

Backup and Restore Procedure

Table of Contents

| | | |
|----------|---|-----------|
| 1 | Introduction | 7 |
| 2 | Backing up Configuration | 9 |
| 2.1 | Backing up Device Configuration through Web Interface | 9 |
| 2.2 | Backing up Device Configuration through CLI | 10 |
| 2.2.1 | Backing Up Configuration on a Data-enabled Device | 10 |
| 2.2.2 | Backing Up Configuration on a Voice-enabled Device..... | 10 |
| 2.3 | Backing Up EMS Configuration Before Upgrade | 12 |
| 2.3.1 | Changing Scheduled Backup Time | 12 |
| 2.3.2 | Collecting EMS Logs | 13 |
| 3 | Restoring Configuration | 15 |
| 3.1 | Restoring Device Configuration through Web Interface | 15 |
| 3.2 | Restoring Device Configuration through CLI..... | 16 |
| 3.2.1 | Restoring Configuration on a Data-enabled Device | 16 |
| 3.2.2 | Restoring Configuration on a Voice-enabled Device..... | 16 |
| 3.3 | Restoring EMS Configuration After Upgrade | 18 |

This page is intentionally left blank.

Notice

Information contained in this document is believed to be accurate and reliable at the time of printing. However, due to ongoing product improvements and revisions, AudioCodes cannot guarantee accuracy of printed material after the Date Published nor can it accept responsibility for errors or omissions. Before consulting this document, check the corresponding Release Notes regarding feature preconditions and/or specific support in this release. In cases where there are discrepancies between this document and the Release Notes, the information in the Release Notes supersedes that in this document. Updates to this document and other documents as well as software files can be downloaded by registered customers at <http://www.audiocodes.com/downloads>.

© Copyright 2017 AudioCodes Ltd. All rights reserved.

This document is subject to change without notice.

Date Published: February-08-2017

Trademarks

©2017 AudioCodes Ltd. All rights reserved. AudioCodes, AC, HD VoIP, HD VoIP Sounds Better, IPmedia, Mediant, MediaPack, What's Inside Matters, OSN, SmartTAP, User Management Pack, VMAS, VoIPerfect, VoIPerfectHD, Your Gateway To VoIP, 3GX, VocaNom, AudioCodes One Voice and CloudBond are trademarks or registered trademarks of AudioCodes Limited. All other products or trademarks are property of their respective owners. Product specifications are subject to change without notice.

WEEE EU Directive

Pursuant to the WEEE EU Directive, electronic and electrical waste must not be disposed of with unsorted waste. Please contact your local recycling authority for disposal of this product.

Customer Support

Customer technical support and services are provided by AudioCodes or by an authorized AudioCodes Service Partner. For more information on how to buy technical support for AudioCodes products and for contact information, please visit our Web site at www.audiocodes.com/support.

Abbreviations and Terminology

Each abbreviation, unless widely used, is spelled out in full when first used.

Document Revision Record

| LTRT | Description |
|-------|---|
| 39621 | Initial document release for Version 7.2. |
| 39622 | Updates for including backup and restore procedure for both data and voice enabled devices and with USB devices. |
| 39624 | Added notes regarding the BootP tool and firmware cmp file backup; added sections for backing up and restoring the EMS configuration. |

Documentation Feedback

AudioCodes continually strives to produce high quality documentation. If you have any comments (suggestions or errors) regarding this document, please fill out the Documentation Feedback form on our Web site at <http://www.audiocodes.com/downloads>.

1 Introduction

This document describes the procedures for backing up and restoring your device's configuration settings.

It is important to back up your configuration on a regular basis in case you need to restore configuration if, for example, any of the following scenarios occurs:

- Your device has a hardware fault that requires it to be replaced entirely.
- A hardware component on the device is faulty (e.g., CPU).
- Firmware upgrade failure
- Undesired configuration upgrade or failure.

**Note:**

- It is your responsibility to save the backup configuration files after every configuration change made on the device.
- It is your responsibility to back up your existing configuration and firmware files to a safe location on your network before upgrading the device.

This page is intentionally left blank.

2 Backing up Configuration

You can save a copy of the device's current configuration settings as a file on a local PC server. This can be used as a backup file for your configuration. The saved file includes only parameters that were modified and parameters with other than default values.

You can also save (create) the current configuration as a configuration file on the device's flash memory and send it to a user-defined URL of a remote server (TFTP or HTTP/S) or to a USB device. The configuration settings in the file are based only on CLI commands. For more information, refer to the *CLI Reference Manual*.

This chapter describes how to backup the configuration through one of the following management interfaces:

- Web interface (see Section 2.1)
- CLI (see Section 2.2)
- EMS (see Section 2.3)



Note:

- Make sure you have a backup copy of all auxiliary files (e.g., CPT and Dial Plan files) before you upload them to the device.
- If you do not have a backup of the device's cmp file on your PC, you must open a service request to receive it.
- In case of outage due to hardware upgrade or replacement or disaster, use the BootP tool to connect directly to the device from a PC. A trained technician should be present on the local site for performing this task.
- If you do not have the BootP tool on your site, open a service request to receive it.

2.1 Backing up Device Configuration through Web Interface

The Web interface allows you to back up the device's configuration as an ini file or a CLI-based file (CLI script) in a folder on the PC client running the Web interface.

➤ To back up the configuration:

1. Open the Configuration File page:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Configuration File**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**.

Figure 2-1: Backing up Configuration through Web Interface

Configuration File

| | |
|--|---|
| SAVE THE INI FILE TO THE PC. | SAVE CLI SCRIPT FILE TO THE PC. |
| <input type="button" value="Save INI File"/> | <input type="button" value="Save CLI Script File"/> |

2. Click one of the following buttons:
 - **Save INI File:** saves the configuration as an ini file.
 - **Save CLI Script File:** saves the configuration as a CLI-based file.

2.2 Backing up Device Configuration through CLI

The CLI allows you to back up the device's configuration as a CLI-based file (CLI command settings). You can back up the CLI-based file to any of the following locations:

- Remote server (HTTP, HTTPS or TFTP)
- USB stick



Note: The USB stick is only applicable to devices that provide USB support.

The procedures below describes how to back up the devices configuration using CLI on a data-enabled and voice-enabled device.

2.2.1 Backing Up Configuration on a Data-enabled Device

This section describes how to back up the devices configuration on a data-enabled device.

➤ **To back up the configuration using CLI on a data-enabled device:**

1. Establish a CLI serial connection with the device (e.g., Telnet).
2. Log in to the CLI.

```
Username: Admin
Password: < Password >
```

3. Access the Enable mode.

```
> enable
Password: < Enable mode password >
```

4. Enter the following command:

```
# copy cli-script to { < URL > | usb:///< File Name > }
source data interface <interface type> <interface id>
```

2.2.2 Backing Up Configuration on a Voice-enabled Device

This section describes how to back up the devices configuration on a voice-enabled device.

➤ **To back up the configuration using CLI on a voice-enabled device:**

1. Establish a CLI serial connection with the device (e.g., Telnet).
2. Log in to the CLI.

```
Username: Admin
Password: < Password >
```

3. Access the Enable mode.

```
> enable
Password: < Enable mode password >
```

4. Enter the following command:

```
# copy cli-script to { < URL > | usb:///< File Name > }
```

| Arguments | Description |
|---------------------|---|
| URL | When copying to a URL, the destination URL can be one of the following: <ul style="list-style-type: none"> • HTTP • HTTPS • TFTP |
| usb:///< File Name> | Backs up the configuration to the USB stick connected to the device. |
| source | Specifies the source CPU to copy from (default data). |
| interface | Specifies the source interface to bind to. |
| source-address | Specifies the source address. |

| | Interface Type | Interface ID |
|-----------------|---|--------------------|
| gigabitethernet | GigabitEthernet interface slot and port (VLAN ID is optional) | [SLOT/PORT.VLANID] |
| cellular | Cellular interface ID | 0/0 |
| Gr-e | Tunnel GRE ID | [1-255] |
| ipip | Tunnel IPIP ID | [1-255] |
| l2tp | L2TP ID | [0-99] |
| pppoe | PPPoE interface ID | [1-3] |
| pptp | PPTP ID | [0-99] |
| vlan | Vlan ID | [1-3999] |
| loopback | Loopback ID | [1-5] |
| bvi | Bridge interface | [1-255] |

2.3 Backing Up EMS Configuration Before Upgrade

Before upgrading the EMS server, it is highly recommended to backup the EMS server database. There are two main backup processes that run on the EMS server:

- **Weekly backup:** runs once a week at a pre-configured date & time (default is Saturday 02:00). In this process, the whole database is backed up into several "RMAN" files that are located in /data/NBIF/emsBackup/RmanBackup directory. In addition, many other configuration and software files are backed up to a TAR file in the /data/NBIF/emsBackup directory. In general, this TAR file contains the entire /data/NBIF directory's content (except 'emsBackup' directory), EMS Software Manager content and server_XXX directory's content.

To change the weekly backup's time and date, see Section 2.3.1 below.

- **Daily backup:** runs daily except on the scheduled week day (see above). The daily backup process backs up the last 24 hours. There are no changes in the TAR file in this process.



Warning: The Backup process does not backup configurations performed using EMS Server Manager, such as networking and security.

It is highly recommended to maintain all backup files on an external machine.

These files can be transferred outside the server directly from their default location by SCP or SFTP client using 'acems' user. These backup files are as follows:

- /data/NBIF/emsBackup/emsServerBackup_<time&date>.tar file
- All files in /data/NBIF/emsBackup/RmanBackup directory (including control.ctl and init.ora files)

2.3.1 Changing Scheduled Backup Time

This step describes how to reschedule the backup time.

➤ **To reschedule backup time:**

1. From the Application Maintenance menu, choose **Change Schedule Backup Time**.
2. Choose the day of the week that you wish to perform the backup.
3. Copy all files in /data/NBIF/emsBackup/RmanBackup/ directory to an external machine.
4. Copy /data/NBIF/emsBackup/emsServerBackup_<time&date>.tar file to an external machine.

Where <time&date> is only an example; replace this path with your filename.

2.3.2 Collecting EMS Logs

It is recommended to collect EMS logs before upgrading or re-configuring the EMS server. This enables you to restore the MG tree

➤ **To collect logs:**

1. From the EMS Server Management root menu, choose **Collect Logs**, and then press Enter; the EMS server commences the log collection process:

Figure 2-2: EMS Server Manager – Collect Logs

```
Collecting logs
Collecting EMS Server logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Insallation Log Files
Collecting Yafic Scan Files
Collecting GeneralInfo
Collecting Topology File
Packing TAR file...
  adding: logs.tar (deflated 83%)

Logs can be found in /home/acems/logs.tar.zip
```

This process can take a few minutes. Once the file generation has completed, a message is displayed on the screen informing you that a Diagnostic tar file has been created and the location of the tar file:

Figure 2-3: TAR File Location

```
Collecting logs
Collecting EMS Server logs...
Collecting OS logs...
Collecting Oracle DB logs...
Collecting hardware configuration...
Collecting OS configuration...
Collecting Rman Log Files
Collecting Tomcat Log Files
Collecting Insallations Log Files
Collecting Yaffic Scan Files
Collecting GeneralInfo
sh: HA: command not found
Packing IAR file...
updating: home/acems/logs.tar (deflated 95%)

The diagnostics TAR file can be found in /home/acems/logs.tar
Press Enter to continue
```

- The MGs Topology list containing all the devices in the MG Tree is found in the following file:

/data/NBIF/topology/MGsTopologyList.csv

An example of this file is shown in the figure below:

Figure 2-4: MGs Topology List

| Serial | Nur IP | Address:GW Name | Region | Na | Product T | Software | Performa | Descriptio | SBA | FQDN | SBA IP | Adi | SNMP Ver | SNMP Res | SNMP Wri | SNMP Use | Gateway L | Gateway f | HTTPS | Enabled |
|----------|------------|-----------------|------------|----------|--------------|------------|------------|------------|-----|------|--------|-----|----------|-----------|--------------------|----------|-----------|-----------|-------|---------|
| 7963301 | 172.17.175 | HK-MSBR | ACL-Hong | UNKNOW | unknown | Not Pollin | Hongkong | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | Admin | fseUajPSa | | 0 | |
| 3584140 | 10.62.0.41 | VMAS | ACL-Israel | MEDIANT | 6.60A.227 | Polling | MEDIANT | | | | | | SNMPv3 | 8kXtnrBul | f/0B4MNI00.00.00.6 | | | | 0 | |
| 3960688 | 10.62.0.72 | VMAS-Dei | ACL-Israel | Mediante | 8 7.20A.000 | Not Pollin | Mediante 8 | | | | | | SNMPv3 | 8kXtnrBul | f/0B4MNI00.00.00.6 | Admin | s5v9qP29r | | 1 | |
| 3593376 | 172.17.24C | Mobility-£ | ACL-Israel | Mediante | 8 6.80A.021 | Polling | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | | | | 0 | |
| 4936574 | 10.15.54.1 | Uzi-SBC | ACL-Israel | Mediante | 8 6.80A.306 | Not Pollin | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | Admin | fseUajPSa | | 0 | |
| 6484770 | 172.17.24C | WebRtc-S | ACL-Israel | Mediante | 5 7.00A.044 | Not Pollin | WebRtc-S | | | | | | SNMPv3 | 8kXtnrBul | f/0B4MNI00.00.00.6 | Admin | fseUajPSa | | 0 | |
| 5813574 | 10.62.0.10 | E-SBC | ACL-Israel | MEDIANT | 7.00A.067 | Polling | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | | | | 0 | |
| 2265299 | 10.133.10 | TX-GW | ACL-US | MEDIANT | 6.60A.227 | Not Pollin | Texas-GW | | | | | | SNMPv2 | W6PP7IEJ | W6PP7IEJtMD7yHqg | | | | 0 | |
| 6228189 | 172.28.1.3 | NJ-GW | ACL-US | MEDIANT | 7.00A.063 | Not Pollin | | | | | | | SNMPv2 | W6PP7IEJ | W6PP7IEJtMD7yHqg | Admin | Z/nMalpg | | 0 | |
| 6435555 | 192.168.15 | RTP-GW | ACL-US | MEDIANT | 7.00A.067 | Not Pollin | RTP-GW | | | | | | SNMPv2 | W6PP7IEJ | W6PP7IEJtMD7yHqg | Admin | JhsBDPCaj | | 0 | |
| 2578152 | 172.28.1.1 | NJ-MSBG | ACL-US | MEDIANT | 6.60A.227 | Not Pollin | | | | | | | SNMPv2 | W6PP7IEJ | W6PP7IEJtMD7yHqg | | | | 0 | |
| 3245481 | 172.28.1.1 | NJ-GW-fo | ACL-US | Mediante | 8 6.60A.227 | Not Pollin | | | | | | | SNMPv2 | W6PP7IEJ | f/0B4MNTinsMV6ry | | | | 0 | |
| 77227722 | 10.15.70.1 | CCE-2 | AutoDete | Mediante | 8 7.4.002.33 | Not Pollin | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | Admin | fseUajPSa | | 0 | |
| 77117711 | 10.15.70.1 | CCE-1 | AutoDete | Mediante | 8 7.4.002.33 | Not Pollin | 10.15.70.1 | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | Admin | fseUajPSa | | 0 | |
| 1063499 | 172.22.201 | 172.22.201 | AutoDete | MP118 FX | 6.60A.279 | Not Pollin | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | | | | 0 | |
| 3227461 | 172.22.3.1 | 172.22.3.1 | AutoDete | MEDIANT | 7.00A.085 | Not Pollin | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | | | | 0 | |
| 2166884 | 10.21.0.15 | 10.21.0.15 | Demo | MEDIANT | 6.80A.252 | Not Pollin | | | | | | | SNMPv2 | 8kXtnrBul | f/0B4MNTinsMV6ry | | | | 0 | |

3 Restoring Configuration

You can restore the configuration through one of the following management interfaces:

- Web interface (see below)
- CLI (see Section 3.2)
- EMS (see Section 3.3)



Warning:

- When restoring an ini file, the device resets for the settings to take effect.
- When loading an *ini* file using the Configuration File page, parameters not included in the *ini* file are reset to default settings.

3.1 Restoring Device Configuration through Web Interface

The Web interface allows you to restore the device's configuration as an ini file or a CLI-based file (CLI script) from the folder on the PC client running the Web interface, by uploading an ini file or CLI-based file.



Warning: When restoring an ini file using the Configuration File page, parameters excluded from the ini file return to **default settings**. If you want to keep the device's current configuration settings and apply the settings specified in the ini file, load the file through the Auxiliary Files page.

➤ **To restore the configuration file:**

1. Open the Configuration File page:
 - **Toolbar:** From the **Actions** drop-down menu, choose **Configuration File**.
 - **Navigation tree:** **Setup** menu > **Administration** tab > **Maintenance** folder > **Configuration File**.

Figure 3-1: Loading INI File using Configuration File Page

| LOAD THE INI FILE TO THE DEVICE. | | LOAD CLI SCRIPT FILE TO THE DEVICE. | |
|----------------------------------|----------------|-------------------------------------|----------------|
| Choose File | No file chosen | Choose File | No fil...hosen |
| Load INI File | | Load CLI Script File | |

The device will perform a reset after loading the INI file.

2. Click one of the following buttons:
 - **Load INI File:** restores the configuration from the ini file.
 - **Load CLI Script File:** restores the configuration from the CLI-based file.

3.2 Restoring Device Configuration through CLI

The CLI allows you to restore the device's configuration as a CLI-based file (CLI command settings). You can restore the CLI-based file from any of the following locations:

- Remote server (HTTP, HTTPS or TFTP)
- USB stick



Note: The USB stick is only applicable to devices that provide USB support.

The procedures below describe how to restore the devices configuration using CLI on the following platforms:

- Data-enabled device (see Section 3.2.1)
- Voice-enabled device (see Section 3.2.2)

3.2.1 Restoring Configuration on a Data-enabled Device

This section describes how to restore the devices configuration on a data-enabled device.

➤ **To restore the configuration using CLI on a data-enabled device:**

1. Establish a CLI serial connection with the device (e.g., Telnet).
2. Log in to the CLI.

```
Username: Admin
Password: < Password >
```

3. Access the Enable mode.

```
> enable
Password: < Enable mode password >
```

4. Enter the following command:

```
# copy cli-script from { < URL > | usb:///< File Name >
}source data interface <interface type> <interface id>
```

3.2.2 Restoring Configuration on a Voice-enabled Device

This section describes how to restore the devices configuration on a voice-enabled device.

➤ **To restore the configuration using CLI on a voice-enabled device:**

1. Establish a CLI serial connection with the device (e.g., Telnet).
2. Log in to the CLI.

```
Username: Admin
Password: < Password >
```

3. Access the Enable mode.

```
> enable
Password: < Enable mode password >
```

4. Enter the following command:

```
# copy cli-script from { < URL > | usb:///< File Name > }
```

| Arguments | Description |
|---------------------|---|
| URL | When copying to a URL, the destination URL can be one of the following: <ul style="list-style-type: none"> • HTTP • HTTPS • TFTP |
| usb:///< File Name> | Backs up the configuration to the USB stick connected to the device. |
| source | Specifies the source CPU to copy from (default data). |
| interface | Specifies the source interface to bind to. |
| source-address | Specifies the source address. |

| | Interface Type | Interface ID |
|-----------------|---|--------------------|
| gigabitethernet | GigabitEthernet interface slot and port (VLAN ID is optional) | [SLOT/PORT.VLANID] |
| cellular | Cellular interface ID | 0/0 |
| Gr-e | Tunnel GRE ID | [1-255] |
| ipip | Tunnel IPIP ID | [1-255] |
| l2tp | L2TP ID | [0-99] |
| pppoe | PPPoE interface ID | [1-3] |
| pptp | PPTP ID | [0-99] |
| vlan | Vlan ID | [1-3999] |
| loopback | Loopback ID | [1-5] |
| bvi | Bridge interface | [1-255] |

3.3 Restoring EMS Configuration After Upgrade

This section describes how to restore the EMS server after it has been upgraded. This can be done on the original machine from which the backup files were created or on any other machine.



Note:

- If you're running the restore process on a different machine, its disk size should be the same as the original machine from which the backup files were taken.
- Restore actions can be performed only with backup files which were previously created in the same EMS version.
- If you are restoring to a new machine, make sure that you have purchased a new license file machine ID. AudioCodes customer support will assist you to obtain a new license prior to the restore process.

➤ **To restore the EMS server:**

1. Install (or upgrade) EMS to the same version from which the backup files were created. The Linux version must also be identical between the source and target machines.
2. Use the EMS Server Management utility to perform all the required configurations, such as Networking and Security, as was previously configured on the source machine.
3. Make sure all server processes are up in EMS Server Manager / Status menu and the server functions properly.
4. Copy all backup files to /data/NBIF directory by SCP or SFTP client using the 'acems' user.
5. In EMS Server Manager, go to the Application Maintenance menu and select the **Restore** option.
6. Follow the instructions during the process.
7. After the restore process has completed, you will be asked to reboot the machine.
8. If you installed custom certificates prior to the restore, you must reinstall these certificates.

This page is intentionally left blank.

International Headquarters

1 Hayarden Street,
Airport City
Lod 7019900, Israel
Tel: +972-3-976-4000
Fax: +972-3-976-4040

AudioCodes Inc.

27 World's Fair Drive,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: www.audiocodes.com/info

Website: www.audiocodes.com



Document #: LTRT-39624