Using Customer Operations Manager for IP Office Subscription Systems

Release 11.1.3
Issue 8
May 2023

Notice

While reasonable efforts have been made to ensure that the information in this document is complete and accurate at the time of printing, Avaya assumes no liability for any errors. Avaya reserves the right to make changes and corrections to the information in this document without the obligation to notify any person or organization of such changes.

Documentation disclaimer

"Documentation" means information published in varying media which may include product information, subscription or service descriptions, operating instructions and performance specifications that are generally made available to users of products. Documentation does not include marketing materials. Avaya shall not be responsible for any modifications, additions, or deletions to the original published version of Documentation unless such modifications, additions, or deletions were performed by or on the express behalf of Avaya. End user agrees to indemnify and hold harmless Avaya, Avaya's agents, servants and employees against all claims, lawsuits, demands and judgments arising out of, or in connection with, subsequent modifications, additions or deletions to this documentation, to the extent made by End user.

Link disclaimer

Avaya is not responsible for the contents or reliability of any linked websites referenced within this site or Documentation provided by Avaya. Avaya is not responsible for the accuracy of any information, statement or content provided on these sites and does not necessarily endorse the products, services, or information described or offered within them. Avaya does not guarantee that these links will work all the time and has no control over the availability of the linked pages.

Warranty

Avaya provides a limited warranty on Avaya hardware and software. Please refer to your agreement with Avaya to establish the terms of the limited warranty. In addition, Avaya's standard warranty language as well as information regarding support for this product while under warranty is available to Avaya customers and other parties through the Avaya Support website: https://support.avaya.com/helpcenter/getGenericDetails?detailId=C20091120112456651010 under the link "Warranty & Product Lifecycle" or such successor site as designated by Avaya. Please note that if the product(s) was purchased from an authorized Avaya channel partner outside of the United States and Canada, the warranty is provided by said Avaya Channel Partner and not by Avaya.

"**Hosted Service**" means an Avaya hosted service subscription that You acquire from either Avaya or an authorized Avaya Channel Partner (as applicable) and which is described further in Hosted SAS or other service description documentation regarding the applicable hosted service. If You purchase a Hosted Service subscription, the foregoing limited warranty may not apply but You may be entitled to support services in connection with the Hosted Service as described further in your service description documents for the applicable Hosted Service. Contact Avaya or Avaya Channel Partner (as applicable) for more information.

Hosted Service

THE FOLLOWING APPLIES ONLY IF YOU PURCHASE AN AVAYA HOSTED SERVICE SUBSCRIPTION FROM AVAYA OR AN AVAYA CHANNEL PARTNER (AS APPLICABLE), THE TERMS OF USE FOR HOSTED SERVICES ARE AVAILABLE ON THE AVAYA WEBSITE, HTTPS://SUPPORT.AVAYA.COM/LICENSEINFO UNDER THE LINK "Avaya Terms of Use for Hosted Services" OR SUCH SUCCESSOR SITE AS DESIGNATED BY AVAYA, AND ARE APPLICABLE TO ANYONE WHO ACCESSES OR USES THE HOSTED SERVICE. BY ACCESSING OR USING THE HOSTED SERVICE, OR AUTHORIZING OTHERS TO DO SO, YOU, ON BEHALF OF YOURSELF AND THE ENTITY FOR WHOM YOU ARE DOING SO (HEREINAFTER REFERRED TO INTERCHANGEABLY AS "YOU" AND "END USER"), AGREE TO THE TERMS OF USE. IF YOU ARE ACCEPTING THE TERMS OF USE ON BEHALF A COMPANY OR OTHER LEGAL ENTITY, YOU REPRESENT THAT YOU HAVE THE AUTHORITY TO BIND SUCH ENTITY TO THESE TERMS OF USE. IF YOU DO NOT HAVE SUCH AUTHORITY, OR IF YOU DO NOT WISH TO ACCEPT THESE TERMS OF USE, YOU MUST NOT ACCESS OR USE THE HOSTED SERVICE OR AUTHORIZE ANYONE TO ACCESS OR USE THE HOSTED SERVICE.

Licenses

The Global Software License Terms ("Software License Terms") are available on the following website https://www.avaya.com/en/legal-license-terms/ or any successor site as designated by Avaya. These Software License Terms are applicable to anyone who installs, downloads, and/or uses Software and/or Documentation. By installing, downloading or using the Software, or authorizing others to do so, the end user agrees that the Software License Terms create a binding contract between them and Avaya. In case the end user is accepting these Software License Terms on behalf of a company or other legal entity, the end user represents that it has the authority to bind such entity to these Software License Terms.

Copyright

Except where expressly stated otherwise, no use should be made of materials on this site, the Documentation, Software, Hosted Service, or hardware provided by Avaya. All content on this site, the documentation, Hosted Service, and the product provided by Avaya including the selection, arrangement and design of the content is owned either by Avaya or its licensors and is protected by copyright and other intellectual property laws including the sui generis rights relating to the protection of databases. You may not modify, copy, reproduce, republish, upload, post, transmit or distribute in any way any content, in whole or in part, including any code and software unless expressly authorized by Avaya. Unauthorized reproduction, transmission, dissemination, storage, or use without the express written consent of Avaya can be a criminal, as well as a civil offense under the applicable law.

Virtualization

The following applies if the product is deployed on a virtual machine. Each product has its own ordering code and license types. Unless otherwise stated, each Instance of a product must be separately licensed and ordered. For example, if the end user customer or Avaya Channel Partner would like to install two Instances of the same type of products, then two products of that type must be ordered.

Third Party Components

The following applies only if the H.264 (AVC) codec is distributed with the product. THIS PRODUCT IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Service Provider

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE H.264 CODEC OR H.265 CODEC, THE AVAYA CHANNEL PARTNER ACKNOWLEDGES AND AGREES THE AVAYA CHANNEL PARTNER IS RESPONSIBLE FOR ANY AND ALL RELATED FEES AND/OR ROYALTIES. THE H.264 (AVC) CODEC IS LICENSED UNDER THE AVC PATENT PORTFOLIO LICENSE FOR THE PERSONAL USE OF A CONSUMER OR OTHER USES IN WHICH IT DOES NOT RECEIVE REMUNERATION TO: (i) ENCODE VIDEO IN COMPLIANCE WITH THE AVC STANDARD ("AVC VIDEO") AND/OR (ii) DECODE AVC VIDEO THAT WAS ENCODED BY A CONSUMER ENGAGED IN A PERSONAL ACTIVITY AND/OR WAS OBTAINED FROM A VIDEO PROVIDER LICENSED TO PROVIDE AVC VIDEO. NO LICENSE IS GRANTED OR SHALL BE IMPLIED FOR ANY OTHER USE. ADDITIONAL INFORMATION FOR H.264 (AVC) AND H.265 (HEVC) CODECS MAY BE OBTAINED FROM MPEG LA, L.L.C. SEE HTTP://WWW.MPEGLA.COM.

Compliance with Laws

You acknowledge and agree that it is Your responsibility to comply with any applicable laws and regulations, including, but not limited to laws and regulations related to call recording, data privacy, intellectual property, trade secret, fraud, and music performance rights, in the country or territory where the Avaya product is used.

Preventing Toll Fraud

"Toll Fraud" is the unauthorized use of your telecommunications system by an unauthorized party (for example, a person who is not a corporate employee, agent, subcontractor, or is not working on your company's behalf). Be aware that there can be a risk of Toll Fraud associated with your system and that, if Toll Fraud occurs, it can result in substantial additional charges for your telecommunications services.

Avaya Toll Fraud intervention

If You suspect that You are being victimized by Toll Fraud and You need technical assistance or support, please contact your Avaya Sales Representative.

Security Vulnerabilities

Information about Avaya's security support policies can be found in the Security Policies and Support section of https://support.avaya.com/security.

Suspected Avaya product security vulnerabilities are handled per the Avaya Product Security Support Flow (https://support.avaya.com/css/P8/documents/100161515).

Trademarks

The trademarks, logos and service marks ("Marks") displayed in this site, the Documentation, Hosted Service(s), and product(s) provided by Avaya are the registered or unregistered Marks of Avaya, its affiliates, its licensors, its suppliers, or other third parties. Users are not permitted to use such Marks without prior written consent from Avaya or such third party which may own the Mark. Nothing contained in this site, the Documentation, Hosted Service(s) and product(s) should be construed as granting, by implication, estoppel, or otherwise, any license or right in and to the Marks without the express written permission of Avaya or the applicable third party.

Avaya is a registered trademark of Avaya LLC.

All non-Avaya trademarks are the property of their respective owners.

Linux® is the registered trademark of Linus Torvalds in the U.S. and other countries.

Downloading Documentation

For the most current versions of Documentation, see the Avaya Support website: https://support.avaya.com, or such successor site as designated by Avaya.

Contact Avaya Support

See the Avaya Support website: https://support.avaya.com for Product or Cloud Service notices and articles, or to report a problem with your Avaya Product or Cloud Service. For a list of support telephone numbers and contact addresses, go to the Avaya Support website: https://support.avaya.com (or such successor site as designated by Avaya), scroll to the bottom of the page, and select Contact Avaya Support.

Contents

Part 1: Introduction

Chapter 1: Customer Operations Manager

Customer Operations Manager (COM) is an application to assist in the simultaneous monitoring and managing of multiple customer IP Office systems.

There are several different versions of COM. They are:

Version	Description
Cloud COM Service	This version of COM is used to manage Avaya UC and Containerized IP Office systems. It is provided as a service from the cloud hosting the systems. That version of COM is not covered in this document. Instead, refer to Using Customer Operations Manager for IP Office Cloud Systems.
Subscription COM Service	This version of COM is used to manage subscription systems. It is provided as a service from the cloud providing the system subscriptions. This is the version of COM covered in this document.
Standalone COM Server	For maintainers supporting customers with non-subscription Server Edition and Select systems, COM can be installed onto a separate Linux server. That version of COM is not covered in this document. Instead, refer to Using Customer Operations Manager for Standalone IP Office Systems.

Each COM user is configured with a particular role that determines what they can do and the customer systems they can see. For more details, see COM User Roles on page 10.

Related links

COM User Roles on page 10

Read-Only and Wallboard Display Modes on page 12

COM User Roles

Each COM user account is configured with a particular role. That role determines the actions the user can perform and the customer systems they can see.

Function	Administrator	Support	Supervisor	Operator	Read-Only
Used by	Avaya		System provider		
	DevOps	Support	–	Created by the system provider as required.	

Table continues…

Function	Administrator	Support	Supervisor	Operator	Read-Only
See which customers	All		Assigned customers only.[1]		
View Dashboard	✓	✓	✓	✓	✓
View Alarms	✓	✓	✓	✓	✓
View Customer List	✓	✓	✓	✓	✓
View Customer Details	✓	✓	✓	✓	✓
View Remote Support Addresses	–	–	✓	✓	✓
Idle Logout	✓	✓	✓	✓	✓
Launch Application	✓	–	–	✓	–
Customer Management The users can perform the following actions on customer systems:					
Backup/Restore	✓	–	✓	–	–
Upgrade Customers	✓	✓	–	✓	–
Add/Delete Customers	✓	–	–	✓	–
Edit Customers	✓	–	–	–	–
Log File Management	✓	✓	✓	✓	–
Refresh Customization Files	✓	✓	✓	✓	–
Customization File Management	✓	–	–	–	–
Resend System Email	✓	✓	✓	✓	–
COM Service Management The users can perform the following COM server actions:					
COM Preferences	✓	–	–	–	–
Create COM Users	✓	–	✓[2]	–	–
Assign COM Users	✓	–	✓[2]	–	–

1. **Supervisor** users can only see customer systems to which they are assigned. See Assigning Users to a Customer on page 51.
2. **Supervisor** users can create additional **Operator** users and assign them to any of their own assigned systems.

Related links

Customer Operations Manager on page 10

Read-Only and Wallboard Display Modes

Users set to the **Support** or **Read-Only** roles can also be configured to use the following special display modes:

Display Mode	Description
Read-only Mode	This mode allows the user to navigate to most menus and to apply filters and select tags to set the data displayed. However, they cannot perform any actions except editing their user profile.
Wallboard Mode	For these users, when their session timeout occurs, they remain logged in and continue to receive display updates. However, they are no longer able to navigate to any other menus or change the displayed menu in any way.

Related links

Customer Operations Manager on page 10

Chapter 2: Using COM

This chapters covers the basics of using COM.

Related links

Logging In on page 13
Logging Out on page 14
Using the Dashboard on page 14
The Menu Bar on page 15

Logging In

COM is accessed via web browser. It is supported with the current releases of Chrome, Edge and Firefox browsers.

- You will need details of the login name and password of the user created for your use. After logging in, you can change your password yourself.
- Note: 3 Failed login attempts in a 10 minute period will block any further login attempts for the following 10 minutes.

Procedure

1. Start your browser and enter ***https://*** followed by the COM server's IP address or name followed by ***:7080/com***. For example ***https://admin.example.com:7080/com***.
2. The login menu is displayed.
3. If necessary, change the language selection.
4. Enter your user name and password.
5. Click **Log In**.
    a. If details of the software license appear, click **Accept**.
    b. If prompted to change your password, enter and confirm your new password.
        - The password must be between 9 and 31 characters long.
        - It must include characters of 2 or more of the following types: uppercase, lowercase, numbers, special characters.
        - The server will not allow you to reuse previous passwords.

6. If the details are correct, the dashboard is displayed. See main dashboard on page 14.

Related links

Using COM on page 13

Logging Out

You can use the process below to manually log out. The server will also automatically log you out if you are idle for too long, unless you have logged in with a read-only user account.

Procedure

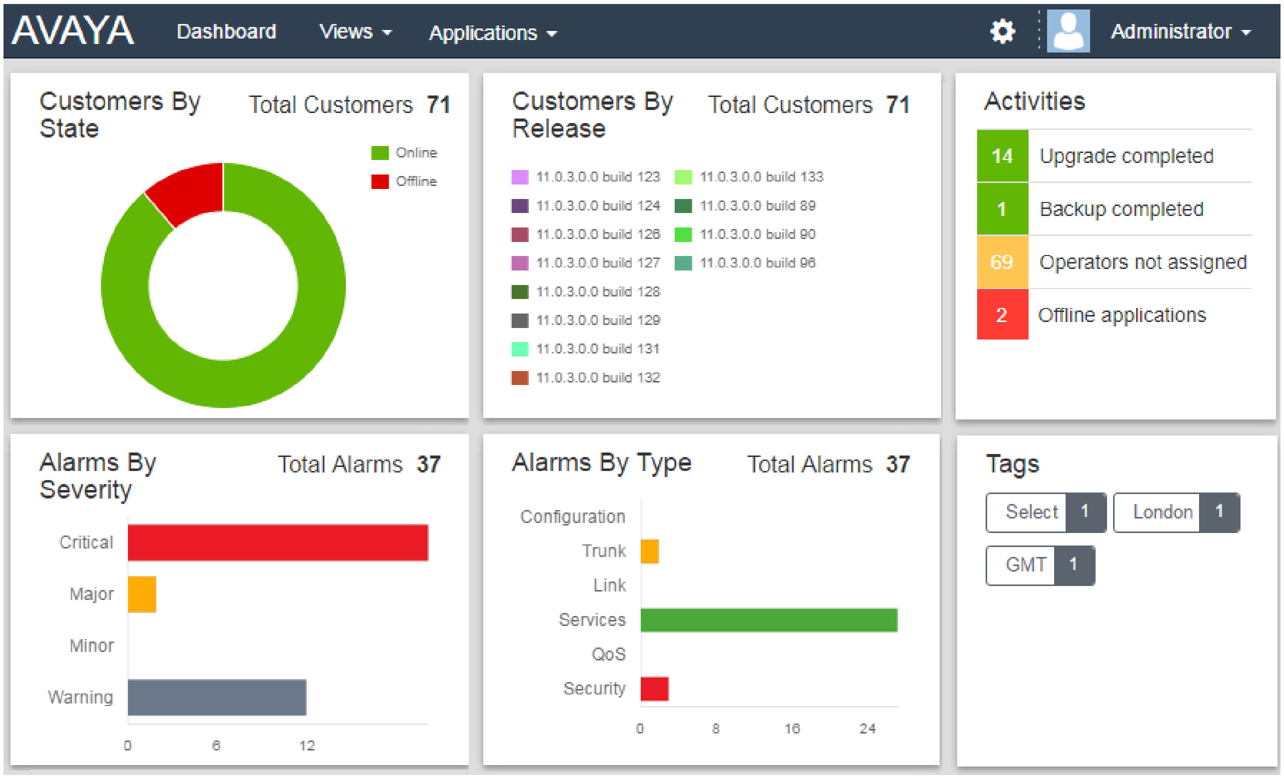
1. Click on your user name shown top-right.
2. Select **Logout**.

Related links

Using COM on page 13

Using the Dashboard

This is the default view presented when you login.



- For components on the dashboard that have a legend, for example **Customers By State**, clicking on items in the legend hides them in the component chart.

Many parts of the dashboard can be clicked to jump to a filtered list of matching entries. For example:

- Clicking on a tag in the **Tags** panel will take you to the customer list pre-filtered to only show systems with the same tag. See customer list on page 19.
- Clicking on an alarm type or severity in the **Alarms By Severity** or **Alarms By Type** panels will take you to the alarms list pre-filtered to only show matching alarms. See alarms list on page 28.

You can return to the main dashboard at any time by clicking on **Dashboard** in the menu bar.

Related links

Using COM on page 13

The Menu Bar

The menu bar at the top of the application window allows you to access a number of menus.

Dashboard

Click to display the dashboard. That screen provides an overview of all the customers you manage and any alarms. See Using the Dashboard on page 14

Views

Click on this drop-down to access the following:

Options	Descriptions
Customers	Selecting this option displays a list of the customers assigned to you. See Using the Customer List on page 19.
Alarms	Selecting this option displays a list of any alarms currently logged for the customers assigned to you. See Alarms on page 28
Scheduled Jobs	Clicking this option displays the list of current scheduled jobs relating to the customers that you manage. See Viewing Scheduled Jobs on page 43
Software Repository	Clicking this option displays the list of files currently available for actions such as upgrading customers systems. See The Software Repository on page 93.
File Management	Upload and manage the files used for various functions: • This is only supported for **Administrator** users. • **Customization File Management:** Upload and manage files such as SIP trunk templates, phone settings and screen saver files, etc. See Creating a New Customization File Folder on page 88. • **Workplace and Vantage Files Management:** Upload and manage the files required by Avaya Vantage™ phones and Avaya Workplace Client applications. See Avaya Workplace Client File Management on page 97 and Vantage File Management on page 94.

Applications

Option	Description
IP Office Admin Tools	Download the installer for the IPO Admin Lite suite of applications (IP Office Manager, System Status Application and SysMonitor). See Downloading the IP Office Admin Tools on page 102.
Download Proxytunnel Utility	Download the files needed to configure remote support connections. See Remote Support Through COM on page 109.
The following additional options are visible for **Administrator** users.	
Application Center	View the status of cloud cluster services, including COM. See The Application Center on page 150.
Stackdriver	This option provides access to the logs provided by the cluster hosting COM. This option requires a cluster administrator password.
Google Dashboard	This options provided access to the menus for cluster administration. This option requires a cluster administrator password.

Settings

Click on the settings icon to access the following:

Options	Description
Account Management	This menu allow you to manage the list of COM users. That is to add, delete and edit users. This option is only displayed for **Administrator** and **Supervisor** users.
Maintenance Proxy Account Management	View the reseller/distributor accounts used for remote access connections. See Proxy Account Management on page 110.
Certificates	Secure access to a customer system may require a certificate. Selecting this option displays the menu where certificates can be added. See Adding a Different Identity Certificate on page 147
Preferences	This option displays a menu for adjusting various COM service settings. This option is only displayed for **Administrator** users. See Preferences on page 141.
Help	This link opens an on-line version of this help in a separate browser tab or window.
About	This screen displays information about the version of COM you are using.

User Name

The drop-down at the right-hand end of the menu bar uses your user name.

Option	Description
Profile	Displays a summary of your user account settings. You can also use this screen to change your password (see change your password on page 73) and avatar (see change your avatar image on page 74).
Logout	Clicking this option will end your COM session and log you out.

Related links

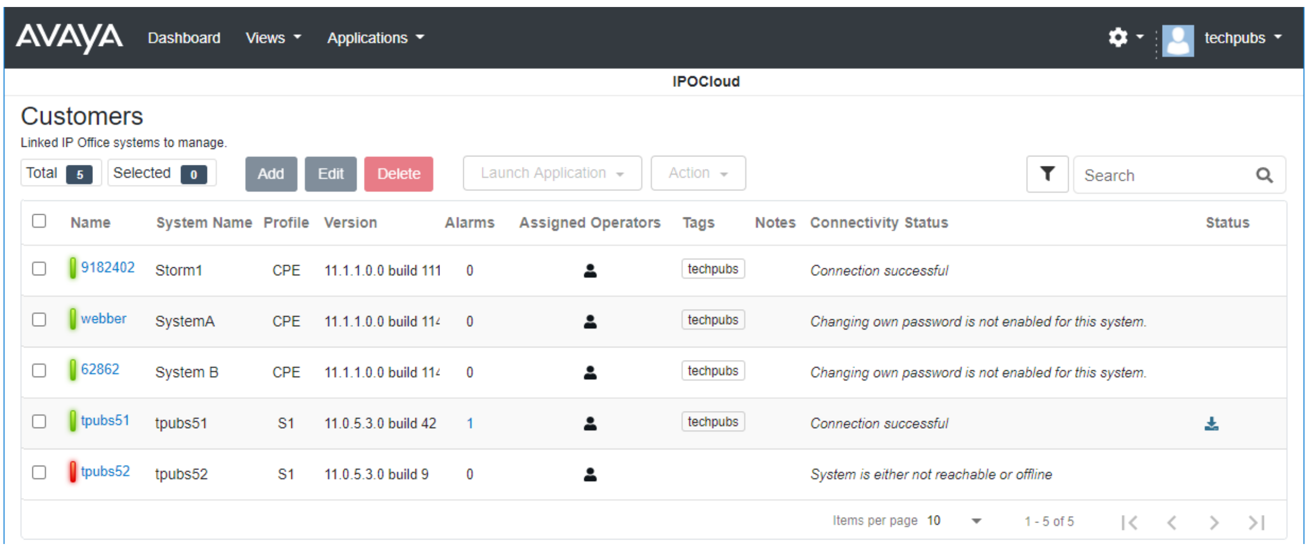
Using COM on page 13

Part 2: Managing Customer Systems

Chapter 3: Using the Customer List

For **Administrator** and **Support** users, the customer list shows all customers. For other users, it only shows those customers to which you have been assigned (see Assigning Users to a Customer on page 51).

If you access the customer list be clicking on a particular tag or category on the dashboard, then only matching customers are shown in the list.



Related links

Viewing the Customer List on page 20
Customer Settings on page 21
Status Icons on page 22
Connectivity Messages on page 23
Viewing the Customer System Details on page 24
Filtering the List on page 25
Hiding the Filter on page 25
Sorting the List on page 26
Searching the List on page 26
Resending the Subscription Email on page 27

Viewing the Customer List

About this task

In addition to the method below, you can click customer information on the dashboard (see dashboard on page 14) to immediately display the list pre-filtered with only matching customers. For example, click on a particular tag or software release.

Procedure

1. Click on **Views** and then click on **Customers**.
2. The list of your existing customers is displayed.
3. The top of the list provides the following options. Note that some options may be grayed out if not supported by your type of user account or the type of systems listed or type of system selected.

Option	Description
Add	Add a new customer. See Adding a New Customer on page 49. This is only supported for **Administrator** and **Operator** users.
Edit	Edit an existing customer. See Editing Customer Details on page 52. This is only supported for **Administrator** and **Supervisor** users.
Delete	Delete an existing customer from being shown. See Deleting Customers on page 52. This is only supported for **Administrator** and **Operator** users.
Launch Application	Start an IP Office Web Manager connection to the currently selected system.
Action	Perform actions on the selected customer systems. The actions shown vary depending on the type of system selected. See the table below.
	Filter the list of customers shown. See Filtering the List on page 25.
	Search the list of customers shown. See Searching the List on page 26.

Actions

Action	Description
Backup	Backup customer system configurations. See Backing Up and Restore on page 35. This is only supported for **Administrator**, **Supervisor** and **Operator** users.
Restore	Restore previous backups. See Backing Up and Restore on page 35. This is only supported for **Administrator**, **Supervisor** and **Operator** users.

Table continues…

Action	Description
Upgrade	Upgrade the system software. See Upgrading Customer Systems on page 40. This is only supported for **Administrator** users.
Log Management	Access and download the system log files. See Managing System Log Files on page 33.
Refresh Customization Files	Update the trunk template and other customization files available to the system. See Customization File Management on page 76.
Send Email	Resend the system subscription email. See Resending the Subscription Email on page 27.

Related links

Using the Customer List on page 19

Customer Settings

When viewing the customer list, the settings listed below are shown. These can be edited by **Administrator** and **Supervisor** users, see Editing Customer Details on page 52.

- Note: The settings shown vary depending on the type of systems being managed.

Setting	Description
Name	The color bar next to the system name indicates the status of the connection between the customer's primary system and COM. It uses traffic-light colors: • Red = For an existing system, no connection. For a new system for which subscriptions have been requested, waiting for initial connection. • Amber = System connected but authorization/authentication failed. For servers in a network, can also indicate that one of the servers is offline or not reachable. • Green = Connected and okay. Clicking on the customer name displays additional details. See Viewing the Customer System Details on page 24.
System Name	The system name. Shown for information only, not editable.
Customer ID	A unique customer ID. This value is used for functions such as connecting to the customer systems through COM.

Table continues…

Setting	Description
Profile	For subscription systems, this displays either **IP500 V2**, **Server Edition** and/or **ACCS**. **Legacy** indicates a pre-11.1 FP1 subscription system. The status of those can still be monitored through COM but no other remote services are supported.
Version	The version of software on the customer's primary server.
Alarms	The current count of alarms logged by COM for the customer's systems. You can click on the number to be transferred to the alarms list pre-filtered to show those alarms.
Connectivity Status	This is a summary of the connection between the COM server and the customer's primary server. See Connection Messages on page 23.
Status	This column uses icons to indicate additional information. • **`Needs Attention`:** Note that this icon does not necessarily indicate a problem. • **`New Version Available`:** A higher version of software is available. This customer could be upgraded if required. • **`In progress`:** The server is performing some action such as an upgrade. Whilst it is performing this action,, COM cannot be used to initiate any other action. • **`Action completed`:** The previously selected action, such as an attempt to upgrade the customer system, was completed successfully. • **`Action failed`:** An action, such as an attempt to upgrade the customer systems, was not successful.

Related links

Using the Customer List on page 19

Status Icons

The following icons can appear next to a customer:

- **`Needs Attention`:** Note that this icon does not necessarily indicate a problem.
- **`New Version Available`:** A higher version of software is available. This customer could be upgraded if required.
- **`In progress`:** The server is performing some action such as an upgrade. Whilst it is performing this action,, COM cannot be used to initiate any other action.
- **`Action completed`:** The previously selected action, such as an attempt to upgrade the customer system, was completed successfully.

- **`Action failed`:** An action, such as an attempt to upgrade the customer systems, was not successful.

Related links

Using the Customer List on page 19

Connectivity Messages

Various messages may appear regarding the connection between the COM server and the customer.

In the following, service user account refers to the service user account in the IP Office system's security settings. This is the account used by the system to establish its connection to COM (by default ***COMAdmin***, see Creating the COMAdmin Service User and Rights Group on page 56). The account used is set in the COM settings for the customer system (see Customer Account Settings on page 50).

Message	Description
"Authorization failed"	Indicates that the service user password was not valid.
"Connection failed"	Indicates that there was no recognized response from the customer address.
"Connection successful"	Indicates a successfully validated connection.
"Insufficient Rights"	The security rights for the service user account on the customer system are not correct.
"Invalid credentials"	Indicates that the connection did not match any service user on the customer's primary system.
"Legacy"	Indicates a pre-11.1 FP1 subscription system. The status of the system can still be monitored by COM but no other remote services are supported.
"Maximum concurrent sessions limit has been exceeded"	Indicates that too many applications are already currently connected to that system.
"New password is required for Service Use account"	The system has requested that a new password be set for the service user account in its security settings.
"No authorization provided. Limited functionality will be available for the customer."	
"No user rights are enable for this system"	The system is connected but the service user account does not have any user rights.
"Remote Operations not permitted"	The system is connected but is not configured to allow remote support operations such as backup, upgrades or remote access. See Enabling Additional COM Support Services on page 58.

Table continues…

Message	Description
“Service Monitor Read rights not enabled”	Indicates that the service user account on the system is not correctly configured.
“Service user account has been disabled by the administrator”	Indicates that the service user account is disabled.
“Service user account has been locked temporarily”	Indicates that the service user account has been locked, for example due to too many incorrect password attempts.
“Service user account is currently disabled”	Indicates that the service user account has been disabled.
"Service User password has expired."	The service user account password has expired.
“System is either not reachable or not a valid primary IP Office system”	Indicates a problem connecting to the system or that it is not a supported type of IP Office system. Note that this message is also shown during some stages of system upgrades.
"System is either not reachable or offline for last XXX"	Connection to the customer system has not been detected for the duration stated.
“Upgrade rights are not enabled for this system”	The service user account is not configured correctly.
"Waiting for initial connection"	Order placed, but connection from the customer system has not occurred.

Related links

Using the Customer List on page 19

Viewing the Customer System Details

About this task

From the customer list, you can view additional information about the customer system.

- Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. Locate the customer system in the list of customers (see Using the Customer List on page 19).
2. Click on the customer name.
3. Details of the customer system are displayed.
    - For Server Edition subscription systems, it includes details of the secondary and expansion servers in the Server Edition network.

- If the system's are configured for remote support through COM, links for the support options are shown:
  - For details of using System Status Application, SysMonitor and IP Office Web Manager, see Using the IP Office Administration Apps on page 101.
  - For access to other services using HTTPS, SSH or RDP, see Remote Support Through COM on page 109.

4. To return to the customer list click on the **X** icon.

Related links

Using the Customer List on page 19

Filtering the List

About this task

There are a number of ways in which you can filter the customer list to shown only a particular set of customers.

- Using a COM user account other than **Administrator** or **Support** means the list automatically only includes customers to which your account has been assigned.
- Click on information on the dashboard displays the customer list pre-filtered to only show matching customers. For example, clicking on a particular tag or software release.
- Once in the customer list, use the process below to override any existing search or filter with a new filter.

Procedure

1. Click on the funnel icon.
2. Enter the criteria that should be matched when the filter is applied.
3. Click **Apply**. The list will only show entries that match the criteria you set in the filter.
4. To hide the filter settings, click on the icon or click on the funnel icon again.

Related links

Using the Customer List on page 19

Hiding the Filter

About this task

When you access the list by clicking an item on the dashboard, the list is pre-filtered based on the item you clicked. The filter used is shown at the top of customer list.

Procedure

To hide the filter settings without removing the filtering, click on the ☰ icon or click on the funnel icon again.

Related links

[Using the Customer List](#) on page 19

Sorting the List

About this task

You can use most columns to sort the displayed list. Only one column can be used for sorting at any time.

Procedure

1. Click on the column header.
2. A ↓ icon appears. This indicates that the list has been sorted in descending order based on that column.
3. Clicking on the column header again changes the sort order between ↑ ascending, ↓ descending and unsorted.

Related links

Using the Customer List on page 19

Searching the List

Note: In addition to searching, you can apply a filter and then a search.

Procedure

1. In the search box, entry the value on which to search. This is used match against the values in all fields of the entries.
2. Press return or click on the search icon.
3. The list now only show matching entries.

Related links

Using the Customer List on page 19

Resending the Subscription Email

About this task

When a subscription system is ordered, a subscription email is sent to the technical contact address specified during the order. The email contains key information required to connect the system to the subscription service. Using COM, you can request another copy of the email be sent.

About this task
Procedure

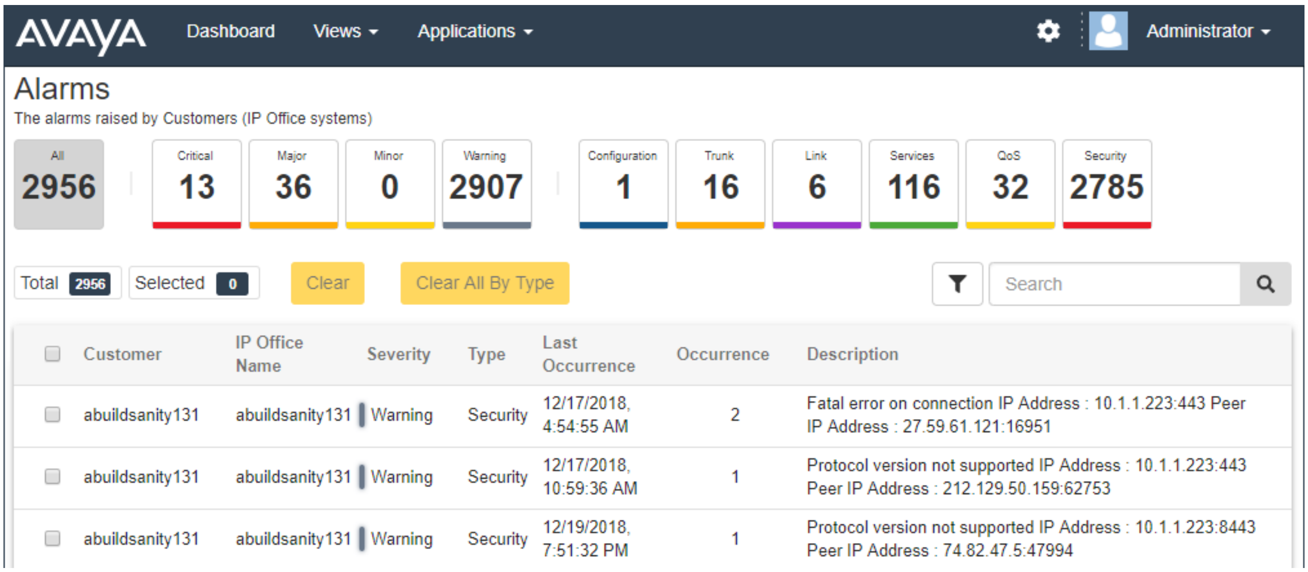
1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems to which you want to apply the action.
3. Click **Action**.
4. Click **Send Email**.

Related links

Using the Customer List on page 19

Chapter 4: Alarms

The alarms list displays a breakdown of the alarms currently logged from your customer's systems.



Each alarm is categorized by its type and its severity. If the alarm has occurred several times, it is only listed once but the time of the last occurrence and number of occurrences are shown.

Related links

- Viewing the Alarms List on page 29
- Searching the Alarms on page 29
- Sorting the Alarms on page 29
- Filtering the Alarms on page 30
- Hiding the Filter on page 30
- Clearing Specific Alarms on page 31
- Clearing All Alarms of a Specific Type on page 31

Viewing the Alarms List

About this task

In addition to the method below:

- You can click alarm information on the dashboard to immediately display the alarm list pre-filtered with only matching alarms. For example, click on an alarm type or severity.
- You can click on the number of alarms shown in the customer list to display the alarm list pre-filtered to show the matching alarms.

Procedure

1. Click on **Views** and then click on **Alarms**.
2. The list of logged customer alarms is displayed.
    - The list can be filtered or searched to show only entries matching your selected criteria.

Related links

Alarms on page 28

Searching the Alarms

Note: In addition to searching, you can apply a filter and then a search.

Procedure

1. In the search box, entry the value on which to search. This is used match against the values in all fields of the entries.
2. Press return or click on the 🔍 search icon.
3. The list now only show matching entries.

Related links

Alarms on page 28

Sorting the Alarms

About this task

You can use most columns to sort the displayed list. Only one column can be used for sorting at any time.

Procedure

1. Click on the column header.

2. A ↓ icon appears. This indicates that the list has been sorted in descending order based on that column.
3. Clicking on the column header again changes the sort order between ↑ ascending, ↓ descending and unsorted.

Related links

Alarms on page 28

Filtering the Alarms

- Once in the customer list, use the process below to override any existing search or filter with a new filter.

About this task

There are a number of ways in which you can filter the customer list to shown only a particular set of customers.

- Using a COM user account other than **Administrator** or **Support** means the list automatically only includes customers to which your account has been assigned.
- Click on information on the dashboard displays the customer list pre-filtered to only show matching customers. For example, clicking on a particular tag or software release.
- Once in the customer list, use the process below to override any existing search or filter with a new filter.

Procedure

1. Click on the funnel icon.
2. Enter the criteria that should be matched when the filter is applied.
3. Click **Apply**. The list will only show entries that match the criteria you set in the filter.
4. To hide the filter settings, click on the icon or click on the funnel icon again.

Related links

Alarms on page 28

Hiding the Filter

About this task

When you access the list by clicking an item on the dashboard, the list is pre-filtered based on the item you clicked. The filter used is shown at the top of customer list.

Procedure

To hide the filter settings without removing the filtering, click on the icon or click on the funnel icon again.

Related links

Alarms on page 28

Clearing Specific Alarms

About this task

If you think the alarm is no longer applicable, that is, the cause of the alarm has been resolved, you can remove the alarm from the list.

Procedure

1. Display the list of alarms. If necessary apply a filter or search.
2. Select the checkbox next to the required alarm or alarms. Use the checkbox at the top of the list to select all alarms in the list.
    - You cannot select alarms for issues which are still occurring. The checkbox on these is grayed out.
3. Click on **Clear**.
4. Click **Confirm** to delete the selected alarms.

Related links

Alarms on page 28

Clearing All Alarms of a Specific Type

About this task

You can clear all alarms of a specific type (**Configuration**, **Trunk**, **Link**, **Services**, **QoS** or **Security**). For example, if a outgoing trunking issue that caused multiple trunk alarms on multiple systems has been resolved, you can clear all the trunk alarms.

Procedure

1. Display the list of alarms.
2. Click on the type of alarm at the top of the screen to show the matching alarms.
3. Click **Clear All By Type**.
4. Click **Confirm** to delete the alarms.
    - Note that alarms for issues which are still occurring are not deleted.

Related links

Alarms on page 28

Chapter 5: Managing System Log Files

For subscription systems, COM can collect and store system log files including Syslog files. Once enabled, the log file collection occurs automatic at approximately 00:30. COM can also be used to manually fetch the latest available logs.

The content of Syslog files for the IP Office service is configured using SysMonitor. See Using Avaya IP Office System Monitor.

Capacity	Details
System Storage	Initially the logs are stored on the individual systems and collected daily at approximately 00:30. The storage limits for local logs depends on the type of system. If the storage limit is reached, the system deletes older logs to provide space for new logs. The limits are: • IP500 V2/V2A systems can retain up to 128MB of log files locally. • Linux-based systems can collect up to 4GB of logs per day.
COM Storage	COM stores all logs files it collects for the duration set by its **CPE Diagnostics Logs Retentions Days** setting. See COM Preferences on page 141. The default is 30 days. This setting applies to all systems being supported by the same instance of COM.

Related links

Enabling Centralized Log Storage on page 33
Managing Customer System Log Files on page 34

Enabling Centralized Log Storage

About this task

Support for uploading logs to COM needs to be enable on the target system before it is allowed.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. Enable the **Centralized Diagnostics Log** option.
5. Click **Update**.

Related links

Managing System Log Files on page 33

Managing Customer System Log Files

Before you begin

- Enable centralized log storage on the system. See Enabling Centralized Log Storage on page 33.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems to which you want to apply the action.
3. Click **Action**.
4. Click on **Log Management**.
5. Use the list to drill down and select the log files that you want.
    - The **Start Date** and **End Date** options can be used to show only logs available between the selected dates.
    - If necessary, click **Fetch New Logs** to connect with the system and upload any logs not already uploaded to COM storage.
6. To download the selected log files, click **Download**. To delete the selected log files, click **Delete**.

Related links

Managing System Log Files on page 33

Chapter 6: Backing Up and Restore

In addition to monitoring customer systems, COM can backup and restore system configuration settings. The backups can be manual or automatic.

- Media Manager application configuration is included in backup/restore operations but the call recordings are not.

Backup	Manual Backup	Automatic
When?	When manually configured through COM. Manual backups can be immediate or scheduled if required.	Automatic backups occur daily between 02:00 and 04:00 system time if not barred by any other running process.
How many backups are stored?	The COM server retains up to 3 manual backups for a customer system. When that limit is reached, adding a new manual backup replaces the oldest manual backup.	The system retains automatic backups for: • The previous 6 days. • The last day of the last 3 weeks. • The last day of the last 11 months.
What is included	For IP500 V2 systems, the system configuration. For Server Edition systems, the configuration elements selected when the manual backup is run or scheduled from COM. For voicemail that can include some or all messages.	For IP500 V2 systems, the system configuration. For Server Edition system, the configuration settings for all services and all servers in the network. For voicemail, the elements included are configured in the system settings. These can only include selective voicemails. See Configuring a System's Selective Voicemail Setting on page 37.
Who can backup?	Manual backups can be configured by **Administrator**, **Supervisor** and **Operator** users.	Performed automatically by the system.
Who can restore?	This is only supported for **Administrator** and **Supervisor** users.	

Related links

Enabling Backup/Restore on page 36
Configuring a System's Automatic Voicemail Backup Options on page 36
Configuring a System's Selective Voicemail Setting on page 37
Manually Backing Up Subscription Systems on page 38
Restoring System Configurations on page 39

Enabling Backup/Restore

About this task

Support for backup/restore from COM needs to be enable on the target system before it is allowed. This also enables upgrading from COM.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. Enable the **Remote Upgrade/Backup** option. This starts automatic backups and allows manual backup and restore actions.
5. Click **Update**.

Related links

Backing Up and Restore on page 35

Configuring a System's Automatic Voicemail Backup Options

About this task

For automatic backups, you can configure which elements of a systems voicemail operation are included.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager. See Using the IP Office Administration Apps on page 101.
2. Select **Applications** > **Voicemail Pro - System Preferences**.
3. Select **Backup Config**.
4. Enable the options required:

Option	Description
Configuration Backup	Include the voicemail service configuration in any backups.
Custom Prompts Backup	Include any prompts in the custom prompts folder.
Selective Mailboxes Backup	Include the messages in the mailboxes of the configured mailboxes. See Configuring a System's Selective Voicemail Setting on page 37.

5. Click **Update**.

Related links

Backing Up and Restore on page 35

Configuring a System's Selective Voicemail Setting

About this task

Whilst backups to COM include the configuration for all services being provides by the customer server, for Server Edition subscription systems they only include emails for a selected set of mailboxes.

- Changing these settings also affect backups run from IP Office Web Manager.

Procedure

1. Access the system using IP Office Web Manager. See Using the IP Office Administration Apps on page 101.
2. Select **Applications** > **Voicemail Pro - System Preferences**.
3. If necessary, select the primary server.
4. Select **User Group**.
5. Use the **+Add User** and **-Remove User** to create a list of the users whose mailboxes should be included in backups.
6. Click **Update**.

Related links

Backing Up and Restore on page 35

Manually Backing Up Subscription Systems

About this task

COM can be used to backup and restore the configuration of customer system. Automatic backups each day are enabled by enabling the customer server's **Remote Upgrade/Backup** setting. The process below is only required for manuals backups.

- The COM server retains up to 3 manual backups for a customer system. When that limit is reached, adding a new manual backup replaces the oldest manual backup.

Before you begin

- This process is only supported to systems on which **Remote Upgrade/Backup** has been enabled. See Enabling Additional COM Support Services on page 58.
- A system can only perform one action (**Backup**, **Restore** or **Upgrade**) at any time. That includes automatic backups which occur between 02:00 and 04:00 each day (system time).
- This is only supported for **Administrator** and **Supervisor** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems to which you want to apply the action.
3. Click **Action**.
4. Click on **Backup**.
5. Enter a name for the job.
6. If the system being backed up is a Server Edition, select what should be included in the backup.
   - The **Selective Voicemails** option only includes voicemail messages from the selected set of mailboxes. See Configuring a System's Selective Voicemail Setting on page 37.
7. If you want to schedule the action:
   a. Select the **Do you want to schedule this job?** checkbox.
   b. Click the calendar icon to select the date and time for the scheduled job to occur.

      The times shown are local to the COM server. The actual times on customer systems may differ if they are located in other regions and countries. Keep this in mind for activities such as scheduling jobs.
8. Click **Backup**.
9. The task is added to the list of scheduled jobs and started immediately if no scheduled date and time was set. See Viewing Scheduled Jobs on page 43.

Related links

Backing Up and Restore on page 35

Restoring System Configurations

About this task

This process can be used to restore the previous backup of a system or systems. See Restoring System Configurations on page 39.

Warning:

- This process will cause the target system to reboot.

Before you begin

- This process is only supported to systems on which **Remote Upgrade/Backup** has been enabled. See Enabling Additional COM Support Services on page 58.
- A system can only perform one action (**Backup**, **Restore** or **Upgrade**) at any time. That includes automatic backups which occur between 02:00 and 04:00 each day (system time).
- This process cannot be scheduled.
- This is only supported for **Administrator** and **Supervisor** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems to which you want to apply the action.
3. Click **Action**.
4. Click on **Restore**.
5. The list of previous backups available is displayed. Click **>** to expand the backup required and select the element(s) from the backup that you want restored.
6. Click **Restore**.

Related links

Backing Up and Restore on page 35

Chapter 7: Upgrading Customer Systems

In addition to monitoring the status of customer systems, COM can be used to upgrade systems.

- For servers in a Server Edition network, this upgrades all IP Office servers in the network.
- For servers in a SCN network, each IP Office server must be upgraded individually.
- Upgrading IP500 V2 systems upgrades any expansion units connected to the control unit.
- The system upgrades includes phone firmware files to upgrade all phones using the upgraded systems as their file server.
- This is only supported for **Administrator**, **Supervisor** and **Operator** users.

Related links

Enabling Upgrading on page 40
Upgrading Systems on page 41

Enabling Upgrading

About this task

Support for upgrade from COM needs to be enable on the target system before it is allowed. This also enables back/restore from COM.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. Enable the **Remote Upgrade/Backup** option.
5. Click **Update**.

Related links

Upgrading Customer Systems on page 40

Upgrading Systems

Before you begin

- This process is only supported to systems on which **Remote Upgrade/Backup** has been enabled. See Enabling Additional COM Support Services on page 58.
- A system can only perform one action (**Backup**, **Restore** or **Upgrade**) at any time. That includes automatic backups which occur between 02:00 and 04:00 each day (system time).
- As with all upgrades, it is recommended that you backup the systems prior to upgrading. See Backing Up and Restore on page 35.

About this task

The following process can be used to upgrade subscription systems.

- This is only supported for **Administrator**, **Supervisor** and **Operator** users.
- Multiple systems can selected for upgrading as part of the same action. However, when doing this all the selected systems must be the same type or server, either **Server Edition** or **IP500 V2**.
- When upgrading a **Server Edition** server, after the primary server is upgraded, all other servers in the primary server's network are upgraded via their websocket connections.
- When upgrading a **IP500 V2** server that is in a SCN network, each server in the network needs to be individually upgraded.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems you want to upgrade. They should display a icon in their status meaning `New Version Available`.
3. Click **Action**.
4. Click on **Upgrade** and then select one of the choices:

Option	Description
Transfer & Upgrade	Transfer the files required to upgrade the selected system/systems and then perform the upgrade.
Transfer	Transfer the files required for upgrading the system but do not perform the upgrade. The upgrade can be completed when required using the **Upgrade** action.
Upgrade	Upgrade the system to which upgrade files have been transferred using the **Transfer** action.

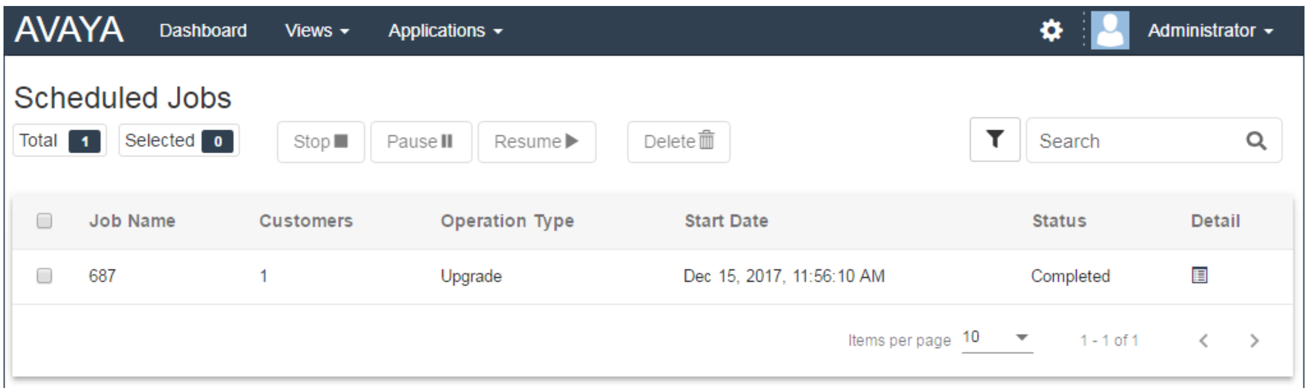
5. Use **Restart IP Phones** to select whether you want all IP phones restarted after the upgrade. If restarted, the phones will update their settings file and, if necessary, firmware.
6. Select the version of the component required from the list.
7. Click **Transfer & Upgrade**, **Transfer** or **Upgrade** as previously selected.
8. The task is added to the list of scheduled jobs and started immediately if no scheduled date and time was set. See Viewing Scheduled Jobs on page 43.

Related links

Upgrading Customer Systems on page 40

Chapter 8: Viewing Scheduled Jobs

You can view the list of scheduled jobs. The list also includes immediate jobs which are already running.



- The times show are local to the COM server. The actual times on customer systems may differ if they are located in other regions and countries. Keep this in mind for activities such as scheduling jobs.

To view the scheduled jobs:

1. Click on **Views** and select **Scheduled Jobs**.
2. The list of scheduled jobs is displayed. A icon indicates jobs which are in progress.

Related links

Filtering the Scheduled Jobs List on page 44
Searching the Scheduled Jobs List on page 44
Sorting the Scheduled Jobs on page 45
Viewing Job Details on page 45
Deleting Scheduled Jobs on page 46
Pausing Scheduled Jobs on page 46
Resuming Scheduled Jobs on page 46
Stopping a Scheduled Job on page 47

Filtering the Scheduled Jobs List

- Once in the customer list, use the process below to override any existing search or filter with a new filter.

About this task

There are a number of ways in which you can filter the customer list to shown only a particular set of customers.

- Using a COM user account other than **Administrator** or **Support** means the list automatically only includes customers to which your account has been assigned.
- Click on information on the dashboard displays the customer list pre-filtered to only show matching customers. For example, clicking on a particular tag or software release.
- Once in the customer list, use the process below to override any existing search or filter with a new filter.

Procedure

1. Click on the funnel icon.
2. Enter the criteria that should be matched when the filter is applied.
3. Click **Apply**. The list will only show entries that match the criteria you set in the filter.
4. To hide the filter settings, click on the icon or click on the funnel icon again.

Related links

Viewing Scheduled Jobs on page 43

Searching the Scheduled Jobs List

Note: In addition to searching, you can apply a filter and then a search.

Procedure

1. In the search box, entry the value on which to search. This is used match against the values in all fields of the entries.
2. Press return or click on the search icon.
3. The list now only show matching entries.

Related links

Viewing Scheduled Jobs on page 43

Sorting the Scheduled Jobs

About this task

You can use most columns to sort the displayed list. Only one column can be used for sorting at any time.

Procedure

1. Click on the column header.
2. A ↓ icon appears. This indicates that the list has been sorted in descending order based on that column.
3. Clicking on the column header again changes the sort order between ↑ ascending, ↓ descending and unsorted.

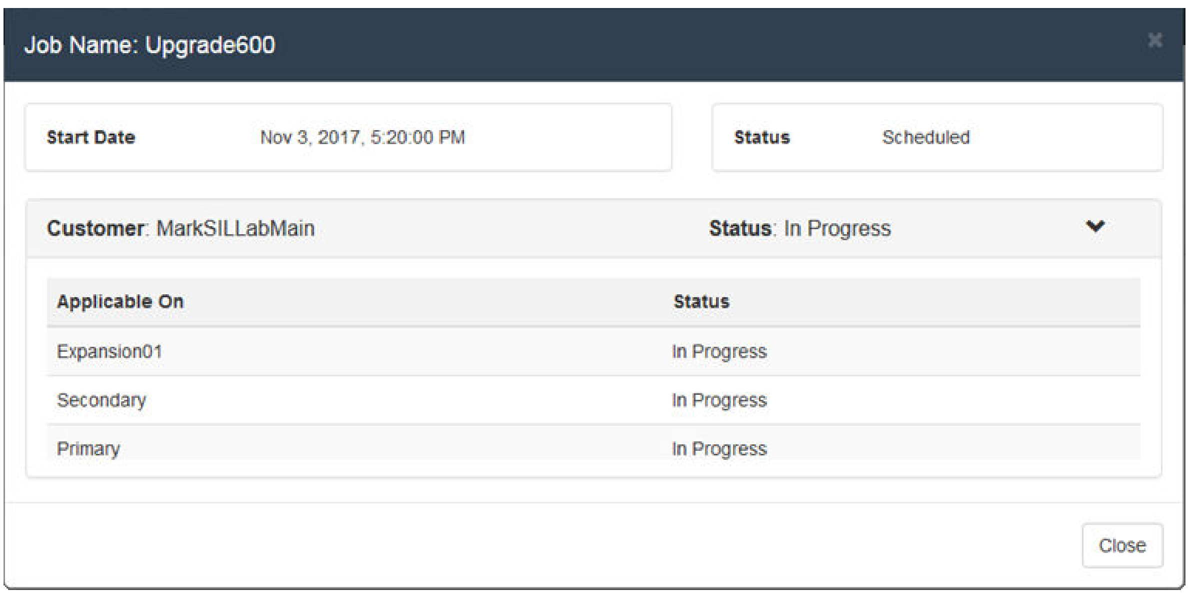
Related links

[Viewing Scheduled Jobs](#) on page 43

Viewing Job Details

Procedure

1. Display the list of scheduled jobs. See Viewing Scheduled Jobs on page 43.
2. Click on the icon next to the job.
3. The details of the job are displayed.



4. Click on **Close** to return to the list of jobs.

Related links

[Viewing Scheduled Jobs](#) on page 43

Deleting Scheduled Jobs

Procedure

1. Display the list of scheduled jobs. See Viewing Scheduled Jobs on page 43.
2. Select the checkbox next to the required jobs. Use the checkbox at the top of the list to select all jobs in the list.

   Note: You cannot delete jobs which are already running (shown by a icon).
3. Click on **Delete** .
4. Click **Confirm** to delete the selected jobs.

Related links

Viewing Scheduled Jobs on page 43

Pausing Scheduled Jobs

To pause scheduled jobs:

Note: You cannot pause, resume or stop jobs that were started immediately, for example upgrades that were scheduled.

1. Display the list of scheduled jobs. See Viewing Scheduled Jobs on page 43.
2. Select the checkbox next to the required jobs. Use the checkbox at the top of the list to select all jobs in the list.
3. Click on **Pause** .
4. Click **Confirm** to pause the selected jobs.
5. The **Status** of those jobs changes to `Paused`.

Related links

Viewing Scheduled Jobs on page 43

Resuming Scheduled Jobs

To resume paused jobs:

1. Display the list of scheduled jobs. See Viewing Scheduled Jobs on page 43.

2. Select the checkbox next to the required jobs. Use the checkbox at the top of the list to select all jobs in the list.
3. Click on **Resume** ▶.
4. Click **Confirm** to resume the selected jobs.
5. The **Status** of those jobs changes to `Scheduled`.

Related links

Viewing Scheduled Jobs on page 43

Stopping a Scheduled Job

To stop a scheduled job:

If a scheduled job is stopped it cannot be restarted.

- You cannot pause, resume or stop jobs that were started immediately, for example upgrades that were not scheduled.

1. Display the list of scheduled jobs. See Viewing Scheduled Jobs on page 43.
2. Select the checkbox next to the required jobs. Use the checkbox at the top of the list to select all jobs in the list.
3. Click on **Stop** ■.
4. Click **Confirm** to stop the selected jobs.
5. The **Status** of those jobs changes to `Stopped`.

Related links

Viewing Scheduled Jobs on page 43

Part 3: Adding Customer Systems

Chapter 9: Adding, Editing and Deleting the Listed Customers

COM can support up to 1000 customers and a total of 3000 IP Office servers within the customer networks.

Normally new customer systems are automatically added when the customer system first subscribes. However, sometimes systems may need to be added manually. In addition, it may be necessary occasionally to edit customer details or to delete a customer.

This is only supported for **Administrator** users.

Related links

[Adding a New Customer](#) on page 49
[Customer Account Settings](#) on page 50
[Assigning Users to a Customer](#) on page 51
[Editing Customer Details](#) on page 52
[Deleting Customers](#) on page 52

Adding a New Customer

About this task

This process can be used to add a customer to COM if they have not been added automatically.

- This is only supported for **Administrator** users.

Before you begin

- Before adding a customer, you must first confirm that the customer system has been enabled for COM support. See [System Configuration for COM](#) on page 54.

Procedure

1. Click on **Views** and then click on **Customers**. The list of existing customers is displayed.
2. Click **Add**.
3. Enter the customer details. See [Customer Account Settings](#) on page 50.
4. When you have added all the customers information, click **Test Connection**.

5. The menu indicates if the connection was successful or not.
6. If the connection was not successful, make any changes necessary and click **Test Connection** again.
7. When finished click **Save**.

Related links

Adding, Editing and Deleting the Listed Customers on page 49

Customer Account Settings

The following data fields are used to configure a customer entry:

Field	Description
Name	Enter a unique name for the customer whose site is to be managed using COM.
System Name	The system name. Shown for information only, not editable.
IP Address/FQDN	Shown for information only, not editable.
Port	Shown for information only, not editable.
Service User Name	The name of the security service user account configured on the customer systems for COM. The default name is ***COMAdmin***. See Enabling COM Support on Server Edition Systems on page 55.
Password	The security password of the security service user specified above.
Tags	Tags are useful in the customer and other menus to identify particular customers. You can associate up to 5 tags with a customer. • To select an existing tag, click on the tags box and select from the list of existing tags shown. • To remove a tag click on the **X** next to the tag name. • To create a new tag click on **New**.
Phone	For information only. Enter a contact phone number for the customer.
Email	Enter a contact email address for the customer.

Table continues…

Field	Description
Assigned Operators	Whilst **Administrator** and **Support** users see all customer systems, other user have to be assigned to systems. Assignment can be done manually and/or automatically as below. This field lists the users who have been manually assigned to the customer system. • **Manual Assignment** – Within the settings for the customer system, the **Assigned Operators** field can be used to select COM users. See Editing Customer Details on page 52. - This can be done by **Administrator** users to assign any other users to any customer systems. - It can also be done by **Supervisor** users. However, they can only assign users that they have created and only to customer systems to which they themselves have been manually assigned. • **Automatic Assignment** – Within the settings for users, the **Labels** field can be set with multiple labels. When the label matches the **Provider** or **Reseller** setting in the configuration of a customer system, those users are automatically assigned to that system. See COM User Settings on page 68.
Address	Enter an address for the customer site.
Notes	Enter any extra information that may be important to anybody using COM to manage this customer.
Reseller	These values indicate the reseller and provider for which the system was created. COM users with the same value as one of their **Labels** settings are automatically assigned to the matching systems.
Provider	

Related links

Adding, Editing and Deleting the Listed Customers on page 49

Assigning Users to a Customer

About this task

Within the customer details, the icon indicates that the system has assigned COM users. Hovering over the icon display a list of those assigned users. It does not include **Administrator** and **Support** users as they can see all customers.

User assignment can be done manually and/or automatically:

- **Manual Assignment** – Within the settings for the customer system, the **Assigned Operators** field can be used to select COM users. See Editing Customer Details on page 52.
  - This can be done by **Administrator** users to assign any other users to any customer systems.
  - It can also be done by **Supervisor** users. However, they can only assign users that they have created and only to customer systems to which they themselves have been manually assigned.

- **Automatic Assignment** – Within the settings for users, the **Labels** field can be set with multiple labels. When the label matches the **Provider** or **Reseller** setting in the configuration of a customer system, those users are automatically assigned to that system. See COM User Settings on page 68.

Related links

Adding, Editing and Deleting the Listed Customers on page 49

Editing Customer Details

About this task

This process can be used to edit the details of a listed customer.

- This is only supported for **Administrator** users.

Procedure

1. Display the list of customers. See Viewing the Customer List on page 20
2. Select the checkbox next to the required customer.
3. Click on **Edit**.
4. Amend the customer details as required. See Customer Account Settings on page 50.
5. Click **Update**.

Related links

Adding, Editing and Deleting the Listed Customers on page 49

Deleting Customers

About this task

This process removes a customer from the list of customers supported by COM.

- This is only supported for **Administrator** users.

Procedure

1. Display the list of customers.
2. Select the checkbox next to the required customer or customers. Use the checkbox at the top of the list to select all customers in the list.
3. Click on **Delete**.
4. Click **Confirm** to delete the selected customers.

Related links

Adding, Editing and Deleting the Listed Customers on page 49

Part 4: System Configuration for COM

System Configuration for COM

This section covers the IP Office system configuration required for the system to be monitored and managed using COM. Normally, this configuration is applied automatically by the customization file applied when the IP Office is initially subscribed. However, some individual customers may require specific settings to be enabled or disabled.

The settings can be divided into two groups:

- The configuration of an IP Office service user for use by COM to connect to the customer systems and monitor their status and alarms. See Configuring the IP Office Service User for COM on page 55.
- Additional configuration to allow COM to support features such as upgrades, backup/restore, log file collection and similar. See Configuration for additional COM features on page 58.
- Configuration necessary to include any IP Office Application Servers within the support. See Application Server Configuration for COM on page 63.

Chapter 10: Configuring the IP Office Service User for COM

The following processes configure the IP Office service user used by COM to connect to the customer systems and monitor their status and alarms.

Related links

Enabling COM Support on Server Edition Systems on page 55
Enabling COM Support on IP500 V2 Systems on page 56
Creating the COMAdmin Service User and Rights Group on page 56

Enabling COM Support on Server Edition Systems

About this task

To connect to a customer's systems, by default COM uses the settings of a security user called ***COMAdmin*** configured on those systems.

- On customer premises systems the ***COMAdmin*** security user is disabled by default and doesn't have a password set. Use the process below to enable the security user requires you to have administrator access to the customer system and may need to be performed by the original system installer or maintainer.
  - If at a later date, the customer adds another IP Office to their network, you should repeat this process to make the new system visible and manageable by COM.

Procedure

1. Log in to IP Office Web Manager on the Server Edition/Select system.
2. Click **Solution**.
3. Click on the **Actions** drop-down and select **Remote Operations Management**.
4. Enter and confirm the password that the systems in the customer solution should use for their COM connection.
5. Click **Enable & Synch**.
6. This enables the ***COMAdmin*** security user account on the primary system and sets its password. The change is then synchronizes to all other systems in the solution. This process can take several minutes depending on the number of systems in the solution.

7. When the successful synchronization message appears, click **Cancel**.

Related links

Configuring the IP Office Service User for COM on page 55

Enabling COM Support on IP500 V2 Systems

About this task

To connect to a customer's system, by default COM uses the settings of a security user called ***COMAdmin*** configured on those systems. On new systems, this service user account exists by default.

Procedure

1. Login to IP Office Web Manager using an account that has rights to security administration.
2. Select **Security** > **Security Settings**.
3. Click **Service Users**.
4. Locate the user ***COMAdmin*** and set their account status to **Enabled**.
    - If the user does not exist, see Creating the COMAdmin Service User and Rights Group on page 56.
5. Enter and confirm the account password.
6. In the **RIGHTS GROUPS** section, select **COM Admin**.
7. Click **Save**.
8. In COM, change the customer details password to match the ***COMAdmin*** password. See Editing Customer Details on page 52.

Related links

Configuring the IP Office Service User for COM on page 55

Creating the *COMAdmin* Service User and Rights Group

To connect to a customer's system, by default COM uses the settings of the ***COMAdmin*** service user and **COM Admin** rights group configured in the system's security settings.

Those settings are present by default on new systems and just need the service user account enabled and service user password set. That is normally done automatically during the initial connection of a subscription to COM.

However, on existing older systems being converted to subscription usage, the service user and rights group may not exist. In that case, they need to be created and configured manually.

About this task

This process use IP Office Web Manager to manually create the ***COMAdmin*** service user and **COM Admin** rights group used for COM connection.

Procedure

1. Login to IP Office Web Manager using an account that has rights to security administration.
2. Select **Security** > **Security Settings**.
3. Click Rights Groups.
4. If a group called **COM Admin** does not already exist, click **+Add Rights Group**. Otherwise, use to the details below to check the settings of the existing group.
5. Check that the group has the following settings enabled:

Tab	Settings
Web Services	• **Security Write Own Password** • **Backup** • **Upgrade** • **Service Monitor Read**.

6. Click **Save**.
7. Click **Service Users**.
8. If the service user ***COMAdmin*** does not already exist, click **+Add Service User**.
9. Enter the name ***COMAdmin*** and set the account status to **Enabled**.
10. Enter and confirm the account password.
11. In the **RIGHTS GROUPS** section, select **COM Admin**.
12. Click **Save**.
13. In COM, change the customer details password to match the ***COMAdmin*** password. See Editing Customer Details on page 52.

Related links

Configuring the IP Office Service User for COM on page 55

Chapter 11: Configuration for additional COM features

The following processes can be used to check and enable support for additional COM features on specific customer IP Office systems.

Related links

Enabling Additional COM Support Services on page 58
Configuring a System's Selective Voicemail Setting on page 59
Configuring a System's Voicemail Backup Settings on page 60
Enabling Automatic Certificate Management on page 61
Enabling HTTP Server Support on page 61

Enabling Additional COM Support Services

About this task

In addition to monitoring the status and alarms of customer systems, COM can also support a number of other actions. The actions supported are configured using the settings below.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. Select the required settings:

Setting	Description
Centralized Management	Support remote connections to IP Office servers using IP Office admin tools (System Status Application, SysMonitor and IP Office Web Manager). See Using the IP Office Administration Apps on page 101.
Centralized Diagnostics Log	Support the uploading and storage of system log files to COM. See Managing System Log Files on page 33.
Remote Upgrade/ Backup	Support backup and restore from COM. Enabling this setting automatically enables automatic daily backups. See Backing Up and Restore on page 35. Also support system upgrades. See Upgrading Customer Systems on page 40.
Remote Access	Support HTTPS, SFTP, SSH and RDP connections to IP Office servers managed by COM. See Remote Support Through COM on page 109.
Co-located Servers	This option allows **Remote Access** support to be extended to other servers on the same network as the COM managed IP Office systems. That includes connection to UCM modules and standalone IP Office Application servers. This also requires configuration of a TCP tunnel for each connection (see Creating Tunnels for Remote Servers and Services on page 112).

5. Click **Update**.

Related links

Configuration for additional COM features on page 58

Configuring a System's Selective Voicemail Setting

About this task

Whilst backups to COM include the configuration for all services being provides by the customer server, for Server Edition subscription systems they only include emails for a selected set of mailboxes.

- Changing these settings also affect backups run from IP Office Web Manager.

Procedure

1. Access the system using IP Office Web Manager. See Using the IP Office Administration Apps on page 101.
2. Select **Applications** > **Voicemail Pro - System Preferences**.
3. If necessary, select the primary server.
4. Select **User Group**.

5. Use the **+Add User** and **-Remove User** to create a list of the users whose mailboxes should be included in backups.
6. Click **Update**.

Related links

Configuration for additional COM features on page 58

Configuring a System's Voicemail Backup Settings

About this task

For automatic backups, you can configure which elements of a systems voicemail operation are included.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager. See Using the IP Office Administration Apps on page 101.
2. Select **Applications** > **Voicemail Pro - System Preferences**.
3. Select **Backup Config**.
4. Enable the options required:

Option	Description
Configuration Backup	Include the voicemail service configuration in any backups.
Custom Prompts Backup	Include any prompts in the custom prompts folder.
Selective Mailboxes Backup	Include the messages in the mailboxes of the configured mailboxes. See Configuring a System's Selective Voicemail Setting on page 37.

5. Click **Update**.

Related links

Configuration for additional COM features on page 58

Enabling Automatic Certificate Management

About this task

COM can perform the role of providing certificates to the subscriptions system and updating those certificates when required.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Login to IP Office Web Manager using an account that has rights to security administration.
2. Select **Security** > **Security Settings**.
3. Select **Certificates**.
4. Enable the options required:

Option	Description
Automatic Certificate Management	Use certificates provided by COM and updated by COM when required.
Automatic Phone Provisioning	Automatically update phone certificates when the system certificates change. This setting is only supported when **Automatic Certificate Management** is enabled.

5. Click **Save**.

Related links

Configuration for additional COM features on page 58

Enabling HTTP Server Support

About this task

While most phones obtain their firmware files direct from their IP Office system, some (for example Vantage phones) need to be redirected to a separate HTTP file server. For subscription systems, that alternate file server is provided by COM.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.

3. Set the **HTTP Server IP Address** back to 0.0.0.0 to disable that setting. The **HTTP Server UI**is now used for redirected HTTP requests made by phones. The address in the **HTTP Server UI** field is automatically set by the configuration file used by the system when it initially subscribed.
4. Click **Update**.

Related links

Configuration for additional COM features on page 58

Chapter 12: Application Server Configuration for COM

For IP Office R11.1 FP2 and higher, IP Office Application servers and UCM modules are included in the servers supported by Customer Operations Manager.

For UCM modules, the required configuration changes are applied automatically. However, the application servers the required configuration changes need to be applied manually.

Related links

Setting the websocket connection password on page 63
Configuring the Application Server on page 64

Setting the websocket connection password

About this task

If using the application server with a subscription mode IP Office system, use the following process to set the password for the websocket connected required between the two servers to allow COM support of the application server. This password is required for the initial configuration of the application server.

Procedure

1. Connect to the IP Office system using IP Office Web Manager.
2. Select **Security** > **Security Settings**
3. Click **Service Users**.
4. Locate the **Adjunct Server** service user and click .
5. Click the icon next to **Password** and enter the password for the websocket connection between the two servers.
6. Change the service user's **Account Status** to **Enabled**.
7. Click **Save**.

Next steps

- Rerun the initial configuration of the application server. See Configuring the Application Server on page 64.

Related links

Application Server Configuration for COM on page 63

Configuring the Application Server

Procedure

1. Connect to the application server using IP Office Web Manager.
2. Click on the ☰ icon adjacent to the server details and select **Initial Configuration**.
3. The initial configuration menu for the server is displayed with the server's existing settings.
4. In **IP Office FQDN/IP Address**, enter the address of the IP Office system which the application server will be supporting.
5. For the **Web Socket Password**, enter the password set for the **Adjunct Server** service user configured on the IP Office system the application server will be supporting. See Setting the websocket connection password on page 63.
6. Click **Apply**.

Related links

Application Server Configuration for COM on page 63

Part 5: COM User Settings

Chapter 13: Managing the COM Users

The actions you can perform to add, edit and delete other COM users depends on your own account type:

- If you are logged in as an **Administrator** user, you can view, add, edit and delete other user accounts.
- If logged in as a **Supervisor** user you can add additional **Operator** users. You can also view, edit and delete those additional users. For those users, you can only assign labels and customers which are also assigned to your user account.

Related links

Viewing the User Accounts on page 66
Assigning Users to a Customer on page 67
COM User Settings on page 68
Filtering the List of Users on page 69
Sorting the Users on page 70
Searching the User List on page 70
Adding a New User on page 71
Editing a User’s Settings on page 71
Deleting Users on page 72

Viewing the User Accounts

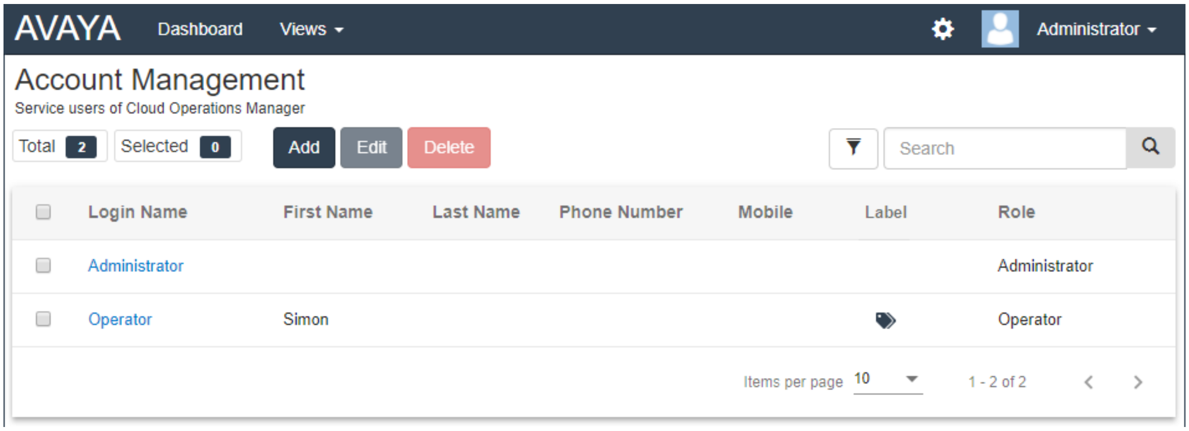
Note:

- If you are logged in as an **Administrator** user, you can view, add, edit and delete other user accounts.
- If logged in as a **Supervisor** user you can add additional **Operator** users. You can also view, edit and delete those additional users. For those users, you can only assign labels and customers which are also assigned to your user account.

Procedure

1. Click on .

2. Click on **Account Management**. The list of users and their details is shown.



Related links

[Managing the COM Users](#) on page 66

Assigning Users to a Customer

About this task

Within the customer details, the icon indicates that the system has assigned COM users. Hovering over the icon display a list of those assigned users. It does not include **Administrator** and **Support** users as they can see all customers.

User assignment can be done manually and/or automatically:

- **Manual Assignment** – Within the settings for the customer system, the **Assigned Operators** field can be used to select COM users. See [Editing Customer Details](#) on page 52.
  - This can be done by **Administrator** users to assign any other users to any customer systems.
  - It can also be done by **Supervisor** users. However, they can only assign users that they have created and only to customer systems to which they themselves have been manually assigned.
- **Automatic Assignment** – Within the settings for users, the **Labels** field can be set with multiple labels. When the label matches the **Provider** or **Reseller** setting in the configuration of a customer system, those users are automatically assigned to that system. See [COM User Settings](#) on page 68.

Related links

[Managing the COM Users](#) on page 66

COM User Settings

When adding or editing a user account, the settings listed below are available.

<table>
<tr><th>Field</th><th>Description</th></tr>
<tr><td>Login Name</td><td>This is the name the account user needs to use to login to COM. This field must be set. The maximum length is 15 characters.</td></tr>
<tr><td>Password/Confirm Password</td><td>This is the password that the account user needs to use to login. This field must be set.
• The password must be between 9 and 31 characters long.
• It must include characters of 2 or more of the following types: uppercase, lowercase, numbers, special characters.
• The server will not allow you to reuse previous passwords.</td></tr>
<tr><td>Role</td><td>Select the user role. The options are:
• Administrator – Users with this role can access all COM menus and functions.
• Support – Users with this role are similar to Administrator users. However, their account operates in read-only mode. See Read-Only and Wallboard Display Modes on page 12.
• Operator – Users with this role can only see and manage customers to which they have been assigned. See Assigning Users to a Customer on page 51.
• Supervisor – Users with this role are similar to Operator users. However, they are able to create and manage additional user accounts (other than Administrator and Support users).
- They are only able to assign labels to those users that have been assigned to their own account.
- Through the customer list, in the customer system settings they can manually assign or remove the users that they have created.
- They can change the customer system’s CMS/IMS setting.
• Read-Only – Users with this role are similar to Operator users. However, their account operates in read-only mode. See Read-Only and Wallboard Display Modes on page 12.</td></tr>
<tr><td>Labels</td><td>This setting is only shown for operator type users. The labels set are used to automatically assign the users to any customer systems that have the same Provider or Reseller values configured in the system.
Supervisor users creating or editing additional users, can only see and select labels already assigned to their own user account.</td></tr>
<tr><td>First Name</td><td rowspan="2">The account user's name details for display within menus. The total length, including spaces, is limited to 31 characters.</td></tr>
<tr><td>Last Name</td></tr>
<tr><td>Phone Number</td><td>Enter a number that can be used to contact the user if necessary. Maximum length 15 digits.</td></tr>
</table>

Table continues…

Field	Description
Mobile	Enter a number that can be used to contact the user if necessary. Maximum length 15 digits.
Email Address	Enter an address that can be used to contact the user if necessary.
Session Timeout	Select the time after which the user should be automatically logged out if there has been no activity. The option allows the selection of a value between 5 minutes and 30 minutes in 5 minute increments.
Wallboard Mode	This option is available for users with their **Role** set to **Support** or **Read-Only**. When selected, the user is no longer automatically logged out when their **Session Timeout** expires. However, after that, whilst they still receive screen updates they are no longer able to navigate to any other menus or make any new filter or tag selection changes.
Disable Account	If the selected, the account is disabled and the user is not able to login.
Force New Password	If selected, the user is forced to change their password when they next login.
Enable Account Expiration	If selected, the user account can be automatically disabled on a set date. When this occurs the Account Status is automatically disabled and must be selected again for the user to be able to login again.
Select Date	The date on which the user account is disabled if **Enable Account Expiration** is selected. By default, the date is set to one year forward but you can change this to a different date if required.

Related links

Managing the COM Users on page 66

Filtering the List of Users

- Once in the customer list, use the process below to override any existing search or filter with a new filter.

About this task

There are a number of ways in which you can filter the customer list to shown only a particular set of customers.

- Using a COM user account other than **Administrator** or **Support** means the list automatically only includes customers to which your account has been assigned.
- Click on information on the dashboard displays the customer list pre-filtered to only show matching customers. For example, clicking on a particular tag or software release.
- Once in the customer list, use the process below to override any existing search or filter with a new filter.

Procedure

1. Click on the funnel icon.
2. Enter the criteria that should be matched when the filter is applied.

3. Click **Apply**. The list will only show entries that match the criteria you set in the filter.
4. To hide the filter settings, click on the ☰ icon or click on the ▼ funnel icon again.

Related links

Managing the COM Users on page 66

Sorting the Users

About this task

You can use most columns to sort the displayed list. Only one column can be used for sorting at any time.

Procedure

1. Click on the column header.
2. A ↓ icon appears. This indicates that the list has been sorted in descending order based on that column.
3. Clicking on the column header again changes the sort order between ↑ ascending, ↓ descending and unsorted.

Related links

Managing the COM Users on page 66

Searching the User List

Note: In addition to searching, you can apply a filter and then a search.

Procedure

1. In the search box, entry the value on which to search. This is used match against the values in all fields of the entries.
2. Press return or click on the 🔍 search icon.
3. The list now only show matching entries.

Related links

Managing the COM Users on page 66

Adding a New User

- If you are logged in as an **Administrator** user, you can view, add, edit and delete other user accounts.
- If logged in as a **Supervisor** user you can add additional **Operator** users. You can also view, edit and delete those additional users. For those users, you can only assign labels and customers which are also assigned to your user account.

Procedure

1. Select the users view. See Viewing the User Accounts on page 66
2. Click **Add**.
3. Enter the details for the user account settings. See COM User Settings on page 68.
4. When completed, click **Save**.

Related links

Managing the COM Users on page 66

Editing a User's Settings

- If you are logged in as an **Administrator** user, you can view, add, edit and delete other user accounts.
- If logged in as a **Supervisor** user you can add additional **Operator** users. You can also view, edit and delete those additional users. For those users, you can only assign labels and customers which are also assigned to your user account.

Procedure

1. Select the users view.
2. Either:
    - Click on the user's displayed **Login Name**.
    - Select the checkbox next to the user and click **Edit**.
3. Enter the details for the user account settings. See COM User Settings on page 68.
4. When completed click **Save**.

Related links

Managing the COM Users on page 66

Deleting Users

- If you are logged in as an **Administrator** user, you can view, add, edit and delete other user accounts.
- If logged in as a **Supervisor** user you can add additional **Operator** users. You can also view, edit and delete those additional users. For those users, you can only assign labels and customers which are also assigned to your user account.

Procedure

1. Select the users view. See Viewing the User Accounts on page 66.
2. Select the checkbox next to each user to be deleted.
   - The checkbox at the top of the list of users can be used to select or deselect all.
   - You cannot select and then delete the account which you have used to login.
3. Click **Delete**.

Related links

Managing the COM Users on page 66

Chapter 14: Your User Account

You can view and adjust some of your COM user account settings.

Related links

Viewing Your User Profile on page 73
Changing Your Password on page 73
Adding an Avatar on page 74

Viewing Your User Profile

Procedure

1. Click on your user name shown top-right and select **Profile**.
2. The information about your user account is displayed.
3. You can use the profile to change your password or add an avatar image for your account.

Related links

Your User Account on page 73

Changing Your Password

About this task

Note that changing your password will require you to login again.

Procedure

1. Click on your user name shown top-right and select **Profile**.
2. Click on the edit icon shown bottom-right.
3. Enter your existing password and then enter and confirm the new password you want to use. Note that the application remembers your previous passwords and will not let you reuse them.
   - The password must be between 9 and 31 characters long.

- It must include characters of 2 or more of the following types: uppercase, lowercase, numbers, special characters.
- The server will not allow you to reuse previous passwords.

4. Click **Submit** to make the password change.
5. You will be asked to login again using the new password.

Related links

Your User Account on page 73

Adding an Avatar

Procedure

1. Click on your user name shown top-right and select **Profile**.
2. Click on the edit icon shown under the current avatar image.
3. Select to the new image file you want to use and click **Open**.

Related links

Your User Account on page 73

Part 6: Customization File Management

Chapter 15: Customization File Management

When a new customer system first connects to COM, it is provided with various files (if they exist) which can be used to customize its operation. For example, templates for preferred SIP line provider's lines. Those files are provided from sets of files stored with COM.

In addition, when required the system can be instructed to update the customization files again.

The files are stored and used in a hierarchical structure. That that is:

- A set of customization files can be provided for all customer systems supported by the same distributor.
- A set of customization files can be provided for all customer systems supported by the same reseller.
- A set of customization files can be provided for an individual customer system.
- Customization files may affect the Avaya Vantage™ and Avaya Workplace Client software settings but they are not used for the Avaya Vantage™ and Avaya Workplace Client software file. Those are managed separately. See Avaya Workplace Client File Management on page 97 and Vantage File Management on page 94.

Related links

The Customization Files on page 76
How the Customer Systems Load and Use the Files on page 77

The Customization Files

When instructed to load any customization files available, the customer system requests the following `.tar` format archive files. It then downloads and unpacks those files (see How the Customer Systems Load and Use the Files on page 77). Note that the limit for file size is 10MB.

The supported files and their contents are:

File	Contents and Role
`CustomPhoneFiles.tar`	A file with this name can be used to hold files (other than firmware) for use by the system's phones. See The CustomPhoneFiles.tar File (Phone Settings and Image Files) on page 80. • A `46xxspecials.txt` file containing phone settings that are in addition to the auto-generated `46xxsettings.txt` settings file the customer system provides. • Any screen saver and/or background image files for the phones as specified in the `46xxspecials.txt` file.
`CustomTemplates.tar`	A file with this name can be used to hold `.xml` format SIP trunk template files that can be used when adding SIP lines. See The CustomTemplates.tar File (SIP Trunk Templates) on page 83. • A maximum of 4 SIP line templates are supported by any individual system. • Templates can be exported from a working configuration using IP Office Manager.
`CustomData.xml`	This file is only loaded once when a system is first connected to COM. It is used to set the default values of various configuration settings. See The "CustomData.xml" File on page 79.

Warning:

- Care must be taken with the planning of the files included and the contents of those files. Currently there is no remote method through COM for removing incorrect and invalid files from systems. Instead, such files need to be overwritten by a corrected file.
- Files other than those listed above should not be included in the `.tar`. Any additional files are still unpacked and so may affect correct system operation.

Related links

Customization File Management on page 76

How the Customer Systems Load and Use the Files

When a system first connects to COM, it requests the customization files. Later, using COM or web manager, a customer system can be instructed to reload any customization files available. See Refreshing a Customer's Customization Files on page 85.

The customer system does the following when it requests the customization files:

- The first time the system connects it requests the `CustomData.xml` file (see The "CustomData.xml" File on page 79). This is used to set the initial value of various configuration settings. This file is only loaded once. It is not included in subsequent customization file refreshes.

- The system requests the `CustomPhoneFiles.tar` and `CustomTemplates.tar` files from its provider's customization files folder. It present, it downloads and unpacks the contents of those files.
  - New files are added to the system.
  - Files with the same name as any existing files overwrite the existing files.
- The system then requests the same files from its reseller's customization files folder. If they exist it repeats the download and unpacking process.
- The system then requests the same files from its own server name customization files folder and repeats the download and unpacking process.
- Once all the customization files have been unpacked and loaded:
  - New and updated template files do not affect any existing operation, but are available for use when configuring new items in web manager.
  - New and updated phone files are used when the phones are next restarted.

Related links

Customization File Management on page 76

Chapter 16: The Customization Files

This sections provides details and examples of the contents of the customization files.

Related links

The "CustomData.xml" File on page 79
The CustomPhoneFiles.tar File (Phone Settings and Image Files) on page 80
The CustomTemplates.tar File (SIP Trunk Templates) on page 83
Uploading Customization Files on page 84

The "CustomData.xml" File

This file is loaded by subscription systems when they first connect to COM. The values in the file are used to set various configuration settings relating to IP Office/COM operation.

Unlike other customization file, this file is only loaded once. It is not reloaded by refresh customization file commands.

Sample CustomData.xml File

The following is a sample file. The values are used to enable (`1`) or disable (`0`) the related IP Office configuration settings.

```
<?xml version="1.0" encoding="utf-8"?>
<customdata version="1">
  <security>
    <centralmgmt>1</centralmgmt>
    <centralcert>1</centralcert>
    <remoteaccess>0</remoteaccess>
    <remoteupgrade>1</remoteupgrade>
    <logtransfer>1</logtransfer>
    <externalremoteaccess>0</externalremoteaccess>
  </security>
  <vmpro>
    <backupconfig>1</backupconfig>
    <backupprompts>0</backupprompts>
    <backupmailboxes>1</backupmailboxes>
  </vmpro>
</customdata>
```

The values are used to enable (`1`) or disable (`0`) the related IP Office configuration settings.

- The `<security>` tags relate to the additional COM support features such as upgrades, log storage, etc. See Enabling Additional COM Support Services on page 58.

- The `<vmpro>` tags relate to the voicemail features that should be included in automatic backups. See Configuring a System's Voicemail Backup Settings on page 60.

Related links

The Customization Files on page 79

The CustomPhoneFiles.tar File (Phone Settings and Image Files)

The `CustomPhoneFiles.tar` file can be used to load files for phone settings onto customer systems. For example:

- A `46xxspecials.txt` file containing phone settings that are in addition to the auto-generated `46xxsettings.txt` settings file the customer system provides.
- Any screen saver and/or background image files for the phones as specified in the `46xxspecials.txt` file.

Notes

- This does not include phone firmware files such as `.bin` files.
- It is strongly advised not to include any `46xxsettings.txt` file. Allow the customer systems to auto-generate that file.
- The settings in the `46xxspecials.txt` file will override the same setting in a preceding file such as `46xxsettings.txt`.
- If a phone has already loaded an image file with a particular name, it will not load that file again even if its contents have changed. To change an existing image, the image file should also be renamed and the settings files updated to use the new name.

Related links

The Customization Files on page 79
The 46xxspecials.txt File on page 80
Example 46xxspecials.txt File on page 81
Phone Image File Details on page 82

The 46xxspecials.txt File

A `46xxspecials.txt` file can be used to provide phone settings that are not included in the customer system's auto-generated `46xxsettings.txt` file.

A `46xxspecials.txt` file for editing can be obtained from an IP Office system by browsing to `http://<server_address>/46xxspecials.txt`. If the system does not have an existing file, it provides an auto-generated version which includes the commands for grouping settings by phone type.

Details of the commands are included in the sample `46xxsettings.txt` files available from Avaya support.

Related links

The CustomPhoneFiles.tar File (Phone Settings and Image Files) on page 80

Example 46xxspecials.txt File

In the example below, a number of images files are specified for use as background images and screen savers by different phone types. For details of the supported image sizes, see Phone Image File Details on page 82.

Each of the specified image files needs to be included in the `CustomPhoneFiles.tar` file with the `46xxspecials.txt`.

```
## CUSTOM SETTINGS FOR PROVIDER / CUSTOMER
##
IF $MODEL4 SEQ 9608 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9611 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9621 GOTO 96X1SPECIALS
IF $MODEL4 SEQ 9641 GOTO 96X1SPECIALS
IF $MODEL4 SEQ J129 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J139 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J169 GOTO J1X9SPECIALS
IF $MODEL4 SEQ J179 GOTO J1X9SPECIALS
IF $MODEL4 SEQ K165 GOTO K1XXSPECIALS
IF $MODEL4 SEQ K175 GOTO K1XXSPECIALS
GOTO GENERALSPECIALS
##
# 96X1SPECIALS
SET SCREENSAVERON 40
SET SCREENSAVER 9600_screen_saver.jpg
GOTO GENERALSPECIALS
##
# J1X9SPECIALS
SET BACKGROUND_IMAGE "J100_back.jpg"
SET BACKGROUND_IMAGE_DISPLAY "J100_back.jpg"
SET BACKGROUND_IMAGE_SELECTABLE 0
SET BACKGROUND_IMAGE_SECONDARY "J100_secondary01.jpg"
SET BACKGROUND_IMAGE_DISPLAY_SECONDARY "J100_secondary01.jpg"
SET BACKGROUND_IMAGE_SELECTABLE_SECONDARY 0
SET SCREENSAVERON 40
SET SCREENSAVER_IMAGE "J100_saver01.jpg,J100_saver02.jpg"
SET SCREENSAVER_IMAGE_DISPLAY J100_saver01.jpg
SET SCREEN_SAVE_IMAGE_SELECTABLE 1
SET SCREENSAVER_IMAGE_SECONDARY "J100_secondary_saver01.jpg,secondary_saver_02.jpeg"
SET SCREENSAVER_IMAGE_DISPLAY_SECONDARY secondary_saver01.jpg
SET SCREENSAVER_IMAGE_SELECTABLE_SECONDARY 0
GOTO GENERALSPECIALS
##
# K1XXSPECIALS
SET CLICKS 0
SET BRANDING_FILE "acme_logo.png"
SET LOGOS "ACME=acme_vantage.jpg"
SET CURRENT_LOGO "ACME"
SET LOGOSTAT 0
GOTO GENERALSPECIALS
##
# GENERALSPECIALS
SET PROCPSWD 72779673
SET ADMIN_PASSWORD password
# END
```

Related links

The CustomPhoneFiles.tar File (Phone Settings and Image Files) on page 80

Phone Image File Details

The following is a summary of phone image files supported:

Phone Series	Usage	Supported Image Details
9600 Series	Screensaver	• `.jpg` format: - For color images use 16-bit. For non-color images, 2 levels of greyscale are supported. - To invoke a transparent background, use a background color of 0,255,0 (brightest possible green). • 9611: 160 x 160 • Others: 320 x 160
J100 Series	Background Screensaver	• Up to 5 images are supported for each function. • 16-bit `.jpg` and `.jpeg` files. The maximum size for any file is 156KB. • Main screen: - J139/J159/J169/J179: 320 x 240 pixels. - J189: 800 x 480 pixels. • Secondary screen: - J159: 160 x 240 pixels. - J189: 240 x 320 pixels.
K100 Series	Background	• Up to 16 images: • 24-bit colour `.png`, `.jpg`, `.jpeg`, `. gif` and `.bmp` • K155: 720 x 1280 • K165/175: 1280 x 800
	Branding	• 24-bit colour `.png`, `.jpg`, `.jpeg`, `. gif` or `.bmp` • 142 x 56 pixels.

Related links

The CustomPhoneFiles.tar File (Phone Settings and Image Files) on page 80

The CustomTemplates.tar File (SIP Trunk Templates)

The `CustomTemplates.tar` file can be used to load SIP trunk templates onto systems.

- A maximum of 4 SIP line templates are supported by any individual system.
- Templates can be exported from a working configuration using IP Office Manager.
- Template files are also included with the DevConnect applications notes produced by Avaya.

Related links

The Customization Files on page 79
Downloading a SIP Trunk Template from IP Office Manager on page 83
Using a SIP Trunk Template in IP Office Web Manager on page 83

Downloading a SIP Trunk Template from IP Office Manager

The configuration of an existing SIP trunk can be saved as a template file for use with other systems.

Procedure

1. Open the system configuration in IP Office Manager.
2. In the list of lines, right-click on the required line and select **Export as Template**.
3. Save the `.xml` file.

Related links

The CustomTemplates.tar File (SIP Trunk Templates) on page 83

Using a SIP Trunk Template in IP Office Web Manager

When a customer system has received a `CustomTemplates.tar` from COM and unpacked the templates, they can be used when adding a new SIP trunk to the system's configuration.

Procedure

1. Open the system configuration in IP Office Web Manager.
2. Select **System Settings** > **Lines** > **+Add Line** > **SIP Line** to add a new line.
3. Use the **Select Template** drop-down to select the required template and click **Apply**.
4. Amend the settings as required and save the new configuration.

Related links

The CustomTemplates.tar File (SIP Trunk Templates) on page 83

Uploading Customization Files

Before you begin

- Ensure that the file is in the correct format and has the expected file name. See Customization File Management on page 76.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. Browse to the required folder. Check that the **Path** shown lists the required folder name.
3. Click **Upload File**.
4. Either click **Choose File** and select the required file or drag and drop the file onto the upload file window.
5. Click **Upload File**.
6. Repeat the process for any other files that you want added.
7. When finished, click **OK**.
8. Browse the folder structure again to confirm that the action has been completed.

Related links

The Customization Files on page 79
Managing the Customization Files Folders on page 88

Chapter 17: Refreshing a Customer's Customization Files

Customer systems can be instructed to update their customization files using those available on the COM server. This can be done using either web manager or directly from within COM.

- Using web manager allows the selection of when the system should update it files to be made by a maintainer with web manager access to the system.
- Using COM allows the selection of multiple customer systems to update their customization files. This process can also be scheduled rather than performed immediately.
- Note that the `CustomData.xml` is not included in any refresh. It is only loaded once when during the systems initial connect to COM.

Related links

[Refreshing Customization Files Using Web Manager](#) on page 85
[Refreshing the Customization Files Using COM](#) on page 86

Refreshing Customization Files Using Web Manager

You can instruct a system to update its set of customization files through web manager.

- Note that the `CustomData.xml` is not included in any refresh. It is only loaded once when during the systems initial connect to COM.

Procedure

1. Using web manager, log into the system.
2. Click on ⚙.
3. Click **Refresh Customization Files**.
4. The system will request the customization files:
   - The system requests the `CustomPhoneFiles.tar` and `CustomTemplates.tar` files from its provider's customization files folder. It present, it downloads and unpacks the contents of those files.
     - New files are added to the system.

- Files with the same name as any existing files overwrite the existing files.

- The system then requests the same files from its reseller's customization files folder. If they exist it repeats the download and unpacking process.
- The system then requests the same files from its own server name customization files folder and repeats the download and unpacking process.
- Once all the customization files have been unpacked and loaded:
    - New and updated template files do not affect any existing operation, but are available for use when configuring new items in web manager.
    - New and updated phone files are used when the phones are next restarted.

Related links

Refreshing a Customer's Customization Files on page 85

Refreshing the Customization Files Using COM

The cluster administrator can make files such as trunk templates, screen saver images and prompt files available for use when a new system is created in the cluster. This process allows the set of files on an existing server to be updated.

- Note that the `CustomData.xml` is not included in any refresh. It is only loaded once when during the systems initial connect to COM.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. Select the checkbox next to the systems to which you want to apply the action.
3. Click **Action**.
4. Click on **Refresh Customization Files**.
5. If the license detail are displayed, click **Accept** to continue.
6. Enter a name for the job.
7. When prompted to confirm the action, click **Yes**.
8. The system will request the customization files:
    - The system requests the `CustomPhoneFiles.tar` and `CustomTemplates.tar` files from its provider's customization files folder. It present, it downloads and unpacks the contents of those files.
        - New files are added to the system.
        - Files with the same name as any existing files overwrite the existing files.
    - The system then requests the same files from its reseller's customization files folder. If they exist it repeats the download and unpacking process.

- The system then requests the same files from its own server name customization files folder and repeats the download and unpacking process.
- Once all the customization files have been unpacked and loaded:
    - New and updated template files do not affect any existing operation, but are available for use when configuring new items in web manager.
    - New and updated phone files are used when the phones are next restarted.

Related links

Refreshing a Customer's Customization Files on page 85

Chapter 18: Managing the Customization Files Folders

This section covers managing the customization files and folders used by COM.

Related links

[Viewing the Customization File Folders] on page 88
[Creating a New Customization File Folder] on page 88
[Uploading Customization Files] on page 84
[Deleting Customization Files] on page 90
[Renaming a Customization File] on page 90
[Downloading Customization Files] on page 91

Viewing the Customization File Folders

Procedure

1. Click **Views**.
2. Click **File Management**.
3. Click **Customization File Management**.
4. Browse the folder structure shown on the left by clicking on the folders. The **Path** shown is the location of the current folder being displayed.

Related links

[Managing the Customization Files Folders] on page 88

Creating a New Customization File Folder

The customization folders are automatically nested in a provider/reseller/customer folder hierarchy. When adding a new folder, you select what type of folder you want to create (reseller, provider or customer).

The folders are also used in their hierarchical order. A system can obtain files from all three folders that are applicable to it. See Customization File Management on page 76.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. You do not need to browse to the existing folder structure to create a new folder, however it is useful in order to confirm the actions required.
3. Select **Action** and then the type of folder you want using either **Add Provider**, **Add Reseller** or **Add Customer**.
    a. If adding a reseller or customer folder, first select the relevant provider for the reseller or customer.
    b. If adding a customer folder, select the relevant reseller for the customer.
    c. If adding a customer folder, enter the name of the customer system.
4. Click the **Add** button to add the folder.
5. Browse the folder structure again to confirm that the action has been completed.

Related links

Managing the Customization Files Folders on page 88

Uploading Customization Files

Before you begin

- Ensure that the file is in the correct format and has the expected file name. See Customization File Management on page 76.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. Browse to the required folder. Check that the **Path** shown lists the required folder name.
3. Click **Upload File**.
4. Either click **Choose File** and select the required file or drag and drop the file onto the upload file window.
5. Click **Upload File**.
6. Repeat the process for any other files that you want added.
7. When finished, click **OK**.
8. Browse the folder structure again to confirm that the action has been completed.

Related links

The Customization Files on page 79

Managing the Customization Files Folders on page 88

Deleting Customization Files

You can delete existing files from a folder. This does not affect any existing files that have already be downloaded to any customer systems.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. Browse to the required folder. Check that the **Path** shown lists the required folder name.
3. Select the checkbox next to the files or use the checkbox at the top to select all files.
4. Click **Delete**.
5. When prompted to confirm the action, click **Yes**.
6. Browse the folder structure again to confirm that the action has been completed.

Related links

Managing the Customization Files Folders on page 88

Renaming a Customization File

You can rename an existing customization file. However, if the new name does not match those expected by the systems (see Customization File Management on page 76), the file will not be used for customization file updates.

This may be useful if you want multiple customization files of the same type available but some control over which one is currently used.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. Browse to the required folder. Check that the **Path** shown lists the required folder name.
3. Select the checkbox next to the file that you want to rename.
4. Click **Rename**.
5. Enter the new name for the file. Do not include the file extension in the new name.
6. Click **OK**.
7. Browse the folder structure again to confirm that the action has been completed.

Related links

Managing the Customization Files Folders on page 88

Downloading Customization Files

You can download existing customization files to your own PC.

Procedure

1. View the customization folders. See Viewing the Customization File Folders on page 88.
2. Browse to the required folder. Check that the **Path** shown lists the required folder name.
3. Select the checkbox next to the files or use the checkbox at the top to select all files.
4. Click **Download**.
5. The selected files are downloaded to your browser as a single .zip file.

Related links

Managing the Customization Files Folders on page 88

Part 7: Software File Management

Chapter 19: The Software Repository

The software repository is used to contain the files available for upgrading customer systems.

Related links

[Viewing the File Repository](#) on page 93

Viewing the File Repository

Procedure

1. Click on **Views**.
2. Select **Software Repository**.
    - If a previous attempt to upload a file to the software repository was interrupted, for example you were logged out of COM, when you return to the repository you may be prompted whether you want to resume the transfer.
3. The software repository and any files already in it are displayed.

Related links

[The Software Repository](#) on page 93

Chapter 20: Vantage File Management

COM can be used to view and manage the set of Avaya Vantage™ (K100 Series) phone firmware and dialer application files that the cluster has available. Those files are used to support Avaya Vantage™ phones hosted on the customer systems.

- This is only supported for **Administrator** users.
- Avaya support – The file sets for Vantage phones can be obtained from the Avaya support.
- **K100 Settings Files** – The file sets may include `K1xxSupgrade.txt` and `K1xxBSupgrade.txt` files. If so, those files are not used. The customer systems auto-generate their own files. It is important that the settings in the auto-generated file match the firmware and dialer applications available.
- The individual customer systems need their address for the separate HTTP file server set to that required by COM. This is normally done automatically when the system is initially subscribed.

Related links

Enabling HTTP Server Support on page 94
Viewing Vantage Files on page 95
Downloading Vantage Files on page 95
Uploading Vantage Files on page 96
Deleting Vantage Files on page 96

Enabling HTTP Server Support

About this task

While most phones obtain their firmware files direct from their IP Office system, some (for example Vantage phones) need to be redirected to a separate HTTP file server. For subscription systems, that alternate file server is provided by COM.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.

2. Select **System Settings** > **System**.
3. Set the **HTTP Server IP Address** back to 0.0.0.0 to disable that setting. The **HTTP Server UI**is now used for redirected HTTP requests made by phones. The address in the **HTTP Server UI** field is automatically set by the configuration file used by the system when it initially subscribed.
4. Click **Update**.

Related links

Vantage File Management on page 94

Viewing Vantage Files

Before you begin

- This is only supported for **Administrator** users.

Procedure

1. Click **Views**.
2. Click **File Management**.
3. Click **Workplace and Vantage Files Management**.
4. Click on the **Vantage** folder.

Related links

Vantage File Management on page 94

Downloading Vantage Files

Procedure

1. View the **Vantage** files. See Viewing Vantage Files on page 95.
2. Select the checkbox next to the files or use the checkbox at the top to select all files.
3. Click **Download**.
4. The selected files are downloaded to your browser as a single .zip file.

Related links

Vantage File Management on page 94

Uploading Vantage Files

Before you begin

- Place the file or files being uploaded into a `.zip` or `.tar` file. That contents of that file are automatically unpacked after it is uploaded.

Procedure

1. View the **Vantage** files. See Viewing Vantage Files on page 95.
2. Click **Upload File**.
3. Select **Vantage**.
4. Either click **Choose File** and select the required file or drag and drop the file onto the upload file window.
5. Click **Upload File**.
6. Repeat the process for any other files that you want added.
7. When finished, click **OK**.
8. Browse the folder structure again to confirm that the action has been completed.

Related links

Vantage File Management on page 94

Deleting Vantage Files

Procedure

1. View the **Vantage** files. See Viewing Vantage Files on page 95.
2. Select the checkbox next to the files or use the checkbox at the top to select all files.
3. Click **Delete**.
4. When prompted to confirm the action, click **Yes**.
5. Browse the folder structure again to confirm that the action has been completed.

Related links

Vantage File Management on page 94

Chapter 21: Avaya Workplace Client File Management

Through the web manager and self-administration applications, the customer systems provide links for downloading the installers for the various Avaya Workplace Client clients.

- The installers for the Windows and macOS clients are provided from a set that can be managed through COM. This chapter details how to update and manage those files.
- The installers for Android and iOS clients are provided through links to the app stores for those operating systems and so not covered here.
- This is only supported for **Administrator** users.

The file set for the Windows and macOS installers consists of the following files:

- **Client Installer Files** – Updated versions of these file are provided from the Avaya support website.
  - **An Avaya .msi File** – This `.msi` file is used for Windows PC installations of the Avaya Workplace Client.
  - **An Avaya .dmg File** – The `.dmg` file is used for macOS PC installations of the Avaya Workplace Client.
- **An appcast.xml File** – This file is used to provide the links shown to users of the web manager and self-administration applications. In order to create a new file, download and update the existing file.

Related links

Viewing the Avaya Workplace Client Files on page 97
Downloading Avaya Workplace Client Files on page 98
Uploading Avaya Workplace Client Files on page 98
Deleting Avaya Workplace Client Files on page 99

Viewing the Avaya Workplace Client Files

Before you begin

- This is only supported for **Administrator** users.

Procedure

1. Click **Views**.
2. Click **File Management**.
3. Click **Workplace and Vantage Files Management**.
4. Click on the **Workplace** folder.

Related links

Avaya Workplace Client File Management on page 97

Downloading Avaya Workplace Client Files

Procedure

1. View the **Workplace** files. See Viewing the Avaya Workplace Client Files on page 97.
2. Select the checkbox next to the files or use the checkbox at the top to select all files.
3. Click **Download**.
4. The selected files are downloaded to your browser as a single .zip file.

Related links

Avaya Workplace Client File Management on page 97

Uploading Avaya Workplace Client Files

Before you begin

- If uploading a new `.msi` or `.dmg` file, ensure that you also include an updated `appcast.xml` file whose contents match the new `.msi` or `.dmg` file names. To do this, download and edit the existing `appcast.xml` file using a text editor.
- Place the file or files being uploaded into a `.zip` or `.tar` file. That contents of that file are automatically unpacked after it is uploaded.

Procedure

1. View the **Workplace** files. See Viewing the Avaya Workplace Client Files on page 97.
2. Click **Upload File**.
3. Select **Workplace**.
4. Either click **Choose File** and select the required file or drag and drop the file onto the upload file window.
5. Click **Upload File**.

6. Repeat the process for any other files that you want added.
7. When finished, click **OK**.
8. Browse the folder structure again to confirm that the action has been completed.

Related links

Avaya Workplace Client File Management on page 97

Deleting Avaya Workplace Client Files

Procedure

1. View the **Workplace** files. See Viewing the Avaya Workplace Client Files on page 97.
2. Select the checkbox next to the files or use the checkbox at the top to select all files.
3. Click **Delete**.
4. When prompted to confirm the action, click **Yes**.
5. Browse the folder structure again to confirm that the action has been completed.

Related links

Avaya Workplace Client File Management on page 97

Part 8: Remote Support Services

Remote Support Services

COM can relay a variety of administration connections. These can be to the IP Office servers managed by COM and to non-IP Office servers on the same networks.

Access is control by the remote operation settings of the primary server. The levels of access are:

Access	Description
Centralized Management	Allows IP Office Web Manager, System Status Application and SysMonitor access, using HTTPS, to the IP Office servers managed by COM. See Using the IP Office Administration Apps on page 101.
Remote Access	Allows HTTPS browser access to a number of other services on IP Office servers managed by COM. This is supported for access to the web control panel, one-X Portal admin menus and WebLM server menus. See Remote Support Through COM on page 109. It also allows SSH access to the IP Office servers managed by COM.
Remote Access + Co-located Servers	Extends remote access to other servers on the same network as those managed by COM. • It supports HTTPS, SSH and RDP access to non-IP Office servers. • For each connection, the COM managed IP Office through which the connection is routed needs a tunnel for the connection added to its configuration.

Chapter 22: Using the IP Office Administration Apps

COM can relay connections to the customer IP Office servers for the IP Office admin tools System Status Application, SysMonitor and IP Office Web Manager.

- Access to the IP Office web control panel, one-X Portal admin menus and WebLM server is supported using the remote support options. See Remote Support Through COM on page 109.
- The processes in this section only work for IP Office servers managed by COM. That is, those shown in the customer details (see Viewing the Customer System Details on page 24).

Related links

Enabling IP Office Admin Tool Connection

About this task

Support for centralized management connections through COM needs to be enable on the target system before they are allowed.

- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.

2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. Enable the options required:

Options	Description
Centralized Management	Support remote connections to IP Office servers using IP Office admin tools (System Status Application, SysMonitor and IP Office Web Manager).

5. Click **Update**.

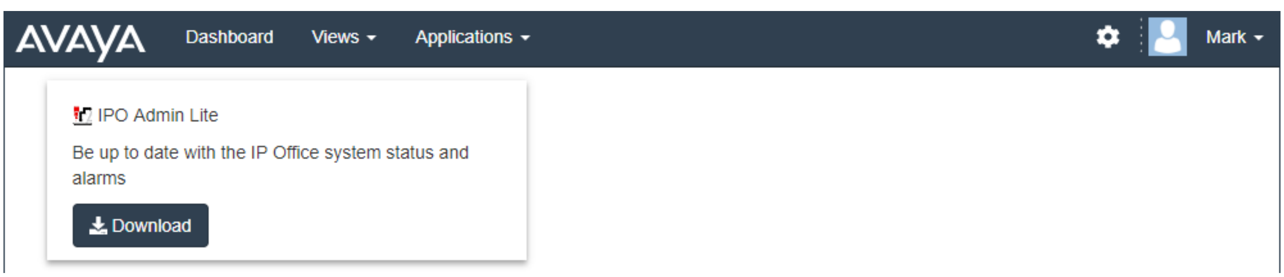
Related links

[Using the IP Office Administration Apps](#) on page 101

Downloading the IP Office Admin Tools

This menu can be used to download a copy of the installer for the IP Office administration suite. It can be used to install copies of the IP Office Manager, System Status Application and SysMonitor applications onto Windows PCs.

- The version of IP Office Manager installed by the IPO Admin Lite does not include the files necessary for System SD card maintenance actions such as recreating the SD card. Those are only available using the version of IP Office Manager installed from the full IP Office Administration suite.



Procedure

1. Click **Applications**.
2. Select **IP Office Admin Tools**.
3. Click on the **Download** link.

Related links

[Using the IP Office Administration Apps](#) on page 101

Getting the Address for System Connection via COM

About this task

The address for connection to customer systems via COM is shown as part of the system details display in COM.

Procedure

1. Locate the customer system in the list of customers (see Using the Customer List on page 19).
2. Click on the customer name.
3. Details of the customer system are displayed.
4. For additional details, click on **Show details**.
5. The address for connection through COM is shown as the **Sysmon and SSA URL**. The address takes the form admin.<com-domain>/<customer-id>/<target-ip-office-ip-address> where:
   - <com-domain> is the domain part of the address normally used to connect to COM, prefixed with admin. For example, admin.example.com.
   - <customer-id> is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
   - <target-ip-office-ip-address> is the optional IP address of the IP Office system connected to the primary server.
6. For Server Edition subscription servers, scroll down to view the address for another other servers in the network.
7. Click on **Copy to Clipboard** to copy the address to your computer's clipboard.

Related links

Using the IP Office Administration Apps on page 101

Connecting with SysMonitor

About this task

The following process connects to the customer system via COM.

Before you begin

- Enable **Centralized Management** on the system. See Enabling IP Office Admin Tool Connection on page 101.
- Obtain a service user username and password for administrator access to the customer system.

- Obtain the address for connection to the customer systems. See Getting the Address for System Connection via COM on page 103.

Procedure

1. On the PC on which the IP Office administration suite has been installed, select **IP Office** > **Monitor**.
2. Select **File** > **Select Unit**.
3. In the login menu, set the **Control Unit Address** to the address shown for the server by COM.
4. Set the **Protocol** to `https`.
5. Set the **Port** to `8443`.
6. Enter the **Username** and **Password** configured in the system's security settings.
7. Click **OK**.

Next steps

- For details of using SysMonitor, see Using Avaya IP Office System Monitor.

Related links

Using the IP Office Administration Apps on page 101

Connecting with System Status Application

About this task

The following process connects to the customer system via COM.

Before you begin

- Enable **Centralized Management** on the system. See Enabling IP Office Admin Tool Connection on page 101.
- Obtain a service user username and password for administrator access to the customer system.
- Obtain the address for connection to the customer systems. See Getting the Address for System Connection via COM on page 103.

Procedure

1. On the PC on which the IP Office administration suite has been installed, select **IP Office** > **System Status**.
2. In the login menu, set the **Control Unit Address** to the address shown for the server by COM.
3. Set the **HTTP Port** to `443` or `8443`.

4. Select **Secure Connection** and **Websocket Connection**.
5. Enter the **Username** and **Password** configured in the system's security settings.
6. Click **Logon**.

Next steps

- For details of using System Status Application, see Using IP Office System Status.

Related links

Using the IP Office Administration Apps on page 101

Connecting with IP Office Web Manager

About this task

The following process can be used to launch an IP Office Web Manager connection to the customer system via COM.

- COM users can also select **Launch Application** > **Web Manager** from the customer list.

Before you begin

- Enable **Centralized Management** on the system. See Enabling IP Office Admin Tool Connection on page 101.
- Obtain a service user username and password for administrator access to the customer system.
- Obtain the address for connection to the customer systems. See Getting the Address for System Connection via COM on page 103.

Procedure

1. Start your web browser.
2. Using the customer system address, enter the address in the form `https://admin.<com-domain>:8443/<customer-id>/WebManagement/WebManagement.html` where:
   - `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `admin`. For example, `admin.example.com`.
   - `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
3. The first time this method of connection is used with a particular PC and browser, there is a delay as various files are cached. This delay reduces on subsequent connections.
4. Login with the system administrator username and password.

Next steps

- For details of using IP Office Web Manager, see Administering Avaya IP Office with Web Manager.

Related links

Using the IP Office Administration Apps on page 101

one-X Portal Connection

Access to the IP Office web control panel, one-X Portal admin menus and WebLM server is supported using the remote support options. See Remote Support Through COM on page 109.

Related links

Using the IP Office Administration Apps on page 101

Web Control Panel Connection

Access to the IP Office web control panel, one-X Portal admin menus and WebLM server is supported using the remote support options. See Remote Support Through COM on page 109.

Related links

Using the IP Office Administration Apps on page 101

WebLM Connection

Access to the IP Office web control panel, one-X Portal admin menus and WebLM server is supported using the remote support options. See Remote Support Through COM on page 109.

Related links

Using the IP Office Administration Apps on page 101

Voicemail Administration Connection

Remote connection of the Voicemail Pro client is not supported. However, remote admin of voicemail server preferences and offline editing of the callflow is supported using web manager. See Connecting with IP Office Web Manager on page 105.

Related links

Using the IP Office Administration Apps on page 101

IP Office Administration Addresses

For HTTPS access to IP Office systems, a number of HTTPS addresses are supported.

Centralized Management Addresses

The following addresses are supported for IP Office systems setup for centralized management (see Using the IP Office Administration Apps on page 101). In this case, the browser does not need any additional configuration.

	Address Format
IP Office Web Manager	`https://admin.<com-domain>:8443/<customer-id>/WebManagement/WebManagement.html` This address can be access directly from COM using **Launch Application** > **Web Manager**.
Sysmon and SSA URL	`admin.<com-domain>/<customer-id>[/<target-ip-office-ip-address>]`

where:

- `< >` indicates a field value to be replaced as detailed below. When replaced, omit the `< >` brackets.
- `[ ]` indicates an optional field. If added, omit the `[ ]` brackets.
- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<target-ip-office-ip-address>` is the optional IP address of the IP Office system connected to the primary server.
- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `admin`. For example, `admin.example.com`.

Remote Support Addresses

The following addresses are supported for IP Office systems setup for remote support (see Enabling Remote Connection on page 111) and using a browser configured for access via a proxy tunnel (see Using HTTPS for Remote Support on page 125).

Function	Address Format
Web Control Panel	`https://<customer-id>-<system-name>.maint.<com-domain>:7071/login`
one-X Portal	`https://<customer-id>-<system-name>.maint.<com-domain>:9443/onexportal-admin.html`
WebLM Server	`https://<customer-id>-<system-name>.maint.<com-domain>:52233/WebLM/index.jps`

where:

- `< >` indicates a field value to be replaced as detailed below. When replaced, omit the `< >` brackets.

- `[ ]` indicates an optional field. If added, omit the `[ ]` brackets.
- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<system-name>` is the IP Office system name as shown in the customer system details (see Viewing the Customer System Details on page 24).
- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.

Related links

Using the IP Office Administration Apps on page 101

Chapter 23: Remote Support Through COM

In addition to relaying IP Office admin connections to the customer IP Office servers (see Using the IP Office Administration Apps on page 101), COM can relay HTTPS, RDP and SSH connections. This can be to any servers and services on the same network as the customer's IP Office servers (and including those servers).

- The client used must support authenticated HTTPS Proxy and HTTP Connect Method. This is used for authentication of the initial connection to COM using the reseller/distributor username and password set in COM.
  - This is supported for the latest versions of major browsers (Chrome, Edge and Firefox).
  - For SSH access, support is enabled by installation of the Proxytunnel utility.
- If the connection is accepted by COM, the connection is then onward routed to the customer's IP Office using a secure websocket connection.
- If the target address is another server on the same network as the IP Office, a connection is established from the customer's IP Office using RDP, SSH or HTTPS as appropriate.

These methods of connection are intended for administration support only. They are not supported for end-user client applications such as web self-administration.

Related links

Enabling Remote Support on an IP Office System on page 109
Proxy Account Management on page 110
Enabling Remote Connection on page 111
Creating Tunnels for Remote Servers and Services on page 112
View System Details, Files and Links for Remote Support on page 112

Enabling Remote Support on an IP Office System

COM can relay HTTPS, RDP and SSH connections to the customer's IP Office servers and other servers on the same network as the IP Office servers.

In order to do this:

#	Stage	See ...
1.	**Set a COM proxy account user name and password:**	The reseller or distributor associated with the system needs to have a COM proxy account enabled. • See Proxy Account Management on page 110.
2.	**Enable remote support on the customer system:**	The customer's primary server needs to be configured to allow remote support. • See Enabling Remote Connection on page 111.
3.	**Create tunnels for co-located remote servers**	Remote support to non-IP Office servers requires the addition of tunnels to the IP Office configuration.
4.	**Configure the remote support method:**	• **For HTTPS browser access:** - See Using HTTPS for Remote Support on page 125. • **For SSH access:** - **Windows:** See Using SSH from Windows on page 114. - **Linux:** See Using SSH from Linux on page 120. • **For RDP access:** - See Using Windows RDP on page 135.

Related links

Remote Support Through COM on page 109

Proxy Account Management

About this task

Each reseller and distributor with systems managed through COM is automatically assigned an account for use with proxy connections. The same account is used for all customer systems managed by the same reseller/distributor through COM.

The process below is used to configure the username and password details for an account. Those details are then used to authenticate the initial leg of any remote support connections.

Procedure

1. Login to COM using a user other than an **Administrator** user.
2. Click on the ⚙ icon.
3. Select **Maintenance Proxy Account Management**.
4. Next to the required account, click on the ☑ icon.
5. Set the **Username** and **Password** fields as required.

6. Click **Update**.

Related links

[Remote Support Through COM](#) on page 109

Enabling Remote Connection

About this task

Support for remote connections from COM needs to be allowed by the customer's IP Office server.

- This is necessary even if the planned connection is to other servers on the same network as the IP Office server rather than the IP Office server itself.
- If the server is part of a network of IP Office servers, the servers should be connected using websocket SCN lines (the default).
- Normally these settings are set to the reseller/distributors required defaults by the customization file applied to the system when it was initially subscribed. See The "CustomData.xml" File on page 79.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **System**.
3. Select **Remote Operations**.
4. For remote support, enable the following setting:

Options	Description
Remote Access	Support HTTPS, SFTP, SSH and RDP connections to IP Office servers managed by COM.
Co-located Servers	This option allows **Remote Access** support to be extended to other servers on the same network as the COM managed IP Office systems. That includes connection to UCM modules and standalone IP Office Application servers. This also requires configuration of a TCP tunnel for each connection (see Creating Tunnels for Remote Servers and Services on page 112).

5. Click **Update**.

Related links

Remote Support Through COM on page 109

Creating Tunnels for Remote Servers and Services

About this task

Remote support connections to servers that are not managed through COM, require the addition of a tunnel entries for each server/service. These are added to the configuration of the customer's IP Office server through which the connection will be routed.

Before you begin

- The server must also have the **Co-located Servers** option enabled. See Enabling Remote Connection on page 111.

Procedure

1. Access the system using IP Office Web Manager.
2. Select **System Settings** > **Services**. A **Remote Support** service is listed for each IP Office in the network.
3. Click the edit icon next to the **Remote Support** service of the server through which the connection to the remote server will be routed.
4. Click **+Add Tunnel** and select **TCP Tunnel**.
5. Select the **Application** to indicate the role of the tunnel, for example **RDP** or **SSH**.
    - This setting is used to identify the role of the tunnel and set the default port. However, the port can be changed below if required.
6. Set the **Server IP Address** to match the IP address of the remote server.
7. Check that the **Server Port Number** matches the port that will be used for the service.
8. Click **Save**.
9. Add any other additional tunnels required. Then click **Create**.
10. If the server is part of a network of IP Office servers, repeat the process for any other servers through which you want to provide remote support.

Related links

Remote Support Through COM on page 109

View System Details, Files and Links for Remote Support

COM displays details of the links that can be used for remote support of a customer system. It also displays links for the files needed to configure remote support access on your PC.

- Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Before you begin

- The links described are only shown if the IP Office system has been configured to allow remote support connections. See Enabling Remote Connection on page 111. Until then, it displays **Remote Access is Disabled**.

Procedure

1. From the customer list, you can click on the name of a customer system to view details of the system (see Viewing the Customer System Details on page 24).
2. The details include a number of links:

Link	Description
Sysmon and SSA URL	This link can be used with the SysMonitor and the System Status Application for access through COM. See Using the IP Office Administration Apps on page 101.
Web Control Panel	These links can be used to access those named services if your browser has been configured for remote access. See Using HTTPS for Remote Support on page 125.
one-X Portal	
WebLM Server	
Remote Support Services	Clicking this link displays a menu with additional details for configuring browser, SSH or RDP remote support. • See Using HTTPS for Remote Support on page 125. • See Using SSH from Windows on page 114. • See Using SSH from Linux on page 120. • See Using Windows RDP on page 135.

Related links

Remote Support Through COM on page 109

Chapter 24: Using SSH from Windows

This section covers using SSH/SFTP to connect to customer IP Office servers and to other servers on the same network as the customer's IP Office servers.

This section covers the processes needed to connect using SSH from a Windows PC.

#	Stage	See ...
1.	**Enable remote support to the customer system:**	See Enabling Remote Support on an IP Office System on page 109.
2.	**Download the Proxytunnel utility files:**	See Downloading the Proxytunnel Utility Files (Windows) on page 114.
3.	**Check that the PC supports Open SSH:**	See Checking Open-SSH Support (Windows) on page 115.
5.	**Connect Using SSH:**	**Using the command line:** • See SSH Command Line Connection (Windows) on page 116. **Using Putty:** • See SSH PuTTY Connection (Windows) on page 117.

Related links

Downloading the Proxytunnel Utility Files (Windows) on page 114
Checking Open-SSH Support (Windows) on page 115
SSH Command Line Connection (Windows) on page 116
SSH PuTTY Connection (Windows) on page 117
Windows SSH Address Format on page 118

Downloading the Proxytunnel Utility Files (Windows)

About this task

In order to use SSH from a Windows PC, a number of files need to be present on that PC:

- Proxytunnel is a utility used to tunnel connections via an HTTPS proxy. In this case, RDP and SSH connections to a customer's servers tunneled via COM to the customer IP Office.

- `isrgrootx1.pem` is a security certificate used for part of the remote connection. The certificate file needs to be available on the PC but does not need to be installed in the PC's security settings.

These files can be downloaded from COM using the process below.

Note:

- This process only needs to be done once on a particular PC. The files downloaded from COM are common for all systems being managed by that COM service.

Procedure

1. Display the list of customer systems. See Viewing the Customer List on page 20.
2. Click **Applications** > **Download Proxytunnel Utility**
3. Unzip the contents of the file to a folder on the PC. The path to the files in the folder is needed for various commands.

   Important:

   - If planning to use PuTTY, the application must have been installed with the option **Put install directory on the PATH for command prompts** selected.

Next steps

- **Check that the PC has Open SSH installed:** See Checking Open-SSH Support (Windows) on page 115.

Related links

Using SSH from Windows on page 114

Checking Open-SSH Support (Windows)

About this task

To support remote HTTPS connections, the Windows PC must support Open-SSH. This is normally the default but should be checked before proceeding.

Before you begin

- **Download the utility files:** See Downloading the Proxytunnel Utility Files (Windows) on page 114.

Procedure

1. In Windows, select **Settings**.
2. Select **Apps**.
3. Select **Manage optional features**.
4. Check that the list of optional features includes **Open SSH Client**. If not, click **Add a feature** and select **Open SSH Client**.

Next steps

The Windows PC can now be used to connect remotely to customer servers:

- **Command Line Connection:** See SSH Command Line Connection (Windows) on page 116.
- **Putty Connection:** See SSH PuTTY Connection (Windows) on page 117.

Related links

Using SSH from Windows on page 114

SSH Command Line Connection (Windows)

Before you begin

- **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
- **Download the utility files:** See Downloading the Proxytunnel Utility Files (Windows) on page 114.
- **Check that the PC supports Open SSH:** See Checking Open-SSH Support (Windows) on page 115.
- **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
- Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. In the customer list, click on the customer's system name:
    a. For the IP Office server to which you want to connect or connect through, click **Remote Support Services**.
    b. Click **SSH Access Information**.
    c. Replace **Full Path of Proxy Tunnel Utility** with the full path of the folder in which you stored the downloaded utility files. For example; `C:\\Proxytunnel\proxytunnel.exe`.
    d. Click **Generate SSH Command**.
3. Example addresses are shown for the customer's server (**Primary Server (Windows)**) and for other server's accessed through it (**External Server (Windows)**). Click the icon to copy the required address.
    - Strings shown as `********` are automatically replaced with the required value when cut and pasted.
4. From the Windows command line, paste the address into the command line by pressing `Ctrl+V` or right-clicking the mouse.

5. For connections to a server co-located with the customer's IP Office server, replace the values in < > brackets:
    - `<username-for-co-located-server>` is a username used to authenticate SSH connections on the co-located server.
    - `<co-located-server-ip-address>` is the IP address of the co-located server.

Related links

Using SSH from Windows on page 114

SSH PuTTY Connection (Windows)

About this task

This process uses the information provided in the COM menus to setup a PuTTY connection.

Before you begin

- **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
- **Download the utility files:** See Downloading the Proxytunnel Utility Files (Windows) on page 114.
- **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
- Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. In the customer list, click on the customer's system name:
    a. For the IP Office server to which you want to connect or connect through, click **Remote Support Services**.
    b. Click **SSH Access Information**.
    c. Replace **Full Path of Proxy Tunnel Utility** with the full path of the folder in which you stored the downloaded utility files. For example; `C:\\Proxytunnel\proxytunnel.exe`.
    d. Click **Generate SSH Command**.
3. Example addresses are shown in the **SSH Access Using Putty** and **SSH Access pf servers co-located to IP Office using Putty** sections. In the following steps, click on the icon to copy and paste the required address for the step.
    - Strings shown as `********` are automatically replaced with the required value when cut and pasted.

4. Start PuTTY.
5. Click **Session**.
6. In **Host Name**, paste the appropriate **Putty Hostname (Windows)** from the COM menu.
    - For a server co-located with the customer's IP Office, replace the <co-located-server-ip-address> value with the IP address of the server.
7. Set the **Port** to 22.
8. Click **Proxy**.
9. Set the **Proxy Type** to **Local**.
10. In **Telnet command or local proxy command**, paste the appropriate **Local Proxy Command for Putty (Windows)** from the COM menu.
    - For a server co-located with the customer's IP Office, replace the <co-located-server-ip-address> value as above.
11. Click **Open**.

Related links

Using SSH from Windows on page 114

Windows SSH Address Format

The address format takes the following forms:

Windows SSH Command Line

```
ssh <user-name>@<external-server-ip-address> -p 22
-oProxyCommand="<full-path-to-proxytunnel.exe> -E --proxy="maint.<com-
domain>:6443" --dest='<customer-id>[-<system-name>][-<co-located-server-
ip-address>].maint.<com-domain>:22' -P '<proxy-username>:<proxy-
password>' -C '<full-path-ISRGRootX1-Pem-File>'"
```

Windows Putty Host Name

```
<customer-id>[-<system-name>][-<co-located-server-ip-
address>].maint.<com-domain>
```

Windows Putty Telnet command or local proxy command

```
proxytunnel.exe -E --proxy="maint.<com-domain>:6443" --dest="<customer-
id>[-<system-name>][-<co-located-server-ip-address>].maint.<com-domain>"
-P '<proxy-username>:<proxy-password>' -C 'isrgrootx1.pem'
```

where:

- < > indicates a field value to be replaced as detailed below. When replaced, omit the < > brackets.
- [ ] indicates an optional field. If added, omit the [ ] brackets.

Destination Server Address

The `--dest=`/hostname part of the command line varies based on the type of destination server. See the following examples.

Server	Address
Primary	`--dest="<customer-id>.maint.<com-domain>:22"`
Secondary or Expansion	`--dest="<customer-id>-<system-name>.maint.<com-domain>:22"`
Co-located Server	`--dest="<customer-id>-<system-name>-<co-located-server-ip-address>.maint.<com-domain>:22"`

Address Fields

The fields used in the addresses are:

- `<user-name>` is a user name for authentication on the target server. For IP Office servers, this is a Linux administrator account on the server.
- `<external-server-ip-address>` is the IP address of the server to which you are connecting.
- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<system-name>` is the optional non-primary IP Office system name to or through which, the connection is needed. The system names are shown in the customer system details (see Viewing the Customer System Details on page 24). Needed for
- `<co-located-server-ip-address>` is the optional IP address of the server co-located with the IP Office through which you are connecting, prefix with `-`. A tunnel must also be configured in the IP Office configuration (see Creating Tunnels for Remote Servers and Services on page 112).
- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.
- `<proxy-username>:<proxy-password>` are the user name and password of the reseller or distributor proxy management account for the IP Office system to which or through which the remote support connection is being routed. See Proxy Account Management on page 110.

Related links

Using SSH from Windows on page 114

Chapter 25: Using SSH from Linux

This section covers using SSH/SFTP to connect to the IP Office servers and other servers on the same network as the customer's IP Office servers.

This section covers the processes needed to connect from a Linux PC.

#	Stage	See ...
1.	**Enable remote access to the customer system:**	See Enabling Remote Support on an IP Office System on page 109.
2.	**Install Proxytunnel:**	See Installing Proxytunnel on Linux on page 120.
3.	**Connect using the command line:**	See SSH Command Line Connection (Linux) on page 121.

Related links

Installing Proxytunnel on Linux on page 120
SSH Command Line Connection (Linux) on page 121
SSH PuTTY Connection (Linux) on page 122
Linux SSH Address Format on page 123

Installing Proxytunnel on Linux

About this task

The Linux PC requires the Proxytunnel installed in order to support remote connections via COM.

For additional information on using Proxytunnel on a Linux server, see http://manpages.ubuntu.com/manpages/xenial/man1/proxytunnel.1.html.

Procedure

1. Access the command line on the Linux PC.
2. Enter `sudo apt-get update`
3. Enter `sudo apt-get install proxy-tunnel`

Next steps

- See SSH Command Line Connection (Linux) on page 121.

Related links

Using SSH from Linux on page 120

SSH Command Line Connection (Linux)

About this task

This process describes connecting from a Linux PC to a customer server via COM.

Before you begin

1. **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
2. **Install Proxytunnel utility:** See Installing Proxytunnel on Linux on page 120.
3. **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
4. Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. In the customer list, click on the customer's system name:
    a. For the IP Office server to which you want to connect or connect through, click **Remote Support Services**.
    b. Click **SSH Access Information**.
    c. Replace **Full Path of Proxy Tunnel Utility** with the full path of the folder in which you stored the downloaded utility files. For example; `C:\\Proxytunnel\proxytunnel.exe`.
    d. Click **Generate SSH Command**.
3. Example addresses are shown for the customer's primary server (**Primary Server (Linux)**) and for other server's (**External Server (Linux)**). Click the icon to copy the required address.
    - Strings shown as `********` are automatically replaced with the required value when cut and pasted.
4. For connections to a server co-located with the customer's IP Office server, replace the values in < > brackets:
    - `<username-for-co-located-server>` is a username used to authenticate SSH connections on the co-located server.
    - `<co-located-server-ip-address>` is the IP address of the co-located server.

Related links

Using SSH from Linux on page 120

SSH PuTTY Connection (Linux)

About this task

This process uses the information provided in the COM menus to setup a PuTTY connection.

Before you begin

- **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
- **Install Proxytunnel utility:** See Installing Proxytunnel on Linux on page 120.
- **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
- Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. View the customer list. See Using the Customer List on page 19.
2. In the customer list, click on the customer's system name:
    a. For the IP Office server to which you want to connect or connect through, click **Remote Support Services**.
    b. Click **SSH Access Information**.
    c. Replace **Full Path of Proxy Tunnel Utility** with the full path of the folder in which you stored the downloaded utility files. For example; `C:\\Proxytunnel\proxytunnel.exe`.
    d. Click **Generate SSH Command**.
3. Example addresses are shown in the **SSH Access Using Putty** and **SSH Access pf servers co-located to IP Office using Putty** sections. In the following steps, click on the icon to copy and paste the required address for the step.
    - Strings shown as `********` are automatically replaced with the required value when cut and pasted.
4. Start PuTTY.
5. Click **Session**.
6. In **Host Name**, paste the appropriate **Putty Host Name (Linux)** value from the COM menu.
    - For a server co-located with the customer's IP Office, replace the <co-located-server-ip-address>value with the IP address of the server.

7. Set the **Port** to `22`.
8. Click **Proxy**.
9. Set the **Proxy Type** to **Local**.
10. In **Telnet command or local proxy command**, paste the appropriate **Local Proxy Command for Putty (Linux)** from the COM menu.
    - For a server co-located with the customer's IP Office, replace the `<co-located-server-ip-address>` value as above.
11. Click **Open**.

Related links

Using SSH from Linux on page 120

Linux SSH Address Format

The address format takes the following forms:

Linux SSH Command Line

```
ssh <user-name>@<external-server-ip-address> -p
22 -oProxyCommand="proxytunnel -E --proxy="maint.<com-
domain>:6443" --dest='<customer-id>[-<system-name>][-<co-located-server-
ip-address>].maint.<com-domain>:22' -P '<proxy-username>:<proxy-
password>'"
```

Linux Putty Host Name

```
<customer-id>[-<system-name>][-<co-located-server-ip-
address>].maint.<com-domain>
```

Linux Putty Telnet command or local proxy command

```
proxytunnel -E --proxy="maint.<com-domain>:6443" --dest="<customer-id>[-
<system-name>][-<co-located-server-ip-address>].maint.<com-domain>" -P
'<proxy-username>:<proxy-password>'
```

where:

- `< >` indicates a field value to be replaced as detailed below. When replaced, omit the `< >` brackets.
- `[ ]` indicates an optional field. If added, omit the `[ ]` brackets.

Destination Server Address

The `--dest=`/hostname part of the command line varies based on the type of destination server. See the following examples.

Server	Address
Primary	--dest="<customer-id>.maint.<com-domain>:22"
Secondary or Expansion	--dest="<customer-id>-<system-name>.maint.<com-domain>:22"
Co-located Server	--dest="<customer-id>-<system-name>-<co-located-server-ip-address>.maint.<com-domain>:22"

Address Fields

The fields used in the addresses are:

- <user-name> is a user name for authentication on the target server. For IP Office servers, this is a Linux administrator account on the server.
- <external-server-ip-address> is the IP address of the server to which you are connecting.
- <customer-id> is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- <system-name> is the optional non-primary IP Office system name to or through which, the connection is needed. The system names are shown in the customer system details (see Viewing the Customer System Details on page 24). Needed for
- <co-located-server-ip-address> is the optional IP address of the server co-located with the IP Office through which you are connecting, prefix with -. A tunnel must also be configured in the IP Office configuration (see Creating Tunnels for Remote Servers and Services on page 112).
- <com-domain> is the domain part of the address normally used to connect to COM, prefixed with maint. For example, if you normally connect to COM using admin.example.com, for remote support use maint.example.com.
- <proxy-username>:<proxy-password> are the user name and password of the reseller or distributor proxy management account for the IP Office system to which or through which the remote support connection is being routed. See Proxy Account Management on page 110.

Related links

Using SSH from Linux on page 120

Chapter 26: Using HTTPS for Remote Support

This section covers using HTTPS in a web browser to connect to services on the customer's IP Office and other servers on the same network as that IP Office.

Note that only HTTPS is supported. HTTP connections are not supported.

#	Stage	See ...
1.	**Enable remote support on the customer system**	See Enabling Remote Support on an IP Office System on page 109.
2.	**Get the COM PAC file address**	See Getting the COM PAC File Address on page 125.
3.	**Configure the browser to use the .pac file**	See Browser PAC File Configuration on page 126.
4.	**Connect the browser**	See HTTPS Browser Connection on page 127.

Related links

Getting the COM PAC File Address on page 125
Browser PAC File Configuration on page 126
HTTPS Browser Connection on page 127
Browser Connection Workarounds on page 128
IP Office Administration Addresses on page 132
HTTPS Address Format on page 133

Getting the COM PAC File Address

About this task

HTTPS browser connection for remote support through COM requires the use of a browser 'proxy auto-configuration' (`.pac`) file. The COM server hosts a `.pac` file, the address of which can be used for the connection.

The commands inside the `.pac` file look for a match to the URL entered in browser and, when a match occurs, redirects it. In this case, it redirects any request for a URL containing `.maint.` to COM. COM then uses the original address to route the request to the required customer server.

Note:

- The same address can be used for all customer's managed through a particular COM server.

Before you begin

- **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.

Procedure

1. View the customer list (see Viewing the Customer List on page 20) and click on the customer's systems name.
   - Any customer already setup for remote connection can be selected. The same address is used for all customer's managed through a particular COM server.
2. Click on **Remote Support Services**.
3. Click **HTTP Access Information**.
4. Note the address shown for the **PAC file URL**. For example: `https://admin.example.com/com/remoteproxy/proxy.pac`
5. Click the icon to copy and paste the address into a text document or into your browser settings (see Browser PAC File Configuration on page 126).

Next steps

- **Configure the browser:** See Browser PAC File Configuration on page 126.

Related links

Using HTTPS for Remote Support on page 125

Browser PAC File Configuration

About this task

Use the following process to connect to a server/service on the customer network using a web browser.

Important:

- These instructions assume that the browser is not already configured to use a `.pac` or has its settings under IT management control. If that is the case, refer to Browser Connection Workarounds on page 128.

Procedure

1. Obtain the address for the COM `.pac` file. See Getting the COM PAC File Address on page 125. For example https://admin.example.com/com/remoteproxy/proxy.pac.
2. Enter the address into the browser settings:

Browser	Steps
Chrome	a. Click ⋮ > **Settings** > **Advanced** > **System** > **Open your computer's proxy settings** > **Use Setup script**. b. Enter the address of the COM `.pac` file and save the change.
Edge	a. Click **...** > **Settings** > **System** > **Open your computer's proxy settings** > **Use Setup script**. b. Enter the address of the COM `.pac` file and save the change.
Firefox	a. Click the ≡ icon and select ⚙ **Options**. b. Scroll down to **Network Settings** and click **Settings**. c. Select **Automatic proxy configuration URL**. d. Enter the address of the COM `.pac` file and click **OK**.

Next steps

- **Enter the customer's HTTPS address:** See HTTPS Browser Connection on page 127.

Related links

Using HTTPS for Remote Support on page 125

HTTPS Browser Connection

About this task

Use the following process to connect to a server/service on the customer network using a web browser.

Before you begin

1. **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
2. **Configure the browser to use the .pac file:** See Browser PAC File Configuration on page 126.
3. **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
4. Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. View the customer list (see Viewing the Customer List on page 20) and click on the customer's systems name.
2. Click on **Remote Support Services**.
3. Click **HTTP Access Information**.

4. A number of addresses are shown:
    - **Primary Server Service:**

      A number of addresses to services on the customer's primary server are shown (**Web Control Panel**, **one-X Portal**, **WebLM Server**). If you need one of these, click on the adjacent icon to copy and paste the address into the browser address bar.
    - **Other Server:**

      To connect to another server on the same network as the customer's primary server, copy and paste the **HTTPS via external servers or Apps Server** address. Replace the variable fields with the required values for the target server and service on that server:
        - <co-located-server-ip-address> is the IP address of the server co-located with the IP Office through which you are connecting. A tunnel must also be configured in the IP Office configuration (see Creating Tunnels for Remote Servers and Services on page 112).
        - <remote-port> is the port required on the remote server.
        - /<required-path> is the optional path to the page required on the remote server.
5. Enter the address.
6. The browser matches the address with the pattern specified in the COM .pac file and reroutes the request to COM.
7. When prompted to enter a user name and password, enter the values set for the reseller/distributor proxy account.
8. COM establishes a connection to the customer's IP Office and, if necessary, from that server to the required server on the same network as the IP Office.
9. Edge: If the error “Authentication not supported from the browser” is shown, enter edge://policy in the address bar and check that **AuthSchemes** includes the option **basic**.
10. The remaining actions depend on the remote path selected.

Related links

Using HTTPS for Remote Support on page 125

Browser Connection Workarounds

The previous topics in this documentation assume that the browser is able to directly use the COM .pac file address.

However, if that is not the case, for example the browser is already using another .pac file or is under IT management control, then the possible solutions are:

- If agreed by the owner of the existing .pac file being used by the browser, incorporate the commands from the COM .pac file. See PAC File Editing on page 129.

- Use the following workarounds to apply the COM `.pac` file settings locally to the browser or browser session:
  - **Chrome:** See Adding Additional PAC Commands in Chrome on page 131.
  - **Edge:** See Overriding the Default PAC File in Edge on page 130.

Related links

Using HTTPS for Remote Support on page 125
PAC File Editing on page 129
Overriding the Default PAC File in Edge on page 130
Adding Additional PAC Commands in Chrome on page 131

PAC File Editing

About this task

This process downloads the COM `.pac` file so that it can be opened in a text editor. The commands in the file can then be incorporated into the exist `.pac` file already being used.

Procedure

1. Obtain the address for the COM `.pac` file. See Getting the COM PAC File Address on page 125.
2. Enter the address of the COM `.pac` into the browser address bar and download the file.
3. Open the file in a text editor. It will look similar to the following:

```
function FindProxyForURL(url, host) {
  if (shExpMatch(host, "[a-zA-Z0-9]*-*.maint.<com_domain>")) { return "HTTPS
maint.<com_domain>:6443"; }
  else {
       return "DIRECT";
   }
}
```

   where:

   - `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.

   For example:

```
function FindProxyForURL(url, host) {
  if (shExpMatch(host, "[a-zA-Z0-9]*-*")) { return "HTTPS
admin.example.com:6443"; }
  else {
       return "DIRECT";
   }
}
```

4. Working with your local IT administrator, incorporate the '`if`' command into the existing `.pac` file used by your browsers.

Next steps

- **Enter the customer's HTTPS address:** See HTTPS Browser Connection on page 127.

Related links

Browser Connection Workarounds on page 128

Overriding the Default PAC File in Edge

About this task

Use this process with Edge if it is already configured to use an existing `.pac` file that cannot be changed.

Tip:

- Once this process has been tested successfully, the commands can be saved in a script/ batch file for future use.

Procedure

1. Obtain the address for the COM `.pac` file. See Getting the COM PAC File Address on page 125.
2. Access the Windows command line.
    a. Right-click on the start icon and select **Run**.
    b. Enter `cmd` and click **Open**.
    c. The Command Prompt window is opened.
3. Navigate to the folder in which the Edge browser application has been installed. In it default folder, this can be done with the command `cd C:\Program Files (x86)\Microsoft\Edge\Application`.
4. Launch the browser with the `.pac` file using the command:

   ```
   msedge.exe --proxy-pac-url=<pac-file-url>
   ```

   where:

   - `<pac-file-url>` is the web address of the `.pac` file provided by the COM service. For example; `https://admin.example.com/com/remoteproxy/proxy.pac`.

   For example:

   ```
   msedge.exe --proxy-pac-url=https://admin.example.com/com/
   remoteproxy/proxy.pac
   ```

Next steps

- **Enter the customer's HTTPS address:** See HTTPS Browser Connection on page 127.

Related links

Browser Connection Workarounds on page 128

Adding Additional PAC Commands in Chrome

About this task

This process is only required if the browser does not allow normal configuration of the a COM `.pac` file (see Browser PAC File Configuration on page 126).

This process downloads a set of file which includes a JavaScript file that contains the same commands as in the COM `.pac` file. Chrome is then configured to use these files as an extension, which adds the commands in the JavaScript file to any settings it is already using.

Before you begin

Procedure

1. View the customer list (see Viewing the Customer List on page 20) and click on the customer's systems name.
2. Click on **Remote Support Services**.
3. Click **HTTP Access Information**.
4. Click the icon next to **Download Chrome Extension to configure PAC file** and download the file.
5. Unzip the file into a folder and note the file path.

   Tip:

   - If also using SSH or RDP connections from the same PC, use the same folder that has been used to store the downloaded Proxytunnel and `isrgrootx1.pem` files.
6. Start Chrome and go to ⋮ > **More tools** > **Extensions**.
7. Select **Developer mode**.
8. Click **Load unpacked**.
9. Select the folder where the unzipped files are stored and click **Select Folder**.
10. Chrome reads the settings from the JavaScript file and uses them in future.

    Caution:

    - Note that the JavaScript file is read just once. If you need to make any future changes to it, click the reload icon shown in the Chrome extension details.

Next steps

- **Enter the customer's HTTPS address:** See HTTPS Browser Connection on page 127.

Related links

Browser Connection Workarounds on page 128

IP Office Administration Addresses

For HTTPS access to IP Office systems, a number of HTTPS addresses are supported.

Centralized Management Addresses

The following addresses are supported for IP Office systems setup for centralized management (see Using the IP Office Administration Apps on page 101). In this case, the browser does not need any additional configuration.

	Address Format
IP Office Web Manager	https://admin.<com-domain>:8443/<customer-id>/WebManagement/WebManagement.html This address can be access directly from COM using **Launch Application** > **Web Manager**.
Sysmon and SSA URL	admin.<com-domain>/<customer-id>[/<target-ip-office-ip-address>]

where:

- < > indicates a field value to be replaced as detailed below. When replaced, omit the < > brackets.
- [ ] indicates an optional field. If added, omit the [ ] brackets.
- <customer-id> is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- <target-ip-office-ip-address> is the optional IP address of the IP Office system connected to the primary server.
- <com-domain> is the domain part of the address normally used to connect to COM, prefixed with admin. For example, admin.example.com.

Remote Support Addresses

The following addresses are supported for IP Office systems setup for remote support (see Enabling Remote Connection on page 111) and using a browser configured for access via a proxy tunnel (see Using HTTPS for Remote Support on page 125).

Function	Address Format
Web Control Panel	https://<customer-id>-<system-name>.maint.<com-domain>:7071/login
one-X Portal	https://<customer-id>-<system-name>.maint.<com-domain>:9443/onexportal-admin.html
WebLM Server	https://<customer-id>-<system-name>.maint.<com-domain>:52233/WebLM/index.jps

where:

- < > indicates a field value to be replaced as detailed below. When replaced, omit the < > brackets.

- `[ ]` indicates an optional field. If added, omit the `[ ]` brackets.
- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<system-name>` is the IP Office system name as shown in the customer system details (see Viewing the Customer System Details on page 24).
- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.

Related links

Using HTTPS for Remote Support on page 125

HTTPS Address Format

HTTPS connections for remote support of servers co-located with IP Office systems managed by COM, use the address format below.

- The request must be redirected to the COM by the actions of another service such as a 'proxy auto-configuration' (`.pac`) file.
- Access to IP Office services use a different format. See IP Office Administration Addresses on page 132.

Address Format

The address format takes the form:

```
https://<customer-id>[-<system-name>]-<co-located-server-ip-
address>.maint.<com-domain>[:<remote-port>][/<required-path>]
```

where:

- `< >` indicates a field value to be replaced as detailed below. When replaced, omit the `< >` brackets.
- `[ ]` indicates an optional field. If added, omit the `[ ]` brackets.

Destination Server Address

The address varies based on the type of destination server through which the co-located server is being accessed:

Via	Address
Primary	`https://<customer-id>-<co-located-server-ip-address>.maint.<com-domain>[:<remote-port>][/<required-path>]`
Secondary or Expansion	`https://<customer-id>-<system-name>-<co-located-server-ip-address>.maint.<com-domain>[:<remote-port>][/<required-path>]`

Address Fields

The fields used in the addresses are:

- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<system-name>` is the optional non-primary IP Office system name to or through which, the connection is needed. The system names are shown in the customer system details (see Viewing the Customer System Details on page 24). Needed for
- `<co-located-server-ip-address>` is the IP address of the server co-located with the IP Office through which you are connecting. A tunnel must also be configured in the IP Office configuration (see Creating Tunnels for Remote Servers and Services on page 112).
- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.
- `<remote-port>` is the port required on the remote server.
- `/<required-path>` is the optional path to the page required on the remote server.

Related links

Using HTTPS for Remote Support on page 125

Chapter 27: Using Windows RDP

This section covers using RDP to connect to servers on the same network as the customer's IP Office systems.

#	Stage	See ...
1.	**Enable remote support on the customer system:**	See Enabling Remote Support on an IP Office System on page 109.
2.	**Download the Proxytunnel files:**	See Downloading the Utility Files on page 135.
4.	**Check the currently used ports:**	See Checking Available Local Ports on page 136.
5.	**Connect to the remote PC:**	See Connecting Using RDP on page 137.

Related links

Downloading the Utility Files on page 135
Checking Available Local Ports on page 136
Connecting Using RDP on page 137
RDP Address Format on page 138

Downloading the Utility Files

About this task

In order to use SSH from a Windows PC, a number of files need to be present on that PC:

- Proxytunnel is a utility used to tunnel connections via an HTTPS proxy. In this case, RDP and SSH connections to a customer's servers tunneled via COM to the customer IP Office.
- `isrgrootx1.pem` is a security certificate used for part of the remote connection. The certificate file needs to be available on the PC but does not need to be installed in the PC's security settings.

These files can be downloaded from COM using the process below.

Note:

- This process only needs to be done once on a particular PC. The files downloaded from COM are common for all systems being managed by that COM service.

Procedure

1. Display the list of customer systems. See Viewing the Customer List on page 20.

2. Click **Applications** > **Download Proxytunnel Utility**
3. Unzip the contents of the file to a folder on the PC. The path to the files in the folder is needed for various commands.

   Important:

   - If planning to use PuTTY, the application must have been installed with the option **Put install directory on the PATH for command prompts** selected.

Next steps

- Check the currently used ports. See Checking Available Local Ports on page 136.

Related links

Using Windows RDP on page 135

Checking Available Local Ports

About this task

For an RDP connection via COM, Proxytunnel needs to be associated with an unused IP port on the PC. The port should not be in use by any other application.

The process below can be used to list which ports the PC is currently using in order to select a free port.

Before you begin

- **Download the utility files:** See Downloading the Utility Files on page 135.

Procedure

1. Access the Windows command line.
   a. Right-click on the start icon and select **Run**.
   b. Enter `cmd` and click **Open**.
   c. The Command Prompt window is opened.
2. Enter `netstat -an` to see a list of ports currently being used by the PC.
   - To have the list sent to a text file, enter the command `netstat -an > c:\temp\ports.txt`, adjusting the file path to match an existing folder.
3. Once you think you have identified the local port you want to use, enter `netstat -ano | find ":<free-port-on-local-host>"`. If the port is in use, details of the usage are displayed, otherwise the results are blank.

Next steps

- The Windows PC can now be used to connect remotely to customer servers. See Connecting Using RDP on page 137.

Related links

Using Windows RDP on page 135

Connecting Using RDP

About this task

RDP connection is a two stage process:

1. Proxytunnel is used to bind a local port on the PC to the proxy address (COM) and the destination PC address, including the customer ID.
2. RDP is connected to the local port.

Before you begin

1. **Enable remote access to the system:** See Enabling Remote Support on an IP Office System on page 109.
2. **Download the utility files:** See Downloading the Utility Files on page 135.
3. **Check the currently used ports:** See Checking Available Local Ports on page 136.
4. **Ensure you have all the information required:** Read the process below before actually beginning and ensure that you have all the information required to complete the steps.
5. Viewing the remote support addresses is only supported for **Supervisor**, **Operator** and **Read-Only** users.

Procedure

1. Obtain an example command line for the customer system from COM:
    a. In the customer list, click on the customer's system name.
    b. Click **Remote Support Services**.
    c. Click **RDP via co-located IP Office**.
    d. Replace **Full Path of Proxy Tunnel Utility** with the full path of the folder in which you stored the downloaded files. For example; `C:\\Proxytunnel\proxytunnel.exe`.
    e. Click **Generate RDP Command**.
    f. Click the icon to copy the address shown.
        - Strings shown as `********` are automatically replaced with the required value when cut and pasted.
2. Access the Windows command line.
    a. Right-click on the start icon and select **Run**.
    b. Enter `cmd` and click **Open**.
    c. The Command Prompt window is opened.

3. Press Ctrl+V or right click the mouse to paste the address into the command line.
4. Replace the <external-server-ip-address> with the IP address of the remote server and enter the command.
5. Start RDP by selecting **Start** > **Windows Accessories** > **Remote Desktop Connection**.
6. In **Computer**, enter localhost:<free-port-on-local-host>, for example localhost:5000.

Related links

Using Windows RDP on page 135

RDP Address Format

Command Line Format

The address format takes the form:

```
<full-path-to-proxytunnel.exe> --standalone=<free-port-on-local-host> -E
--proxy="maint.<com-domain>:6443" --dest="<customer-id>[-<system-name>]-
<co-located-server-ip-address>.maint.<com-domain>:3389" -P '<proxy-
username>:<proxy-password>' -C '<full-path-ISRGRootX1-Pem-File>'
```

where:

- < > indicates a field value to be replaced as detailed below. When replaced, omit the < > brackets.
- [ ] indicates an optional field. If added, omit the [ ] brackets.

Destination Server Address

The --dest= part of the command line varies based on the type of destination server:

Server	Address
Primary	--dest="<customer-id>.maint.<com-domain>:3389"
Secondary or Expansion	--dest="<customer-id>-<system-name>.maint.<com-domain>:3389"
Co-located Server	--dest="<customer-id>-<system-name>-<co-located-server-ip-address>.maint.<com-domain>:3389"

Address Fields

The fields used in the address are:

- <full-path-to-proxytunnel.exe> is the path to the proxytunnel.exe file. For example, C:\\Proxytunnel\proxytunnel.exe.
- <free-port-on-local-host> is an available (unused) port of your local PC.

- `<com-domain>` is the domain part of the address normally used to connect to COM, prefixed with `maint`. For example, if you normally connect to COM using `admin.example.com`, for remote support use `maint.example.com`.
- `<customer-id>` is customer ID from COM. This is shown on the customer list view that includes the system. See Viewing the Customer List on page 20.
- `<system-name>` is the optional non-primary IP Office system name to or through which, the connection is needed. The system names are shown in the customer system details (see Viewing the Customer System Details on page 24). Needed for
- `<co-located-server-ip-address>` is the optional IP address of the server co-located with the IP Office through which you are connecting, prefix with `-`. A tunnel must also be configured in the IP Office configuration (see Creating Tunnels for Remote Servers and Services on page 112).
- `<proxy-username>:<proxy-password>` are the user name and password of the reseller or distributor proxy management account for the IP Office system to which or through which the remote support connection is being routed. See Proxy Account Management on page 110.
- `<full-path-ISRGRootX1-Pem-File>` is the path to the `isrgrootx1.pem` file. For example, `C:\\Proxytunnel\isrgrootx1.pem`.

Related links

Using Windows RDP on page 135

Part 9: COM Server Settings

Chapter 28: Managing the COM Server Preferences

Administrator users role can alter a number of COM server settings. These settings apply to all COM users and operation.

Related links

[Viewing the Application Preferences](#) on page 141
[COM Preferences](#) on page 141
[Changing the Application Logging Level](#) on page 142
[Setting the System Name](#) on page 143
[Changing the Password History Control](#) on page 143

Viewing the Application Preferences

Procedure

1. Click on the ⚙ icon.
2. Select **Preferences**. See COM Preferences on page 141.

Related links

[Managing the COM Server Preferences](#) on page 141

COM Preferences

Setting	Description
Session Timeout	Set the number of minutes after which inactive log-ins (other than wallboard mode users) are automatically logged out.
Enforce Password History	When users, including yourself, change their password, the application restricts them from using a previous password. This setting sets the number of previous passwords, per user, remembered.
Security Level	Set the level of certificate security checks applied for connections to COM.

Table continues…

Setting	Description
Server Side Log Level	The application can record details of its operations to log files. Those files may be useful to diagnose problems if the application does not appear to be performing correctly and may be requested by Avaya. See Changing the Application Logging Level on page 142.
System Name	If set, the system name is displayed just below the menu bar.
CPE Diagnostics Logs Retentions Days	Set the number of days that the COM server should retain log files from subscription systems. See Managing System Log Files on page 33.
Enable Security Banner	If enabled, the security banner is displayed is displayed as part of the login menu.
Security Banner Title	The title to be displayed above the **Security Banner Description** on the login menu when security banner display is enabled.
Security Banner Description	The additional text displayed on the login menu when **Enable Security Banner** is enabled. • The text can include basic HTML tags for header levels, paragraphs and text formatting such as bold, italic and underline.
Enable client logging	
Enable Downgrade	If enabled, COM can be used to downgrade systems to a lower level of software.
Enable System ID Change	If enabled, the existing ID of customer systems can be changed.

Related links

Managing the COM Server Preferences on page 141

Changing the Application Logging Level

About this task

The application can record details of its operations to log files. Those files may be useful to diagnose problems if the application does not appear to be performing correctly and may be requested by Avaya.

You can adjust the level of information that is logged. However, logging too much information can impact system performance and so should not be enabled unless necessary to resolve an issue.

Procedure

1. Click on the icon.
2. Select **Preferences**.
3. The options are:
   - **ERROR:** Only include error reports in the application logs.
   - **INFO:** Include general information and error reports in the application logs.

- **DEBUG:** Include comprehensive application information and errors reports in the application logs.

4. Click **Save**.

Related links

Managing the COM Server Preferences on page 141

Setting the System Name

About this task

You can enter a system name which, when set, is displayed just below the menu bar on the dashboard. For example, if you have more than one COM server, each support different sets of customers, use the label to indicate which set of customers the COM user is looking at.

Procedure

1. Click on the ⚙ icon.
2. Select **Preferences**.
3. Select **System Name**.
4. Enter the text that you want displayed above the dashboard. You can enter up to 32 characters.
5. Click **Save**.

Related links

Managing the COM Server Preferences on page 141

Changing the Password History Control

About this task

When users, including yourself, change their password, the application restricts them from using a previous password. The number of previous passwords the application remembers for each user can be adjusted.

Procedure

1. Click on the ⚙ icon.
2. Select **Preferences**.
3. Use **Enforce Password History** to set how many previous passwords the application should remember.
4. Click **Save**.

Related links

Managing the COM Server Preferences on page 141

Chapter 29: Server Certificates

This menu allows to see details of the service's own identity certificate and other certificates that it has stored.

Identity Certificate

By default the service has its own self-signed identity certificate which is valid for 3 years from installation. A 90-day warning is provided if the existing certificate being used by the server is about to expire.

This sections includes general instructions for adding a certificate to your browser. Normally your system maintainer will provide a copy of the application certificate which you can then add to your browser's certificate store. However, if necessary you can download a copy of the certificate using Chrome.

Trusted Certificate

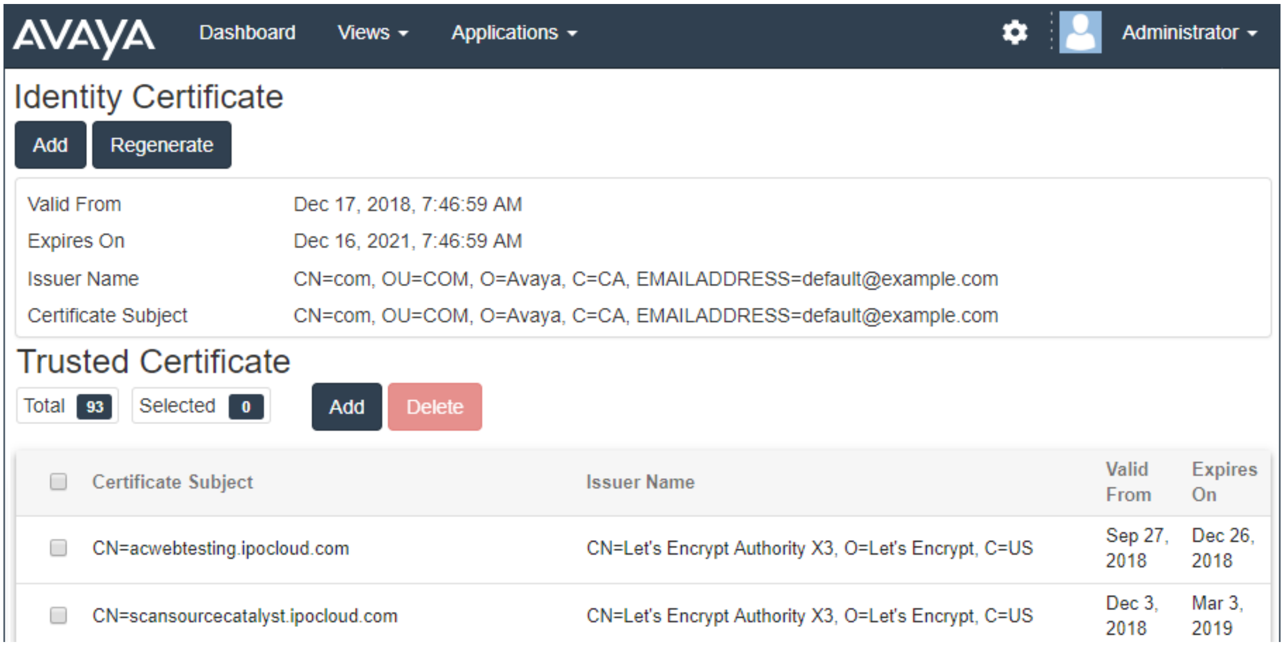
This table lists the other certificates that the service has stored. These can be IP Office system certificates and intermediate certificates.

Related links

Server Certificates on page 145
Adding a Certificate to a Browser on page 147

Server Certificates

This menu allows to see details of the COM service's own identity certificate and other certificates that it has stored.



Identity Certificate

By default the service has its own self-signed identity certificate which is valid for 3 years from installation. A 90-day warning is provided if the existing certificate being used by the server is about to expire.

This sections includes general instructions for adding a certificate to your browser. Normally your system maintainer will provide a copy of the application certificate which you can then add to your browser's certificate store. However, if necessary you can download a copy of the certificate using Chrome.

Trusted Certificate

This table lists the other certificates that the service has stored. These can be IP Office system certificates and intermediate certificates.

Related links

[Server Certificates](#) on page 145
[Regenerating the Identity Certificate](#) on page 146
[Adding a Different Identity Certificate](#) on page 147

Regenerating the Identity Certificate

About this task

You can replace the current identity certificate with a self-signed certificate generated by the COM application. This certificate will be valid for 3 years.

Procedure

1. Click on and then click on **Certificates**.
2. Click **Regenerate**.

3. Click **Yes**.

Related links

Server Certificates on page 145

Adding a Different Identity Certificate

About this task

You can replace the current identity certificate being used by the COM application. The same certificate can then be installed in any browsers and systems that need access to COM.

Procedure

1. Click on and then click on **Certificates**.
2. Click **Add**.
3. Click **Choose File** and select the new certificate file.
4. In the **Certificate Password** field enter the password for the certificate file.
5. Click **Submit**.

Related links

Server Certificates on page 145

Adding a Certificate to a Browser

If necessary, use the following process to add the certificate for access to COM to your browser.

Related links

Server Certificates on page 145
Downloading the Server Certificate on page 147
Adding a Certificate to Chrome on page 148
Adding a Certificate to Windows on page 149
Adding a Certificate to Firefox on page 149

Downloading the Server Certificate

About this task

Normally your system maintainer will provide a copy of the application certificate which you can then add to your browser's certificate store. However, if necessary you can download a copy of the certificate using Chrome.

Procedure

1. Login to COM.
2. Press `Ctrl+Shift+I`.

3. From the panel on the right select **Security**. If necessary click on the **>>** icon to select **Security**.
4. Click on **View certificate**. The certificate is displayed.
5. Click on **Details**.
6. Select **Copy to File**.
7. Click **Next**.
8. Select **DER encoded binary X.509 (.CER)** and click **Next**.
9. Enter the path where to save the file and the file name. This can be done using the **Browse** button.
10. Click **Next**.
11. Click **Finish** and then click **OK**.

Related links

[Adding a Certificate to a Browser] on page 147

Adding a Certificate to Chrome

About this task

Use the following process to add the COM certificate to your browser.

On Windows PCs, Edge and Chrome share the same certificate store.

Procedure

1. Click the ⋮ icon and select **Settings**.
2. Click **Advanced**.
3. Scroll to **HTTP/SSL** and click **Manage certificates**.
4. Click **Import**.
5. Click **Next** and **Browse** to the location of the downloaded certificate. Select it and click **Open**.
6. Click **Next**. Click **Place all certificates in the following store**.
   - If using the server's own generated certificate, select the **Trusted Root Certification Authorities**.
   - If using a certificate from another source, select **Intermediate Certification Authorities**.
7. Click **Next** and then **Finish**.
8. Click **OK** and then **Close**.

Related links

[Adding a Certificate to a Browser] on page 147

Adding a Certificate to Windows

About this task

On Windows PCs, Edge and Chrome share the same certificate store.

Procedure

1. Double-click on the certificate file.
2. On the **General** tab click **Install Certificate**.
3. Select **Current User** and click **Next**.
4. Select **Place all certificates in the following store**.
   - If using the server's own generated certificate, select the **Trusted Root Certification Authorities**.
   - If using a certificate from another source, select **Intermediate Certification Authorities**.
5. Click **Next**. A summary of the options selected is shown.
6. Click **Finish**.

Related links

Adding a Certificate to a Browser on page 147

Adding a Certificate to Firefox

About this task

Use the following process to add the COM certificate to your browser.

Procedure

1. Click the ≡ icon and select ⚙ **Options**.
2. Click **Advanced** and select **Certificates**.
3. Click **View Certificates**.
4. Click **Authorities**.
5. Click **Import**. Browse to the location of the CRT or PEM file downloaded from the server. Select the file and click **Open**.
6. Select all the check boxes to trust the certificate.
7. Click **OK** twice.

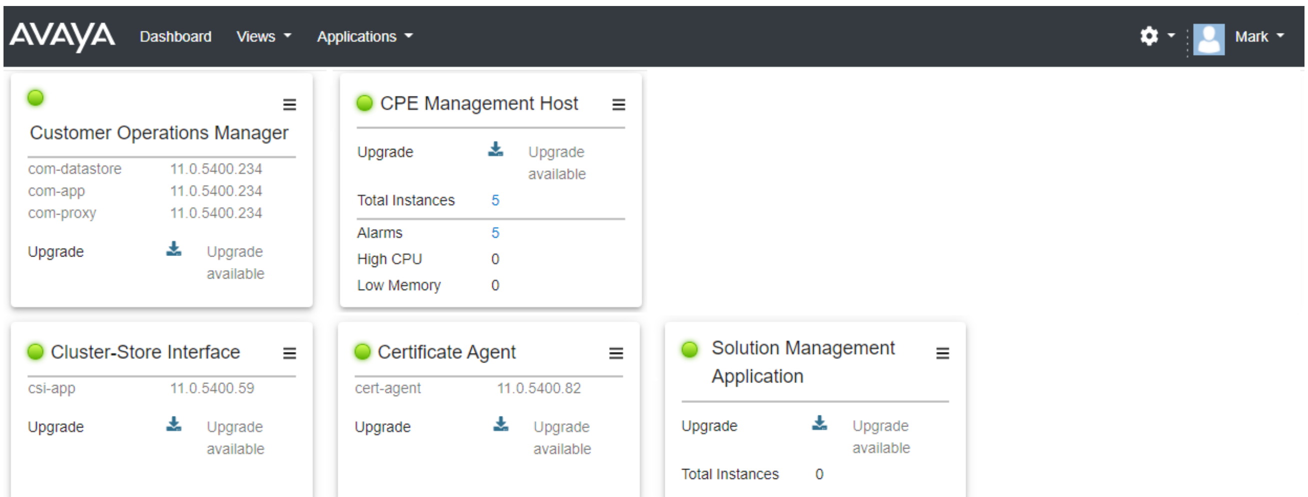
Related links

Adding a Certificate to a Browser on page 147

Chapter 30: The Application Center

The application center shows the status and version of various services used by the cloud cluster to support customer systems. The ≡ icon provides access to options to backup, restore or upgrade each service and its settings.

This is only supported for **Administrator** users.



- **Customer Operations Manager (COM)** – The COM service (this application) used to monitor and manage the customer systems.
- **Certificate Agent (CA)** – This service provides certificates for new systems and automatically renews the certificate of existing systems when required.
- **Cloud Diagnostic Agent (CDA)** – This service collects and stores log files from systems. See Managing System Log Files on page 33.
- **Cluster Store Interface (CSI)** – This service is used to launch new customer systems (and delete no longer needed systems).
- **CPE Management Host** - This service manages the monitoring and provision of subscriptions for customer systems.
- **Session Management Host** - COM can act as a proxy to relay remote connections to customer systems. This service supports those connections.

Part 10: Further Help

Chapter 31: Additional Help and Documentation

The following pages provide sources for additional help.

Related links

Additional Manuals and User Guides on page 152
Getting Help on page 152
Finding an Avaya Business Partner on page 153
Additional IP Office resources on page 153
Training on page 154

Additional Manuals and User Guides

The Avaya Documentation Center website contains user guides and manuals for Avaya products including IP Office.

- For a listing of the current IP Office manuals and user guides, look at the Avaya IP Office™ Platform Manuals and User Guides document.
- The Avaya IP Office Knowledgebase and Avaya Support websites also provide access to the IP Office technical manuals and users guides.
  - Note that where possible these sites redirect users to the version of the document hosted by the Avaya Documentation Center.

For other types of documents and other resources, visit the various Avaya websites (see Additional IP Office resources on page 153).

Related links

Additional Help and Documentation on page 152

Getting Help

Avaya sells IP Office through accredited business partners. Those business partners provide direct support to their customers and can escalate issues to Avaya when necessary.

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner. See Finding an Avaya Business Partner on page 153.

Related links

Additional Help and Documentation on page 152

Finding an Avaya Business Partner

If your IP Office system currently does not have an Avaya business partner providing support and maintenance for it, you can use the Avaya Partner Locator tool to find a business partner.

Procedure

1. Using a browser, go to the Avaya Website at https://www.avaya.com
2. Select **Partners** and then **Find a Partner**.
3. Enter your location information.
4. For IP Office business partners, using the **Filter**, select **Small/Medium Business**.

Related links

Additional Help and Documentation on page 152

Additional IP Office resources

In addition to the documentation website (see Additional Manuals and User Guides on page 152), there are a range of website that provide information about Avaya products and services including IP Office.

- Avaya Website (https://www.avaya.com)

  This is the official Avaya website. The front page also provides access to individual Avaya websites for different regions and countries.

- **Avaya Sales & Partner Portal** *(https://sales.avaya.com)*

  This is the official website for all Avaya business partners. The site requires registration for a user name and password. Once accessed, you can customize the portal to show specific products and information type that you want to see.

- **Avaya IP Office Knowledgebase** *(https://ipofficekb.avaya.com)*

  This site provides access to an online, regularly updated version of IP Office user guides and technical manual.

- **Avaya Support** *(https://support.avaya.com)*

This site provide access to Avaya product software, documentation and other services for Avaya product installers and maintainers.

- **Avaya Support Forums** (https://support.avaya.com/forums/index.php)

  This site provides forums for discussing product issues.

- **International Avaya User Group** (https://www.iuag.org)

  This is the organization for Avaya customers. It provides discussion groups and forums.

- **Avaya DevConnect** (https://www.devconnectprogram.com/)

  This site provides details on APIs and SDKs for Avaya products, including IP Office. The site also provides application notes for third-party non-Avaya products that interoperate with IP Office using those APIs and SDKs.

- **Avaya Learning** (https://www.avaya-learning.com/)

  This site provides access to training courses and accreditation programs for Avaya products.

Related links

Additional Help and Documentation on page 152

Training

Avaya training and credentials ensure our Business Partners have the capabilities and skills to successfully sell, implement, and support Avaya solutions and exceed customer expectations. The following credentials are available:

- Avaya Certified Sales Specialist (APSS)
- Avaya Implementation Professional Specialist (AIPS)
- Avaya Certified Support Specialist (ACSS)

Credential maps are available on the Avaya Learning website.

Related links

Additional Help and Documentation on page 152

Index

Special Characters

Numerics

A

B

C

J

L

M

N

O

P

Q

R

S

T

U

V

W