



Avaya Solution & Interoperability Test Lab

Secrets Management on an Avaya G450 Media Gateway - Issue 1.0

Abstract

The Avaya G450 Media Gateway supports a mechanism in Release 5.0 of Avaya Communication Manager that encrypts all secrets saved in the startup and running configuration files. This approach prevents an unauthorized person from observing the device secrets and enables a complete restore of the device configuration from the startup configuration saved on a USB flash drive or a remote file server. These Application Notes describe this feature.

1. INTRODUCTION	3
2. REFERENCE CONFIGURATION	3
3. EQUIPMENT AND SOFTWARE VALIDATED	4
4. CONFIGURATION OF THE AVAYA G450 MEDIA GATEWAY	5
4.1 Master Configuration Key (MCK)	5
5. COPY AVAYA G450 MEDIA GATEWAY CONFIGURATION FILES	6
5.1 Avaya G450 Startup Configuration File	6
5.2 Copy the Startup Configuration to a USB Flash Drive	7
5.3 Copy the Configuration from a USB Flash Drive to the Startup Configuration	8
5.4 Copy the Startup Configuration to a File Server	9
5.5 Copy the Configuration from the File Server to the Startup Configuration	10
5.6 Master Configuration Key (MCK) Mismatch	11
6. VERIFICATION	11
7. CONCLUSIONS	11
8. REFERENCES	12

1. Introduction

The Avaya G450 Media Gateway supports a mechanism in Release 5.0 of Avaya Communication Manager that encrypts all secrets saved in the startup and running configuration files. This approach prevents an unauthorized person from observing the device secrets and enables a complete restore of the device configuration from the startup configuration saved on a USB flash drive or a remote file server (e.g., FTP, TFTP, SCP).

The Avaya G450 Media Gateway supports two types of backup/restore operations: a configuration backup and a full backup. In both types, the configuration backup/restore operation backs up the Avaya G450 Media Gateway *startup-config*. The *startup-config* contains the operational configuration of the Avaya G450 Media Gateway as well as secret files such as passwords and keys. Both types of backups can be used to restore an Avaya G450 Media Gateway configuration.

However, if a backup is used to recreate an existing configuration on a replacement Avaya G450 Media Gateway, then a new *vpn_license.cfg* file (used for VPN tunnels) and an *auth-file.cfg* file (used for Avaya Services login) must be generated, as these files are device specific. In addition, the same Master Configuration Key defined in the original Avaya G450 Media Gateway (and used in the backup generation) must also be provisioned in the replacement Avaya G450 Media Gateway, or the restoration will fail (see **Section 5**). Refer to [1] and [2] for more information.

2. Reference Configuration

Figure 1 shows the reference network used for the verification of these Application Notes. The reference network is comprised of a “Main Office” and a “Branch Office” connected via an MPLS core network. The Main Office contains an Avaya S8500 Server, an Avaya G650 Media Gateway (containing IPSI, C-LAN, and MedPro cards), an Avaya 4621 IP telephone, and a Windows XP PC running Avaya TFTP Server and ArgoSoft FTP Server software. The Branch Office contains an Avaya G450 Media Gateway, an Avaya 4621 IP telephone, and an Avaya 8410 digital telephone.

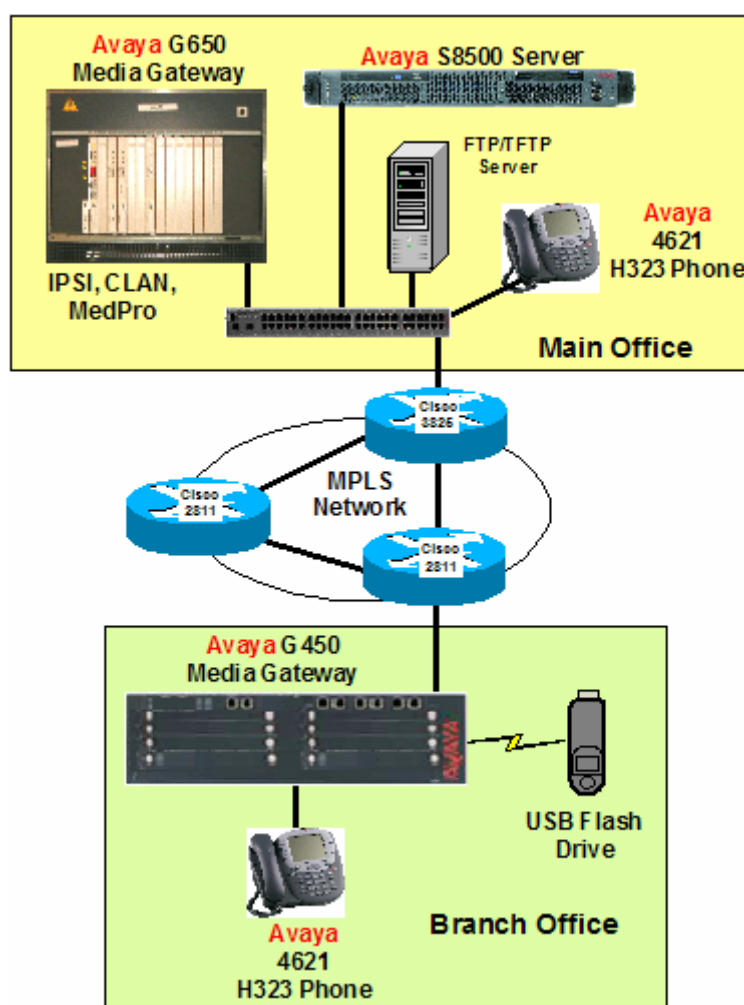


Figure 1 – Reference Configuration

3. Equipment and Software Validated

The following equipment and software were used to test the sample configuration.

Network Component	Hardware/Firmware Version	Software Version
Avaya S8500 Server	-	Avaya Communication Manager 5.0 (R015x.00.0.825.4)
Avaya G650 Media Gateway	-	-
IPSI – TN2312BP	HW15 FW040	-
C-LAN – TN799DP	HW01 FW024	-
MedPro – TN2302AP	HW02 FW018	-
Avaya G450 Media Gateway	27.26.0	-
Avaya 4621 H.323 telephone	a20d01b3_8.bin	-
Avaya 8410 DCP telephone	-	-
Memorex TravelDrive Flash Drive	USB 2.0	-
Avaya TFTP Server		3.6.1
ArgoSoft FTP Server		1.4.3.7
Cisco 3825 router	-	c3825-spservicesk9-mz 12.3(11)T
Cisco 2811 router	-	c2800nm-adventerprisek9-mz 12.4(10a)

Table 1: Test Equipment List

4. Configuration of the Avaya G450 Media Gateway

The following secrets were verified in these Application Notes.

- User Name and Password - A user name and password is created in the Avaya G450 Media Gateway.
- Station Passwords - The Avaya G450 Media Gateway is configured with the Standard Local Survival Processor (SLS). IP station extensions and passwords are configured in the Branch Offices.

Note - Although not part of the reference configuration, VPN authentication keys as well as an OSPF authentication keys are also supported.

Encryption of secrets is performed using 128-bit user defined Master Configuration Key (MCK). The G450 Media Gateway is shipped with an Avaya Default Master Config Key (ADMCK) as a default hard coded secret value common to all Media Gateways. The ADMCK can be used for decryption of a configuration file on initial installation or when customers are not interested in maintaining user defined MCK. Avaya recommends changing the ADMCK to a user defined MCK for greater security.

4.1 Master Configuration Key (MCK)

The Avaya G450 Media Gateway contains a Master Configuration Key (MCK). This key is written to the *startup_config.cfg* file. The *startup_config.cfg* file can only be copied back to an Avaya G450 Media Gateway if the MCK in the *startup_config.cfg* file matches the MCK defined in the destination Avaya G450 Media Gateway. Therefore, when a MCK is defined it should be documented otherwise the *startup_config.cfg* file cannot be restored. If the MCK for a particular Avaya G450 Media Gateway is not known, then it should be changed with the following command and documented prior to backup.

1. Enter the command ***key config-key password-encryption <string>*** where *<string>* is a phrase of 13-64 printable ASCII characters.
2. Copy the running configuration to the start-up configuration using the ***copy running-config startup-config*** command. The new MCK is now in effect.
3. Document the new MCK.

Refer to [1] and [2] for details.

5. Copy Avaya G450 Media Gateway Configuration Files

The startup configuration can be copied to a file server or a USB flash drive. The USB flash drive can connect to the USB port on the Avaya G450 Media Gateway. The file server can be a TFTP, HTTP or SCP server. The copy commands are:

- **copy startup-config ftp**
- **copy ftp startup-config ftp**
- **copy startup-config tftp**
- **copy tftp startup-config**
- **copy startup-config scp**
- **copy scp startup-config**
- **copy startup-config usb**
- **copy usb startup-config**

Refer to [1] for more information on these commands.

To copy the configuration file back from the saved configuration, the current MCK on the Avaya G450 Media Gateway must match the MCK in the saved configuration (see **Section 4.1**). If the Avaya G450 Media Gateway needs to be replaced, the MCK must be configured on the replacement Avaya G450 Media Gateway in order to restore the original configuration on the new media gateway. Refer to [2] for more details on backup and restore.

5.1 Avaya G450 Startup Configuration File

The following display shows the annotated **startup-config** file on the Avaya G450 Media Gateway, which is encrypted with the user defined MCK. Note that all the encrypted secrets in the startup-config are shown with the encrypted prefix. (**Note** – Some of the configuration was removed for brevity)

```
G450-001(super)# show run
! version 27.26.0
Config info release 27.26.0 time "06:08:38 21 FEB 2008 " serial_number
03IS07109075
!
encrypted-username GfWwC0Q6ePKKhaj0f1/nIQ== password
hCP0YjiQny/YKPxmG4i1mFh0r/Ov/P2SAABDUMjoXQc= access-type EBKswinRsIgMPv4kY4efeQ==
set system name "G450_Branch"
!
sls
!
station 60003 ip
  set encrypted-password "9Ve6J3iEV9SN8fHZUDlTpw=="
  set type ip4610sw
  exit
!
exit
!
exit
!# End of configuration file. Press Enter to continue.
G450-001(super)#
```

Figure 2 – Avaya G450 Media Gateway Startup Configuration

5.2 Copy the Startup Configuration to a USB Flash Drive

From the Avaya G450 Media Gateway Command Line Interface (CLI), enter the following commands.

1. Enter the command ***copy running-config startup-config*** to insure that any changes to the active configuration are saved.
2. Insert a USB flash drive into a USB slot on the Avaya G450 Media Gateway. A message similar to the following will be displayed depending on the USB device used:

```
usb device TD CLASSIC 003B (devID 514),
compliant to USB standard 2.0, full-speed, bus-powered,
connected on product id N/A
```

Figure 3 – USB Device Detection

3. Enter the command ***show usb all*** to identify the USB device. The following will be displayed depending on the USB device used. In this example, the USB device is **usbdevice0**.

G450-001(super)# show usb all									
USB Dev Id	Description		Manufacturer		USB Power Ver Mode		Max Power (mA)		Speed
1	Root Hub (OHCI)		N/A		1.1 Self		0		Full
257	Root Hub (OHCI)		N/A		1.1 Self		0		Full
513	Root Hub (EHCI)		N/A		2.0 Self		0		High
514	TD CLASSIC 003B		Memorex		2.0 Bus		200		Full
USB Dev Id	Vendor ID	Product ID	Device Ver	Serial Number	FileSystem	Storage (MB)	Free (MB)	FS	
1	0x0	0x0	0.0	N/A	N/A	N/A	N/A	N/A	
257	0x0	0x0	0.0	N/A	N/A	N/A	N/A	N/A	
513	0x0	0x0	0.0	N/A	N/A	N/A	N/A	N/A	
514	0x12f7	0x1900	1.0	075410921891	/usbdevice0	983	616	FAT16	

Figure 4 – USB Device Display

4. Enter the command ***copy startup-config usb G450_startup_backup usbdevice0*** where ***G450_startup_backup*** is the name of the file being created.
5. Enter the command ***show upload status***. A successful completion will have the following displayed.

```
G450-001(super)# show upload status
Module #10
=====
Module           : 10
Source file      : startup-config
Destination file : /usbdevice0/G450_startup_backup
Host             : 0.0.0.0
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
```

Figure 5 – Backup Upload Status

6. Enter the command ***safe remove usb usbdevice0*** before removing the USB flash drive.

5.3 Copy the Configuration from a USB Flash Drive to the Startup Configuration

From the Avaya G450 Media Gateway CLI, enter the following commands.

1. Insert the USB flash drive used in **Section 5.2**.
2. Enter the command ***dir usbdevice0***. Verify that the correct file is on the drive.

G450-001(super)# dir usbdevice0			
Date	Type	Size(Bytes)	Filename
-----	-----	-----	-----
2008-02-07, 16:29:46	file	3233	
G450_startup_backup.CFG			
G450-001(super)#			

Figure 6 – USB Drive File Contents

3. Enter the command ***copy usb startup-config usbdevice0 G450_startup_backup*** where *G450_startup_backup* is the name of the startup file being restored.
4. Enter the command ***show upload status***. A successful completion will have the following displayed.

```
G450-001(super)# show upload status
Module #10
=====
Module           : 10
Source file      : startup-config
Destination file : /usbdevice0/G450_startup_backup
Host             : 0.0.0.0
Running state    : Idle
Failure display  : (null)
Last warning     : No-warning
G450-001(super)#
```

Figure 7 – File Copy Status

5. Enter the command ***safe remove usb usbdevice0*** before removing the USB flash drive from the Avaya G450 Media Gateway.

5.4 Copy the Startup Configuration to a File Server

As described previously, the startup configuration on the Avaya Media Gateway can also be copied to a TFTP, HTTP or SCP file server. In the following examples an FTP server was used. TFTP and SCP procedures are similar.

1. Enter the command ***copy running-config startup-config*** to insure that any changes to the active configuration are saved.
2. Enter the command ***copy startup-config ftp G450_FTP 50.50.50.10*** where *G450_FTP* is the name of the backup file being created and *50.50.50.10* is the IP address of the FTP server.
3. Enter the login and password for the FTP server.

Note – An anonymous login was used on the FTP server in the reference configuration

```
G450-001(super)# copy startup-config ftp G450_FTP 50.50.50.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show upload status 10' command
```

Figure 8 – Initiate File Copy to FTP Server

4. Enter the command ***show upload status***. A successful completion will have the following displayed.

```
G450-001(super)# show upload status 10
Module #10
=====
Module : 10
Source file : startup-config
Destination file : G450_FTP
Host : 50.50.50.10
Running state : Idle
Failure display : (null)
Last warning : No-warning
```

Figure 9 – File Copy to FTP Server Status

5.5 Copy the Configuration from the File Server to the Startup Configuration

1. Enter the command ***copy ftp startup-config G450_FTP 50.50.50.10*** where *G450_FTP* is the name of the backup file being restored and *50.50.50.10* is the IP address of the FTP server.
2. Enter the login and password for the FTP server.

Note – An anonymous login was used on the FTP server in the reference configuration

```
G450-001(super)# copy ftp startup-config G450_FTP 50.50.50.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning upload operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show upload status 10' command
```

Figure 10 – Initiate File Copy From FTP Server

3. Enter the command ***show upload status***. A successful completion will have the following displayed.

```
G450-001(super)# show upload status 10
Module #10
=====
Module : 10
Source file : G450_FTP
Destination file : startup-config
Host : 50.50.50.10
Running state : Idle
Failure display : (null)
Last warning : No-warning
```

Figure 11 – File Copy From FTP Server Status

5.6 Master Configuration Key (MCK) Mismatch

If the MCK in the backup startup configuration does not match the MCK in the startup configuration running on the Avaya G450 Media Gateway, the copy command will fail as shown in the following example.

```
G450-001(super)# copy ftp startup-config G450_Backup_test 50.50.50.10
Confirmation - do you want to continue (Y/N)? y
Username: anonymous
Password:
Beginning download operation ...
This operation may take up to 20 seconds.
Please refrain from any other operation during this time.
For more information , use 'show download status 10' command

G450-001(super)# Failed Testing Line 4 in G450_Backup_test file:
"encrypted-username aLEHX7l+cmhuqwnBpCkRfA== password
RpyiV36d2wiUXpXyjmDyapFa/rUR5Q+MTxrbX+auwYM= access-type
2dkdf69qy3Sd02fzja4gQg=="
Failed Testing Line 135 in G450_Backup_test file:
"set encrypted-password "VaHGMPWH07Z5NZbJ4xFjgA=="

G450-001(super)#
```

Figure 12 – MCK Failure During File Copy

6. Verification

The administrator needs to make sure that the Media Gateway functions as expected with the new startup configuration copied from the USB flash drive or a file server. Based on the configuration in **Figure 1**, the following should be verified:

- The Avaya G450 Media Gateway registers to Avaya Communication Manager.
- The IP telephone registers to Avaya Communication Manager.
- Calls can be made successfully between all locations.
- The IP telephone in a branch office can register to the Standard Local Survival (SLS) Processor of the Avaya G450 Media Gateway in the branch office when the connection is lost to the Main office.

Open the configuration files on the file servers and USB flash drive with a text editor and verify that all secrets in the configuration file are encrypted.

7. Conclusions

These Application Notes illustrate that the Avaya G450 Media Gateway can encrypt all secrets using the MCK in the startup and running configuration files, which can be copied to an external file server or a USB flash drive. The Avaya G450 Media Gateway can also decrypt the configuration copied back from an external file server or a USB flash drive when the same MCK is used. The backup configuration file cannot be copied back if a different MCK is used.

8. References

The following documents can be found at <http://support.avaya.com>:

[1] *Administration for the Avaya G450 Media Gateway*, Doc ID 03-602055, Issue 1, January 2008.

[2] *Configuring the Backup and Restore on an Avaya G450 Media Gateway with a USB Flash Drive*, April 2008.

[3] *Configuring Secrets Management on the Avaya G250 and G350 Media Gateways*, Issue 1, April 2007.

©2008 Avaya Inc. All Rights Reserved.

Avaya and the Avaya Logo are trademarks of Avaya Inc. All trademarks identified by ® and ™ are registered trademarks or trademarks, respectively, of Avaya Inc. All other trademarks are the property of their respective owners. The information provided in these Application Notes is subject to change without notice. The configurations, technical data, and recommendations provided in these Application Notes are believed to be accurate and dependable, but are presented without express or implied warranty. Users are responsible for their application of any products specified in these Application Notes.

Please e-mail any questions or comments pertaining to these Application Notes along with the full title name and filename, located in the lower right corner, directly to the Avaya Solution & Interoperability Test Lab at interoplabnotes@list.avaya.com