

# Authorization Code for Extension

OPERATIONAL DIRECTIONS



## 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.

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](mailto: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>.

© Copyright 2018, Mitel Networks Corporation

All rights reserved

## 1

## GENERAL

Authorization codes can be initiated in the system to temporarily increase the Trunk Call Discrimination (TCD) category at a specific extension, that is, by using an authorization code a user can get other access possibilities for public calls.

A Call Information Logging (CIL) code, associated to every authorization code, is used to identify the calling party for call information logging.

To each authorization code a customer number can be affiliated. Then an AS parameter decides whether it is the customer number of the extension or of the authorization code that will be used to route outgoing traffic.

To an authorization code a common category code and a common service profile are affiliated and used to give the calling party another, higher category or service profile when a valid authorization code has been dialed.

The procedure with an authorization code will give category or service profile increase during one call.

An authorization code can be of the following two different functionality groups:

- **Common authorization code**

A common authorization code is shared by all extensions in the system.

A common authorization code can use both a common category code and a common service profile at the same time. Hereby all types of telephones, whether analogue, digital, or generic, can be given similar limitations.

If the authorization code is used for unlocking an extension, the category code or service profile given, when initiating the extension, will be used until the extension is locked again.

The common authorization code cannot be changed by a user.

An extension can be forbidden to use a common authorization code.

- **Individual authorization code**

An individual authorization code, previously also called Regional Authorization Code (RAC), is always affiliated to a directory number in the system.

An individual authorization code can use both a common category code or a common service profile.

The individual authorization code can be used for dialing from an own or another extension and to lock or unlock a telephone. The categories or service profiles are used for individual authorization codes as they are used for common authorization codes.

The individual authorization code can be locked to an extension. If an individual authorization code is locked to an extension, it cannot be used for pre-dialing from other extensions.

The individual authorization code can be changed by a user.

The individual authorization code can be hashed, or in clear-text. This is configured by the administrator.

A common service profile can only be used with a generic extension and a common category code can only be used with a normal extension.

**Note:** Authorization Code for Extension can also be configured with MX-ONE Service Node Manager.

## 2 TOOLS

I/O terminal.

## 3 REFERENCES

In these operational directions reference is made to the following documents:

**Operational directions:**

Administrator User's Guide

**Command descriptions:**

Technical Reference Guide, unix commands:

auth\_code

Generic extension (profile)

Technical Reference Guide, MML commands:

Application System Parameters, AS

Analog extension, EX

Digital key system telephone, KS

## 4 PROCEDURE

1. Define the AS parameter (*PARNUM=179*) that sets the minimum number of digits in an authorization code, when changed by the user using service code procedure.
2. Define the AS parameter (*PARNUM=180*) that determines the type of authorization code that shall be used for the function keys on the DTS.
3. Initiate necessary authorization code data.
4. If relevant, initiate encryption of the individual authorization code data (using the command `auth_code --encrypt`).

## 5 EXECUTION

### 5.1 INITIATE THE COMMON CATEGORY CODE

#### General

The category code (-cat), used in *auth\_code*, refers to the common category, CAT, specified in *EXCCS*. All common category codes are set with the *EXCCS* command, where the TCD category is set in the parameter *TRAF*.

The following common category codes are used in conjunction with an authorization code:

- A minimum category code, used from locked extensions.
- The normal category code, used in most cases.

With the optional parameter *CATTYP* in *EXCCS*, it is decided whether the category code should be minimum, or normal. Since *CATTYP* is optional, it might not be set at all. If a minimum category is needed during the procedure, an extra category will be used instead. This extra category will set all parameters affiliated to the common category to zero.

#### Procedure

Key the command *EXCCS*, with parameter *CATTYP* if the minimum category code is to be initiated.

Use the command *auth\_code*.

Use the command *auth\_code* to verify that the function is initiated.

A normal category code is affiliated to the extensions when they are initiated with command *EXTEI* or *KSEXI* for analog or digital extensions, respectively.

### 5.2 INITIATE THE COMMON SERVICE PROFILE

#### General

The common service profile, CSP, used in *auth\_code*, is specified in the command *extension\_profile -i --csp*. All common service profiles are set with the *extension\_profile -i* command, where the TCD category is set in the parameter *--ext-traf*.

The common service profile used in conjunction with an authorization code is in most cases the normal service profile.

With the parameter *--csp* in *extension\_profile -i*, it is decided whether the service profile should be normal. To initiate the default common service profile, use CSP (0).

**NOTE:** The default common service profile (CSP 0) must be initiated with category allowing use of Common Authorization Code.

#### Procedure

Use the command *extension\_profile -i*, with CSP=0 (*--csp 0*), if a default common service profile is to be initiated.

Use the command *auth\_code -i*.

Use the command *auth\_code -p* to verify that the function is initiated.

## 5.3 INITIATE THE COMMON AUTHORIZATION CODE

### General

The category code (CAT), used in *auth\_code*, refers to the common category specified in *EXCCS*. The common service profile (CSP), also used in *auth\_code*, refers to the common service profile specified in command *extension\_profile -i*, used for generic extensions. A common authorization code can be affiliated to both a CAT and a CSP.

### Procedure

Key the command *EXCCS*, with a common category code, specified higher than the normal category . For generic extension, key the command *extension\_profile -i*, with a common service profile, specified higher than the normal service profile .

Use the command *auth\_code -i*.

Use the command *auth\_code -p* to verify that the function is initiated.

## 5.4 REMOVE THE COMMON AUTHORIZATION CODE

Use the command *auth\_code -e*.

Use the command *auth\_code -p* to verify the function.

## 5.5 PRINT THE COMMON AUTHORIZATION CODE

Use the command *auth\_code -p*.

## 5.6 INITIATE A INDIVIDUAL AUTHORIZATION CODE

Use the command *auth\_code -i*, specify the parameter *-dir*.

Use the command *auth\_code -p* to verify that the function has been initiated.

## 5.7 REMOVE THE INDIVIDUAL AUTHORIZATION CODE

Use the command *auth\_code -e*.

**Note:** The system administrator has to ensure that the individual authorization code (RAC) is not erased for a secure extension, with *SECEXC = NO*.

Use the command *auth\_code -p* to verify the function .

## 5.8 PRINT THE INDIVIDUAL AUTHORIZATION CODE

Use the command *auth\_code -p*.

## 5.9

### INITIATE HASHING OF THE INDIVIDUAL AUTHORIZATION CODES

Use the command *auth\_code -encrypt*, if the individual authorization codes shall be hashed (i.e. changed from clear text to hashed format). Only relevant for SIP terminals that support this functionality.

Use the command *auth\_code -p* to verify that the encryption function has been initiated.

## 6

### TERMINATION

Inform the person responsible for telephony matters at the customer of all alterations made.

If exchange data have been altered, that is, if *auth\_code -i* or *auth\_code -e* has been used, make a dump to backup media, see operational directions for *ADMINISTRATOR USER'S GUIDE*.