

Mitel TA7100

58014902 REV00

SECURING A MITEL UNIT

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>.

**Mitel TA7100 Securing a Mitel Unit
58014902 REV00 - May 2016**

®,™ Trademark of Mitel Networks Corporation
© Copyright 2016, Mitel Networks Corporation
All rights reserved

Management Interfaces	4
Associating the Network Interface to the System Management Services	4
Stopping Services - Web Interface	4
Securing SNMP Interface	4
Forcing the Use of HTTPS	5
SIP	6
Configuring the Local Firewall	6
Enabling TLS Transport	6
Setting the RTP Mode - Secure	7
Configuration Files	8
Disabling DHCP Download	8
Configuring a Privacy Key	8
Disabling Partial Reset - ResetButtonManagement	9
Requirements	10
CLI	10
Additional considerations	10

Management Interfaces

Associating the Network Interface to the System Management Services

Steps

1. Go to Management > Misc.
2. From the Network Interface selection list, select the Network Interface you wish to bound to the system management services to.
3. Click Apply.

Result: The user will access the System Management through the selected Network Interface.

Stopping Services - Web Interface

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to System > Services.
2. In the User Service table, click  next to the service you want to disable.
3. Click Apply.

Securing SNMP Interface

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > SNMP.
2. In the SNMP Configuration table, set the following parameters:
 - a. Set Enable SNMP V1 to Disable.
 - b. Set Enable SNMP V2 to Disable.
 - c. Set Privacy Protocol.

- d. In the Privacy Password field, enter a password of your choosing.
3. Click Apply.

Result:

SNMP Configuration	
General Configuration	
SNMP Port:	<input type="text" value="161"/>
SNMP Protocol	
Enable SNMP V1:	<input type="button" value="Disable"/> ▾
Enable SNMP V2:	<input type="button" value="Disable"/> ▾
Enable SNMP V3:	<input type="button" value="Enable"/> ▾
Authentication Protocol:	<input type="button" value="MD5"/> ▾
Privacy Protocol:	<input type="button" value="DES"/> ▾
Privacy Password:	<input type="password" value="*****"/>
Community:	<input type="text" value="public"/>
SNMP Trap	
Enable SNMP Trap:	<input type="button" value="Disable"/> ▾
Trap Destination(s):	<input type="text" value="192.168.10.10:162"/>

Forcing the Use of HTTPS

Steps

1. Open CLI (Command Line Interface).
2. Set Web.HttpMode to Secure.

Result: The unit will now be forced to use HTTPS.

SIP

Configuring the Local Firewall

Prerequisite If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name. You must have a Network Interface created.

Steps

1. Go to Network > Local Firewall.
2. In the Local Firewall Configuration table, complete the fields as required.
3. In the Local Firewall Configuration table, from the Default Policy selection list, select Drop.

NOTE: Before setting the Default Policy to Drop, review your rules to make sure that at least one rule accepts incoming packets, otherwise the communication with the Mitel unit will be lost.

4. Click **Submit**.
5. Click Submit and Apply to apply all changes to the configuration.
6. Click **Restart required services**, located at the top of the page.

Result: The Local Firewall will drop packets instead of rejecting the calls with a SIP message.

Enabling TLS Transport

Prerequisite A TLS certificate must be installed on the Mitel unit.

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to SIP > Transport.
2. In the Protocol Configuration table, set TLS to Enable.
3. Click Apply.

Result:

Protocol Configuration					
UDP	UDP QValue	TCP	TCP QValue	TLS	TLS QValue
Enable ▾	<input type="text"/>	Disable ▾	<input type="text"/>	Enable ▾	<input type="text"/>

Setting the RTP Mode - Secure

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Media > Security.
2. Select the endpoint you want to configure with the help of the dropdown menu Select Endpoint.
3. Under the RTP section, set Mode to Secure.
4. Set the other parameters based on your desired configuration.
5. Click Apply.

Result:

[Show Help](#) | [Log Out](#)

[System](#)
[Network](#)
[SBC](#)
[ISDN](#)
[POTS](#)
[SIP](#)
[Media](#)
[Telephony](#)
[Call Router](#)
[Management](#)
[Reboot](#)

[Codecs](#)
[Security](#)
[RTP Statistics](#)
[Misc](#)

➤ Security

Select Endpoint: ▼

Security	
RTP	
Mode:	<input type="text" value="Secure with fallback"/> ▼
Key Management Protocol:	<input type="text" value="Encryption type to be used with SRTP"/> ▼
Encryption:	<input type="text" value="Key Management Protocol for SRTP"/> ▼
T.38	
Allow unsecure T.38 with secure RTP:	<input type="text" value="Yes"/> ▼

Configuration Files

Disabling DHCP Download

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Configuration Scripts.
2. In the Automatic Script Execution table, set Allow DHCP to Trigger Scripts Execution to Disable.
3. Click Apply.

Result: Ensures that no one can send a new configuration file to the unit if the DHCP server is compromised.

Automatic Script Execution	
Execute On Startup:	Disable ▼
Execute Periodically:	Disable ▼
Time Unit:	Hours ▼
Period:	1
Time Range:	
Allow DHCP to Trigger Scripts Execution:	Disable ▼

Configuring a Privacy Key

If you are not familiar with the meaning of the fields, click Show Help, located at the upper right corner of the Web page, to display field description when mousing over the field name.

Steps

1. Go to Management > Configuration Scripts.
2. In the Execute Scripts table, set a privacy key of your choosing in the Privacy Key field.

Result: The unit will only accept scripts that have been encrypted with this privacy key. The privacy key also ensures that the files are encrypted when using unsecure transfer mode (HTTP,TFTP,FTP).

Disabling Partial Reset - ResetButtonManagement

Steps

1. Open CLI (Command Line Interface).
2. Set ResetButtonManagement to DisablePartialReset.

Result: The Mitel unit will no longer partially reset the unit.

Requirements

CLI

Make sure the Telnet access is disabled. You can look at the `Cli.EnableTelnet` variable to verify if Telnet connections are allowed. The access is disabled by default.

Additional considerations

- In the initial configuration of the unit, review the users and change their passwords and access rights according to your security policy.
- On FXS devices, the Vocal Unit Information allows a caller on an FXS port to dial codes to get information on the unit like the IP addresses and the MAC address. It is recommended to turn this feature off to prevent attackers from gaining information on the Mitel unit setup.

