# VoIP Security

OPERATIONAL DIRECTIONS

Mitel®

**NOTICE**

The information contained in this document is believed to be accurate in all respects but is not warranted by Mitel Networks™ Corporation (MITEL®). Mitel makes no warranty of any kind with regards to this material, including, but not limited to, the implied warranties of merchantability and fitness for a particular purpose. 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.

# 1 GENERAL

By default Voice over IP (VoIP) security is disabled.

VoIP signaling between IP terminals and the SIP proxy or the H.323 Gatekeeper (the MX-ONE Service Node can be protected by the Transport Layer Secure (TLS) cryptographic protocol. TLS provides a safe way to interchange the cipher keys needed in the later Secure Real-time Transport Protocol (SRTP) during media negotiation. TLS is valid for both H.323 and SIP extensions.

Media encryption for IP extensions, inter media gateway connections, H.323, or SIP routes can be enabled or disabled, independently of each other, in the MX-ONE Service Node.

The Security Policy determines how IP entities in the system are allowed to register in the system. If security exceptions are allowed certain directory numbers or terminal types can be allowed to be used although they do not support TLS or SRTP.

All generic extensions must be treated equally.

The Regional Authorization Code (RAC) is used as PIN code for the extensions. See the description for *AUTHORIZATION CODE FOR EXTENSION*, about Individual Authorization Code.

**Note:** VoIP Security can also be configured with the MX-ONE Service Node Manager.

# 2 GLOSSARY

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

Here is a list over some common terms in VoIP security:

**Security Exception**
A property by which IP extensions without signaling or media encryption can exist in the system.

**Secure Extension**
An extension number that supports encryption. Set by the command *extension --security-exception* with either the *--initiate (-i)* or *--change (-c)* switch.

For an ALL_SECURE system the *--security-exception* parameter should be set to NO.

For example, *extension -c -d 12345 --security-exception no*

When a security exception is allowed the --security-exception parameter should be YES.

For example, *extension -i -d 12345 --csp 1 --lim 1 --security-exception yes*

**Note:** A RAC is mandatory when *--security-exception* is no.

**Secure Terminal**
Terminals that support both TLS and SRTP, that is, both signaling and media encryption.

For H.323 DBC42x02 and DBC 44601 (D4 and D5 phones) are secure terminals.

For SIP DBC42x02 (D4 phones) and Mitel 6900/6800/6700i are secure terminals.

**Insecure Extension**
An extension number with a security exception.

Security exceptions can be set per extension number by the command *extension -d --security-exception*.

For example, *extension -c -d 12345 --security-exception yes*

A PIN code (RAC) is optional, and the directory number 12345 will have no security.

The command will succeed only when allowed by the system security policy.

**Insecure Terminal**
All third party H.323/SIP telephones and soft clients, as well as DBC422 01 and DBC425 01 telephones. Whether they can register or not depends on the security policy set in the system.

# 3 PREREQUISITES

A VoIP Security license, called *VOIP-SECURITY,* is needed. For information, see the operational directions for *ADMINISTRATOR USER'S GUIDE*, chapter License Handling.

A valid security certificate, signed by an authorized Certificate Authority, is needed. For information, see the operational directions for *CERTIFICATE MANAGEMENT*.

# 4 TOOLS

-

# 5 PROCEDURE

## 5.1 ENABLE SECURITY WITH A VALID VOIP SECURITY LICENSE

### 5.1.1 ACTIONS ON THE MIVOICE MX-ONE SERVICE NODE

**Enable SRTP**

1. Enable SRTP for extensions. Use the command

   *media_encryption_enable -type extension*
2. Enable SRTP for routes (tielines or trunks). Use the command

   *media_encryption_enable -type route*
3. Enable SRTP for inter media gateways connections. Use the command

   *media_encryption_enable -type intermgw*
4. Make a data backup to store these settings. Use the command

   *data_backup*.

**Enable TLS for Terminals, SIP trunks and H.323 trunks**

5. Install certificates. See the operational directions for *CERTIFICATE MANAGEMENT*.

### 5.1.2 ACTIONS ON THE TERMINALS

**Enable TLS and SRTP on D4 and D5 Terminals**

6. Enable security for SIP and H.323 terminals. On D4 or D5 terminals, the following parameter shall be set in the configuration file. For information, see the description for *CONFIGURATION FILE FOR DBC 42X* and see the description for *CONFIGURATION FILE FOR DBC 44X*. (For the D42X (D4) terminals the configuration file is d42x02-config.txt and for the D44X (D5) terminals it is d44x01-config.txt.

   SECURITY = enabled
7. For IP terminals that are registered to the PBX re-boot these to make them reread the updated configuration file. This can be done in MX-ONE Service Node

Manager or with the command *extension_unregistration*. For more information, see the description for *CONFIGURATION FILE FOR DBC 42X* and see the description for *CONFIGURATION FILE FOR DBC 44X*in the chapter Changing an existing configuration file.

8. Verify that the extension has logged on to a secure port. See 6.5 Check Signaling Security on page 12.

### 5.1.3 ACTIONS FOR TLS OVER H.323 TRUNK

Enable security for H.323 trunk by specifying appropriate value for the TLS parameter in the *RIANI/RIANC* command for the route. Please see command and parameter descriptions for IP Networking for details.

## 5.2 CHANGE SECURITY POLICY

When the security policy is to be changed in an existing system the following procedure is valid:

1. If the new security policy will be All Secure or All Secure with Exception Type, set *--security-exception no* for all extensions with the *extension* command.
2. Set the new security policy.
3. Unregister all terminals (by *extension_unregistration*). When the IP extensions then register they will get the new security policy activated.

For details, see 6.3 Change Security Policy on page 10.

# 6 EXECUTION

## 6.1 INSTALL CERTIFICATE

Install the security certificate for the system. See the command description for *CERTIFICATE MANAGEMENT*.

## 6.2 SECURITY POLICY MANAGEMENT

The security policy is set per system with the *sec_policy* command. The security policy will affect the entire system. Changing the policy will not affect the extensions which are already logged on. For the new policy to be effective the extension must be re-registered.

In case no security policy is set, all types of terminals can register.

### 6.2.1 NO SECURITY POLICY

When a system security policy has not been set, the system is open for all types of initiations and registrations. To remove a security policy, use the command *sec_policy -remove*.

The parameter effects of the command *extension --security-exception* can be summarized, see Table below for details.

**Table 1 No Security**

| Terminal Type | Extension Number Type | Logon Authentication [1)] | Registration Allowed or Not Allowed | Secure or Insecure Registration |
|---|---|---|---|---|
| Secure | security-exception YES,<br>RAC not configured | Authentication not done | Allowed | Signaling is not encrypted. |
| Secure | security-exception YES,<br>RAC configured | Prompts for PIN and validates it | Allowed | Signaling is encrypted. |
| Secure | security-exception NO,<br>RAC configured | Prompts for PIN and validates it | Allowed | Signaling is encrypted. |
| Insecure | security-exception YES,<br>RAC configured | Prompts for PIN and validates it | Allowed | Signaling is not encrypted. |
| Insecure | security-exception YES,<br>RAC not configured | Authentication not done | Allowed | Signaling is not encrypted. |
| Insecure | security-exception NO,<br>RAC configured | Prompts for PIN and validates it | Allowed | Signaling is not encrypted. |

1) If RAC is configured, logon authentication is done irrespective of if security-exception = YES or NO. That is, the IP terminal prompts for a PIN and validates it while registration takes place.

### 6.2.2 ALL SECURE

Example of how to proceed:

Set the system security policy to ALL_SECURE. Use the command *sec_policy -set 1*

The *security-exception* parameter must explicitly be given with NO for the *extension* command to be accepted.

| | |
|---|---|
| RAC configured<br>*extension -c -d 12345 --security-exception no* | Accepted. |

*extension* will be rejected if stated with a security exception. It will also be rejected if it is given with no exception, but with a blank PIN code.

| | |
|---|---|
| *extension -c -d 12345 security-exception yes* | Rejected. Security exception is not allowed. |
| RAC not configured<br>*extension -c -d 12345 security-exception yes* | Rejected. Security exception is not allowed. |
| RAC not configured<br>*extension -c -d 12345 security-exception no* | Rejected. The PIN code may not be blank. |
| Activate the selected security policy:<br>*extension_unregistration -d 12345* | Unregister, and then re-register the IP-terminal. |

See table below for a summary.

**Table 2 All Secure**

| Terminal Type | Extension Number Type | Registration Allowed or Not Allowed | Secure or Insecure Registration |
|---|---|---|---|
| Secure | security-exception YES, RAC not configured | Not allowed | Not registered. |
| Secure | security-exception YES, RAC configured | Not allowed | Not registered. |
| Secure | security-exception NO, RAC configured | Allowed | Signaling is encrypted. |
| Insecure | security-exception YES or NO, RAC configured or not | Not allowed | Not registered |

**Note:** This statement will be printed if there is any insecure extension in the system while executing the *sec-policy -set 1.*

Example:*sec_policy -set 1*

NOT EXECUTED

DIRECTORY NUMBERS WITH SECURITY EXCEPTION EXIST

### 6.2.3 ALL SECURE WITH EXTENSION EXCEPTION

Example of how to proceed:

Set the system security policy to ALL_SECURE + EXC_EXT. Use the command *sec_policy* -set 2

The following commands will all be accepted (where the mandatory parameters --csp and --lim have been excluded for clarity):

| | |
|---|---|
| *extension -i -d 12345 --security-exception yes* | Accepted. |
| RAC not configured<br>*extension -i -d 12345 --security-exception yes* | Accepted. |

| | |
|---|---|
| RAC configured<br>*extension -i -d 12345 --security-exception yes* | Accepted. |
| *extension -i -d 12345 --security-exception no* | Accepted. |
| RAC not configured<br>*extension -i -d 12345 --security-exception n*o | Accepted. |
| Activate the selected security policy:<br>*extension_unregistration -d 12345* | Unregister, and then re-register the IP-terminal. |

Table below gives a summary.

**Table 3 All Secure with Extension Exception**

| Terminal Type | Extension Number Type | Registration Allowed or Not Allowed | Secure or Insecure Registration |
|---|---|---|---|
| Secure | security-exception YES,<br>RAC not configured | Allowed | Signaling is not encrypted. |
| Secure | security-exception YES, RAC configured | Allowed | Signaling is encrypted. |
| Secure | security-exception NO, RAC configured | Allowed | Signaling is encrypted. |
| Insecure | security-exception YES, RAC configured or not configured | Allowed | Signaling is not encrypted. |
| Insecure | security-exception NO, RAC configured | Not allowed | Not registered |

If an extension number with no security exception tries to logon insecurely the registration will fail.

### 6.2.4 ALL SECURE WITH EXCEPTION TYPE

Example of how to proceed:

Set the system security policy to ALL_SECURE + EXC_TYPE.

Use the command *sec_policy* -set 3

The following commands will all be accepted (where the mandatory parameters --csp and --lim have been excluded):

| | |
|---|---|
| *extension -i -d 12345 --security-exception no*<br>RAC configured | Accepted. |
| *extension -i -d 12345 --security-exception no* | Accepted. |

The following commands will be rejected:

| | |
|---|---|
| *extension -i -d 12345 --security-exception yes*<br>RAC not configured | Rejected. |
| *extension -i -d 12345 --security-exception yes* | Rejected. |
| *extension -i -d 12345 --security-exception yes* | Rejected. |
| *extension -i -d 12345 --security-exception no* | Rejected. RAC is mandatory if security-exception = no. |
| Activate the selected security policy:<br>*extension_unregistration -d 12345* | Unregister, and then re-register the IP-terminal. |

Table below gives a summary.

**Table 4 All Secure with Exception Type**

| Terminal Type | Extension Number Type | Registration Allowed or Not Allowed | Secure or Insecure Registration |
|---|---|---|---|
| Secure | security-exception YES,<br>RAC not configured | Not allowed | Not registered |
| Secure | security-exception YES,<br>RAC configured | Not allowed | Not registered |
| Secure | security-exception NO,<br>RAC configured | Allowed | Signaling is encrypted. |
| Insecure | security-exception NO,<br>RAC configured | Allowed | Signaling is not encrypted. |

If a DBC 42x02 or DBC 44601 that has no security exception try to logon insecurely the registration will fail.

**Note:** When using SIP extensions, this policy will have the same behavior as the policy All Secure, see 6.2.2 All Secure on page 8.

## 6.3 CHANGE SECURITY POLICY

When the security policy is to be changed in an existing system the following procedure is valid:

1. If the new security policy is All Secure or All Secure with Exception Type, check that all extensions have the right security exemption parameter value. Print with

*extension -p* and check that *security-exception is NO*. Change the value if there are extensions that have *security-exception* = *YES*.

2. Set the new security policy.
3. Unregister all terminals (by *extension_unregistration*). When the telephones then register they will get the new security policy activated.

## 6.4 MEDIA ENCRYPTION

### 6.4.1 IP EXTENSIONS

#### *6.4.1.1 Enable Media Encryption*

Media encryption is disabled by default. If the VoIP Security license is enabled, use the command *media_encryption_enable -type extension* to enable SRTP encryption in the MX-ONE Service Node for IP extensions.

For H.323 extensions, this setting only affect calls that are routed through a gateway. For non-gateway H.323 calls (H.323 to H.323), the SRTP support instead depends on the configuration file settings of the extensions.

For SIP extensions, this setting affect both gateway and non-gateway calls.

#### *6.4.1.2 Disable Media Encryption*

Use the command *media_encryption_disable -type extension* to disable SRTP encryption in the MX-ONE Service Node for IP extensions.

For H.323 extensions, this setting only affect calls that are routed through a gateway. For non-gateway H.323 calls (H.323 to H.323), the SRTP support instead depends on the configuration file settings of the extensions.

For SIP extensions, this setting affect both gateway and non-gateway calls.

**Note:** The command will only be successful when there is no security policy. For any other security policy the command will fail.

#### *6.4.1.3 Print Media Encryption settings*

Use the command *media_encryption_print -type extension* to print the SRTP status in the MX-ONE Service Node for IP extensions.

### 6.4.2 IP ROUTES

Media encryption is disabled by default.

#### *6.4.2.1 Enable Media Encryption*

Use the command *media_encryption_enable -type route* to enable SRTP encryption in the MX-ONE Service Node for IP routes. This action only affect the Gateway calls made from or to IP routes.

For non-Gateway calls the command has no effect. For non-Gateway calls the SRTP support depends on the SRTP support of the endpoints.

#### 6.4.2.2 *Disable Media Encryption*

Use the command *media_encryption_disable -type route* to disable SRTP encryption in the MX-ONE Service Node for IP routes. This will only affect the gateway calls made from or to IP routes.

For non-Gateway calls the command has no effect. For non-Gateway calls the SRTP support depends on the SRTP support of the endpoints.

#### 6.4.2.3 *Print Media Encryption settings*

Use the command *media_encryption_print -type route* to print the SRTP status in the MX-ONE Service Node for IP routes.

### 6.4.3 INTER MEDIA GATEWAY CONNECTIONS

Media encryption is disabled by default.

#### 6.4.3.1 *Enable Media Encryption*

Use the command *media_encryption_enable -type intermgw* to enable SRTP encryption in inter media gateway connections.

#### 6.4.3.2 *Disable Media Encryption*

Use the command *media_encryption_disable -type intermgw* to disable SRTP encryption in inter media gateway connections.

#### 6.4.3.3 *Print Media Encryption settings*

Use the command *media_encryption_print -type intermgw* to print the SRTP status inter media gateway connections.

## 6.5 CHECK SIGNALING SECURITY

Verify that TLS is working in the system. Use the command *ip_extension -p*. Check that the secure H.323 terminals are registered on the secure port 3727, instead of the insecure port 1719. For SIP the secure port is 5061 and the insecure port is 5060.