MiVoice MX-ONE

Authorization Code for Extension - Operational Directions

Release 7.5 SP1

September, 2023

Notice

Trademarks

Contents

Chapter: 1 **General** 1

Chapter: 2 **Tools** 2

Chapter: 3 **References** 3

Chapter: 4 **Procedure** 4

Chapter: 5 **Execution** 5

Initiate the Common Service Profile 5
Initiate the Common Authorization Code 5
Remove the Common Authorization Code 5
Print the Common Authorization Code 6
Initiate the Individual Authorization Code 6
Remove the Individual Authorization Code 6
Print the Individual Authorization Code 6
Initiate Hashing of the Individual Authorization Codes 6

Chapter: 6 **Termination** 7

General

Authorization codes can be initiated in the system to temporarily change properties, permissions, and characteristics at a specific extension by using an authorization code with another CSP than was originally defined for that extension. Example wise TCD, diversion characteristics, or different services can be blocked, opened, or extended.

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

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

Predialling an authorization code when establishing a call gives the service profile from the authorization code only for that particular 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 uses a common service profile. 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 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.
  When common authority code is configured with the `--customer` parameter, then only users, assigned to the same customer may dial this code.
  If customer groups are initiated in the system, more than one hash can be created; one for the long number, and one for the short number.
- **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 uses 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 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.
  When initiating an individual authority code, no customer number can be selected. The customer number of the user applies, if present. If not present, customer number 0 will be used. In calls, when individual authority code is dialed, the customer of the user applies, unless `--new-customer` is configured.
  If customer groups are initiated in the system, more than one hash can be created; one for the long number, and one for the short number.

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

Tools

I/O terminal.

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

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`).

Execution

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

1. Use the command `extension_profile -i`, with CSP=0 (--csp 0), if a default common service profile is to be initiated.
2. Use the command `auth_code -i`.
3. Use the command `auth_code -p` to verify that the function is initiated.

Initiate the Common Authorization Code

General

The common service profile (CSP), also used in auth_code, refers to the common service profile specified in command `extension_profile -i`. A common authorization code can be affiliated to a CSP.

Procedure

1. Key the command `extension_profile -i`, with a common service profile, specified higher than the normal service profile.
2. Use the command `auth_code -i`.
3. Use the command `auth_code -p` to verify that the function is initiated.

Remove the Common Authorization Code

1. Use the command `auth_code -e`.
2. Use the command `auth_code -p` to verify that the function.

Print the Common Authorization Code

Use the command `auth_code -p`.

Initiate the Individual Authorization Code

1. Use the command `auth_code -i`, specify the parameter `-dir`.
2. Use the command `auth_code -p` to verify that the function is initiated.

Remove the Individual Authorization Code

1. 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.
2. Use the command `auth_code -p` to verify that the function.

Print the Individual Authorization Code

Use the command `auth_code -p`.

Initiate Hashing of the Individual Authorization Codes

1. Use the command `auth_code -encrypt`, if the individual authorization codes shall be hashed (that is, changed from clear text to hashed format). Only relevant for SIP terminals that support this functionality.
2. Use the command `auth_code -p` to verify that the encryption function has been initiated.

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*.