MiVoice MX-ONE

SIP networking, General Configuration, Operational Directions

Release 7.2
September 24, 2019

Notice

The information contained in this document is believed to be accurate in all respects but is not warranted by **Mitel Networks™ Corporation (MITEL®)**. The information is subject to change without notice and should not be construed in any way as a commitment by Mitel or any of its affiliates or subsidiaries. Mitel and its affiliates and subsidiaries assume no responsibility for any errors or omissions in this document. Revisions of this document or new editions of it may be issued to incorporate such changes.No part of this document can be reproduced or transmitted in any form or by any means - electronic or mechanical - for any purpose without written permission from Mitel Networks Corporation.

Trademarks

The trademarks, service marks, logos and graphics (collectively “Trademarks”) appearing on Mitel's Internet sites or in its publications are registered and unregistered trademarks of Mitel Networks Corporation (MNC) or its subsidiaries (collectively "Mitel") or others. Use of the Trademarks is prohibited without the express consent from Mitel. Please contact our legal department at legal@mitel.com for additional information. For a list of the worldwide Mitel Networks Corporation registered trademarks, please refer to the website: http://www.mitel.com/trademarks.

163/154 31-ANF 901 14 Uen Uen PB1 2019-09-24

Contents

Chapter: 1 **GENERAL** **1**

Introduction 1

Glossary 1

Chapter: 2 **Prerequisites** **2**

Chapter: 3 **Aids** **3**

Chapter: 4 **References** **4**

Chapter: 5 **Procedure** **5**

Initiation 5

Removal 5

Chapter: 6 **Execution** **6**

Configuration of SIP-Related, General Data 6

Matching Order in SIP Invite, SIP Options, etc. 6

Considerations When Setting Up SIP Trunks 6

Using TRUNK_INFO 7

Using TRUNK_USER 7

Using CONTACT_DOMAIN 7

Using FROM_DOMAIN 7

Using REMOTE_IP 7

Using ALL 8

SIP Route 8

SIP Extension 8

Incoming SIP route Settings when WebRTC is Used in Client/Gateway . 8

Chapter: 7 **Termination** **9**

GENERAL

Introduction

The actual management of SIP routes and SIP extensions is described in the ROUTE DATA Operational Directions and in the IP EXTENSION Operational Directions, but this document provides some general considerations and prerequisites for the planning and configuration of the SIP resources.

The MX-ONE is using matching of data in the incoming SIP INVITEs (and other SIP messages) to determine how a SIP message should be handled.

If the information elements conflict, it is impossible to determine if the calls originate from a SIP extension or a SIP route. Care has to be taken when planning the network regarding server/domain names and handling of calls via boarder-gateways or

SIP-aware NAT gateways.

Glossary

For a complete list of abbreviations and glossary, see the description for ACRONYMS, ABBREVIATIONS AND GLOSSARY.

Prerequisites

SIP extensions and SIP trunks are used.

Aids

I/O terminal.

References

In these operational directions, references are made to the following documents:

Command Descriptions:	Route Data, RO (in the Technical Reference Guide, MML commands)
	sip_route and sip_domain (in the Technical Reference Guide, unix commands)
Operational Directions:	Route Data
	IP extension

Procedure

SIP configuration procedures are listed in this section.

Initiation

The following work flow must be followed when initiating a SIP route/extension:

1. Configuration of SIP-related, system- or domain-wide data
2. Initiation of the SIP route/extension.

Removal

The following work flow must be followed when removing a SIP route/extension:

1. Removal of a SIP route/extension.

Execution

SIP execution information is presented in this section.

Configuration of SIP-Related, General Data

The general SIP configuration details are discussed in this section.

Matching Order in SIP Invite, SIP Options, etc.

1. If a SIP INVITE is received, a check is done of the dialed number. If it matches a configured emergency number set in any configured route (-match EMERGENCY) the call will be accepted as an emergency call and will not be checked for passwords etc.
2. If the INVITE does not have an emergency number, tests are made on other parts of the request, each route is tested according to the setting for the trunk. Each trunk will test one of:
   a. Match any string in the header information (-match TRUNK_INFO).
   b. Match user part of the header information (-match TRUNK_USER).
3. Match host/domain part of the contact information (-match CONTACT_DO- MAIN).
4. Match host/domain part of the from information (-match FROM_DOMAIN). e: Matching the sender's IP address (-match REMOTE_IP).

Only one test type will be done per route, but the information to match may be a comma separated list.

The order the tests are made is determined by the -priority parameter, and secondly by the route number, starting with the lowest number.

If a match is found the call will continue as a trunk call.

5. If the test for route traffic failed, the system will test if the request is matching the MX-ONE domain of the PBX, or own LIM's address, set during installation, see the installation instructions INSTALLING AND CONFIGURING MIVOICE MX-ONE or (optionally) by the `sip_domain` command. If the "from domain" matches, the call will proceed as an extension call.
6. A route may be programmed to accept all calls, without other tests (-match ALL).

This (ALL) should only be used when testing, as it abandons all security, since the call will be admitted as trunk call.

Considerations When Setting Up SIP Trunks

Using different domain information is important, and planning the DNS and IP network structure is key to solving how to differentiate extensions from trunks and different trunks from each other.

Modification of SIP information in border-gateways might be a method to get the information needed when handling both trunks and extensions connected from public Internet, or VPN tunnels.

The sub-sections below refer to parameters in the `sip_route` command.

Using TRUNK_INFO

Normally this is used together with optional parameters like tgrp and trunk-context sent from the remote side.

This would also require that the from information sent from local side is configured correctly, as this is the basis for re-invite information from remote side.

Normally trunk-context is used to transfer TypeOfNumber information, by matching trunk-context to contextXX settings. Matching is normally used to identify the route to tgrp string.

Example:

-uristring0 "sip:?;tgrp=mitel;trunk-context=cana**da.mitel.com@ca.mitel.com"**

-uristring1 "sip:+?;tgrp=mitel;trunk-context=pub**lic.mitel.com@ca.mitel.com"**

-fromstring0 "sip:?;tgrp=mitel;trunk-context=sweden.mitel.com@se.mitel.com"

-fromstring1 "sip:+?;tgrp=mitel;trunk-context=public**.mitel.com@se.mitel.com"**

-accept TRUNK_INFO -match "tgrp=mitel"

-contexta0 "trunk-context=canada.mitel.com"

-contexta1 "trunk-context=public.mitel.com"

Using TRUNK_USER

This setting will match the user part of the INVITE header.

Used normally when the invite URI is sent to a common user, and the “to” field is used for the called number. (TrunkProfile:XXX:bNumberSource to_header)

Example:

-accept TRUNK_USER -match "+4681230000"

Using CONTACT_DOMAIN

This setting will match the information in the server part of the contact header. Be sure this information is unique, and only sent from the remote switch.

Example:

-accept CONTACT_DOMAIN -match "ca.mitel.com"

Using FROM_DOMAIN

This setting will match the information in the server part of the from header. Be sure this information is unique, and only sent from the remote switch.

Example:

-accept FROM_DOMAIN -match "ca.mitel.com"

Using REMOTE_IP

Matching remote IP address from sender requires that the sender is unique for this route.

If for instance the proxy/gateway is also used for externally connected extensions, there will be problems to as you will catch also those telephones as trunk users.

Example:

-accept REMOTE_IP -match "1.2.3.4"

Using ALL

This is purely intended for testing and should never be used in production. Example:

-accept ALL

SIP Route

See the Operational Directions ROUTE DATA, section on SIP route, and the command description for `sip_route`.

SIP Extension

See the Operational Directions IP EXTENSION.

Incoming SIP route Settings when WebRTC is Used in Client/Gateway

When setting up incoming SIP routes (or trunks) you may limit access to the routes (or trunk) by using incoming firewalls with TLS or tunneling. You can, and must for security reasons, set up rules for authentication on the trunk interface by using digest credentials (controlled by "401 Unauthorized" or "407 Proxy Authentication Required"). See Operational Directions Route Data for details.

Termination

Inform the system or IT department manager if any alteration is made.

If any system data have been changed, a data backup operation must be performed.