Security Configuration Note

400HD Series IP Phones

Teams Compatible and Generic SIP

Version 3.4.3

audiocodes

Table of Contents

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. Updates to this document can be downloaded from https://www.audiocodes.com/library/technical-documents.

This document is subject to change without notice.

Date Published: June-14-2020

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 website at https://www.audiocodes.com/services-support/maintenance-and-support.

Stay in the Loop with AudioCodes

Abbreviations and Terminology

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

Throughout this manual, unless otherwise specified, the term *device* refers to AudioCodes products.

Document Revision Record

LTRT	Description
11311	This is the first release of this document.

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 website at https://online.audiocodes.com/documentation-feedback.

1 Introduction

This document describes AudioCodes recommendations on how to enhance the security level of AudioCodes IP phones.

Note: Though the recommended actions described in this document are based on AudioCodes accumulated experience with VoIP deployments worldwide, it is important to understand that each organization has its own network structure, security and limitations. Consequently, it's up to the relevant IT or security team to define and implement the best possible security mechanisms according to their specific network architecture, including additional and/or different security measures.

2 Limit Access to the IP Phone

It's important to limit the possible methods for accessing IP phones and their configuration only to the Device Manager or to specific trusted entities.

This includes the following configuration:

```
security/whitelist/ip=<Device-Manager-IP-ADDR>
security/whitelist/web_server/enabled=1
security/whitelist/telnet_server/enabled=1
security/whitelist/ssh_server/enabled=1
```

Other trusted IP addresses can be added to the list by separating the value field with a semi-colon, as follows:

```
security/whitelist/ip=<IP-ADDR-1>;<IP-ADDR-2>;<IP-ADDR-3>
```

The maximum length of the value field is 128 bytes.

The above settings will result in access being granted only to the whitelisted IP address over Telnet, SSH and the Web interface.

3 Disable Unsecured Web HTTP Access

Disabling unsecured access to Web interface (HTTP) can be done by setting:

```
security/web/https_only=1
```

Note: When the phone is being accessed via the Web interface, it will present its factory (server) certificates. In order for the secured session to be established, the client should be loaded with Audiocodes public Root CA certificate, which can be downloaded from website www.audiocodes.com/library.

Loading custom server certificates to the IP phone is not supported.

4 Disable Web Access Entirely (HTTP and HTTPS)

Disabling all HTTP access to the Web interface can be done by setting:

```
system/web/enabled=0
```

The IP phone will still be able to be managed and provisioned via the provisioning server even if Web interface access is restricted.

5 Telnet Access

By default, Telnet access is disabled:

```
management/telnet/enabled=0
```

However, once enabled, the IP phone can be accessed from any IP address.

To limit the entities that can access the device over Telnet, you need to enable the Telnet whitelist feature as specified in Section 2, Limit Access to the IP Phone.

6 SSH Access

By default, SSH access is disabled:

```
management/ssh/enabled=0
```

However, once enabled, the IP phone can be accessed from any IP address.

To limit access to the device over SSH, you need to enable the SSH whitelist feature as specified in Section 2, Limit Access to the IP Phone.

7 Client Certificates for Mutual Authentication

The initial TLS communication between the IP phone and the authentication server, provisioning server or SIP server, can be authenticated both ways.

By using a pre-defined client certificate and a server Root CA, both sides (client and server) authenticate each other during the TLS handshake.

Uploading a server's Root CA to the IP phone – Root CA for authenticating the server can be uploaded or provisioned to the IP phone.

Uploading a Client certificate and private key can be done for three session contexts – 802.1x, SIP and provisioning server.

For more details see the *Administrator's Manual,* section *3.4.3 Managing Security Certificates*.

8 Server Certificate Validation

Server Certificate validation for secured HTTPS communications over SSL, configured via the configuration file parameter 'security/SSLCertificateErrorsMode', decreases vulnerability to breaches of security.

If validation fails after installing phone firmware, HTTPS communication with Skype for Business and EWS servers are impacted, including but not restricted to Skype for Business auto-discover, contacts search, EWS auto-discover, Outlook Calendar, Authorization, etc.

The certificate is verified in two steps:

1. The Root CA is installed using DHCP Option 43, LDAP or the Web interface.
2. The server's hostname is validated; for each certificate in the chain, the 'issuer' field in the certificate must match the 'subject' field of the issuer (uppermost in the chain) certificate. Backward compatibility is supported. To implement backward compatibility, the configuration file parameter 'security/SSLCertificateErrorsMode' must be changed from the default to **Ignore**:
   - SSLCertificateErrorsMode = **Disallow** (default); TLS connection will be rejected and the phone will not communicate with the server.
   - SSLCertificateErrorsMode = **Ignore** (allows backward compatibility though vulnerability will increase); the phone will proceed without checking the received certificates and without any notifications.

For more details on TLS and managing device certificates, refer to *LTRT-11330 400HD IP Phones Certificate Management Configuration Note*.

9 Editing TLS Cipher Suites

Cipher suites used by the phone for a TLS session can be edited via the parameters below:

- voip/signalling/sip/tls_cipher_list=
- voip/signalling/sipe/tls_cipher_list=

Note: The above parameters are hidden parameters so they'll not show in normal configuration view. To view hidden parameters, you must log in to the Web interface and in the URL line, replace the string 'mainframe' with 'full_config'.

The cipher list can be edited to exclude unwanted cipher suites. The value is a string value, which follows the openssl cipher list format.

The following example shows the exclusion of several DHE based cipher suites, along with permanent removal from the list of un-encrypted and un-authenticated cipher suites, and list sorting in order of encryption algorithm key length:

```
voip/signalling/sip/tls_cipher_list=ALL:!DHE-RSA-AES256-GCM-
SHA384:!DHE-RSA-AES256-SHA256:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-
GCM-SHA256:!DHE-RSA-AES128-SHA256:!DHE-RSA-AES128-SHA:!DHE-RSA-
3DES-EDE-SHA:!DHE-RSA-DES-SHA:!DHE-RSA-EXPORT-DES40-
SHA:!aNULL:!eNULL:@STRENGTH
voip/signalling/sipe/tls_cipher_list=ALL:!DHE-RSA-AES256-GCM-
SHA384:!DHE-RSA-AES256-SHA256:!DHE-RSA-AES256-SHA:!DHE-RSA-AES128-
GCM-SHA256:!DHE-RSA-AES128-SHA256:!DHE-RSA-AES128-SHA:!DHE-RSA-
3DES-EDE-SHA:!DHE-RSA-DES-SHA:!DHE-RSA-EXPORT-DES40-
SHA:!aNULL:!eNULL:@STRENGTH
```

For more details regarding cipher suite format, refer to:
https://www.openssl.org/docs/man1.1.0/man1/ciphers.html

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

AudioCodes Inc.
200 Cottontail Lane,
Suite A101E,
Somerset, NJ 08873
Tel: +1-732-469-0880
Fax: +1-732-469-2298

Contact us: https://www.audiocodes.com/corporate/offices-worldwide
Website: https://www.audiocodes.com/

Document #: LTRT-11311