **Submit**.
4. Go to **Configuration > Outbound Calls**.

5. Add a dial plan entry for the Avaya CM – see the example below.

The highlighted IP address below matches the C-LAN or Processor Ethernet address on the CM side and represents the CM interface used in the Signaling Group created later.

Outbound calls

Filter

	Domain	SIP proxy to use	Local contact domain	Trunk type	Behavior	Priority	Encryption	
<input type="checkbox"/>	lync.example.com	<none; call directly>	example.com	Standard SIP	Stop	2	Auto	[edit]
<input type="checkbox"/>	<match all domains>	10.1.1.77	example.com	Standard SIP	Stop	1	Auto	[edit]
<input type="checkbox"/>	avaya.example.com	192.168.20.103	example.com	Avaya	Stop	1	Auto	[edit]
<input type="text"/>	<input type="text"/>	<input type="text"/>	<input type="text"/>	Standard SIP ▼	Stop ▼	<input type="text" value="0"/>	Auto ▼	<input type="button" value="Add New"/> <input type="button" value="Reset"/>

6. Click **Add New**.

2.3 Avaya CM Configuration

1. Add a node name for the Meeting Server signaling interface.

		IP NODE NAMES
Name	IP Address	
Cisco	192.168.110.51	
App1-AAM	10.22.4.38	

2. Add an Avaya Signaling Group with the following:
 - Group Type = SIP
 - Near-end Node Name = C-LAN or Processor Ethernet interface indicated in the dial plan setting in the previous section
 - Far-end Node Name = Node name for the Meeting Server signaling interface created above.
 - Port settings for both Near-end and Far-end = 5060
 - Far-end Domain = SIP domain associated with the Meeting Server
 - Direct IP-IP Audio Connections = n. This ensures that all traffic from the Avaya CM comes from the Near-end Node

SIGNALING GROUP		
Group Number: 105	Group Type: sip	
IHS Enabled? n	Transport Method: tcp	
Q-SIP? n	SIP Enabled LSP? n	
IP Video? n	Enforce SIPS URI for SRTP? y	
Peer Detection Enabled? y	Peer Server: Others	
Near-end Node Name: clan-1a11	Far-end Node Name: Cisco	
Near-end Listen Port: 5060	Far-end Listen Port: 5060	
	Far-end Network Region: 1	
	Far-end Secondary Node Name:	
Far-end Domain: mycompany.com	Bypass If IP Threshold Exceeded? n	
Incoming Dialog Loopbacks: eliminate	RFC 3389 Comfort Noise? n	
DTMF over IP: rtp-payload	Direct IP-IP Audio Connections? n	
Session Establishment Timer(min): 3	IP Audio Hairpinning? y	
Enable Layer 3 Test? y	Alternate Route Timer(sec): 6	

3. Add an Avaya Trunk Group with the following:

- Group Type = SIP
- Direction = two way
- Service Type = tie
- Additional settings may vary, but see the examples below for possible configuration

TRUNK GROUP			
Group Number: 105	Group Type: sip	CDR Reports: y	
Group Name: Cisco	COR: 1	TN: 1	TAC: 175
Direction: two-way	Outgoing Display? n	Night Service:	
Dial Access? n	Auth Code? n		
Queue Length: 0	Member Assignment Method: auto		
Service Type: tie	Signaling Group: 105		
	Number of Members: 24		

Group Type: sip	
TRUNK PARAMETERS	Auto Page Line Retrieval? n
Unicode Name: auto	
Redirect On OPTIM Failure: 5000	
SCCAN? n	Digital Loss Group: 18
Preferred Minimum Session Refresh Interval(sec): 600	
Disconnect Supervision - In? y Out? y	
XOIP Treatment: auto	Delay Call Setup When Accessed Via IGAR? n

TRUNK FEATURES	
ACA Assignment? n	Measured: none
Maintenance Tests? y	
Numbering Format: public	
UUI Treatment: service-provider	
Replace Restricted Numbers? n	
Replace Unavailable Numbers? n	
Modify Tandem Calling Number: no	
Show ANSWERED BY on Display? y	
DSN Term? n	

PROTOCOL VARIATIONS

```

Mark Users as Phone? n
Prepend '+' to Calling Number? n
Send Transferring Party Information? n
Network Call Redirection? n
Send Diversion Header? n
Support Request History? y
Telephone Event Payload Type:

Overwrite Calling Identity? n
Convert 180 to 183 for Early Media? n
Always Use re-INVITE for Display Updates? n
Identity for Calling Party Display: P-Asserted-Identity
Enable Q-SIP? n

```

TRUNK GROUP

```

Administered Members (min/max): 1/24
Total Administered Members: 24

```

GROUP MEMBER ASSIGNMENTS

Port	Name
1: T00001	Cisco
2: T00002	Cisco
3: T00003	Cisco
4: T00004	Cisco
5: T00005	Cisco
6: T00006	Cisco
7: T00007	Cisco
8: T00008	Cisco
9: T00009	Cisco
10: T00010	Cisco
11: T00011	Cisco
12: T00012	Cisco
13: T00013	Cisco
14: T00014	Cisco
15: T00015	Cisco

4. Add an Avaya Route Pattern to routes calls to trunk group 105 and delete the first two digits (deletes the prefix digits 49).

Pattern Number: 105 Pattern Name: Cisco													
SCCAN? n Secure SIP? n													
Grp	FRL	NPA	Pfx	Hop	Toll	No.	Inserted	DCS/ IXC					
No			Mrk	Lmt	List	Del	Digits	QSIG					
								Intw					
1:	105	0					2	n	user				
2:								n	user				
3:								n	user				
4:								n	user				
5:								n	user				
6:								n	user				
BCC		VALUE		TSC	CA-TSC	ITC		BCIE	Service/Feature	PARM	No.	Numbering	LAR
0		1 2 M 4 W			Request						Dgts	Format	
											Subaddress		
1:	y	y	y	y	y	n	n		rest				none
2:	y	y	y	y	y	n	n		rest				none
3:	y	y	y	y	y	n	n		rest				none
4:	y	y	y	y	y	n	n		rest				none
5:	y	y	y	y	y	n	n		rest				none
6:	y	y	y	y	y	n	n		rest				none

5. Add a Uniform Dial Plan to provide a routing for a 6-digit number with a prefix of 49. These calls must be set to be routed to AAR tables in Avaya.

48	6	0	aar	n
49	6	0	aar	n
5004	4	4	5316	ext y

6. Add an AAR setting to routes all calls of 6 digits in length and beginning with 49 (i.e. 498320) to route pattern 105 (the Meeting Server Trunk Group).

Dialed String		Total		Route	Call	Node	ANI
		Min	Max	Pattern	Type	Num	Reqd
49		6	6	105	aar		n
5		7	7	999	aar		n

7. Assign an Extension and DID.

Optionally, in the Uniform Dial Plan you can add a setting for a DID extension (in this example, **x5328**) to route a call via digits **498320** to the Cisco Systems server.

3 Configuring a Polycom DMA for the Cisco Meeting Server

For calls from a Polycom DMA environment to the Cisco Meeting Server, create an External SIP Peer on the Polycom DMA that will point to the Meeting Server, and then configure a Dial Rule on the Polycom DMA that will direct calls to it.

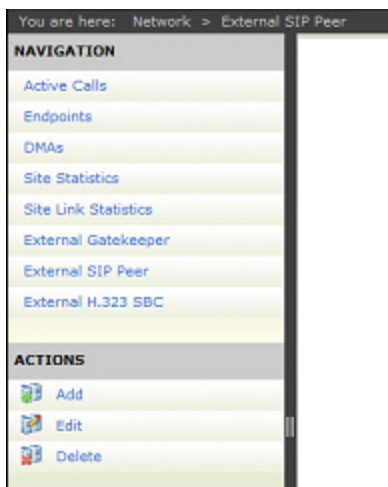
The following is an example of configuring the Meeting Server for the Polycom DMA, and may need to be adapted. Follow the instructions in the Deployment guides to set up a dial plan rule that points to the Polycom DMA server in the Web Admin Interface **Configuration > Outbound Calls** page. Also ensure that the correct ports are open (Incoming/Outgoing UDP 32768–65535 – RTP).

Note: If you are not your organization's Polycom server administrator, then Cisco strongly advises you to seek the advice of your local administrator on the best way to implement the equivalent on your server's configuration.

3.1 Setting up the External SIP Peer

On the Polycom DMA:

1. Go to **Network > External SIP Peer > Add**



2. In the External SIP Peer page configure the following:
 - Name: Cisco Systems
 - Description: a meaningful phrase, possibly Cisco Systems IP Peer
 - Next hop Address: IP Address of the Meeting Server Call Bridge

- Port: 5060
- User Route Header: selected
- Type: Other
- Transport Type: TCP

Edit External SIP Peer

- ☒ Enabled
- Name: Cisco Meeting Server1 *
- Description: CMS1 in UK colo
- Next hop address: 10.34.1.7 *
- Destination network:
- Port: 5060
- Use route header: ☒
- Prefix range:
- Strip prefix: ☐
- Type: Other ▼
- Transport type: TCP ▼
- Downgrade: ☐ Downgrade "sips:" to "sip:" if TLS is not supported by this sip peer.
- Register externally: ☐

3. Leave the Domain List page blank.

Edit External SIP Peer

- External SIP Peer
- Domain List**
- Postliminary
- Authentication
- External Registration

Add new domain:

Authorized domains (if there is no domain in the list, all domains are supported):

4. In the Postliminary page Header Options section configure the following:
 - a. Copy All Parameters: Checked
 - b. Format: Use original request's To
5. In the Postliminary page Request URI options section configure the following:
 - a. Format: Original user, configured peer's Destination Network or next hop address

Edit External SIP Peer

- External SIP Peer
- Domain List
- Postliminary
- Authentication
- External Registration

☒ Use output format:

To header options

☒ Copy all parameters of original "To" headers.

Format:

Template:

Request URI options

Format:

Template:

☐ Use customized script:

```

var otdisplay = getDisplayName(getHeader("To")); // return display name of the To header
var otscheme = getScheme(getHeader("To")); // return scheme of the To header
var otuser = getUser(getHeader("To")); // return user of the To header
var othost = getHost(getHeader("To")); // return host of the To header

var toHeader = "" + otdisplay + " <" + otscheme + ':' + otuser + '@' + othost + '>';
var paramString = getParameterString(getHeader("To"));
toHeader = appendParameterString(toHeader, paramString);
setHeader("To", toHeader); // change the To header

var pscheme = getPeerScheme(); // return scheme of the peer.
var pnetorphost = getPeerNetOrNextHop(); // return peer's destination network, or next hop.
var oruser = getUser(DIAL_STRING); // return user of the Request-URI.

```

[Debug this script](#)

6. In the Authentication page configure the following:
 - a. Authentication: Pass authentication
 - b. Proxy authentication: Pass Proxy authentication

Edit External SIP Peer

- External SIP Peer
- Domain List
- Postliminary
- Authentication
- External Registration

Authentication

☐ Handle authentication

☒ Pass authentication

Proxy authentication

☐ Handle proxy authentication

☒ Pass proxy authentication

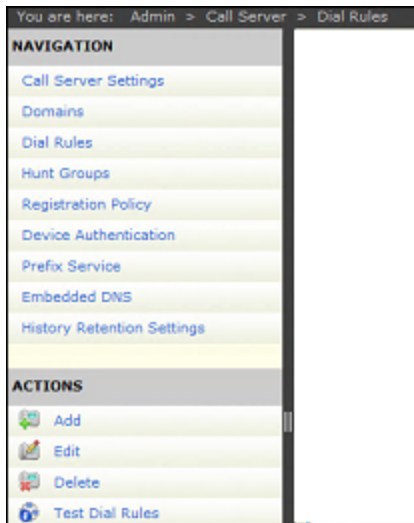
Realm	User Name

7. Click **Save**.

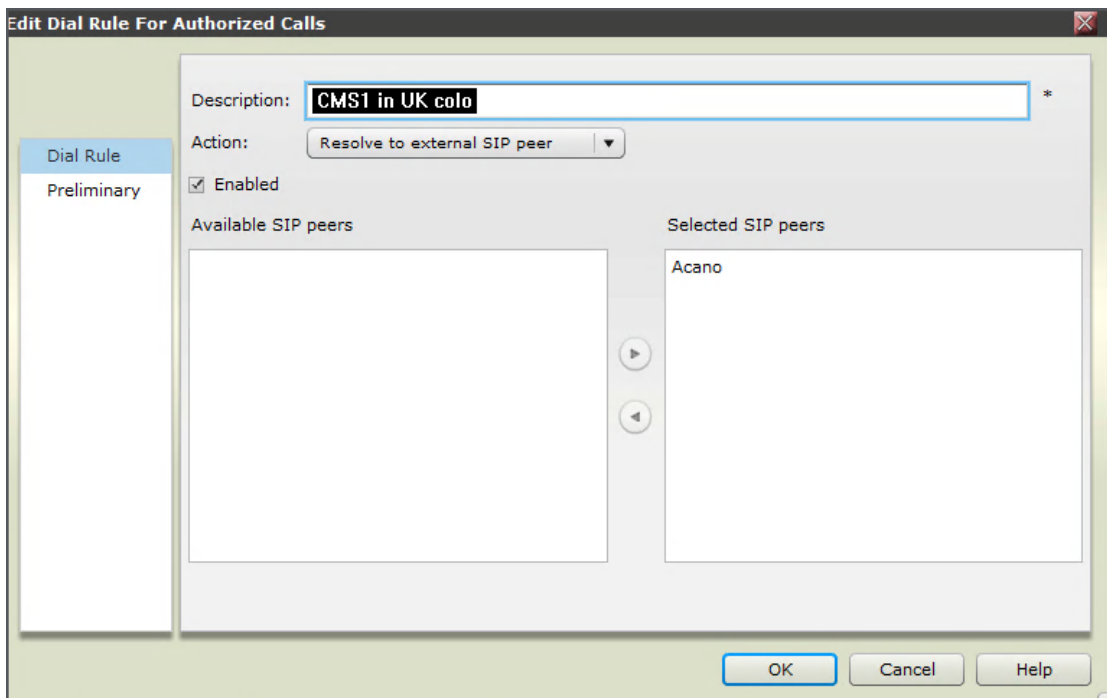
3.2 Creating the Dial Rule

In the Polycom DMA:

1. Go to **Admin > Call Server > Dial Rules > Add**.



2. In the Edit Dial Rule for Authorized Calls page, configure the following (see below):
 - a. Description: Cisco <Description of pattern>
3. Select **Enabled**.
4. Select the Cisco Systems SIP Peer in the left pane and click the arrow to move it to the Selected SIP Peers.

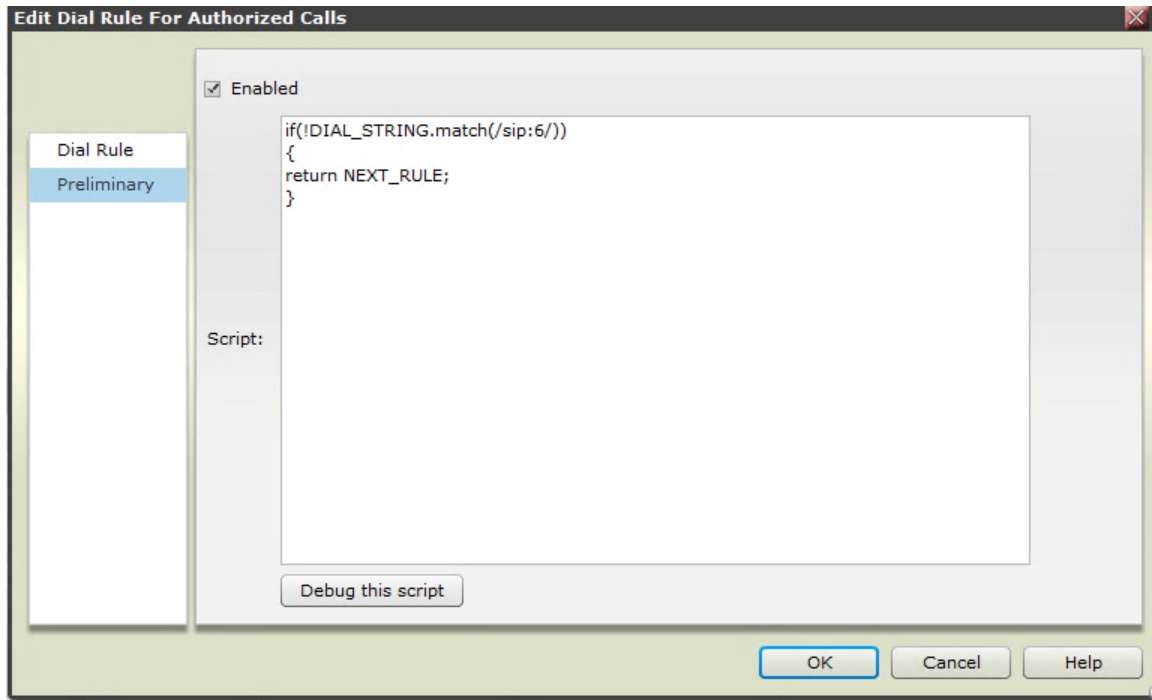


5. In the Preliminary page create a string to represent how calls will match this rule (see below).

Consult the DMA Admin Guide for more detail. The example below matches any call that begins with a 6 and sends it to the [[[Undefined variable BrandingTypeVariables.solution or server]]].

```
if(!DIAL_STRING.match(/sip:6/))  
{  
  return NEXT_RULE;  
}
```

6. Click OK.



You should now be able to dial from any SIP-enabled Polycom DMA endpoint to the Cisco Meeting Server using the rule created.

Cisco Legal Information

THE SPECIFICATIONS AND INFORMATION REGARDING THE PRODUCTS IN THIS MANUAL ARE SUBJECT TO CHANGE WITHOUT NOTICE. ALL STATEMENTS, INFORMATION, AND RECOMMENDATIONS IN THIS MANUAL ARE BELIEVED TO BE ACCURATE BUT ARE PRESENTED WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED. USERS MUST TAKE FULL RESPONSIBILITY FOR THEIR APPLICATION OF ANY PRODUCTS.

THE SOFTWARE LICENSE AND LIMITED WARRANTY FOR THE ACCOMPANYING PRODUCT ARE SET FORTH IN THE INFORMATION PACKET THAT SHIPPED WITH THE PRODUCT AND ARE INCORPORATED HEREIN BY THIS REFERENCE. IF YOU ARE UNABLE TO LOCATE THE SOFTWARE LICENSE OR LIMITED WARRANTY, CONTACT YOUR CISCO REPRESENTATIVE FOR A COPY.

The Cisco implementation of TCP header compression is an adaptation of a program developed by the University of California, Berkeley (UCB) as part of UCB's public domain version of the UNIX operating system. All rights reserved. Copyright © 1981, Regents of the University of California.

NOTWITHSTANDING ANY OTHER WARRANTY HEREIN, ALL DOCUMENT FILES AND SOFTWARE OF THESE SUPPLIERS ARE PROVIDED "AS IS" WITH ALL FAULTS. CISCO AND THE ABOVE-NAMED SUPPLIERS DISCLAIM ALL WARRANTIES, EXPRESSED OR IMPLIED, INCLUDING, WITHOUT LIMITATION, THOSE OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OR ARISING FROM A COURSE OF DEALING, USAGE, OR TRADE PRACTICE.

IN NO EVENT SHALL CISCO OR ITS SUPPLIERS BE LIABLE FOR ANY INDIRECT, SPECIAL, CONSEQUENTIAL, OR INCIDENTAL DAMAGES, INCLUDING, WITHOUT LIMITATION, LOST PROFITS OR LOSS OR DAMAGE TO DATA ARISING OUT OF THE USE OR INABILITY TO USE THIS MANUAL, EVEN IF CISCO OR ITS SUPPLIERS HAVE BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

Any Internet Protocol (IP) addresses and phone numbers used in this document are not intended to be actual addresses and phone numbers. Any examples, command display output, network topology diagrams, and other figures included in the document are shown for illustrative purposes only. Any use of actual IP addresses or phone numbers in illustrative content is unintentional and coincidental.

All printed copies and duplicate soft copies of this document are considered uncontrolled. See the current online version for the latest version.

Cisco has more than 200 offices worldwide. Addresses and phone numbers are listed on the Cisco website at www.cisco.com/go/offices.

© 2019 Cisco Systems, Inc. All rights reserved.

Cisco Trademark

Cisco and the Cisco logo are trademarks or registered trademarks of Cisco and/or its affiliates in the U.S. and other countries. To view a list of Cisco trademarks, go to this URL:

www.cisco.com/go/trademarks. Third-party trademarks mentioned are the property of their respective owners. The use of the word partner does not imply a partnership relationship between Cisco and any other company. (1721R)