ReVeal

Data Download Guide.

Instructions on how to extract your data from your specific system

Faster. Smarter. More

Pure IP
Just voice.

The purpose of this document is to define the Vendors and Systems that support a backup export so that a Pure IP portal can give customers a dropdown menu to select the system which they want to upload a config for in order to get a PB Audit performed.

In addition, once the system is identified, the Pure IP Portal will provide the customer instructions on how to get the information we require.

SYSTEMS THAT SUPPORT BACKUP

These systems below can be audited from backups with step by step instructions:

VENDOR	MODEL	INSTRUCTIONS
Alcatel	OmniPCX	Here
Asterix	FreePBX	Here
Avaya	IP Office	Here
Cisco	Unified Communications Manager (CUCM)	Here
Mitel	MiCollab	Here
Mitel	MiCC	Here
Nortel / Avaya	Business Communications Manager (BCM)	Here
Siemens / Unify	HiPath / HiCom	Here

These systems below can be audited via backup, but require additional intervention or steps:

- BT – MIT usually engage professional services to assist export and import since there are no easy mechanisms.
- Microsoft - we need to share a script with the customer to run.
- Siemens/Unify Openscape – complex procedure requires manual engagement.
- Avaya – Software needs to be shared for the customer to run to gain the information.

VENDOR	MODEL	INSTRUCTIONS
BT	CS2K	Here
Microsoft	Lync / Skype for Business Server (SFB)	Here
Siemens / Unify	OpenScape OSV	Here
Avaya	Communications Manager	Here

ALCATEL OMNIPCX

The standard tab format from an Alcatel OmniPCX appears as follows:

This can be obtained from an SSH shell as follows:

/usr/bin/rsh -l swinst localhost /DHS3bin/soft_install/bin/bck -save mao-acc 1>output.txt 2>&1

The output should appear like this:

```
1   Users
2       Node    Directory Number    Directory name  Directory First Name   Location Node
3       BTA-053 6505311 FAX MF 11   BST 5053    15  1   5   0    ANALOG  15  Default     None
4       BTA-053 6505312 DIR BALC 12 BST 5053    15  1   2   0    4020    0   Default     None
5       BTA-053 6505313 SUBDIR BA 13    BST 5053    15  1   2   1   4004    0   Default
6       BTA-053 6505315 GESTOR 15   BST 5053    15  1   2   3   4004    0   Default     None
7       BTA-053 6505316 ASSISTENT 16    BST 5053    15  1   2   4   4004    0   Default
8       BTA-053 6505320 SALA MF 20  BST 5053    15  1   2   7   4020    0   Default     None
9       BTA-053 6505324 B OFFICE 24 BST 5053    15  1   2   2   4004    0   Default     None
10      BTA-053 6505325 GESTOR 25   BST 5053    15  1   2   5   4004    0   Default     None
11      BTA-053 6505327 GEST TECN 27    BST 5053    15  1   5   1   ANALOG  15  Default
12      BTA-053 6505329 ALARME 29   BST 5053    15  1   5   2   ANALOG  15  Default     None
13      BTA-053 6505339 COF FORT 39 BST 5053    15  1   2   6   4004    0   Default     None
14      BTA-053 6505349 GST ALARM 49    BST 5053    15  1   5   3   ANALOG  15  Default
15
16  Progr.Keys
17      Node    Users   Key No. Function    Content Directory Number    Key Number  Second 1
18      BTA-053 6505312 1   Not Assigned
19      BTA-053 6505312 2   Not Assigned
20      BTA-053 6505312 3   Not Assigned
```

ASTERIX FREE PBX

The backup/information required is the contents of the Asterisk config folder, which contains a number of .conf files as shown below.

adsi.conf	02/02/2018 16:22	CONF File	1 KB
agents.conf	02/02/2018 16:22	CONF File	3 KB
ais.conf	02/02/2018 16:22	CONF File	3 KB
alarmreceiver.conf	02/02/2018 16:22	CONF File	3 KB
alsa.conf	02/02/2018 16:22	CONF File	4 KB
amd.conf	02/02/2018 16:22	CONF File	1 KB
app_mysql.conf	02/02/2018 16:22	CONF File	2 KB
asterisk.adsi	02/02/2018 16:22	ADSI File	4 KB
asterisk.conf	02/02/2018 16:22	CONF File	4 KB
astmanproxy.conf	02/02/2018 16:22	CONF File	4 KB
astmanproxy.users	02/02/2018 16:22	USERS File	39 KB

Follow these instructions to export the required files:

♦ Download WinSCP from here: - https://winscp.net/eng/index.php
♦ Connect to Asterisk-based server using SSH credentials, but select "SCP" as the protocol
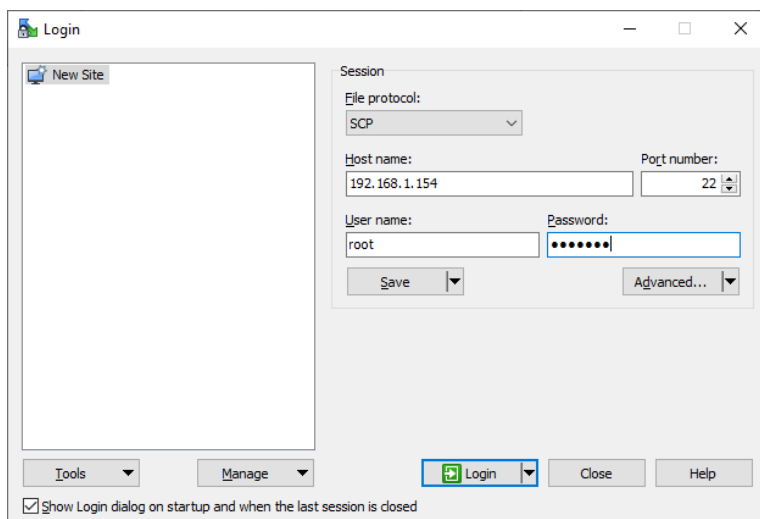
♦ This will land you at /root/ in the right hand pane. Navigate to /etc/asterisk/
♦ Download ALL the .conf files to a folder on your local system
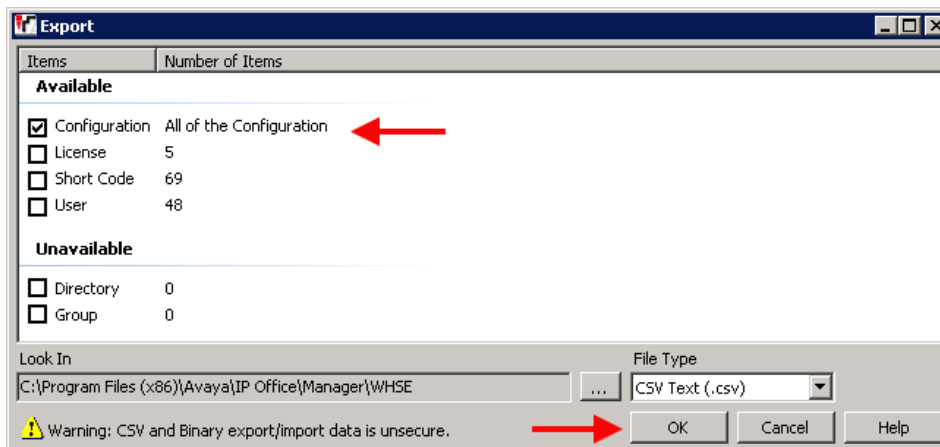
AVAYA IP OFFICE

Perform a backup as described below:

- ◆ Login to IP Office Manager
- ◆ Click on File ➤ Import/Export ➤ Export...
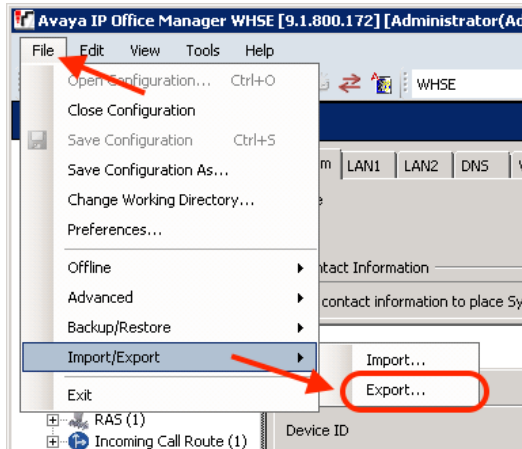
- ◆ Select the Check Box for All of the configuration, and click OK.

BT CS2K

Complex process which requires professional services to extract and import.

Contact the Pure IP team for assistance.

CISCO CUCM & UNITY

CUCM Export:

◆ In order to perform the CUCM BATS backup you will need 'ccm user' access to the Cisco CUCM web portal – however, if there are any issues with the backup job running, you may also need 'admin' access to ensure that services are running.

◆ Login into the "Cisco Unified CM Administration" portal from a Web Browser, note: Firefox is recommended for older Cisco CUCM's due to HTML compatibility issues on other browsers.

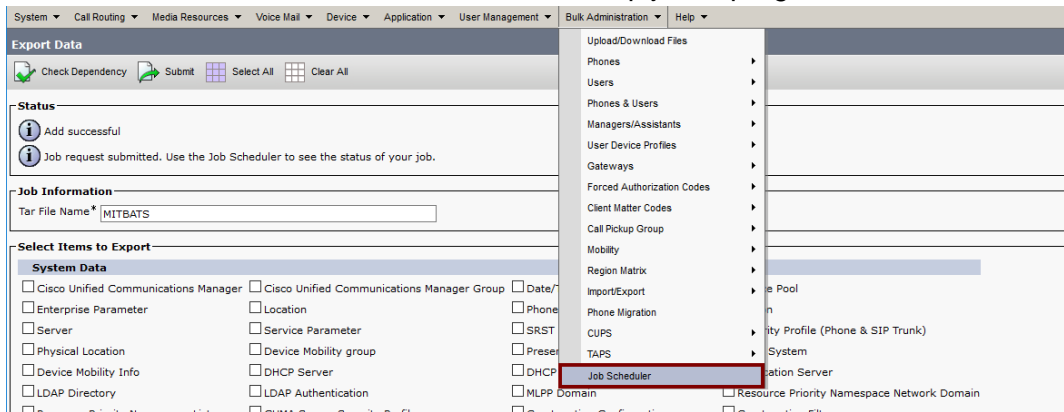◆ Select the "Export" function from "Bulk Administration" in the top menu
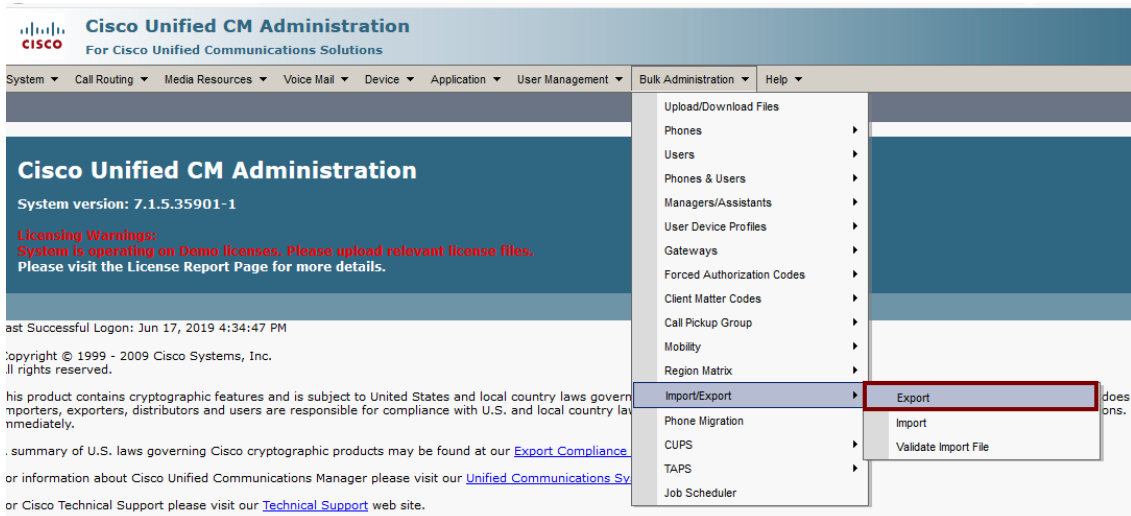
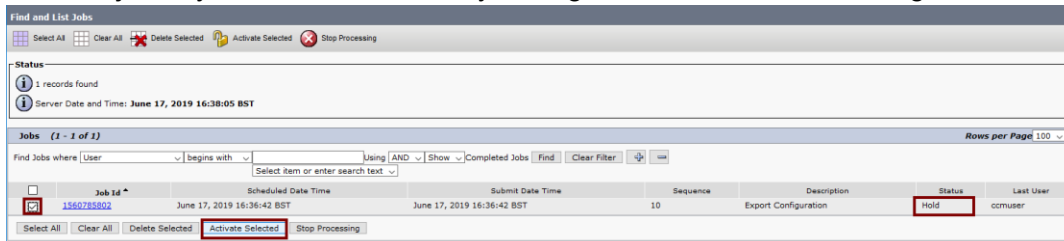◆ Enter a suitable name for the backup and press "Submit"
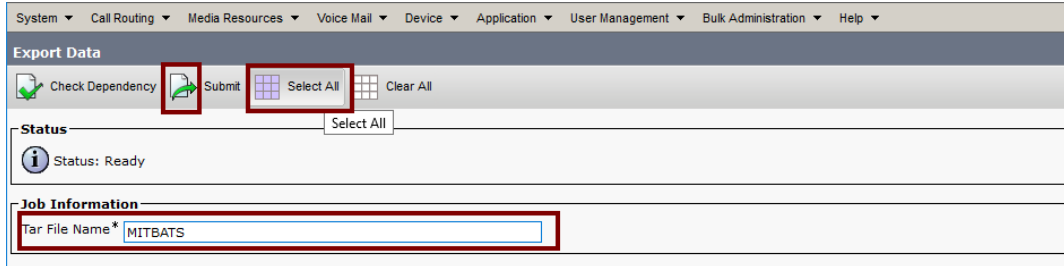
◆ You should see the following message appear in the status panel
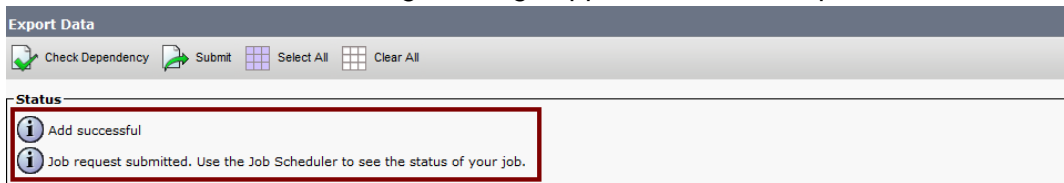
◆ Go to the Scheduler to ensure that the backup job in progress
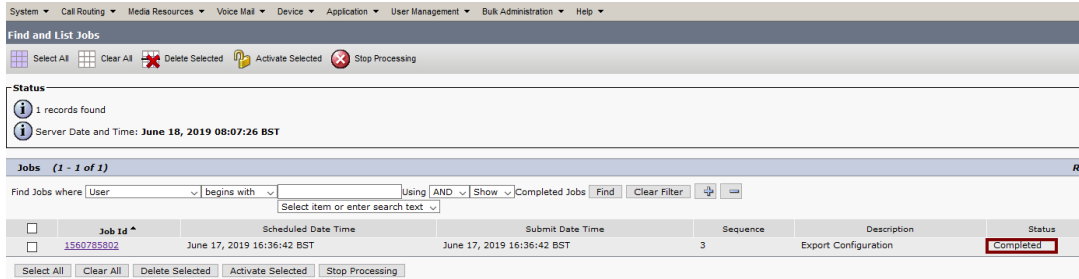

◆ If the job says "Hold", activate it by ticking the checkbox and clicking on "Activate Selected"

◆ If the job appears to get stuck on "Pending", us the "Cisco Unified Serviceability" interface and ensure that the AXL, BPS and TAPS services are all activated (Note: this requires Admin access)
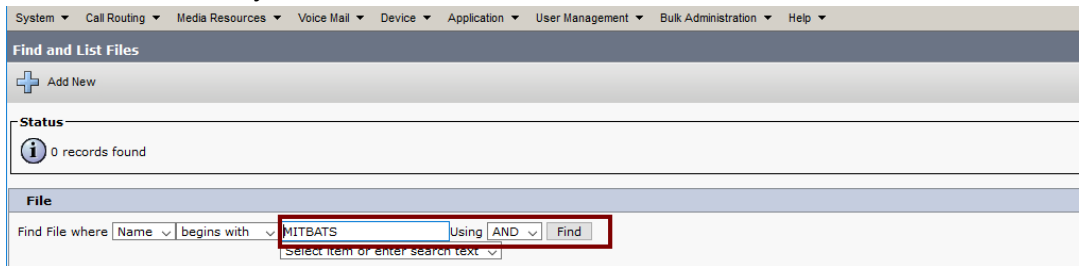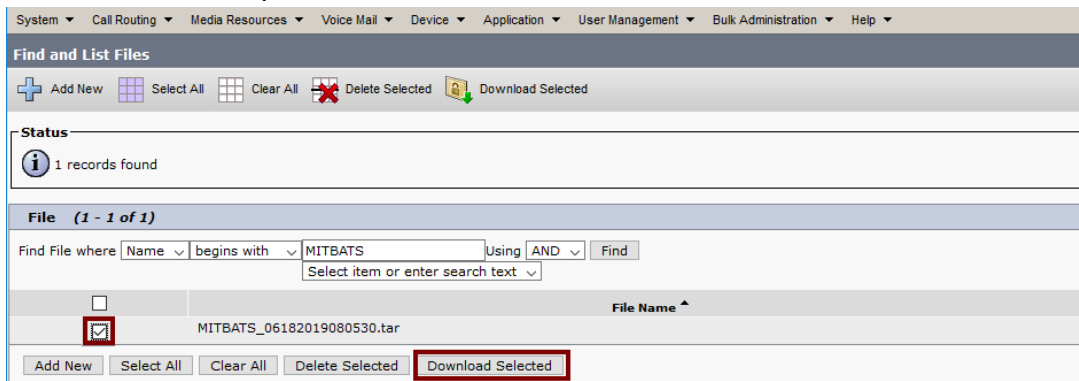
◆ When completed, the status will change

◆ Select "Upload/Download" files in the "Bulk Administration" menu.
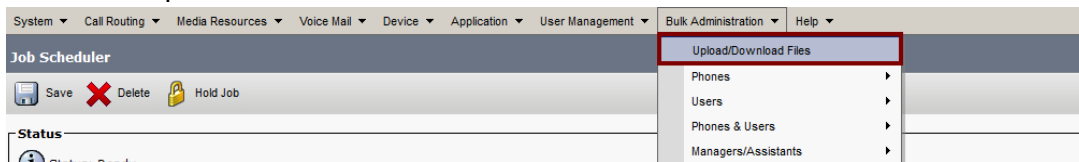
◆ Enter the name you entered earlier and click on "Find"
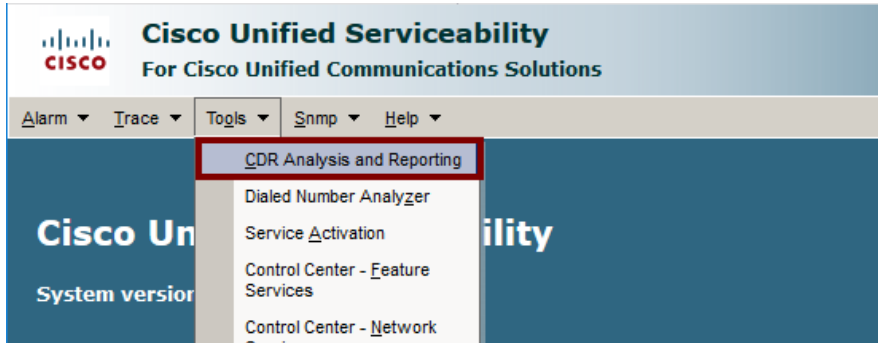

◆ Select the backup and click on "Download Selected"

◆ Finally, save the file on your local system ready for the audit.

CDR Export

♦ Login into the "Cisco Unified Serviceability" portal from a Web Browser, note: Firefox is recommended for older Cisco CUCM's due to HTML compatibility issues on other browsers.
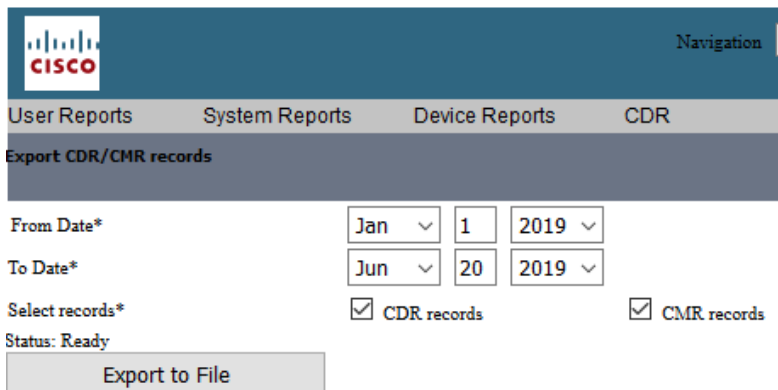

♦ Then select "CDR Analysis and Reporting" from the "Tools" menu.

♦ This will open a new window, select "Export CDR/CMR" from the "CDR" menu
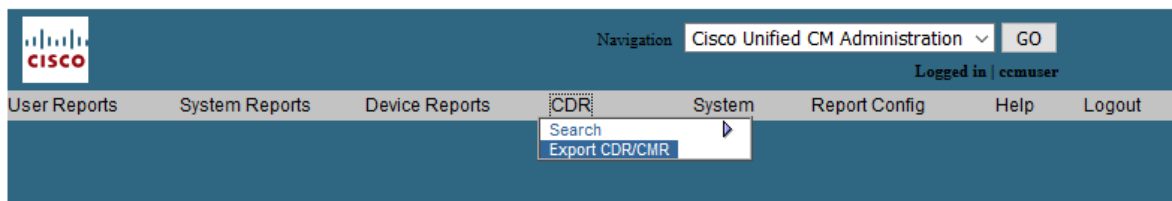
♦ Select the date range (ideally more than 3 months) and click "Export to File"

◆ This will then display the following:

◆ Right-click and save both files then click on "Close"

Unity Connection Export

◆ Navigate to the Administration tools within the Cisco Unity Tools
◆ Open Bulk Administration Manager.
◆ On the Cisco Unity Connection Bulk Administration Manager Welcome page, click Next.
◆ On the Select Operation screen, click Export.
◆ Click Users With Voice Mail (Subscribers), and click Next.
◆ In the Output File field, enter the full path to the applicable file.
◆ Click Next.
◆ On the Select Criteria to Use for Exporting screen, select the all users option
◆ Click Next to begin the export. The Summary page displays the results when the operation has completed.
◆ To view the export CSV file, click View Export Objects File.
◆ Click Finish.

MICROSOFT LYNC / SKYPE FOR BUSINESS

We need to provide you with a PowerShell script to be run on your Front End server which compiles a number of CSV files which then need to be provided to perform the audit.

To audit an on-premise Skype-for-Business or Lync server, you will need to run the LyncDataCollector.ps1 script provided. You will need admin/domain privileges elevated PowerShell prompt.

MITEL MICOLLAB MICC

Backups are achieved through importing standard 'backups' which can be downloaded through the MiCollab and MiCC web portals.

The backups are a Standard MSL Server backup and are .tgz format.

The MiCollab and MiCC backup are obtainable via the server manager using the below instructions (Taken from the MiCollab Installation and Maintenance Guide, please refer to the latest version available online for up to date instructions)

- Log into the Administrator portal (server manager).
- Under Administration, click Backup.
- Select the Backup to desktop option.
- Click Perform. MSL prepares the system for backup and displays the following:
- The "Operation status report" with the estimated backup size. Ensure that your browser and target file system support downloads of this size.
- The "Backup Encryption" option.
- Click Download Backup File.
- When prompted to Open or Save, click Save.
- In the file download window that appears:
- Name the file and then select the location where the file will be saved.
- Click Save.
- In the Download Complete Window, click Close

NORTEL AVAYA BCM

The BCM audit can be imported from either an Excel config file that looks like this:-

Use the BCM Configuration Tool and then select the **Backup to Network Folder** and provide a network path (including folder), e.g. \\IP_of_WinServer\BCM, the username and password, and leave the directory option blank.

SIEMENS UNIFY HIPATH HICOM

HiPath's can be audited from what is called a "Regen" or "LastLoad" file. Both are .txt files and look something like this:

```
 1   A001
 2   C001 *P30252B4500B00108P30252B4500B00108P30252B4500S00108
 3   M2 1 ADD-CODEW:6RB31VUFA4FPJT7KUVPX78PKDPPCWKPB3D1R4YGMK79DX6PXVTL8HHG44KN81ZTZ,M2HA
 4   M2 1 ADD-ANSU:SYSNO,"L31999W2041X00001","ZDBCCDSF";
 5   M2 1 ADD-ANSU:SYSNO,"L31999W2041X00001","ZDBCCDS1";
 6   M2 1 ADD-ANSU:SYSNO,"L31999W2041X00001","ZDBCCDS4";
 7   M2 1 ADD-DIMSU:ADMCC,2000,2000;
 8   M2 1 ADD-DIMSU:ADMLTG,800;
 9   M2 1 ADD-DIMSU:APPLICAT,98,5,1,200,3000,256,128,256,128,1500,512,300,900,300,256,320
10   M2 1 ADD-DIMSU:BASIC,4000,4120,4000,2000,8,200,1200,2,0,20,480,120,1000,200,3000,368
11   M2 1 ADD-DIMSU:NETWORK,3,400,400,1200,1024,200,1000,500,1000,16,400,50,120,0,0,1500,
12   M2 1 ADD-DIMSU:SYSTEM,900,300,1,4,4,128,4,20,40,4,8,40,1000,1000,0,0;
13   M2 1 ADD-DIMSU:USER,4000,800,2000,600,2800,16,1500,800,4000,500,4000,400,4000,4000,4
14   M2 1 CHA-SIPCO:DIFFSERV,48,72,N,0,AUTONEG,16384;
15   M2 1 CHA-SIPCO:TIMING,60,60,4,0,60;
16   M2 1 CHA-SIPCO:PLQUAL,200,120,3,2;
17   M2 1 CHA-SIPCO:BANDW.1.83.;
```

- ♦ You can use the HiCom management tool for this, or using "Comwin" run the following commands:
- ♦ When complete go into file transfer (6th Icon from Left Hand Side on Comwin)
- ♦ Click on the 2nd Icon down on the left-hand side (A1H1F)
- ♦ Find the L31905 Folder - go into that folder and you will find an 'ALL' File
- ♦ Drag a copy out to your computer.

SIEMENS UNIFY OPENSCAPE OSV

At present this is only supported by professional services engagement. A number of data files are required from the OSV in order to process the audit. Please contact the Pure IP team for details.

- ♦ CSV exports for each 'location' in the following format:

```
Directory Number;External Number;Display Name;Feature
Profile;Keyset;Numbering Plan;Business Group;Branch Office;Language;Displayed
Extension Number;Rate Area;Class Of Restriction;Calling Location
Code;Transport Protocol;IP Address;Associated Endpoint

'441245112233';'441245112233;Bloggs,
Fred;;Phantom;np_uktest;IFF;bo_uktest;System
Default;;ra_uktest;;;TCP;10.10.148.223;ep_ uktest1000;
```

- ◆ CSV of Mediatric Servers in following format:

```
IP,HOSTNAME,MODEL,VERSION
10.10.148.11,uktest4124-4,Mediatrix 4124,2.0.40.747
```

- ◆ CSV of hunt groups in following format:

```
Hunt Group Name;Pilot DN;Hunt Type;Status;Stopped;Hunt Group Members
UK Test; '44124599887766';Manual;;false;441245112233,441245909090'
```

- ◆ An "Export All" txt file of this type:

```
#INFO: Host Name: <uktestsvn1>
#INFO: Software Version: <V9R3.34.16>
FILE VERSION:11.00.01:MP2
#INFO: Export of RTP Parameter Data Started on <2019-04-18 15:04:08>
```

- ◆ A 'Configuration script' for each Mediatix Gateway in the following format:

```
#################################################
# Configuration Script.
# Automatically generated on 29/04/2019 14:53:15.
#################################################
# System Name        : Mediatrix C733
# Firmware           : Dgw 2.0.40.747
# Profile            : CXXX-MX-D2000-128
# MAC Address        : 0090fxxxxx
# Serial Number      : 00281xxxxxxxxx
# Description        : Automatically generated on 29/04/2019 14:53:15.
#################################################
```

AVAYA COMMUNICATIONS MANAGER

There is currently no support for Avaya CM auditing via Backup however we do support an additional alternative access method to facilitate a quick audit process.

A standalone applet can be provided to the customer, maintainer or placed directly on a PC, laptop or server which has network access to the Avaya CM.

- ♦ This applet can be run from a command line:
- ♦ Audit.exe Avaya -i "IP Address of Avaya" -u "username" – p "password" -o "avaya.bin"

Switches are explained below:

-i - IP address of the main Avaya CM should added here replacing the information in quotes above

-u - Username of the ASA login (See section 2 for the exact credentials required)

-p - Password of the ASA login (See section 2 for the exact credentials required)

-o - This can be change to any name .bin, this will be where the information collected is output to.

An example command line may look like:

Audit.exe Avaya -i 192.168.1.2 -u admin -p password -o avaya.bin

Further information on the commands can be found directly in the tool using -help command