



Avaya Aura[®] Conferencing Quick Start

Getting started on Conferencing

A license for Conferencing

Every instance of Conferencing ships from the factory with a license that covers a grace period of 30 days. After this period, you must formally license the solution. You can obtain a valid license from the Avaya Product License and Delivery System (PLDS) Web site at <https://plds.avaya.com/submitRegistration.htm>. The license is in the format of an .XML file. You must save it to your desktop computer. This license is for the Conferencing product and you install it using Conferencing Manager, not System Platform.

As an aside, licenses are also required for:

- The Windows operating system on the Avaya Web Conferencing (AWC) virtual machine.
- The Windows operating system on the Client Registration Server (CRS) virtual machine.
- The Avaya Web Conferencing (AWC) application, running on the Avaya Web Conferencing (AWC) virtual machine.

Applying a Conferencing license

Every instance of Conferencing ships from the factory with a license that covers a grace period of 30 days. After this period, you must formally license the solution.

Prerequisites

Before you apply a license to your Conferencing server, you must obtain the license from the PLDS Web site.

The purpose of this task is to apply a license to the Conferencing solution.

-
1. Log in to Conferencing Manager by entering the Conferencing Manager virtual machine IP address in a Web browser, as follows:
http://<Conferencing Manager IP address>/SMGR
Some of the fields on the interface refer to Conferencing Manager as SMGR.
By default, the username is `admin` and the password is `admin123`. You can change these username and password settings at any time.
 2. Navigate to **Licenses > Install License**.
 3. At the **Enter License Path** field, click **Browse** and locate the license file which you obtained from the PLDS Web site and saved to your desktop.
 4. Click **Open** followed by **Install** to install the license.
Conferencing Manager installs the license.

Example

The solution is licensed against the MAC address of the Conferencing Manager. The unique index for the license is the LAN MAC address of the Conferencing Manager. You can view the MAC address using System Platform.

Next steps

Now you can configure the Conferencing solution to suit the customer requirements.

Introduction to network information

When you buy Avaya Aura® Conferencing Standard Edition, you receive an Avaya common server with all the required Conferencing software installed by default.

Avaya ships each server with a series of default or dummy IP addresses for each of the Conferencing components. These default IP addresses and hostnames are listed here. You must replace these IP addresses with the IP addresses from the customer site.

Component	Explanation of Component	Default Information
System Platform	This is a generic virtual server software platform.	Dom0 IP address 192.168.11.10 Dom0 Host Name <code>acevms1</code> Cdom IP Address 192.168.11.11 Cdom Host Name <code>acevms1cdom</code>

Component	Explanation of Component	Default Information
Avaya Web Conferencing (AWC)	This is a data conferencing server.	IP Address 192.168.11.15 Host Name xxxawc.avaya.com
Client Registration Server (CRS)	This is a customer booking server.	IP Address 192.168.11.16 Host Name xxxcrs.avaya.com
Application server (bridge)	Within the Conferencing environment, this is called a bridge. It hosts the conference calls.	IP Address 192.168.11.17 Host Name mfg700a.avaya.com
Web Portal	This is a customer booking Web server.	IP Address 192.168.11.18 Host Name xxxweb.avaya.com
Conferencing Manager	This is a central management and configuration console. It enables you to manage and configure the other four virtual machines. Some of the fields on the interface refer to Conferencing Manager as SMGR. It is a good idea to keep this point in mind while you are navigating through the Conferencing installation pages.	IP Address 192.168.11.19 Host Name xxxsmgr.avaya.com

A series of short tasks

It is a good idea to think of the task of updating network information as a series of smaller tasks. There are eight small tasks in total.

For previous versions of Conferencing, Avaya provided the `mx-ipChange.sh` script to manage the process of customizing Conferencing server network information. This script modified the IP address, host name, domain name, netmask, gateway NTP, and the DNS of the server.

For this release of Conferencing, you can make changes to the IP addresses and hostnames of the virtual machines in your network using System Platform. Each of the virtual machines running on an instance of System Platform, must belong to the same subnet.

System Platform has two IP addresses or points of access. The browser access to System Platform is sometimes called Customer/Console Domain (Cdom). The access to the base operating system of System Platform is sometimes called Domain 0 (Dom0).

The other virtual machines that make up the Conferencing solution include:

- An application server

Within the Conferencing environment, this is called a bridge.

- A central management console

Within the Conferencing environment, this is called Conferencing Manager. It enables you to manage the other four virtual machines. Some of the fields on the interface refer to Conferencing Manager as SMGR. It is a good idea to keep this point in mind while you are navigating through the Conferencing installation pages.

- A data conferencing server

Within the Conferencing environment, this is called Avaya Web Conferencing, or AWC.

- A customer booking server

Within the Conferencing environment, this is called a Client Registration Server or CRS.

- A customer booking Web server

Within the Conferencing environment, this is called Web Portal.

If you do not have network connectivity to the System Platform virtual machine, you must use a crossover cable and a terminal emulator application called PuTTY to access System Platform. PuTTY is a Linux SSH client that allows you to connect to other machines, giving you a terminal window. You can download PuTTY from <http://www.chiark.greenend.org.uk/~sgtatham/putty/download.html>.

The eight steps

The eight tasks that are required to change the IP and hostname of Conferencing are as follows:

- Updating network information on System Platform
- Verifying network information on System Platform
- Verifying connectivity
- Updating network information on Conferencing Manager
- Updating information on the CRS virtual machine
- Making changes to date and time
- Verifying the management servlet on the application server (bridge)
- Manually restarting the Avaya Management Service on AWC

Related topics:

[Updating network information on System Platform](#) on page 5

[Verifying network information on System Platform](#) on page 8

[Verifying connectivity](#) on page 9

[Updating network information on Conferencing Manager](#) on page 11

[Updating information on the CRS virtual machine](#) on page 12

[Making changes to date and time](#) on page 13

[Verifying the management servlet on the application server](#) on page 15

[Restarting the Avaya management servlet on AWC](#) on page 15

Updating network information on System Platform

This is the first task.

Prerequisites

Create new IP addresses and/or hostnames and make a note of them. You require seven IP addresses for each deployment of Conferencing.

The purpose of this task is to update the IP and hostname details of the Conferencing instance on System Platform.

-
1. If you do not have network connectivity to System Platform, which is the case when you first change from the default IP addresses, you must use a crossover cable from your services laptop to access the management port, which is Eth1/Gig2:
 - a. Configure your laptop with the following details:
 - IP address: 192.11.13.5
 - Subnet Mask: 255.255.255.252
 - Gateway IP: 192.11.13.6 (this is the IP address of the management port)
 - b. On your laptop, navigate to **Start > Run** and enter `cmd` in the **Open** field.
 - c. At the command line, enter `ping 192.11.13.6`.
 - d. Open the PuTTY application and enter the IP address `192.11.13.6`.
 - e. Log in with the username `admin` and the password `admin01`.
 - f. Run the command:

```
ip_forwarding enable
```

This command may already be enabled in a default version of Conferencing Standard Edition.

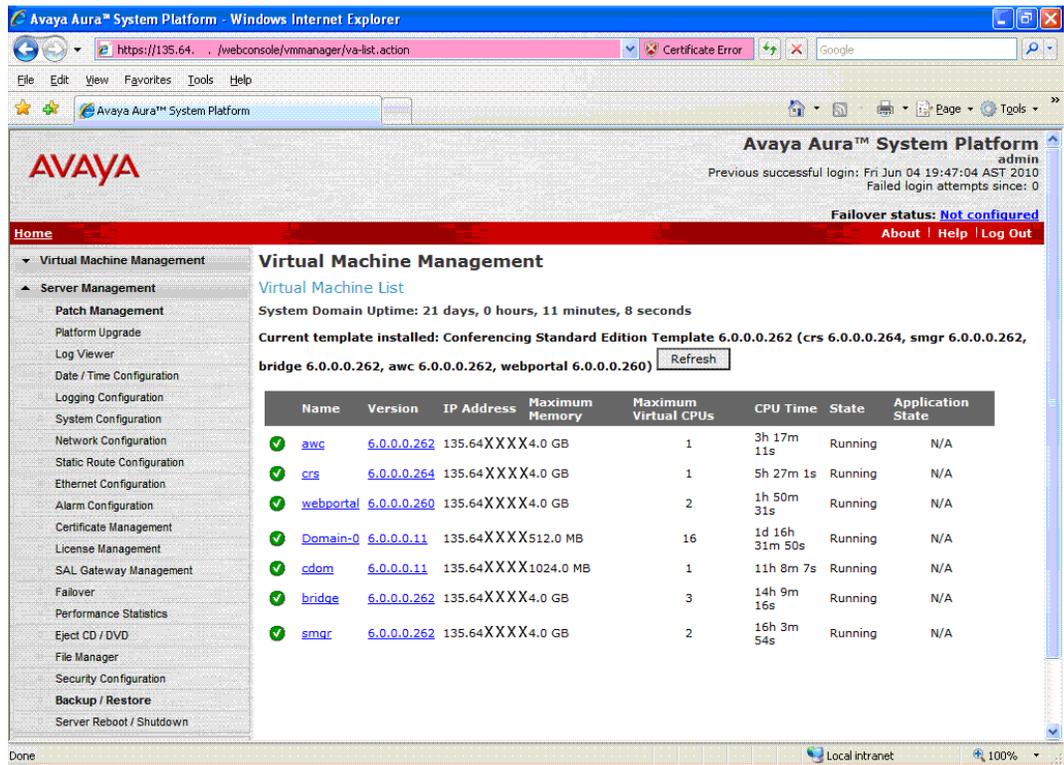
Now, you should be able to access System Platform directly, using your Web browser.

2. On the services laptop, open an Internet browser and ensure that there is no proxy enabled for connections that use a crossover cable.

For example, in Microsoft Internet Explorer, navigate to **Tools > Options > Connections** and select **LAN Settings**. On the **Local Area Network (LAN) Settings** dialog, ensure that **Use a proxy server for your LAN** is not selected.

3. In the Internet browser, enter the IP address of System Platform (Cdom).
This is `http://192.168.11.11/`
This link redirects to `http://<System Platform IP>/webconsole`
4. On the Login screen, in the **User Id** field, enter `admin` and click **Continue**.
5. In the **Password** field, enter `admin01` and click **Log On**.
6. Navigate to **Virtual Machine Management** and confirm that each of the Conferencing components are running.

Here is an example of the **Virtual Machine Management** screen on System Platform.



7. Navigate to **Server Management > Network Configuration** and update three sections, called the **General Network Settings**, **Domain Network Interface**, and **Global Template Network Configuration** sections, as follows:
 - a. Scroll to **General Network Settings** and enter the following information:

Field	Information
Default Gateway	<The IP address of the gateway>
Primary DNS	Domain name server
Secondary DNS	Optional field. You can leave this field blank
Domain Search List	Optional field. You can leave this field blank

Field	Information
Cdom Hostname	Hostname
Dom0 Hostname	Hostname

- b. On the same screen, scroll to the **Domain Network Interface** section edit the **avpublic** IP address field in the **Domain-0** sub-section and the **avpublic** IP address field in the **Console Domain** sub-section.

Do not edit the **avprivate** IP address fields or any other field in the **Domain-0** or **Console Domain** sub-sections.

Here is an example of the **Domain Network Interface** section on the Network Configuration screen.

The screenshot displays the Avaya Aura System Platform Network Configuration interface. It features a browser window with the URL `https://135.64.../webconsole/systemaint/vspnetwork.action?PAGE_ID=NETWORK&cid=8915`. The main content area is organized into several sections:

- Bridge:** A table with columns 'Bridge' and 'Interface'. It lists 'avprivate' (NA) and 'avpublic' (eth0).
- Domain Network Interface:**
 - Domain-0:** A table with columns 'Bridge', 'Interface', 'IP', 'Netmask', and 'Gateway'. It lists 'avprivate' (NA, 172.20.10.1, 255.255.255.0, no gateway), 'avpublic' (eth0, 135.64.XXXX, 255.255.255.0, 135.64.26.1), and 'local service access' (eth1, 192.11.13.6).
 - Console Domain:** A table with columns 'Bridge', 'Interface', 'IP', 'Netmask', and 'Gateway'. It lists 'avprivate' (eth2, 172.20.10.2, 255.255.255.0) and 'avpublic' (eth0, 135.64.XXXX, 255.255.255.0, 135.64.26.1).
- Template Network Configuration:** A section with fields for 'Global Template Network Configuration', 'AWC IP Address' (135.64.XXXX), and 'AWC Host Name' (aac-awc-2614.du.rnd.avaya.com).

- c. On the same screen, scroll to the **Global Template Network Configuration** section and update each of the virtual machine IPs and hostnames.

For the Conferencing Manager virtual machine, you must enter the gateway, netmask, and DNS too. These values must exactly match the values that you entered in the **General Network Settings** section, above.

- Double check all of your these changes in the **General Network Settings**, **Domain Network Interface** and **Template Network Configurations** sections.
- Click **Save** followed by **OK**.

System Platform updates the IP information and displays an information message which states that there are **Network Configuration changes in progress....** When the changes are complete, System Platform displays the Login screen.

Next steps

Now you can verify that the changes have saved successfully.

Verifying network information on System Platform

This is the second task.

Prerequisites

Before you verify the IP and hostname details on System Platform, you must update them on System Platform.

The purpose of this task is to check that the details that you updated in the first task are successfully saved on the System Platform.

-
1. Log in to System Platform again.
 2. On the Login screen, in the **User Id** field, enter `admin` and click **Continue**.
 3. In the **Password** field, enter `admin01` and click **Log On**.
 4. Navigate to **Server Management > Network Configuration**
 5. Check the gateway address listed under the **Console Domain (avpublic)** section.
If this is the old gateway address, click **Save** on the **Network Configuration** screen.
 6. Verify that the gateway address is now updated with the new IP address.
You may need to log out and log back in to System Platform.

Example

Sometimes, the old gateway address still displays on the **Network Configuration** screen. You must ensure that when you finish this task, the new gateway address is correctly displaying.

Next steps

Now you can verify network connectivity.

Verifying connectivity

This is the third task.

At this point, the Conferencing server should be on the network. You can unplug the crossover cable.

When the System Platform virtual machine is not on the network and you only have access to it using a crossover cable and a terminal emulator, you can only browse directly to System Platform and not to any of the other Conferencing components. For example, you cannot browse to the Conferencing Manager virtual machine.

So now, you need access to a PC or a laptop on the customer network.

Prerequisites

Before you 'ping' the various virtual machines that comprise the Conferencing solution, you must update the network information on System Platform and verify that the newly updated information is correctly displaying on System Platform.

The purpose of this task is to ensure that you have network connectivity with each of the Conferencing virtual machines. Traditionally, this task is also known as pinging the virtual machines. Pinging ensures that the virtual machines are reachable across the customer's Internet Protocol (IP) network.

-
1. Access a PC or a laptop on the customer network.
 2. Navigate to **Start > Run** and enter `cmd` in the **Open** field.
 3. Enter the following command using the IP address of one of the Conferencing virtual machines.

```
ping <IP address>
```

The application should display a list of network information relating to the virtual machine.

4. If the Conferencing Manager virtual machine does not respond to the ping, follow these steps:
 - a. On the PuTTY dialog, enter the hostname or IP address of the System Platform machine.
 - b. Enter the username `admin` and the password `admin01`.
 - c. Run the command `su root` to increase the access permissions.

The password is `root01`.

Note:

These usernames and passwords are the System Platform default usernames and passwords. Avaya configures these values when they ship

a new System Platform. It is likely that an administrator has updated this information following the installation of System Platform in your site.

- a. Use the Xen Management tool to access the Conferencing Manager virtual machine, as follows:

```
xm console smgr
```

 **Note:**

Conferencing Manager is a simple version of System Manager. As a result, the abbreviation SMGR refers to System Manager or Conferencing Manager.

After you run the Xen Management command, the Conferencing Manager virtual machine becomes accessible from the current PuTTY dialog, at the resulting prompt line.

- b. Log into Conferencing Manager using the username `root` and the password `root01`.
- c. Navigate to `/etc/hosts` to obtain the IP address and Fully Qualified Domain Name (FQDN) of Conferencing Manager.
- d. Run the network change script to update these network settings. For example:

```
sh /opt/Avaya/Mgmt/3.0.7/Utils/ipfqdnchange/Ip-fqdn-r6.0.sh -OLDIP 135.64.30.111 -NEWIP 135.64.30.112 -GATEWAY 135.64.30.113 -NETMASK 255.255.255.224 -OLDFQDN smgr30243.du.rnd.avaya.com -NEWFQDN smgr30244.emea.avaya.com
```

This step can take up to 15 minutes to complete. During this time, the PuTTY dialog may display a number of warning messages.

- e. Wait until the PuTTY dialog displays the 'shell' prompt.
- f. Update the DNS search domains. For example:

```
echo ProfileList.default.DNS.SearchList.1=emea.avaya.com | system-config-network-cmd -i
```

Replace `emea.avaya.com` with a suitable domain name.

- g. Log out of Conferencing Manager, as follows:

```
exit
```

- h. Close the Xen Management session by pressing `CTRL +]` on your keyboard.

- i. Log out of System Platform, as follows:

```
exit  
exit
```

- j. On the System Platform Web interface, navigate to **Virtual Machine Management > Manage** and reboot Conferencing Manager.
- k. 'Ping' the Conferencing Manager virtual machine to verify that it is now responding.

Next steps

Now you must update the network information on Conferencing Manager.

Updating network information on Conferencing Manager

This is the fourth task.

Prerequisites

Before you update the network information on Conferencing Manager, you must update it on System Platform, verify your updates, and manually restart the AWC service.

The purpose of this task is to update the Conferencing Manager with the same changes that you made on System Platform.

-
1. Log in to Conferencing Manager.
Conferencing Manager is a Web application. You can access it by entering the Conferencing Manager IP address in a Web browser as follows:
<Conferencing Manager IP address>/SMGR
Some of the fields on the interface refer to Conferencing Manager as SMGR or Udom.
By default, the username is `admin` and the password is `admin123`. You can change these username and password settings at any time.
 2. Navigate to **Elements > Inventory > Manage Elements** and change the IP address information of the virtual machines:
 - a. Select a virtual machine.
 - b. Click **Edit**.
 - c. Edit the **Node** and **Name** fields.
The **Name** field is optional.
 - d. Click **Commit**.It is important to edit the node. If you delete it and create a new one, Conferencing Manager deletes all conferences.
 3. Navigate to **Elements > Conferencing** and apply any changes.
 4. Wait for five minutes.
 5. Log back in to Conferencing Manager and ensure that all services are powered on and active. You can check the status of the services by navigating to the **Elements > Conferencing > Services** menu.

The Conferencing Manager Web interface may display the AWC as powered on but inactive. You can continue to the next task.

Example

In a very limited number of circumstances, you may encounter an issue when you are applying the changes. If you experience an issue, log out of Conferencing Manager and then log back in to Conferencing Manager. Navigate to **Elements > Conferencing** and apply any changes. It is important to click **Apply Changes** within a short period of time. When the screen refreshes, the **Apply Changes** button is no longer available. The screen refreshes every 15 seconds. If the **Apply Changes** button is no longer available, you must log out of Conferencing Manager and log back in again. Conferencing Manager will not permit you to make any further updates to Conferencing information until you commit the changes.

Next steps

Now you must update the Client Registration Server (CRS) virtual machine with the new application server (bridge) details.

Updating information on the CRS virtual machine

This is the fifth task.

Prerequisites

Before you enter the application server (bridge) details on the Client Registration Server (CRS) Front End, you must update the details on System Platform and Conferencing Manager, verify your updates, and manually restart the AWC service.

The purpose of this task is to enter the details of the application server in the Client Registration Server (CRS) Front End. This task ensures that the network information is consistent across all applications. On the CRS Front End, you must update the **Bridge name** field. You can use the remote desktop feature to access the CRS virtual machine.

-
1. Click **Start > Run**.
 2. Enter `mstsc /console` in the **Run** dialog.
 3. In the **Computer** field, enter the CRS virtual machine IP address.
 4. Enter a password.
The password is `Avaya123`.
 5. Open the CRS Front End application. The CRS Front End is installed on the CRS virtual machine, by default.

The CRS Front End **Username** is `Administrator` and the **Password** is `Avaya123`.

6. On the CRS Front End, click **System Administration** and click the **Bridge** tab.
7. Update the **Name** and **Bridge DSN** fields.

When Avaya ships your instance of Conferencing, the CRS Front End contains network information relating to the default application server (bridge). You must edit this information to refer to your actual network configuration. The Bridge Data Source Name (DSN) is the connection between the CRS and the bridge. This connection means that database information from the CRS is shared with the bridge.

 - In the **Name** field, enter a name for the bridge, such as `Conferencing123`.
 - In the **Bridge DSN** field, enter the following string `iCacheDB<IP address of your bridge>`.
8. Click the **Cabinets** tab and update the **Name** field.
9. Close the CRS Front End.
10. Whilst still using the remote desktop feature to access the CRS virtual machine, navigate to **Control Panel > Administrative Tools > Data Sources (ODBC)** and select **System DSN** followed by `iCacheDB<IP address>`.
11. Configure `iCacheDB<IP address>`.

As before, this section contains network information relating to the default application server (bridge). You must edit this information to refer to your actual network configuration. The Bridge Data Source Name (DSN) is the connection between the CRS and the bridge. This connection means that database information from the CRS is shared with the bridge. The information here must exactly match the information you entered in CRS Front End.
12. Update the **Data Source** and **Server** fields by entering IP information relating to your bridge.
13. Click **Save**.

Next steps

Now, you can update the date and time on the Conferencing servers.

Making changes to date and time

This is the sixth task.

The purpose of this task is to update your Conferencing network with a new time and/or date.

-
1. On System Platform, navigate to **Server Management > Date/Time Configuration** and stop the Network Time Protocol (NTPD).
 2. Set the timezone and the time, as required and click **Set Timezone** and **Save Date and Time**.
 3. Remove the old NTP server.
 4. Add a new NTP server.
The server will reboot when applying.

If NTPD fails to start:

- a. Navigate to Manage Time Servers and ensure that you can 'ping' the NTP server.
- b. On a PuTTY dialog, enter the hostname or IP address of the System Platform machine.
- c. Enter the username `admin` and the password `admin01`
- d. Run the command `su root` to increase the access permissions.

The password is `root01`.

 **Note:**

These usernames and passwords are the System Platform default usernames and passwords. Avaya configures these values when they ship a new System Platform. It is likely that an administrator has updated this information following the installation of System Platform in your site.

- e. Restart the NTPD service, as follows:

```
service ntpd restart
```

5. Using the remote desktop, connect to the CRS and AWC virtual machines:
 - a. Click **Start > Run**.
 - b. Enter `mstsc /console` in the **Run** dialog.
 - c. In the **Computer** field, enter the CRS virtual machine IP address for the connection to the CRS virtual machine.
 - d. Enter a password.
The password is for the CRS virtual machine is `Avaya123`.
 - e. Verify that the date and time is correct.
If it is incorrect, manually change the date and time on the CRS virtual machine.
 - f. Repeat these steps for the AWC virtual machine.
The password for the AWC virtual machine is `Avaya123`.
-

Next steps

Now, you can verify the management servlet on the application server (bridge).

Verifying the management servlet on the application server

This is the seventh task in the sequence.

Prerequisites

Before you verify the status of the management server on the application server (bridge), you must complete the steps to update the network information on System Platform.

The purpose of this task is to check that the application server is successfully operating, following the change in network information.

-
1. Log in to the application server (bridge) virtual machine using PuTTY.
 2. Enter the name `craft` and the password `craft01`.
 3. Use the `sroot` command to change from `craft` to `sroot` access.

The `sroot` command is:

```
su - sroot
```

The password is `sroot01`.

4. Enter the following command to check that the management servlet is running:

```
service acbms status
```

The PuTTY dialog should respond with the following:

```
acbms (pid 14632) is running...
```

If it does not, enter the following command to restart the management servlet:

```
service acbms restart
```

Next steps

Now, you can restart the management servlet on the AWC.

Restarting the Avaya management servlet on AWC

This is the final task.

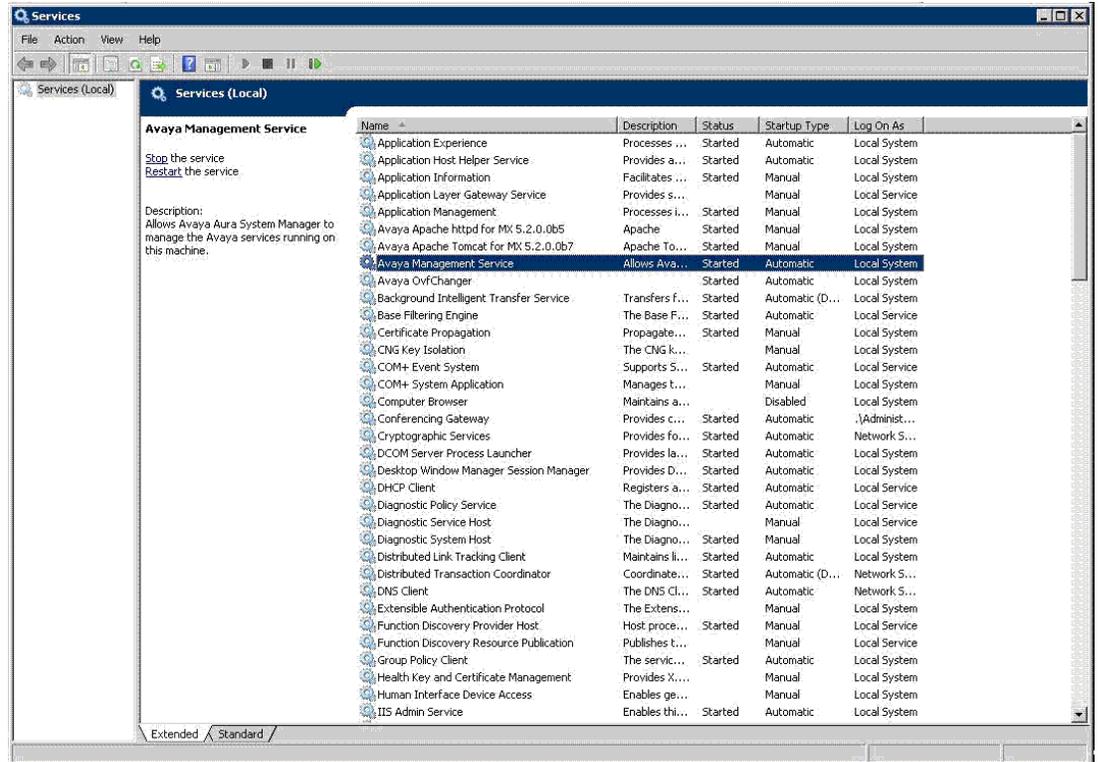
You must perform this task as a result of the IP address change. The purpose of this task is to clear the CPU usage of the AWC. This step ensures that the CPU usage of the AWC is at 0%.

Prerequisites

Before you manually restart the Avaya Management Service, you must update the network information on System Platform and verify that the newly updated information is correctly displaying on System Platform.

The purpose of this task is to restart the management server on the AWC so that Conferencing Manager can successfully connect to the AWC and query its status. You can use the remote desktop feature to access the AWC virtual machine.

-
1. Click **Start > Run**.
 2. Enter `mstsc /console` in the **Run** dialog.
 3. In the **Computer** field, enter the AWC virtual machine IP address.
 4. Select the Administrator tab and enter the password `Avaya123`.
 5. Navigate to **Start > Run**.
 6. Enter `services.msc` in the **Run** dialog.
 7. On the Services tab, select the services **Restart** button to restart the Avaya Management Services service.
Here is an example of the Services tab.



If you receive an error message when attempting to restart the AWC Management Servlet, repeat the step but select the **Start** button instead of the **Restart** button.

Next steps

You are now finished.