

Avaya Switch Configuration

01/10/2024 2:31 pm EST

Setting up Avaya

Configuring the AvayaSwitch.config file

Perform the following steps to configure the AvayaSwitch.config file:

1. Log into the **AES Management Console Administrator** website.
2. Navigate to the **Communication Manager Interface**, and select **Switch Connections**.
3. Get the “**SwitchName**” from the **AES Management Console Administrator**.
4. Replace the existing **SwitchName** in the “**AvayaSwitch.config**” file with the **SwitchName** in the AES Management Console as shown in the following screenshot:

```
<?xml version="1.0" encoding="utf-8"?>
<SwitchConfig xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance" xmlns:xsd="http://www.w3.org/2001/XMLSchema">
  <IPAddressToAESServer>172.16.143.241</IPAddressToAESServer>
  <IPAddressToCMServer>172.16.143.242</IPAddressToCMServer>
  <LoginName>avaya</LoginName>
  <LoginPassword>avayapassword</LoginPassword>
  <IPPortToAESServer>4721</IPPortToAESServer>
  <SwitchName>cmsim</SwitchName>
```

The following text indicates other possible settings for the “AvayaSwitch.config” file:

<IPAddressToAESServer>172.16.143.241</IPAddressToAESServer>

This is the IP address of the Customer’s Application Enablement Server (AES) server.

<IPAddressToCMServer>172.16.143.242</IPAddressToCMServer>

This is the IP address of the Customer’s Communication Manager (CM) server.

<LoginName>BOLDTEST</LoginName>

This is the login name the Customer has programmed for Bold in the Avaya Switch.

<LoginPassword>Boldtest1@</LoginPassword>

This is the password the Customer has programmed for Bold in the Avaya Switch.

<IPPortToAESServer>4721</IPPortToAESServer>

This specifies the port on the AES server on which we should communicate.

<SwitchName>procr</SwitchName>

This is the name of the switch previously discussed in Step 4.

<SessionName>Bold_PBXServer_DEV</SessionName>

This is a name we use when we log into the AES server. It can be anything, but should be used to uniquely identify our application when a user accesses the AES GUI to determine which other users are connected.

<SessionDuration>3000</SessionDuration>

This specifies several milliseconds that an Avaya session stays alive if Bold misses a heartbeat or gets disconnected

from Avaya.

<SessionCleanupDelay>0</SessionCleanupDelay>

This specifies the number of milliseconds that you want Avaya to clean up a Bold session after the "SessionDuration" has expired. This should always be set to "0".

<UseSecureSockets>>false</UseSecureSockets>

This specifies whether you want a secure connection to Avaya at the time of connection. Currently, only the false option is supported.

<EnableAutoKeepAlive>>true</EnableAutoKeepAlive>

This specifies whether the Avaya API should automatically send keep-alive messages to Avaya. This should always be set to true.

<AllowCertificateNameMismatch>>true</AllowCertificateNameMismatch>

This specifies whether you want to continue the connection process if the certificate being used experiences a name mismatch. This should always be set to true.

<ProtocolVersion>http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5</ProtocolVersion>

This specifies the protocol to connect to Avaya. This should always be set to <http://www.ecma-international.org/standards/ecma-323/csta/ed3/priv5>

<SwitchSupportsAllInjection>>true</SwitchSupportsAllInjection>

This specifies whether the user's switch supports ALL injection. If set to true, the user needs to purchase and set up the following feature from Avaya: the "SA8481 Replacing Calling Party Number with ASAI ANI".

<DialAsPriorityCall>>true</DialAsPriorityCall>

This specifies whether you want the phone to automatically dial as a priority call or a regular call.

<Devices>

<DeviceConfig>

<Extension>2223</Extension>

This indicates an extension we are monitoring.

<ExtensionPassword>123456</ExtensionPassword>

This indicates the password for the extension.

<Dependency>Independent</Dependency>

This indicates the type of monitoring being performed. This should always be set to "Independent".

<ExtensionDescription>855-557-1421 192.168.11.62</ExtensionDescription>

This indicates the description of the extension.

<Share>>true</Share>

This setting specifies whether you want more than one application to monitor the extension. If you want more than one application to monitor the extension, then set it to true.

<Instance>1</Instance>

If <Share> is true, then you must specify an instance number. Other applications that want to monitor this device need to specify an instance number, too. Each instance number needs to be unique. Typically, if the user has call recording software, he is monitoring extensions and we need to monitor them, as well. The user must determine which instance the call recording software is using and set the Bold instance number to be different.

</DeviceConfig>

Setting up the Receiver Extensions

Although we know the steps in this section are performed in the Avaya User Interface and are required, we do not have information regarding specifically how to perform these steps. It may be necessary to consult your Avaya representative regarding your specific configuration settings.

Perform the following steps to configure your Receiver settings in the Avaya User Interface:

1. Set up the inbound Receiver extensions as both **SIP and analog**.
2. Set Receiver extensions for **IP Softphone to y**.
3. Set the analog Receiver extensions so that **DNIS** and **ANI** do not send information to the extension between the first and second rings.
4. Enter the **Player Directory** (Server-Media Only) location as the location where **.wav** files reside.
5. Confirm that **no hold music** is set to play when your Receiver lines are placed on hold.
6. Set your **codecs**.