Chapter 7

ENCRYPTED FILES ON THE IP PHONE

ABOUT THIS CHAPTER

This chapter provides information about encryption on the IP phones and provides methods an administrator can use to store encrypted files to a server.

TOPICS

This chapter covers the following topics:

TOPIC	PAGE
Encrypted Files on the IP Phone	page 7-3
• Configuration File Encryption Method	page 7-3
• Procedure to Encrypt Configuration Files	page 7-4
• Vendor Configuration File Encryption	page 7-6

ENCRYPTED FILES ON THE IP PHONE

An encryption feature for the IP phone allows Service Providers the capability of storing encrypted files on their server to protect against unauthorized access and tampering of sensitive information (i.e. user accounts, login passwords, registration information). Service Providers also have the capability of locking a phone to use a specific server-provided configuration only.

CONFIGURATION FILE ENCRYPTION METHOD

Only a System Administrator can encrypt the configurations files for an IP Phone. System Administrators use a password distribution scheme to manually pre-configure or automatically configure the phones to use the encrypted configuration with a unique key.

From a Microsoft Windows command line, the System Administrator uses an Mitel-supplied configuration file encryption tool called "*anacrypt.exe*" to encrypt the *<mac>.tuz* file.

Note: Mitel also supplies encryption tools to support Linux platforms (*anacrypt.linux*) if required.

This tool processes the plain text *<mac>.cfg, <model>.cfg,* and *startup.cfg* files and creates triple-DES encrypted versions called *<mac>.tuz, <model>.tuz,* and *startup.tuz.*

Note: In releases previous to 4.0.0 SP1, the "startup.tuz" file was named "aastra.tuz". Apart from the file names, the "startup.tuz" file acts as an identical replacement for the "aastra.tuz" file. Releases including and above 4.0.0 SP1 support both the "startup.tuz" and "aastra.tuz" files, but if the "startup.tuz" file is available, the phone will disregard the "aastra.tuz" file (if available). The "aastra.tuz" file will be used if the "startup.tuz" file is unavailable and will continue to be supported going forward to ensure backwards compatibility with existing customer deployments.

Encryption is performed using a secret password that is chosen by the administrator.

The encryption tool is also used to create an additional encrypted tag file called *security.tuz*, which controls the decryption process on the IP phones. If *security.tuz* is present on the TFTP/FTP/HTTP server, the IP phones download it and use it locally to decrypt the configuration information from the *startup.tuz* and *<mac>.tuz* files. Because only the encrypted versions of the configuration files need to be stored on the server, no plain-text configuration or passwords are sent across the network, thereby ensuring security of the configuration data.

To make changes to the configuration files, the System Administrator must save the original files.

Note: If the use of encrypted configuration files is enabled (via *security.tuz* or pre-provisioned on the IP phone) the *startup.cfg, <model>.cfg,* and *<mac>.cfg* files are ignored, and only the encrypted equivalent files *startup.tuz, <model>.tuz,* and *<mac>.tuz* are read.

The security feature described above prevents unauthorized parties from **reading** or **writing** the contents of the *<MAC>.tuz* file. It also provides the following:

- Prevents users from using the *<MAC>.tuz* file that does not match the user's phone MAC address.

- Renders the <*MAC*>*.tuz* file invalid if the user renames the file.
- Works with IP phone releases prior to Release 2.2.
- Provides compatibility between the previous encryption routine and the new decryption routine.

PROCEDURE TO ENCRYPT CONFIGURATION FILES

To encrypt the IP phone configuration files (using a Microsoft Windows OS):

1. Obtain the anacrypt encryption tool (anacrypt.exe) from your Mitel representative.
2. Open a command line window application (i.e. DOS window).
3. At the prompt, enter ***anacrypt.exe*** and press <Return>.
4. Enter a command utilizing the details provided in the help screen.

```
C:\> anacrypt.exe -h

Provides encryption of the configuration files used for the
family of Mitel SIP phones.

Copyright (c) 2005-2014, Mitel Networks Corporation.

Usage:

anacrypt {infile.cfg|-d <dir>} [-p password] [-m] [-i] [-v] [-h]
```

ANACRYPT SWITCH	DESCRIPTION
{infile.cfg | -d <dir>}	Specifies that all .cfg files in <dir> should be encrypted.
[-p password]	Specify password used to generate keys.
-m	Generate MAC.tuz files that are phone specific. This switch generates files that are only usable for phones with firmware version 2.2.0 and above.
-v1	Specifies the version of encryption that the anacrypt tool uses. Use version 1 encryption (i.e. -v1) to generate files that are readable by all model phones.
-v2	(Default) Specifies the version of encryption that the anacrypt tool uses. Use version 2 encryption (i.e. -v2) to generate files that are readable by phones with firmware 2.2.0 and above.
-v3	(Enhanced security version) Specifies the version of encryption that the anacrypt tool uses. Use version 3 encryption (i.e. -v3) to generate files that are readable by phones with firmware 3.3.1 and above.
-i	Generate security.tuz file.
-h	Show the help screen.

Notes:

1. Configuration files that are encrypted using v3 encryption can only be decoded by phones on Release 3.3.1 (and above).Customers with v3-encrypted configuration files will lose the ability to decode the files (and in turn will lose all previously configured settings) if they downgrade their phones to any firmware release prior to 3.3.1.
2. An incorrect password produces garbage. For site-specific keyfile security.cfg the plaintext must match the password.

EXAMPLES

The following examples illustrate the use of the anacrypt.exe file.

Example 1

Generating a security.tuz file with password 1234abcd:

For firmware version 3.3.1 (enhanced security):

```
C:\>anacrypt -i -p 1234abcd -v3
```

For firmware version 2.2.0 and above:

```
C:\>anacrypt -i -p 1234abcd
```

or

```
C:\>anacrypt -i -p 1234abcd -v2
```

For any firmware version:

```
C:\>anacrypt -i -p 1234abcd -v1
```

Example 2

Encrypting a single startup.cfg file with password 1234abcd (for firmware version 3.3.1 and above):

```
C:\>anacrypt startup.cfg -p 1234abcd -v3
```

Example 3

Encrypting a <mac>.cfg file with password 1234abcd (for firmware version 3.3.1 and above):

```
C:\>anacrypt 00085d000000.cfg -p 1234abcd -v3
```

Example 4

Encrypting a <mac>.cfg file with password 1234abcd using MAC encryption (for firmware version 3.3.1 and above):

```
C:\>anacrypt 00085d000000.cfg -m -p 1234abcd -v3
```

Example 5

Encrypting all cfg files in C:\data with password 1234abcd using MAC encryption and generating a security.tuz file at the same time (for firmware version 3.3.1 and above):

```
C:\>anacrypt -d C:\data -p 1234abcd -m -i -v3
```

Example 6

Encrypting all cfg files in C:\data with password 1234abcd and generating a security.tuz file at the same time (for firmware version 3.3.1 and above):

```
C:\>anacrypt -d C:\data -p 1234abcd -i -v3
```

VENDOR CONFIGURATION FILE ENCRYPTION

Some vendors can have specific methods to encrypt files on their configuration servers. For each phone, the configuration server can generate a random hex string (encryption key) that is used to encrypt the phone's MAC-specific configuration file.

The encryption key is placed in a plain text MAC-specific configuration file that the server downloads to the phone. After the phone receives the file, it updates the encryption key.

Note: The phone will not reboot automatically after updating the configuration encryption key. Upon the next reboot, the phone will download the encrypted MAC-specific configuration file from configuration server (provided that the unencrypted MAC-specific file is not present on the configuration server)

This method of encryption does not affect the implementation of the Mitel method of file encryption.

Note: The *startup.cfg* file is not encrypted with this feature.

You can set the phone-specific encryption key using the configuration files only.

For more information about configuration file encryption, contact Mitel Technical Support.

CONFIGURING VENDOR CONFIGURATION FILE ENCRYPTION

Use the following procedure to configure vendor configuration file encryption on the IP Phones.

CONFIGURATION FILES

For specific parameters you can set in the configuration files for automatic update, see Appendix A, the section, "Configuration Encryption Setting" on page A-300.