Mitel Setup

Chris Lane & Vo Nguyen
8-20-2019

Contents

1. Introduction:

This document describes the process for setting up your Mitel Phone system to record calls and perform call analytics using the CallN Call Recording service.

2. Prerequisites

The Mitel environment must the following:

- ❖ MSL 10.5.15+ server
- ❖ Mitel Border Gateway (MBG) version 8.0+ / Secure Recording Connector (SRC) protocol 1.3
- ❖ MiVoice Business (MiVB) 8.0 or greater
- ❖ Open Integration Gateway (OIG) 4.1 (protocol Version 1.1) with standard call control

- ❖ Appropriate licensing for Recording Taps. A Recording Tap license will be used for each concurrent call that is being recorded.

- ❖ Station calls for recording are routed through the SRC\MBG Server.

- ❖ Windows Communication Foundation and Window Identity Foundation
- ❖ For more details of compatibility please refer to OIG Engineering Guideline.

CallN Monitors using OIG supports the following Mitel call manager platforms:

- ❖ MiVoice Business on
    - o 3300 ICP, MXe II and MXe III
    - o 3300 ICP, CX and CX II
    - o 3300 ICP, CXi and CXi II
- ❖ MiVoice Business for Industry Standard Servers
- ❖ MiVoice Business Virtual

You will also need a computer to load the CallN VoIP Recording Client. This can be a physical or virtual computer and must be running Windows 7 or higher or Windows Server 2012 or higher and .Net 4.8 or higher. The computer must be part of the same domain as the Mitel Environment or in a trusted domain of the Mitel Environment. You will need to have signed up to CallN or have a trial account as you will need a CallN Portal to store calls.

3. How your calls are recorded

The computer needs to have the CallN VoIP Recording Client installed. The CallN client connects to the Mitel Environment by creating an SSL tunnel through to the Mitel SRC Server. This allows for the recording of the call traffic. A similar connection is opened to the OIG Server where TAPI information for calls is collected. The TAPI information contains call data, such as the numbers involved and direction of the call. The TAPI information and the recorded call are then uploaded to your CallN portal where the call will be displayed for playback and reporting.
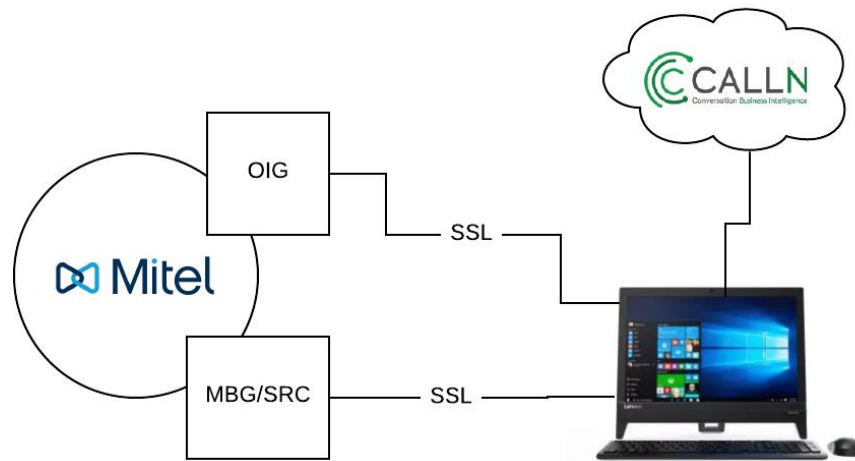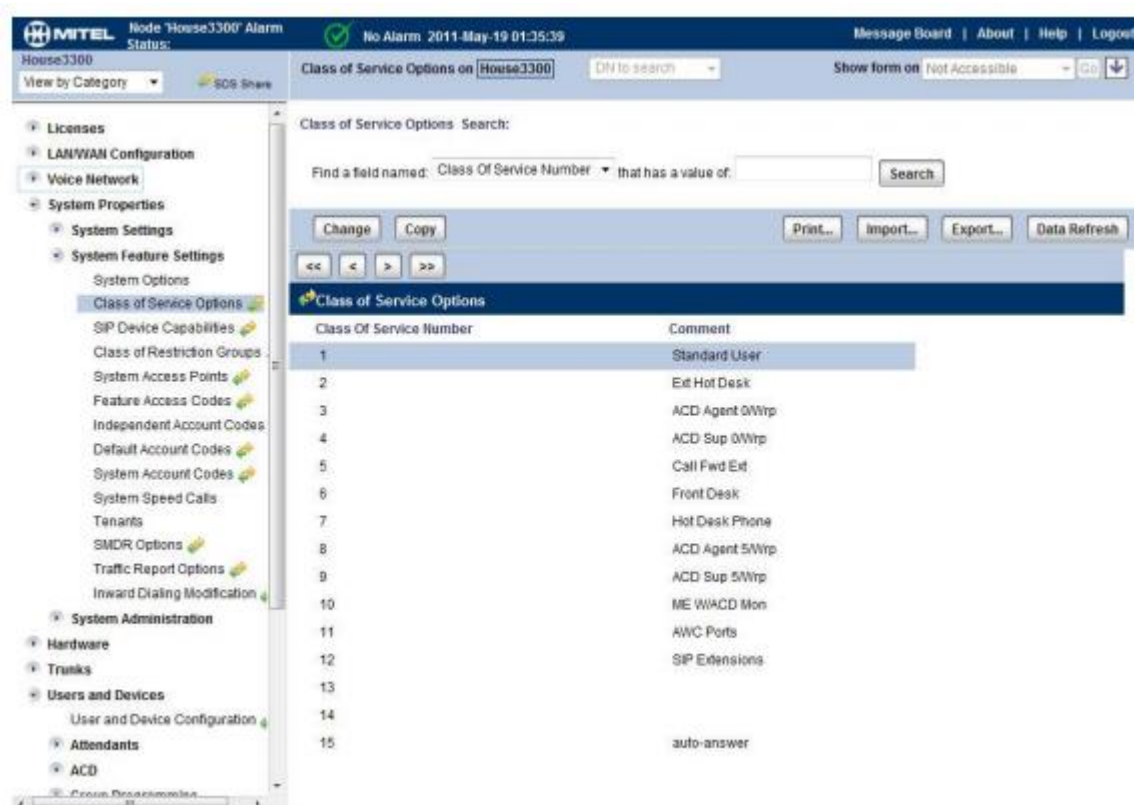
4. TAPI Configuration

TAPI is part of the OIG setup and is require so that the metadata for the recorded call is passed through to your CallN Portal. This is done by altering the Class of Service (COS) of the handsets to be recorded.

Connect to your Mitel PBX system.

Expand the System Properties folder, then expand the System Feature Settings.
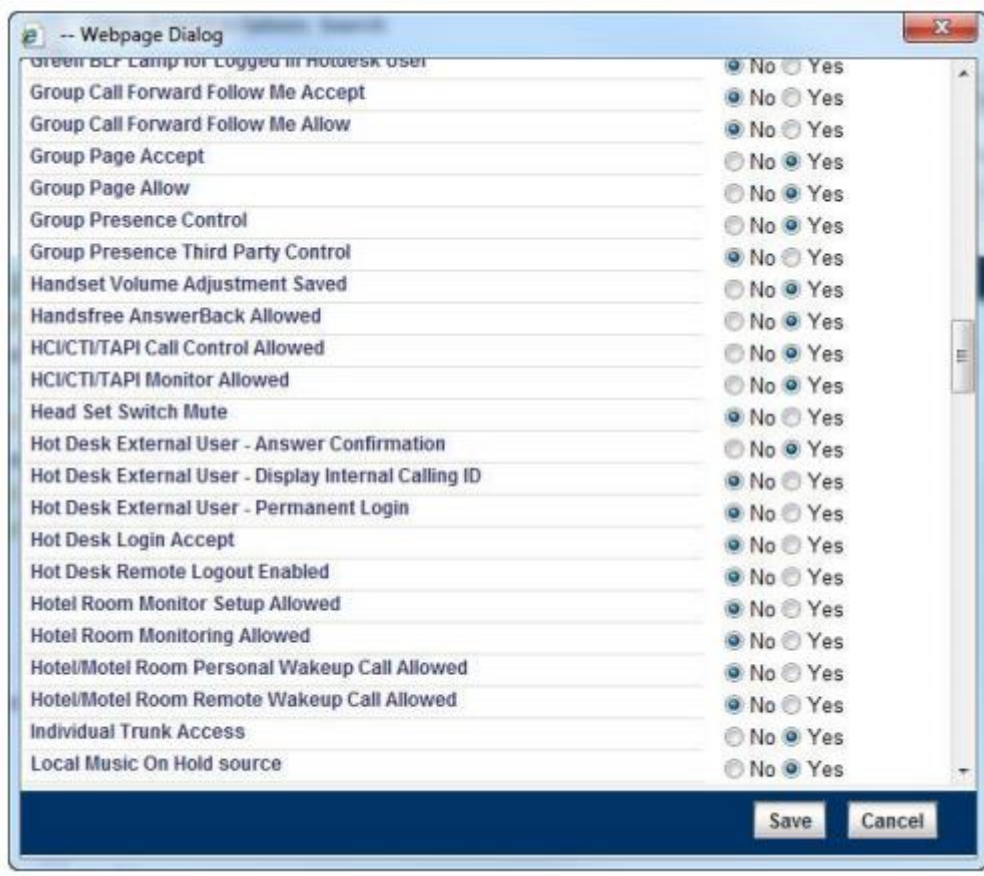
Select Class of Service Options.

Verify each of the **Station COS Assignments** have "Yes" checked for the following:

- o   HCI/CTI/TAPI Call Control Allowed
- o   HCI/CTI/TAPI Monitor Allowed

Save any changes made.

5.   Certificate Approval

Approval of the certificate can be done via the SRC/MBG server. Once the SSL connection to the CallN Client is established, a certificate is created and must be approved.

Approving the certificate through the MBG/SRC, log on to the MBG/SRC server web page.

Under **Security**, click **Certificate Management**. Certificate requests waiting for approval appear under the heading **Queued CSRs**.

Click the **Certificate ID** link.

After confirming the requester, do one of the following:

- Click **Cancel** to return to the Certificate Management main screen without approving/rejecting the request.

- Click **Approve** to approve the CSR.
  Note: The approved CSR is listed as a certificate under the heading **Approved Certificates**. It can take up to two minutes for the approved certificate to appear.

- Click **Reject** to remove the CSR from the list.
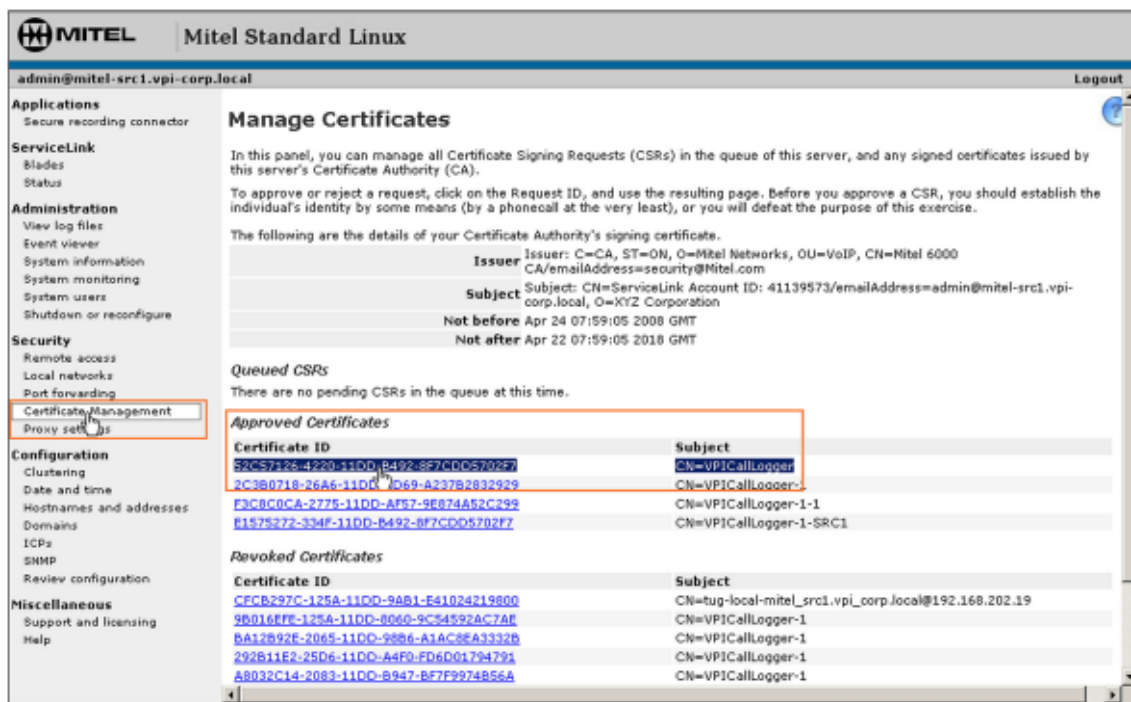
6. Loading the CallN Client

On the recording computer, download the latest CallN client from the CallN web site. (**https://calln.com/support/windows-thin-client-downloads/**)

Install this onto your computer. You will be prompted to enter you CallN portal domain name, a CallN username and the associated password once installation is complete.
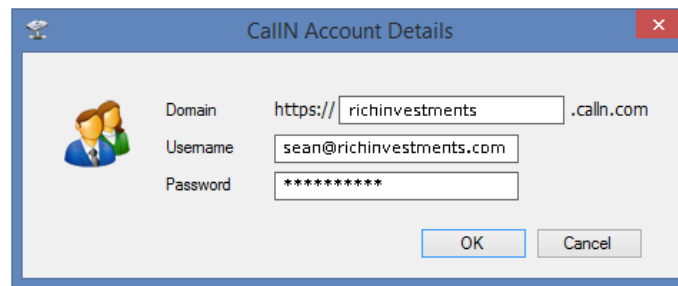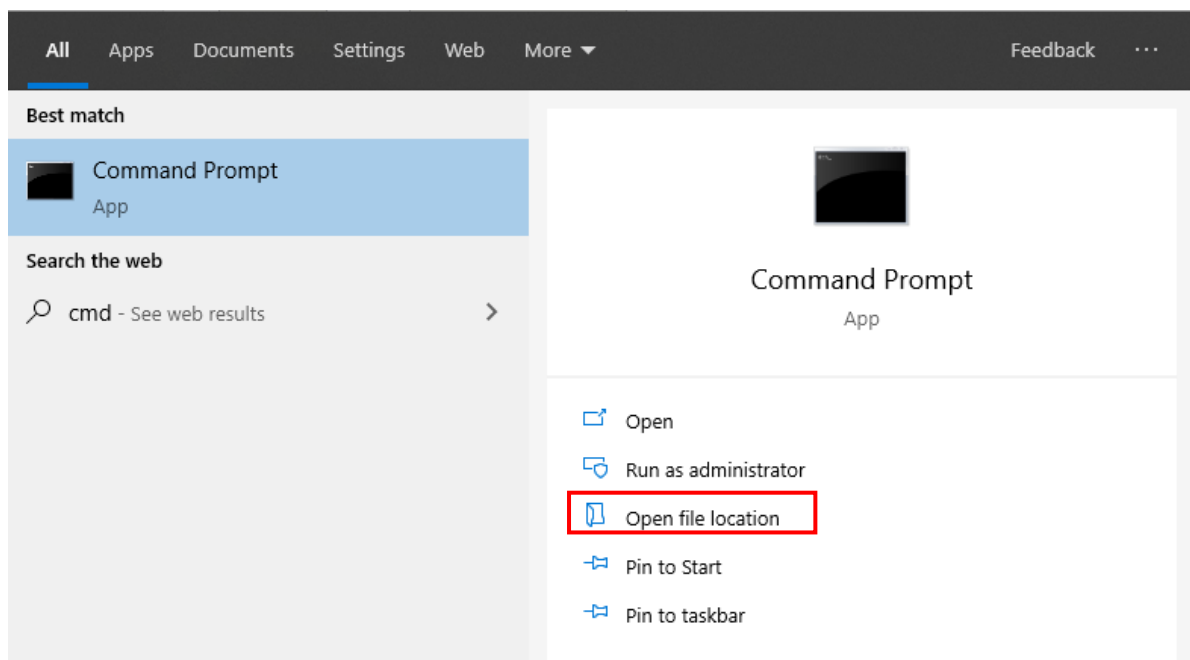
Select ok to save the details.

7. Create certificate and bind port

In order to retrieve the TAPI information securely from OIG, you will need to create SSL certificates and binding to specific port.
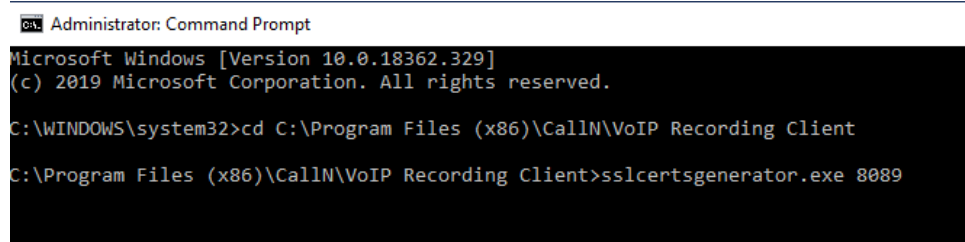
Open a command shell on the recording computer in Administrative Mode.

Navigate to C:\Program Files (x86)\CallN\VoIP Recording Client.

Run the following command to create the certificates and binding to port 8089
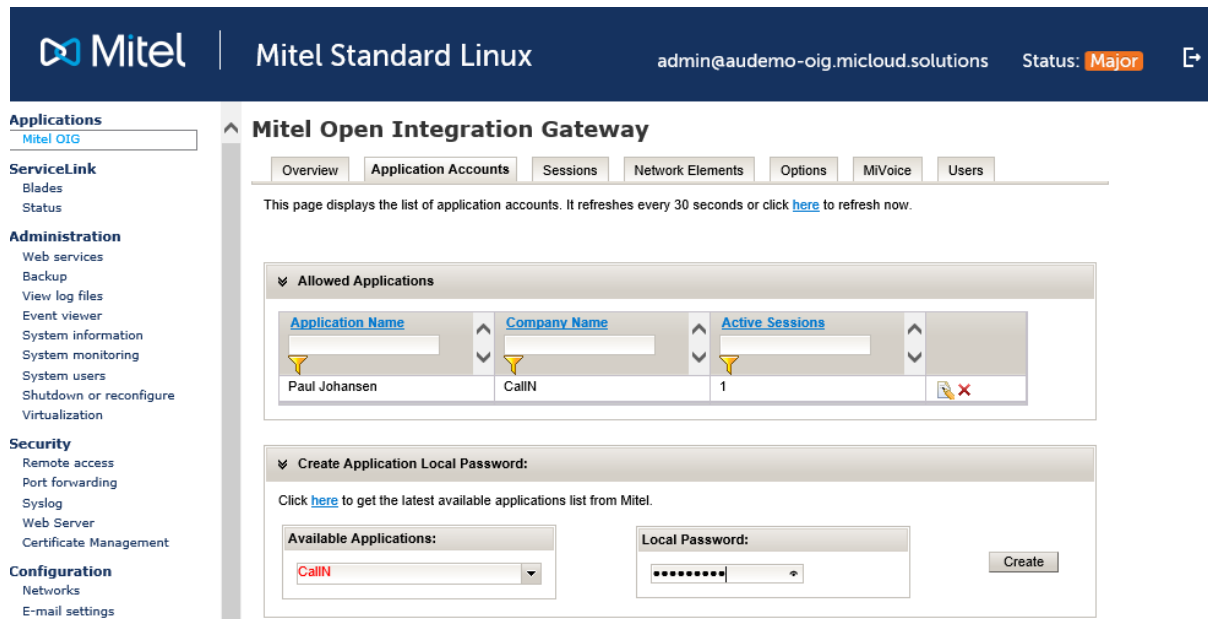
SSLCertsGenerator.exe 8089

To remove the certificates and binding to port 8089 run the following command

SSLCertsGenerator.exe remove 8089

8. Create Local Password

From a Web Browser, connect to your MSL Service. From the menus on the left, select Mitel OIG.

Under the "Create Application Local Password":

- ❖ Set "Available Applications" to CallN
- ❖ Set a Local Password and click Create.

Take not of the created password as you will need it to configure the CallN Client.

9. Configuring CallN Client

From the system tray, double click the CallN tray icon to open the configuration page. The Tray icon is hidden, select ^ to reveal hidden icons.

Select the Network Tab.

With the Mitel integration, you can only monitor one port. In the Adapters section, change from the default setting of "All" to "Only the selected adapters". Select the local ethernet port of the recording computer as the only monitored adapter.
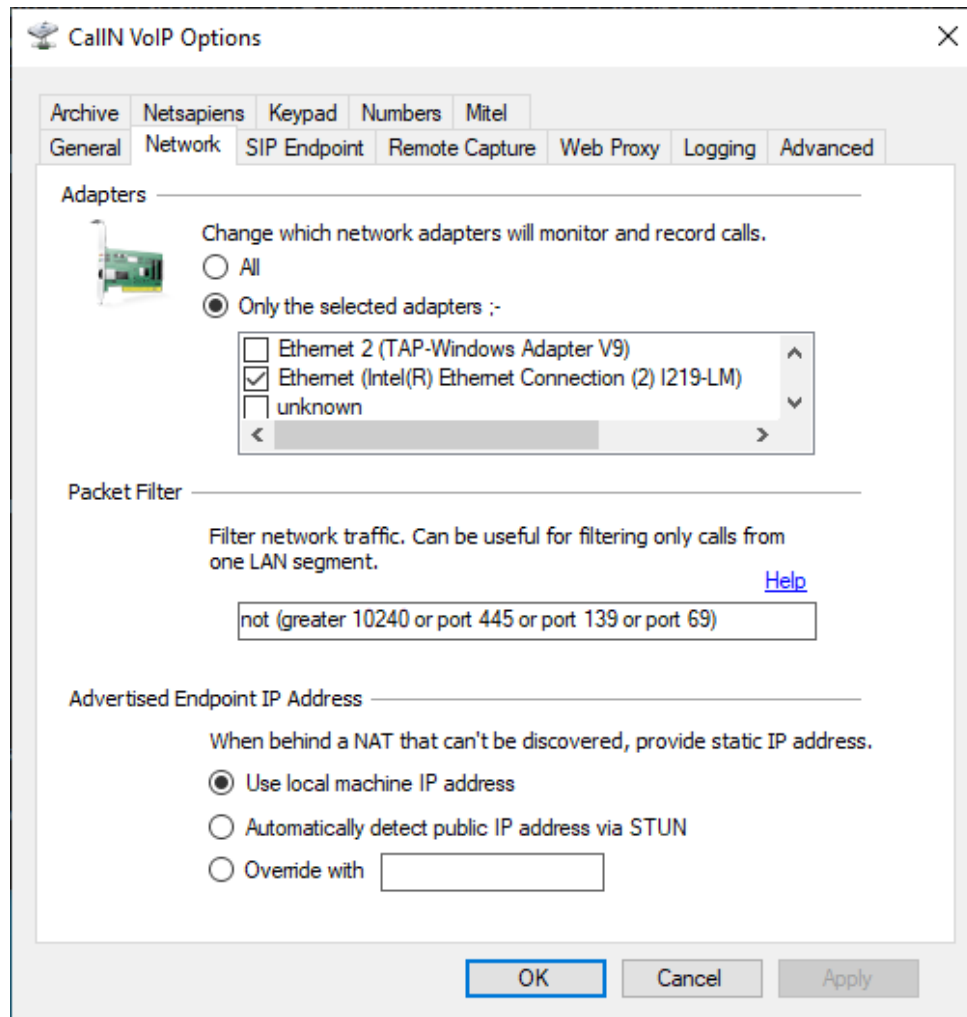
Move to the Mitel Tab.

Input the IP address for the follow:

- ❖ MiSSL Tunnel Endpoint IP address. This is the same as the MGB/SRC. The port is not required.

- ❖ Mitel SRC IP address. This is the IP address of the MBG/SRC. A port is necessary for this entry, with the default being port 6801. If another port has been configured within the SRC, this will need to be changed to the new value.

- ❖ ICP Address is PBX IP address

- ❖ OIG Address is the IP address of the Open Integration Gateway

- ❖ Event handler URL is **https://localhost:8089/EventHandler**

- ❖ Application Name, Application Password, Company name will show default details. These details are shown on the same interface used to create a Local Password.

- ❖ Local Password. This is the password you created in the previous step.

Select OK to save the changes.