AVAYA

Experiences That Matter

MESSAGING ™

Technical Operating Guidelines
(What's new and Pre-sales Support)

AVAYA MESSAGING
TECHNICAL OPERATING GUIDELINES

This document covers the guidelines to be followed when deploying Messaging. Since deployment environments and technology related to Messaging are always changing, this document will also be updated periodically to reflect the latest trends and guidelines set for the industry. Please ensure that you have the latest version of Technical Operating Guidelines before proceeding with your research and deployment.

ferent number of licenses or units of capacity is specified in the documentation or other materials available to You. "Software" means computer programs in object code, provided by Avaya or an Avaya Channel Partner, whether as stand-alone products, pre-installed on hardware products, and any upgrades, updates, patches, bug fixes, or modified versions thereto. "Designated Processor" means a single stand-alone computing device. "Server" means a set of Designated Processors that hosts (physically or virtually) a software application to be accessed by multiple users. "Instance" means a single copy of the Software executing at a particular time: (i) on one physical machine; or (ii) on one deployed software virtual machine ("VM") or similar deployment.

License types

Designated System(s) License (DS). End User may install and use each copy or an Instance of the Software only: 1) on a number of Designated Processors up to the number indicated in the order; or 2) up to the number of Instances of the Software as indicated in the order, Documentation, or as authorized by Avaya in writing. Avaya may require the Designated Processor(s) to be identified in the order by type, serial number, feature key, Instance, location or other specific designation, or to be provided by End User to Avaya through electronic means established by Avaya specifically for this purpose.

Concurrent User License (CU). End User may install and use the Software on multiple Designated Processors or one or more Servers, so long as only the licensed number of Units are accessing and using the Software at any given time. A "Unit" means the unit on which Avaya, at its sole discretion, bases the pricing of its licenses and can be, without limitation, an agent, port or user, an e-mail or voice mail account in the name of a person or corporate function (e.g., webmaster or helpdesk), or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software. Units may be linked to a specific, identified Server or an Instance of the Software.

Named User License (NU). You may: (i) install and use each copy or Instance of the Software on a single Designated Processor or Server per authorized Named User (defined below); or (ii) install and use each copy or Instance of the Software on a Server so long as only authorized Named Users access and use the Software. "Named

User", means a user or device that has been expressly authorized by Avaya to access and use the Software. At Avaya's sole discretion, a "Named User" may be, without limitation, designated by name, corporate function (e.g., webmaster or helpdesk), an e-mail or voice mail account in the name of a person or corporate function, or a directory entry in the administrative database utilized by the Software that permits one user to interface with the Software.

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, and 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. Note, unless otherwise stated, that 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

"Third Party Components" mean certain software programs or portions thereof included in the Software or Hosted Service may contain software (including open source software) distributed under third party agreements ("Third Party Components"), which contain terms regarding the rights to use certain portions of the Software ("Third Party Terms"). As required, information regarding distributed Linux OS source code (for those products that have distributed Linux OS source code) and identifying the copyright holders of the Third Party Components and the Third Party Terms that apply is available in the products, Documentation or on Avaya's website at: https:// support.avaya.com/Copyright or such successor site as designated by Avaya. The open source software license terms provided as Third Party Terms are consistent with the license rights granted in these Software License Terms, and may contain additional rights benefiting You, such as modification and distribution of the open source software. The Third Party Terms shall take precedence over these Software License Terms, solely with respect to the applicable Third Party Components to the extent that these Software License Terms impose greater restrictions on You than the applicable Third Party Terms.

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

THE FOLLOWING APPLIES TO AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS OR SERVICES. THE PRODUCT OR HOSTED SERVICE MAY USE THIRD PARTY COMPONENTS SUBJECT TO THIRD PARTY TERMS AND REQUIRE A SERVICE PROVIDER TO BE INDEPENDENTLY LICENSED DIRECTLY FROM THE THIRD PARTY SUPPLIER. AN AVAYA CHANNEL PARTNER'S HOSTING OF AVAYA PRODUCTS MUST BE AUTHORIZED IN WRITING BY AVAYA AND IF THOSE HOSTED PRODUCTS USE OR EMBED CERTAIN THIRD PARTY SOFTWARE, INCLUDING BUT NOT LIMITED TO MICROSOFT SOFTWARE OR CODECS, THE AVAYA CHANNEL PARTNER IS REQUIRED TO INDEPENDENTLY OBTAIN ANY APPLICABLE LICENSE AGREEMENTS, AT THE AVAYA CHANNEL PARTNER'S EXPENSE, DIRECTLY FROM THE APPLICABLE THIRD PARTY SUPPLIER.

WITH RESPECT TO CODECS, IF THE AVAYA CHANNEL PARTNER IS HOSTING ANY PRODUCTS THAT USE OR EMBED THE G.729 CODEC, 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 G.729 CODEC IS LICENSED BY SIPRO LAB TELECOM INC. SEE WWW.SIPRO.COM/CONTACT.HTML. 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 for complying 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, call Technical Service Center Toll Fraud Intervention Hotline at +1-800-643-2353 for the United States and Canada. For additional support telephone numbers, see the Avaya Support website: https://support.avaya.com or such successor site as designated by Avaya.

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).

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 Hosted Service notices and articles, or to report a problem with your Avaya product or Hosted 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.

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 Inc.

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.

AVAYA MESSAGING
TECHNICAL OPERATING GUIDELINES

Table of Contents

1 NEW FEATURES

New Features

A number of new features have been added to Avaya Messaging in 10.8.

- Rebranded Esna Officelinx to Avaya IX Messaging.
- New Report Server type available in HA environments.   Makes available more of the database for client reporting requirements.
- Compliant with General Data Protection Regulation (GDPR) requirements including the Forget Me utility for data clean-up.
- Now supporting Office 365 integration using Microsoft Graph.
- Support added for Exchange 2019.
- IX Messaging is now using Nuance Recognizer 10 as the ASR Engine.

Report Server

The Web Report feature of Avaya IX Messaging allows you to generate a variety of reports on key areas of the system, such as calls per hour by PBX and company, port usage and mailbox usage. These reports help administrators adjust server load and performance to ensure maximum productivity.

Web reports is limited by the data that is made available, and by what can be built within the user interface in terms of how it is presented (charts, tables, graphs, etc.).

For companies that want tighter control over their reports, a **Report Server** can be setup that has direct access to the database. More of the data is made available to whatever program you want to use to display the data and generate meaningful output.

Important Facts

- The Report Server must be used in conjunction with a **High Availability** installation as it uses features and services (e.g. Mobilink) that are not available when using a Single Server.
- The Report Server feature is included with the HA license. No additional purchase is required.
- The Report Server must be housed on a different computer that any used by the system.
- Multiple Report Servers can be installed.
- The Report Server creates a local, continually updated copy of the database on the Consolidated Server.
- Only usage data is available to the Report Server. System operating information (e.g. passwords, usernames, etc.) is not included.
- The Report Server has no user interface of its own to view the data or generate reports. The data is simply made available to whatever software you already use for your reporting needs. Additional work by the administrator will be required to extract and process the data.

Server Requirements

The Report Server must have at least the following.

Operating System	Windows Server 2012 / 2016 / 2019
CPU	2 or more CPUs @ 2+ GHz
RAM	At least 50% of the RAM on the Consolidated Server (min 4 GB)
HDD	200 GB (100GB for O/S, 100 GB for IX Messaging)

Configuring the Report Server

The Avaya IX Messaging High Availability installation must already be setup and running before adding a Report Server. A different computer must be connected to the same subnet as the Consolidated Server in order to read the database. The Windows operating system must be installed, updated and patched.

On the computer that will host the Remote Report Server:

1. Copy the Avaya IX Messaging installation program to this computer. Run **Setup.exe** <u>as administrator</u> to begin installing.
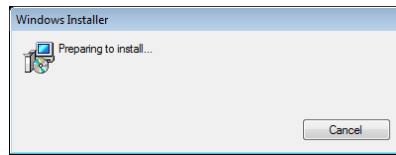
2. Once the Windows components have been verified, click **Next** to begin the installation.

3. Enter the DCOM user info (domain user account which has local administrator rights). This is required by services which use local administrator rights.

   Click **OK** after entering the credentials.
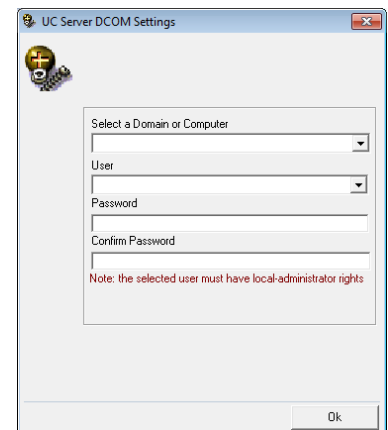
4. Review the EULA and enable **I accept the license agreement**.

   Click **Next** to continue.
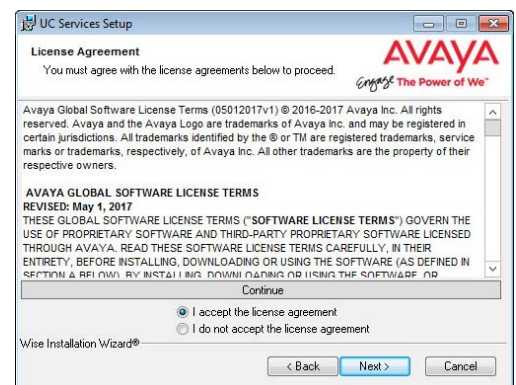
5. You will be asked to select the destination of the installation. You may change the hard drive destination through the drop down menu. By default, the installation will create a UC folder on the C drive.

Click **Next** to continue.
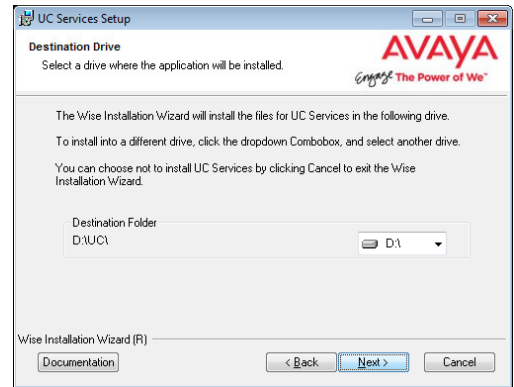
6. Enable **Multiple UC Servers in High Availability**.

Click **Next**.
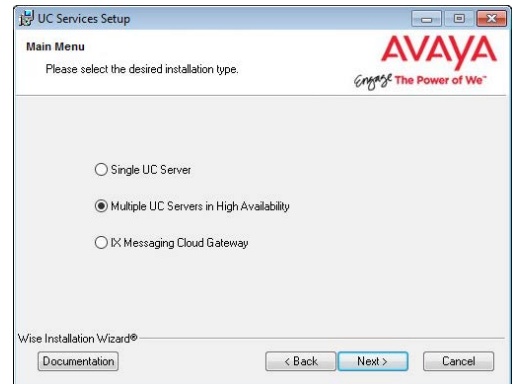
7. Select **Remote Report Server (only)**.

Click **Next.**
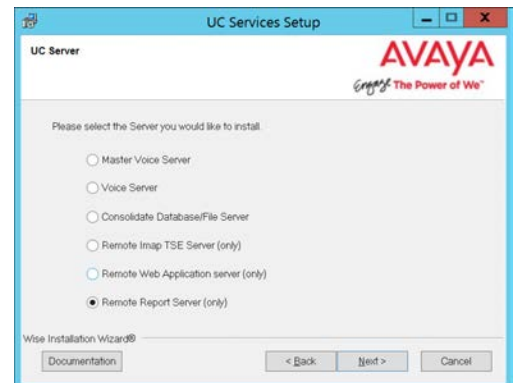
8. Enter a number to identify this Report Server. If you have more than one Report Server, each must be given a unique number.

Click **Next.**

Note: This number is independent of any other server identification numbers (i.e. Secondaries, Remote CSEs).
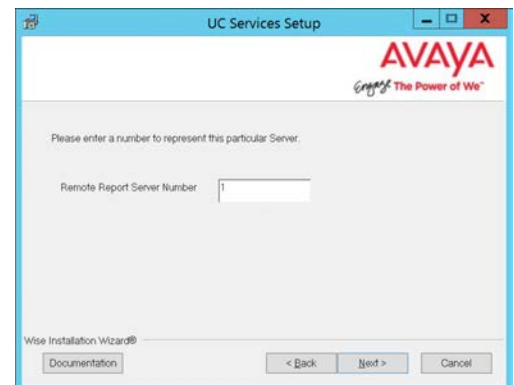
9. Enter the **IP Address** for the Primary Server.

Click **Next**.

10. Enter the **IP Address** for the Consolidated Server.

Click **Next**.
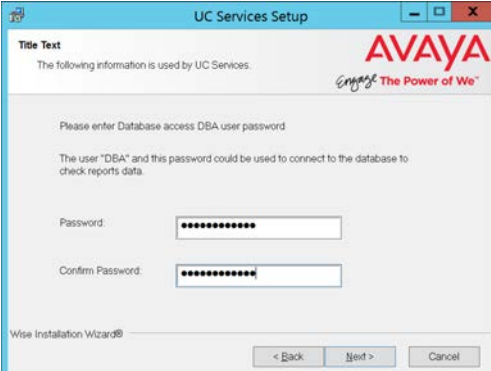
11. Create the Database Access DBA User Password in the space provided. This password will be used by the Report Server to access the database.
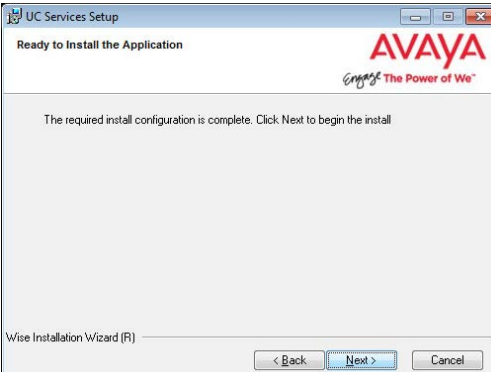
Click **Next**.

12. The preliminary information required for installation is complete.

Click **Next**.

13. The selected components will be installed.
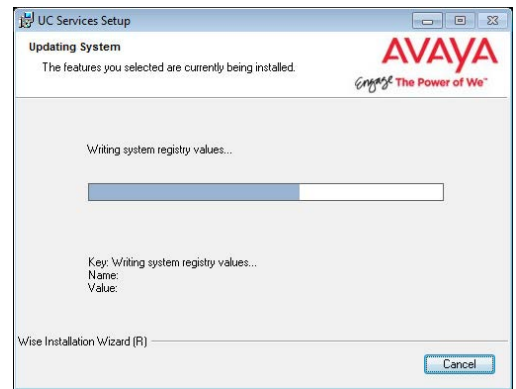
14. The installation of the Report Server is complete.

    Click **Finish** to restart the server.

    If you wish to restart your computer at a later time, disable the **Restart** checkbox then click **Finish**.

15. This alert is to remind you to properly share the UC installation folder.

    Click **OK** to restart the computer.
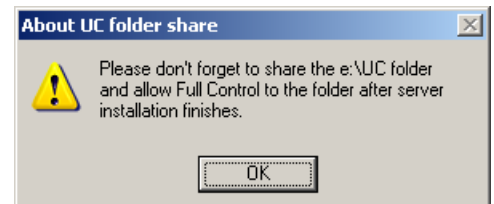
Accessing the Database

The database on the Report Server is only a portion of the full database found on the IX Messaging voice server. It only contains client and system usage data. It does not contain any confidential or system information (i.e. passwords). The Report Server database is continually synchronized with the main database.

On the Report Server, the database is stored in the /UC/DB folder on the installation drive you chose. The database is named **EEAM21.db** and It is an SQL formatted database. You will need to write scripts to import the information you need into whichever program you are using analyze the data.

Sample JDBC Connection to Retrieve Data

Note: The Java Development Kit (**JDK**) must be installed before proceeding with the code sample.

Create JDBCConnect.java file

The following is sample of code using a JDBC connection to access the database.

```java
import java.io.*;
import java.sql.*;

public class JDBCConnect
{
    public static void main( String args[] )
    {
        try
        {
            String userID = "";
            String password = "";
            String server = "";
            String driver = "jdbc4";
            String SQL ="select * from repMailboxActivity";
            if( args.length > 0 ) userID = args[0];
            if( args.length > 1 ) password = args[1];
            if( args.length > 2 ) server = args[2];
            if( args.length > 3 ) driver = args[3];
            if( args.length > 4 ) SQL = args[4];
            Connection con;
            if( driver.compareToIgnoreCase( "jdbc4" ) == 0 )
            {
                con = DriverManager.getConnection(
                    "jdbc:sqlanywhere:uid=" + userID + ";pwd=" + password + ";servername=" + server);
            }
            else
            {
                con = DriverManager.getConnection(
                    "jdbc:sybase:Tds:localhost:2638", userID, password);
            }
            Statement stmt = con.createStatement();
            ResultSet rs = stmt.executeQuery(SQL);
            while( rs != null )
            {
                while (rs.next())
                {
                    for( int i = 1;
                         i <= rs.getMetaData().getColumnCount();
                         i++ )
                    {
                        if( i > 1 ) System.out.print(", ");
                        System.out.print(rs.getString(i));
                    }
                    System.out.println();
                }
                if( stmt.getMoreResults() )
                {
                    System.out.println();
                    rs = stmt.getResultSet();
                }
                else
                {
```

```
            rs.close();
            rs = null;
          }
        }
        stmt.close();
        con.close();
      }
      catch (SQLException sqe)
      {
        System.out.println("Unexpected exception : " +
                  sqe.toString() + ", sqlstate = " +
                  sqe.getSQLState());
        System.exit(1);
      }
      catch (Exception e)
      {
        e.printStackTrace();
        System.exit(1);
      }
      System.exit(0);
    }
  }
```

Running the Sample Application

1. At a command prompt, change to the **%SQLANYSAMP17%\SQLAnywhere\JDBC** directory.
2. Set the CLASSPATH environment variable. The SQL Anywhere JDBC driver is contained in **sajdbc4.jar**.

   set classpath=.;%SQLANY17%\java\sajdbc4.jar.

   If you are using the jConnect driver instead, then set the CLASSPATH as follows (where jconnect-path is your jConnect installation directory).

   set classpath=.;jconnect-path\classes\jconn4.jar

3. Run the following command to compile the example:

   javac JDBCConnect.java

4. Run the following command to execute the example:

   java JDBCConnect DBA "!Password"

   A default SQL query is executed.
   If the attempt to connect fails, an error message appears instead. Confirm that you have executed all the steps as required. Check that your CLASSPATH is correct. An incorrect setting may result in a failure to locate a class.
5. Optional. Include SQL queries on the command line:

   java JDBCConnect DBA "!Password" jdbc4 "SELECT * FROM Customers"

Improved Single Sign-On

Legacy SSO

Logging in to Avaya Messaging applications (**Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**) is handled using a 3rd party authentication provider, such as Salesforce, Google, Office 365 or Windows. This Single Sign-On process let's clients use their credentials from the other applications to access Messaging. This is known as **Legacy SSO**.

Clients open an application, are passed through Messaging and then onto the provider. The client's credentials are authenticated by the provider and access is granted.
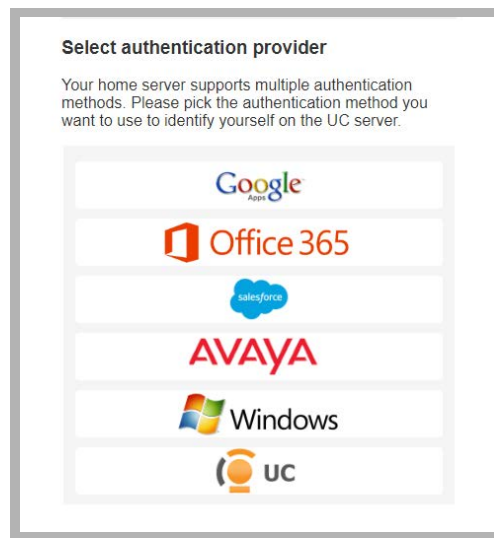
Hybrid SSO

The preferred method for authentication is **Hybrid SSO** as it offers a higher level of security for your connections by adding a certificate validation layer. The Voice Server, or the Consolidated Server in a High Availability environment, is authenticated on the Avaya licensing server through a certificate enabled handshake. The client then uses whichever login credentials they have available to complete the connection from their current location.

Clients open an application and are passed through to Messaging. If the connection to the accounts.zang.io server has been validated by the certificate, the login request is sent to the provider for authentication. If either the connection is not valid, or if the client's credentials are incorrect, then access is denied.

Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down (i.e. at high security, isolated sites).

A the end of the installation routine, you are asked to select the SSO method to employ.

Legacy SSO

To use the **Legacy SSO** login method:

- On the SSO Configuration screen, enable **Legacy SSO**.
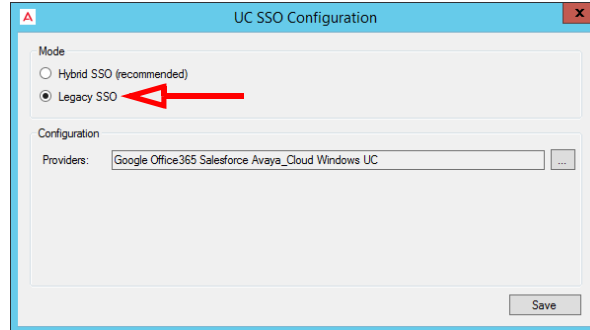
- From the Providers dropdown menu, enable the authentication providers that you want your clients to use to access **Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**. Items that are disabled will not appear during login.
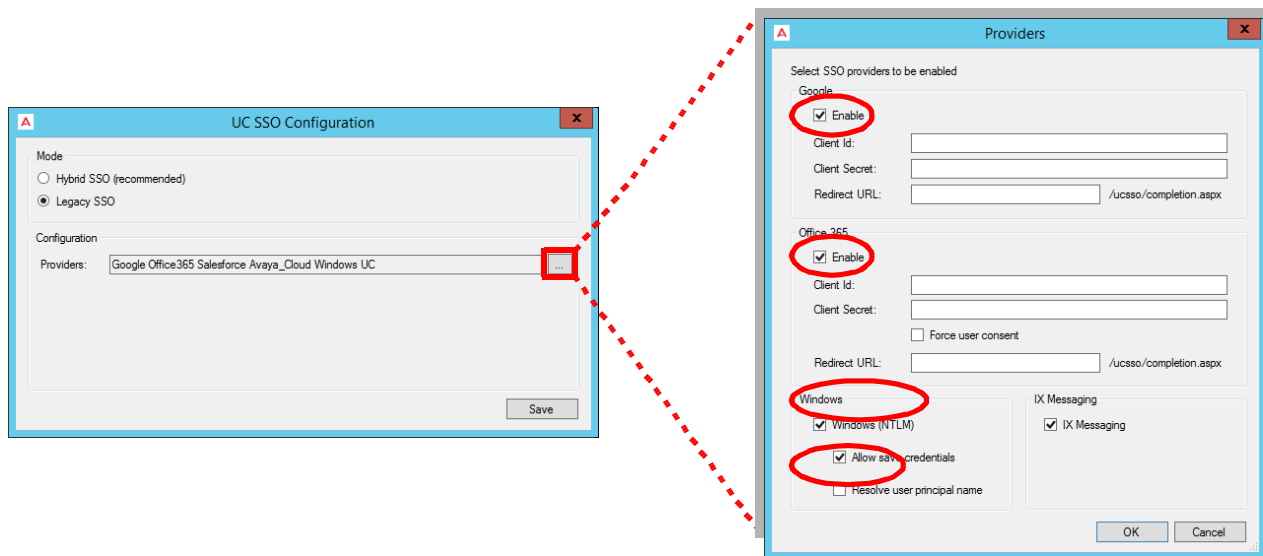
Filling out these fields is optional and only required if you make use of OAuth2 when connecting to these providers.
- **Client Id**: Enter the OAuth2 client ID for the provide you have chosen.
- **Client Secret**: Enter the OAuth2 client secret value for the provide you have chosen.
- **Redirect URL**: Enter the URL for your company given by the provider you have chosen.

- Enable all that apply, then click **OK**.
- Click **Save** when finished.

Hybrid SSO

Important: The **Hybrid SSO** login procedure requires an active Internet connection. Only **Legacy SSO** can be used if Internet access is disabled / locked-down (i.e. at high security, isolated sites).

To use the **Hybrid SSO** authentication method:

- On the SSO Configuration screen, enable **Hybrid SSO**.
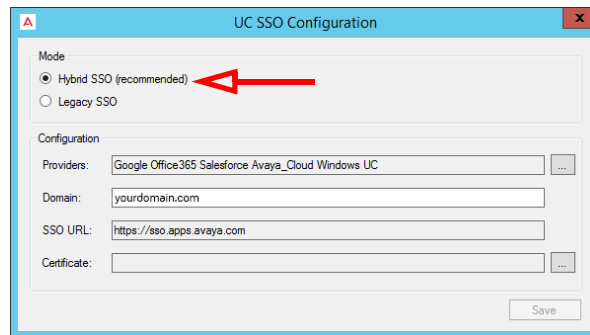
- From the Providers dropdown menu, enable the authentication credentials that you want your clients to use to access **Web Admin**, **Web Access**, **Web Reports** and **Messaging Admin**. Items that are disabled will not appear during login.

  Enable all that apply, then click **OK**.
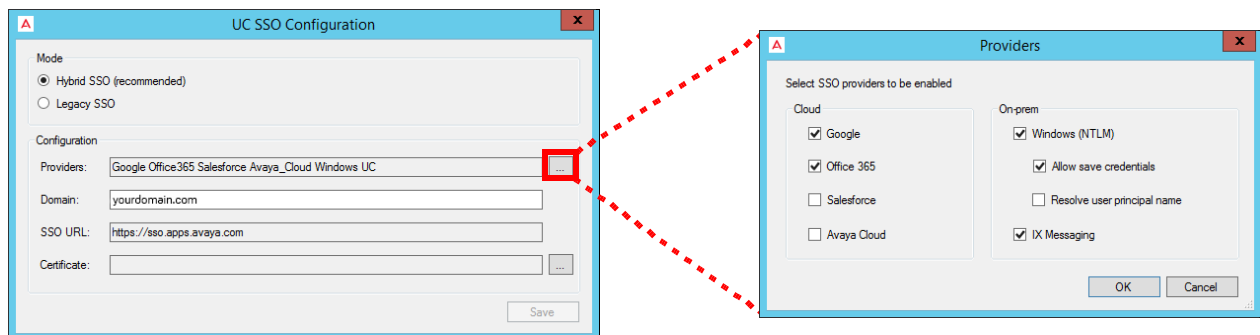
- Enter the domain name where your Voice / Consolidated server is located in the space provided.
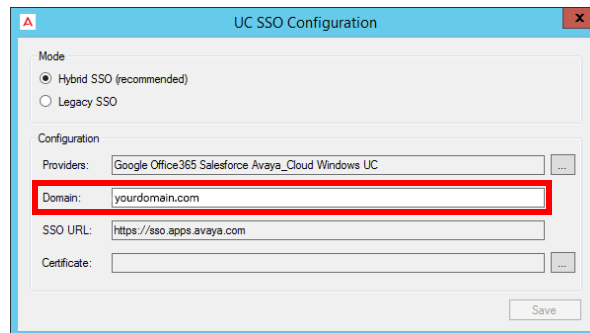
- A certificate is required when using Hybrid SSO. Click the button to the right side of the Certificate field. Choose **Create** to have Messaging build a certificate for you. Or if you have a certificate in **PFX** format that you would rather use, click **Import** and select that file instead.

  Select the certificate to use, then click **OK**.
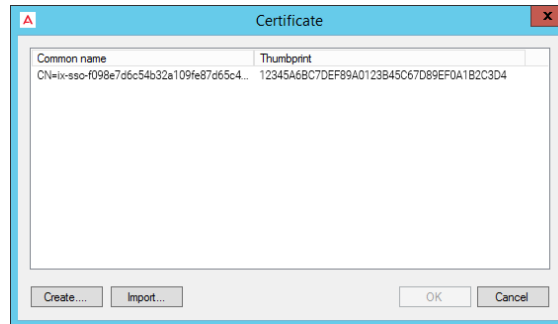
- Once back at the SSO Providers screen, click **Save**.

- Follow the instructions on this window to complete the installation.
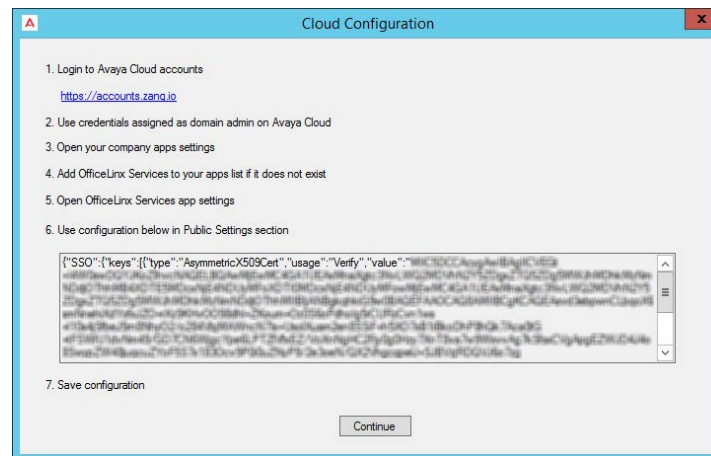
1. Click the link, or enter the URL into the address bar of a web browser to open the Avaya Cloud Accounts site.
2. Login using credentials for an account with administrator rights to the domain.
3. Go to **Manage Companies**, select a company (if more than one), and open the **Apps** tab.
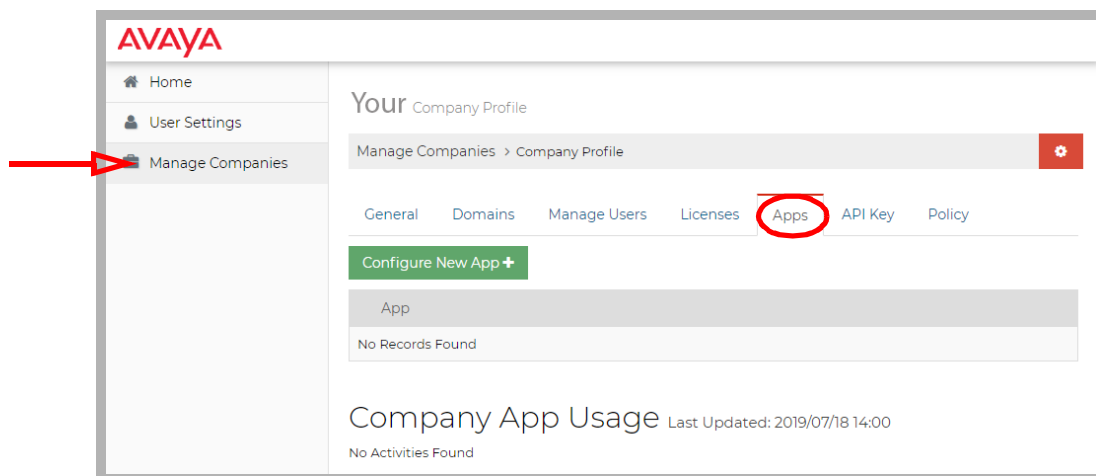
4. Click **Configure New App+**. On the **Product** dropdown menu, select **IX Messaging Services**.
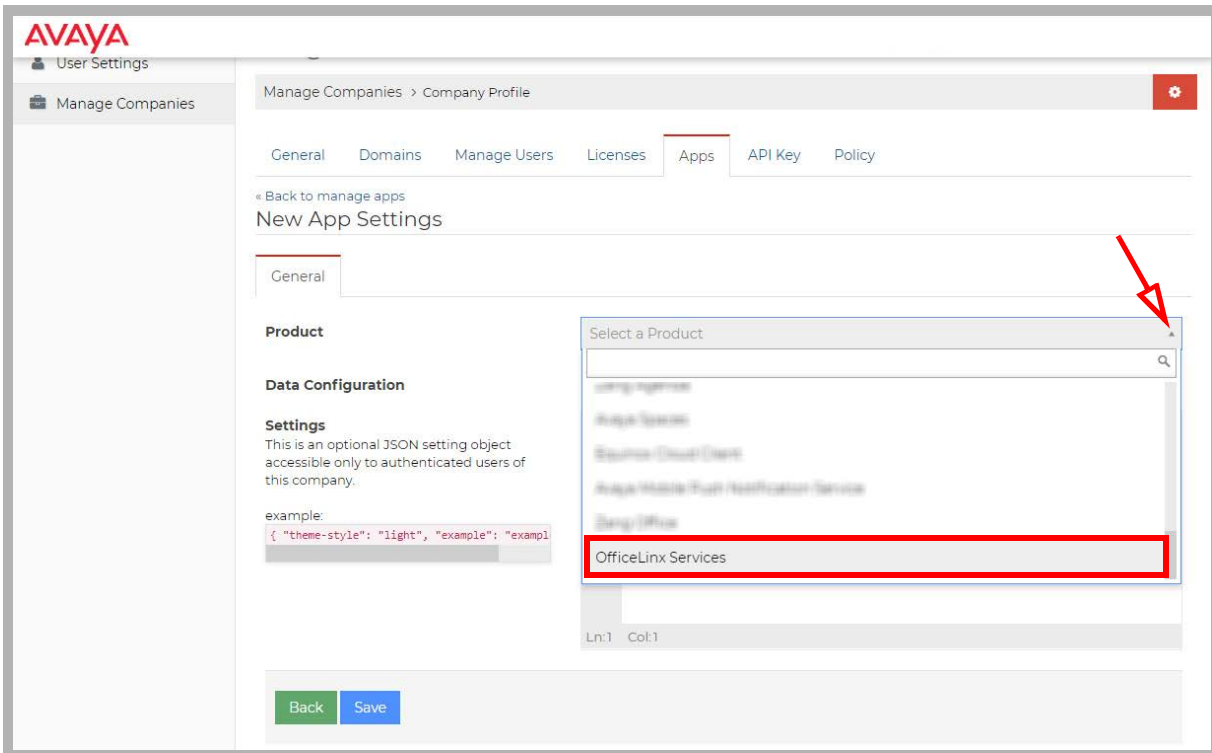
5. You should land on the IX Messaging Services Application Settings page.
6. Ensure that the option for **JSON** is enabled then scroll down to **Public Settings**. Copy the string from the Cloud Configuration panel and paste it into the space provided.

Caution: Be careful to copy the **entire** string from the Cloud Configuration panel. It may extend below the bottom of the pane.

7. Click **Save** when ready. Returning to the Cloud Configuration panel, click **Continue** to complete the Hybrid SSO configuration.

As long as the strings on both the Voice / Consolidated server and the Avaya Cloud server match, users will be able to access the applications using their available credentials.

If these strings are not the same, then users will not be able to login using any credentials.

General Data Protection Regulation (GDPR) Setup

By default, certain information is collected on all incoming calls through Avaya Messaging. This data is collected so that site administrators can generate reports that show traffic flows, system capacity and other usage data. This information includes calling number, caller ID, date and time and length of the call, and so on. Conversations can also be recorded and stored by the system.

Avaya Messaging complies with the General Data Protection Regulation (GDPR) standard, allowing site administrators to delete this information from the database after a request from the caller, maximizing personal data security.

Prompts can be setup to be played before each call starts, alerting the caller that the information is being collected.   They then have the option to terminate the call, or to request that the details be removed from the database afterwards if security is an issue.

Installation

Adding GDPR to Avaya Messaging is typically done during the initial program installation procedure, although it can be added afterwards (see Enable / Disable GDPR).

During installation, at the screen where you are asked whether or not you want to include GDPR with the product, enable **Yes**. This will cause the installer to make the necessary adjustments to the database to accommodate GDPR. It also installs the utility that allows the administrator to remove a caller's details from the database.

Enable / Disable GDPR

Typically, enabling or disabling GDPR is configured during the initial installation of Avaya Messaging.
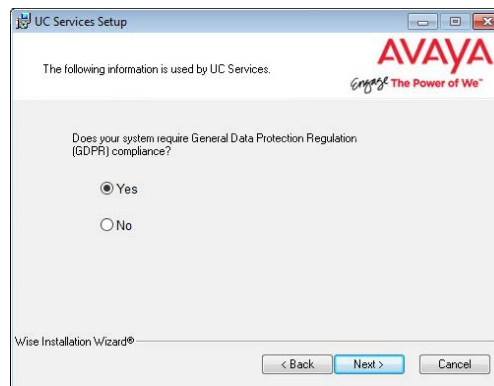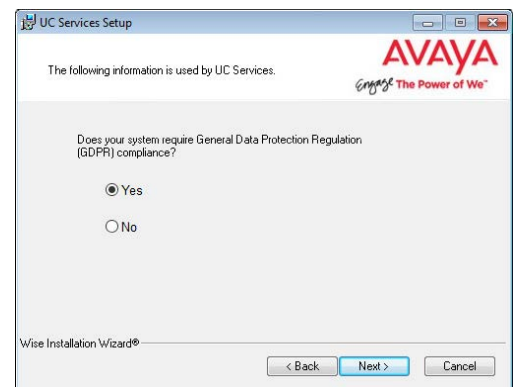
It can always be turned on or off at any time thereafter as required.

1. Open Messaging Admin on the voice server.
2. Open **Configuration > Advanced**.

3. In the right-hand pane, double-click **GDPR compliance** and set the Value Data field to **True** (to enable) or **False** (to disable) this feature.
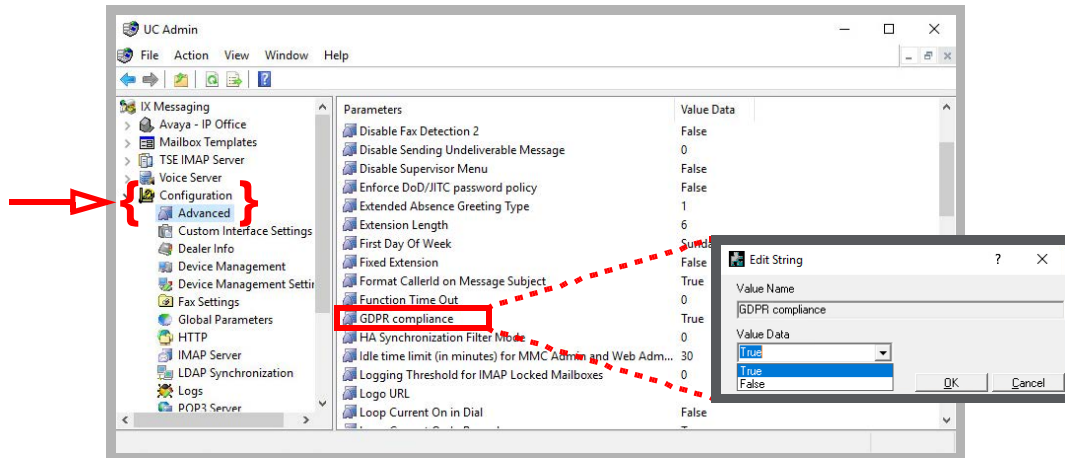
Enabling and Customizing Collection Notification Alerts

An audio alert can be played before an incoming call to notify the caller that their personal information will be collected or that the conversation is being recorded. They have the option to request that this information be deleted.

A standard, generic, system prompt can be used for each case, or you can record custom prompts.

1. Open Messaging Admin on the voice server.
2. Open **Company > Default > Feature Group**. Select a Feature Group to apply GDPR notifications to and double-click.
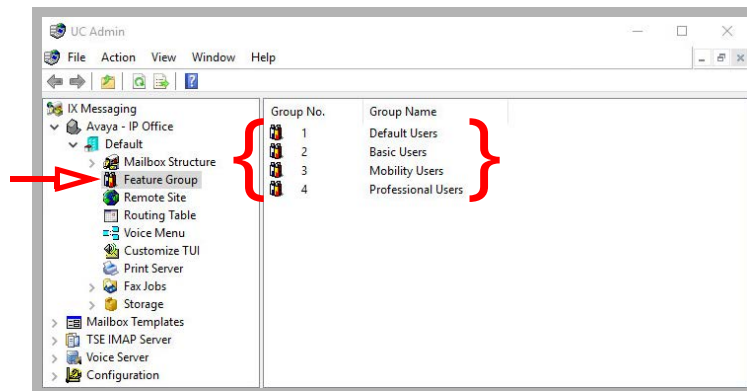
3. Go to the **Transfer Options** tab.
4. In the section for **Record Conversation Warning**, enable **Play record Conversation Warning** to play the system prompt for the incoming caller whenever the call will be recorded.
If you have recorded a customized greeting for this event, enable **Play record Conversation Custom Warning** instead and enter the 4-digit SAL number (digits only) for the custom recording (see Recording a Custom Greeting).
If you do not wish to play a warning when recording a call, disable both options.
5. In the section for **Data Collection Warning**, select an **Announcement Type**.

   None: This option will disable the warning for data collection.

   System Prompt: Plays the system prompt when an incoming caller leaves a message in voicemail.

   Custom Prompt: Plays the custom prompt that you recorded when an incoming caller leaves a message in voicemail. Enter the 4-digit SAL number (digits only) for the custom recording (see Recording a Custom
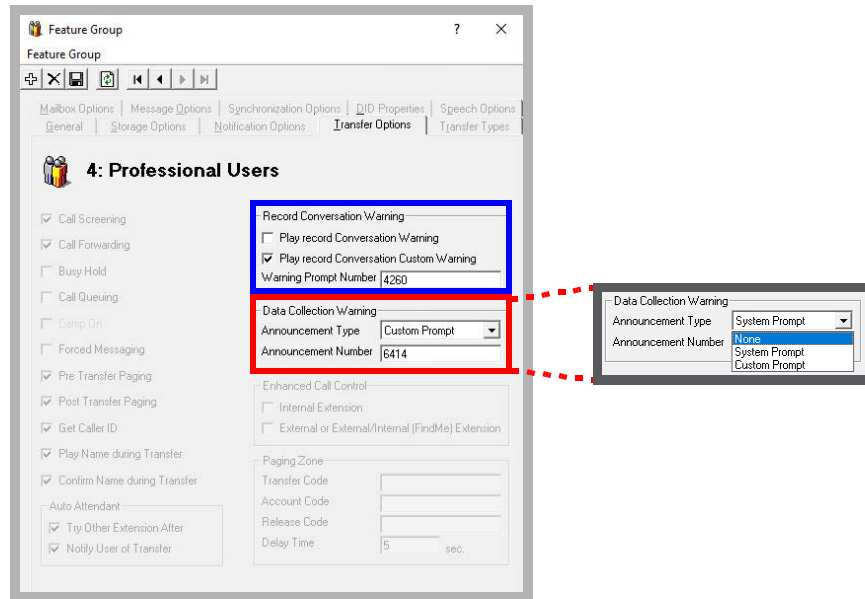
Greeting).

Recording a Custom Greeting

Custom greetings are recorded using a desktop telephone.

1. On a desktop telephone, connect to the system and navigate to the **Record Custom Greeting** prompt in your telephone menus.

    How to reach this menu item depends upon how your **Telephone User Interface (TUI)** is configured. If necessary, add the **Record Custom Greeting** item to one of the telephone menus.
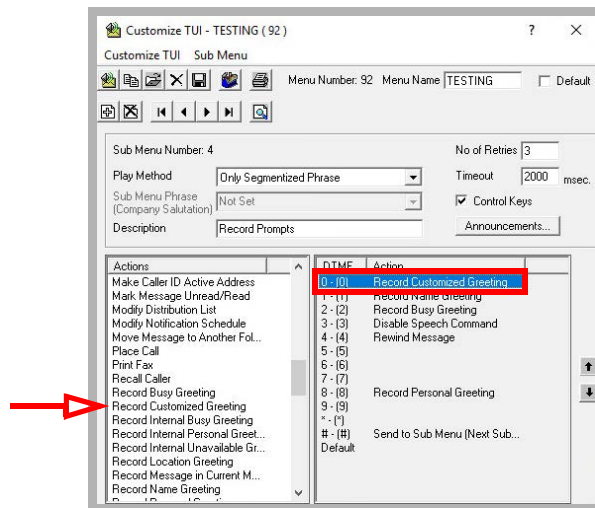
2. When prompted, enter a 4-digit number to identify the file. The recording will be stored in the voice server **Prompts** folder with the format **SALnnnn.vox** where nnnn is the number you entered.
Copy this file into the **\UC\Prompts\Company\1** folder if it is not there already.
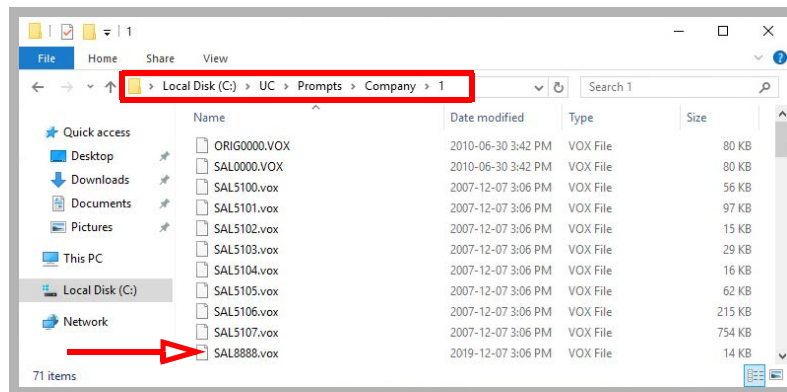
Note: The number 1 used in this example is the company number. If your site hosts more than one company on a single voice server, then enter the appropriate number for that company instead.

Important: Make sure that the number you assign to the custom prompt is unique. It must not be the same as any other prompt or the original prompt will be overwritten by the new one.

This 4-digit number is used when configuring the prompt to play when a recording a meeting, or when a caller chooses to leave a message in a voice mailbox.
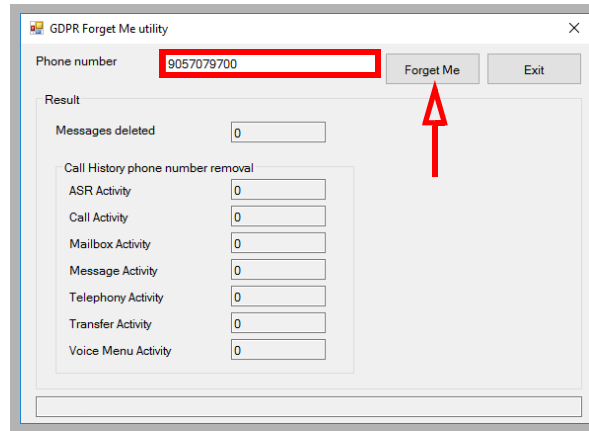
Removing a Caller's Details from the Database

To remove a caller's collected information from the database, run the ForgetMe tool found in the UC directory.

1. In the install directory for Avaya Messaging, open the **UC > GDPR > ForgetMe** folder.
Run (double-click) the **ForgetMe.exe** application.
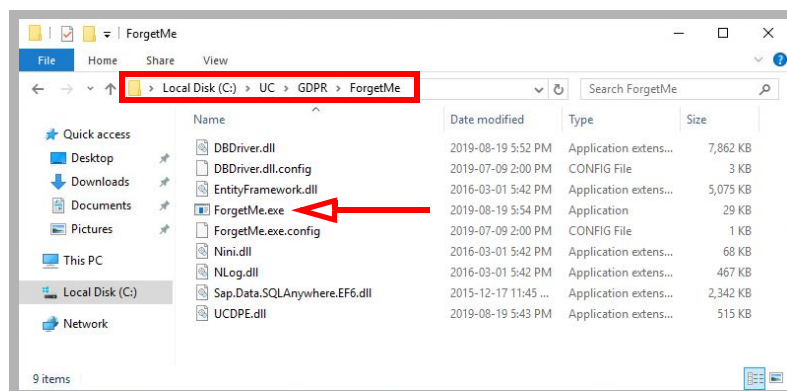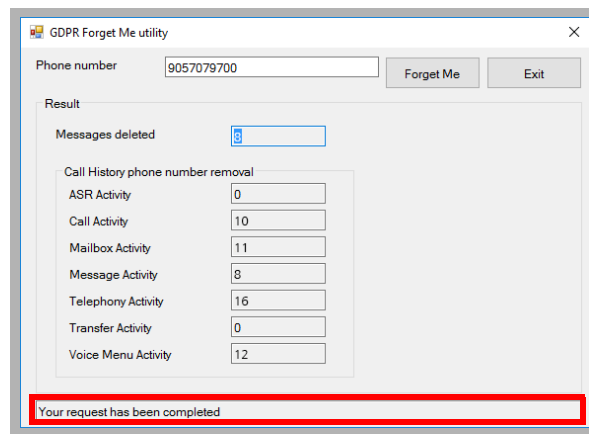
2. Enter the telephone number of the caller to be removed from the database, then click **Forget Me**.

3. The utility will remove all references from the database associated with that number. The entries removed are tallied and displayed in the appropriate spaces on the screen.

4. Enter another number to delete, or click **Exit** when finished.

2 EXISTING & UPGRADED FEATURES

Miscellaneous Changes

- Fax Jobs functions are now available in Web Admin (logs for sent, sending, and failed fax transmissions).
- Reports support Date and Time Range.
- SSO integration with Accounts.zang.io for secure Single Sign On (SSO Hybrid).
- The "Master" server in HA installations has been renamed the "Primary" server.

- Softfax support has been discontinued.

3

CLIENT TYPE CHARACTERISTICS AND DEPLOYMENT SCENARIOS

In This Chapter:

Desktop Capabilities - Types

Messaging can be purchased in several varieties. Options and Add-Ons can be included to extend its capabilities.

Licensing Levels

Basic

Advanced

Messaging Versions

All Messaging versions (Advanced and Basic) are available per user on an **annual subscription** or a **perpetual** basis. Annual subscription licensing includes software assurance for the duration of the license. Per user perpetual licensing includes 1 year of software assurance. Annual software assurance renewal is required for license updates and support entitlement.

> **Note**: A minimum of **50 users**, in any combination, must be purchased with the initial license.

> **Caution**: One site cannot combine both an Messaging Subscription license and an Messaging Perpetual license.

Avaya Messaging Advanced

Messaging Advanced is a comprehensive unified communications and collaboration platform. Messaging offers next generation cloud-enabled communication features that improve collaboration and boost productivity, including Unified Messaging with voicemail, Real-time communication applications like voice and instant messaging and voice conferencing.

Avaya Messaging Basic

AdvancedBasic provides Voicemail integration.

Program Options

Options can be applied to any version of Messaging, and must be purchased **annually** for each user.

Transcription

Voicemail is transcribed into text and delivered to the client's email inbox.

ASR (Automatic Speech Recognition) & Text-to-Speech

Provides voice access and navigation of email, contacts and the calendar. Initiate calls, hear and respond to email and send messages using voice commands instead of the keyboard. Call in and have the system read your emails to you.

Fax Option

eFax services require UM or Collaboration for Google Apps licenses (included with Collaboration Pro).

Add-Ons

Add-Ons are **one time costs** and are not subject to annual subscription fees or renewal costs.

- Per Port License for G.729 (quantity must be equal to voice ports and SIP must be enabled).
- SR140 Fax board support.
- JITC (Joint Interoperability Test Command) compliance for high security environments.
- Integration with Avaya Symposium.

Feature Comparison

The following table demonstrates the different types of license and the features available to each:

Features	User Type	ADVANCED	BASIC
Web config. Access (Mailbox Administration)	●	●
Mobility	●	
All clients - Phone, email, PC Mobile, Web		
Access to Contacts	●	
Web client specific		
Access to Availability filters	●	
Access to Find Me	●	
Access to Assign calls	●	
Access to Locations Calendars	●	●
Phone specific		
Enhanced Call Control	●	
Find Me (Sequential)	●	
Find Me (Broadcast)	●	
Follow Me (One number per location)	●	●
Speech Commands	Optional	
Speech access to public contacts	Optional	Optional
Speech access to private contacts	Optional	Optional
SMS	●	
Remote Notification	●	
Message Forwarding	●	●
Distribution Lists	●	●
iLink Pro Desktop options	●	
Screen POPS	●	
PIM integration	●	
Instant messaging	●	
Presence management	●	
Access to visual directory & buddy list	●	
Desktop Dialing with IP dialer	●	
Call Log window	●	
Desktop SMS (ability to send to SMS)	●	
Synchronized contacts	●	
Synchronized calendar	●	
Inbox Access		
Web client		
Administration	●	●
Access to Inbox	●	●
Access to internal messages	●	●
Access to e-mail messages	●	
Access to voice & Fax messages	●	●
Phone Access		

Features	User Type	ADVANCED	BASIC
Access to VM from Phone	●	●
Access to fax messages from phone	●	●
Access to email messages from phone	●	
Synchronization mode		
Groupware Forms	●	
Sync voice messages to users' email inbox	●	
Contacts	●	
Outbound Desktop Faxing Capabilities (ODFC)	●	
Use eMail to send Fax	●	
Other Features		
Transcription[1]	●	
Send URL (WebLink)	●	
Collaboration		
Presence	●	
Instant messaging	●	
Click-to-call	●	
Voice communication	●	
Geo-location sharing	●	
Screen pops and call logging	●	
Call control	●	
Unified Messaging with Voicemail		
Voicemail	●	
Auto-attendant	●	●
IVR Trees	●	
Unified Messaging	●	
Message Synchronization (MWI)	●	
Call History	●	
Voicemail to contact resolution	●	
Integration with contacts for dialing and replies	●	
Fax		
Fax message access from the inbox	●	●
Fax messaging (Inbound)	●	●
Fax on demand	●	
Application Integration		
Google Apps	●	
Salesforce CRM	●	
Jive	●	
WebEx	●	
Office 365	●	
Avaya Aura Contact Center integration (Meridian IVR and ACCESS caller applications) with M1/CS1000	●	
Clients		
iLink Mobile	●	
iLink Desktop	●	

Features | User Type	ADVANCED	BASIC
Desktop UM client for Outlook, Groupwise	Outlook only	
Web Access - message, manage greetings, user settings	●	
Add-on Applications		
eFax	Optional	
IVR connector	Optional	
Speech-to-text transcription	Optional	
Text-to-speech	Optional	
Automatic speech recognition	Optional	

[1] Transcription requires separate licenses be activated, which is distinct from the user type requirements.

Product Support Requirements

Product Support recommends the following to ensure successful and responsive assistance with regard to any field issues. All systems must be configured for Remotely Accessed support.

The Messaging Server is accessible via an Internet connection. This will enable Avaya's Product Support team to initiate a WebEx session with the administrator of the Messaging Voice Server. This is a low-impact and very powerful tool for remote trouble-shooting.

Prior to loading third-party applications on the system it is strongly advised that a phone call be placed to Product Support to validate that there are no potential conflicts. Examples of third- party applications may include antivirus and backup software applications.

> **Note**: To avoid unnecessary technical support charges, refer first to the product documentation. The Avaya Messaging documentation suite can be found on the Installation DVD or through the documentation website at **resources.zang.io**.

> **Note**: To access technical support you must be a certified technician with a valid PIN number and the site must have an active warranty maintenance contract.

Minimum Client Hardware Specifications

A client workstation should at least meet the following minimum hardware specifications:

- Multimedia PC (sound card + speakers for multimedia playback)

Note: These specifications should be adjusted accordingly depending on other applications that may be running alongside end user Avaya Messaging applications.

Note: For all Windows 2012, 2016 and 2019 installations, disable the User Access Control (**UAC**) feature of Windows to ensure proper operation of the software. Refer to the Server Install Guide for more details.

When utilizing the plug-ins for iLink Pro Desktop (e.g. Outlook Plug-in) please keep in mind that the client machine will have to simultaneously run both the iLink Pro Desktop and the software that the plug-in is integrating with. When looking at the Outlook Plug-in as an example, Microsoft requires minimum of 256MB of ram for the Microsoft Office Suite 2008 and the requirement increases depending on the features that the user employs from the suite. This means that Microsoft's requirements must be added to the iLink Pro Desktop's requirements in order for them to function properly. Please consider exactly how the user will utilize iLink Pro Desktop when deploying the software to client machines.

Like most applications iLink Pro Desktop only uses resources when necessary. When the user has the iLink Pro Desktop window minimized, it will require less resources. When the iLink Pro Desktop is opened, and the user has numerous windows opened (e.g. Chat window, Call Control window, Directory window, etc.), the application will use more resources. So when you are deploying the application to a client machine, please consider the user's habits and general usage estimates as well. When you consider the responsiveness and speed of the application, users that require heavy usage will need additional hardware resources to experience the same level of performance as light users.

Since iLink Pro Desktop requires an Internet and/or network connection to communicate with the Messaging server, having no or very low network resources available on the client machine may prevent proper operation. While iLink Pro Desktop does not require significant amount of network resources, if another application is using up all or most of the resources, iLink Pro Desktop may fail to communicate with the Messaging server when called upon.

Client Deployment Scenarios

> **Note**: All users who wish to utilize Web Client along with iLink Pro Desktop must also have a compatible web browser installed. Please refer to the Web Client requirements section for detailed information.

Deployment Scenario 1 - Basic iLink Pro Desktop Usage

If the user only requires core functionality of iLink Pro Desktop (e.g. Chat, Call Control) and no additional plug-ins, the following setup will prove to be sufficient.

> **Note**: Deployment Scenarios assume that the user's computer does not run any other resource intensive software while utilizing iLink Pro Desktop unless mentioned specifically within the scenario.

The user should not experience any significant delays while using their computer. All notification, messages and windows should appear almost instantly under these conditions. Basic applications such as web browsers may be used without significant effect on performance, which means that Web Client can be loaded without any difficulties.

Scenario 2 - Integrated iLink Pro Desktop with Outlook

If the user requires core functionality of iLink Pro Desktop (e.g. Chat, Call Control) along with Microsoft Outlook plug-ins, the following setup will prove to be sufficient.

> **Note**: The RAM requirement for Microsoft Office Suite varies greatly depending on the user's needs. If the user is only using Outlook from the entire suite, only 256MB of extra RAM is required in addition to it's own requirements.

> **Note**: Deployment Scenarios assume that the user's computer does not run any other resource intensive software while utilizing iLink Pro Desktop, unless mentioned specifically within the scenario.

The user should not experience any significant delays while using their computer. All notification, messages and windows should appear almost instantly under these conditions. Basic applications such as web browsers may be used without significant effect on performance, which means that Web Client can be loaded without any difficulties.

Since the Outlook tool bar contains all the major features of , the user may have the iLink Pro Desktop window minimized for better desktop management. However, minimizing will not reduce the resources that iLink Pro Desktop uses since the Outlook plug-in will always be active in its place. This ensures proper response time of the software at all times by eliminating the need for the application to reallocate the resources that it requires every time it becomes active.

4 SYSTEM REQUIREMENTS AND CAPACITY

In This Chapter:

General Requirements

Maximum System Capacity

Feature	Capacity
Company Directory	80,000 entries [1] [3]
Voice Mailboxes	80,000 - High Availability Server [1] [2] [3] 4,800 - Single Server
Messaging Users	20,000 - High Availability [2] 1,000 - Single Server
Voice Channels	48 ports - SIP with Iwatsu ECS 120 ports - SIP integration, per voice server 2,400 ports - High Availability Environment
Text to Speech Ports	64 ports per server
Automatic Speech Recognition	64 ports per server
Extension Dialing	Unlimited
Number of Tenants	999

1 See the table below for details on calculating this value.

2 The Distributed Server model moves IMAP CSE functions to a separate server from the primary voice server.

3 This is 80,000 users in total, with **up to** 20,000 of those being Advanced users.

Note: Additional licensing may be required to access all program features.

Note: Avaya IX Messaging is a dedicated application which should only be installed as a primary application on any server. Sharing system resources with other applications may reduce the performance.

Hint: For optimal **UC Mobile** performance, it is recommended that the maximum number of users within a single Organizational Unit (OU) be kept below 500.

Bandwidth Requirements

The network bandwidth required to properly support Avaya IX Messaging is dependent upon the number of channels installed onto the system. As a guide, every channel needs 15 kbps bandwidth for inbound, and another 15 kbps for outbound traffic.

# Channels	Recommended Total Bandwidth (incoming + outgoing)
10	300 kbps
20	600 kbps
50	1,500 kbps
100	3 Mbps
2,000	60 Mbps

Maximum Processing Capacity

Messaging can successfully process up to **4000 messages per minute** (combined email and voice) without loss of data, regardless of the number of users. This includes messages left on and retrieved from the system. Traffic loads in excess of this value may result in some loss of information or a decrease in performance.

Storage Capacity

The maximum storage capacity for the system is not a function of the software, but a limitation on the hard drive space available. Be sure to allot sufficient space to handle the expected voice and email traffic for all users, as well as the average time each message is kept on the system before being deleted.

Hard Drives

Avaya IX Messaging must be installed onto servers with a system with a RAID 10 array. Database performance is tied to hard disk performance. RAID 10 provides the same or faster read/write speeds when compared to a single hard disk.

Requirements for High Availability Installations

In addition to all of the normal specifications, High Availability installations have several other requirements that must be met:

- All servers must be in the same local area network.
- All servers must have a minimum 1 GB/s connection to the network.
- The maximum round-trip latency between the servers must be no more than 10 ms.
- The maximum round-trip latency between the voice servers and the PBX must not exceed 200 ms. Optimal round-trip latency is less than 150 ms.
- The path of connectivity must have 20 MB/s guaranteed bandwidth with no steady-state congestion.

Language Support

The languages supported by Messaging in Release 10.8 are:

Chinese (CN, Mandarin)	French	Portuguese BR
Chinese (HK, Cantonese)	French EU	Russian
Chinese (TW, Traditional)	German	Spanish
Dutch	Italian	Spanish EU
English	Japanese	Thai
English UK	Korean	
English AU		
English NZ		

One language is included with the program license, with the files for standard English included with the installation package. Other languages (see the table above) are available for download from Avaya.

Language licenses are not specific to a language. Multiple concurrent languages can be enabled by purchasing additional languages for the license.

All documentation is available in English only.

Pre-Installation Considerations

Avaya IX Messaging uses a dedicated server to enable high performance operation of the program. Other applications running on the same server as Messaging can severely reduce the capacity of the voice server. Processing voice, messaging, presence and telephony data requires a dedicated system if it is to operate quickly and efficiently.

Before installing Avaya IX Messaging, you must have:

- the corporate telephone system and PBX installed and functioning properly.
- the voice server computer operating system installed and fully patched.
- a connection between the voice server to the corporate network and to the Internet.
- all email clients setup and operating according to specifications.
- created all accounts on any cloud-based applications where necessary (i.e. Google Apps).

Caution: Avaya IX Messaging has only been validated on Windows in English and in French. Other varieties of Windows may not work as intended.

Some additional items to consider before installing the voice server:

- How many users will there be in each category - voice / email / fax?
- The expected number of messages of each type per day.
- The number of corporate sites / office locations that are being serviced.
- On-premise versus off-site / mobile traffic.
- Integration with email clients and cloud applications.
- Disaster recovery and redundancy planning.
- The impact of the voice server on network traffic loads and Internet traffic.
- How will Messaging affect any integrated 3rd party and cloud based applications? Email servers?
- What additional software drivers will be required? (i.e. MS Word)

Estimating the Maximum Numbers of Users

Voice Users

Based upon testing by Avaya, Messaging supports up to **80,000**[1] users (see the table below for test criteria). Adding users above this value could impact performance, and may lead to loss of data.

CALCULATING AVAYA IX MESSAGING LIMITATIONS FOR VOICE TRAFFIC

Total Number of Mailboxes Supported based upon Performance Testing = 80,000[1]

Assumptions	
% Heavy Users	5%
% Medium Users	30%
% Light Users	65%
# Daily Voice Messages for Heavy Users	15
# Daily Voice Messages for Medium Users	5
# Daily Voice Messages for Light Users	1
Average Message Length (sec)	40
Average Call Length (sec)	60
Number of Channels	2,400
Operating Hours per Day	13

Test Results	
Total Voice Messages per Day	232,000
Total Calls per Day[2]	464,000
Total Call Minutes per Day	464,000

1 This is 80,000 users in total, with **up to** 20,000 of those being Advanced users.

2 Each message is left on the system by the caller, then retrieved by the callee, requiring 2 calls to complete the messaging process.

Legacy Licensing (Esna)

This section applies to customers with existing licenses issued by Esna. For Officlinx / IX Messaging licenses purchased through Avaya, please refer to the WebLM Licensing (Avaya) section on page 46.

Soft License

Avaya IX Messaging program authorization is managed through a "soft" license. Activation of the program (UC, UM, eFax, etc.), capacity (ports and mailboxes) and features (ASR, TTS) requires an Internet connection. Messaging uses this connection to periodically contact the Avaya license server to enable continued use of the program at the appropriate service level. If the connection to the Internet is lost for a long enough period, then the software will fall into Demo Mode until the connection is re-established. Renewing a license, upgrading or adding new features can be completed with a telephone call to customer service and a refreshing of the license.

Initial Installation

During the initial installation, the administrator will enter the Serial Number and Site ID information included with the installation package. These numbers are unique for each site. The program will also generate a hardware profile of the server computer which becomes a part of the license.

After the initial installation, if the server hardware changes (i.e. the program has been moved to a new server), Messaging will again require an on-line activation with the Site ID and Serial Number to rebuild the license file. This is only permitted once by the software, and subsequent hardware changes will cause the program to immediately revert to Demo Mode. Contact customer service to reactivate the license in this case.

Normal Operation

Once Messaging has been installed and is operating, the program will contact the Avaya license server each day through the Internet for authentication. In the case of a connection failure or other errors that prevent authorization, the program will continue to operate properly for 28 days. If the problems are not corrected and the connection re-established before then, the program will revert to Demo Mode. When errors with authentication do occur, the administrator will receive notifications from Messaging with details of the problem.

If the program detects that the license details are different between the Messaging and license servers, and no updates have been included, the system will immediately revert to Demo Mode until the issue can be resolved.

In the case where 2 computers are associated with the same license, only the first machine to be authenticated will receive the license. The second machine must wait up to 24 hours for authorization, and only if the first machine has relinquished the license.

License Upgrades

To upgrade the Messaging license, such as adding new features or adding more ports or mailboxes, contact your customer service representative. The new details are added to the license server and an email is sent to the administrator with a reminder to refresh the license. The next time that the program contacts the license server for authentication, it will see that the licenses do not match due to the upgrade, and it will prompt the administrator to refresh the license.

To activate the upgrades, run the license activation wizard (UCLicenseUpgrade.exe), verify the updated terms for the license, and click the "Set as Active License" button.

Until the license has been updated, Messaging will continue to operate at its previous levels for another 28 days, then it will revert to Demo Mode if it has still not been refreshed.

License Expiration

Term based licenses last for a specific length of time. As the program nears its termination date, it will begin sending the administrator email reminders that the license is due to expire soon. These messages are sent at 90 days, 60 days, and 30 days prior to expiration. For the last 15 days, notifications will be sent out daily. If the license has not been renewed by the expiration date, the program will continue to operate, but at only 25% of its former capacity. For example, if there were 100 ports and 100 mailboxes licensed, there will now only be 25 ports and 25 mailboxes available on the system. This reduction lasts for 60 days, with reminders sent to the administrator each day, and then Messaging will fall into Demo Mode until a new license is purchased.

The program can be reactivated at any time once a new term has been purchased and the license is refreshed. Please make the necessary arrangements in plenty of time to avoid any disruptions in service.

Offline Verification

For sites that do not permit access to the Internet for security reasons, customers can request an installation that uses Offline License Verification. The licensing information resides upon the voice server computer and does not need to be refreshed each day. This installation comes with a hardware USB dongle/key, and a license file that is copied to the hard drive of the voice server. This file contains the hardware profile and licensed feature information that normally resides on the Avaya license server. Both are required for the program to be authorized.

Any hardware changes or program upgrades require a new license file. These are generated by the customer service department and are sent to the customer. Run the license activation routine again to enable updates.

High Availability Licensing

In a High Availability (HA) installation, only the Primary connects to the license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Primary. Therefore, it is imperative that the Primary Server is the first one installed and operating because the other servers will install only the features appropriate to the license data they receive from the Primary.

Demo Mode

The program can be put into Demo Mode for many reasons, such as the license expiring, or an extended loss of connection to Avaya's license server.

Demo Mode maintains all of the previously licensed features, but operational capacity is reduce to a single port with 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging will continue to run in Demo Mode until the cause for the service reduction has been addressed (i.e. a new license is purchased, and fixing connection problems).

WebLM Licensing (Avaya)

This section applies to current customers that purchased the product through Avaya. For long term customers that purchased Officelinx through Esna, please refer to the Legacy Licensing (Esna) section on page 44.

Soft License

Avaya IX Messaging program authorization is managed through a "soft" license. Activation of the program (UC, UM, eFax, etc.), capacity (ports and mailboxes) and features (ASR, TTS) is controlled by the license which resides on a server on your corporate network. Messaging uses the corporate network to regularly contact the Avaya WebLM license server to enable continued use of the program at the appropriate service level. If the connection to the license server is lost for a long enough period, then the software will fall into Demo Mode until the connection is re-established. Renewing a license, upgrading or adding new features can be completed with a telephone call to customer service and a refreshing of the license.

Host ID and License File

During the initial installation, the administrator must create a Host ID from the WebLM License Server. This number is then sent to Avaya so that a license file can be generated and sent back to the customer. It is this license file that Officelinx / Messaging read to unlock the program features.

Afterwards, if the server hardware changes (i.e. the program has been moved to a new server), the license file must be replaced. Generate a new Host ID from the WebLM server and send that to Avaya Customer Service to receive an updated file.

Normal Operation

Once Messaging has been installed and is operating, the program is in constant contact with the WebLM license server for authentication. In the case of a connection failure or other errors that prevent authorization, the program will continue to operate properly for 28 days. If the problems are not corrected and the connection re-established before then, the program will revert to Demo Mode. When errors with authentication do occur, the administrator will receive notifications from Messaging with details of the problem.

License Upgrades

To upgrade the Messaging license, such as adding new features or adding more ports or mailboxes, contact your customer service representative. The new details will be added to the license file and an email is sent to the administrator for them to refresh the license. You may be required to generate a new Host ID number from the WebLM server.

License Expiration

Term based licenses last for a specific length of time. As the program nears its termination date, it will begin sending the administrator email reminders that the license is due to expire soon. These messages are sent at 90 days, 60 days, and 30 days prior to expiration. For the last 15 days, notifications will be sent daily. If the license has not been renewed by the expiration date, the program will continue to operate, but at only 25% of its former capacity. For example, if there were 100 mailboxes licensed, there will now only 25 mailboxes available on the system. This reduction lasts for 60 days, with reminders sent to the administrator each day, and then Messaging will fall into Demo Mode until a new license is purchased.

The program can be reactivated at any time once a new term has been purchased and the license file is refreshed. Please make the necessary arrangements in plenty of time to avoid any disruptions in service.

High Availability Licensing

In a High Availability (HA) installation, only the Primary voice server connects to the WebLM license server. The Consolidated Server, and all Secondary Servers, get their licensing information from the Primary. Therefore, it is imperative that the Primary Server is the first one installed and operating because the other servers will install only the features appropriate to the license data they receive from the Primary.

Demo Mode

The program can be put into Demo Mode for many reasons, such as the license expiring, or an extended loss of connection to the license server.

Demo Mode maintains all of the previously licensed features, but operational capacity is reduce to 10 mailboxes. No data or settings are lost from the mailboxes, but there will be problems with access.

Messaging will continue to run in Demo Mode until the cause for the service reduction has been addressed (i.e. a new license is purchased, and fixing connection problems).

License Expiration Milestones

These benchmarks apply to all licenses (legacy and WebLM).

Time Before Expiration	Action Taken
+90 days	eMail Administrator
+60 days	eMail Administrator
+30 days	eMail Administrator
+15 days to 0 days	daily eMails to Administrator
License Expires	
Demo Mode	

Licensing Grace Periods and Actions

Condition	Grace Period	Action Taken after Grace Period
Failure to authenticate license	28 days	Demo Mode
Upgraded license not activated	28 days	Demo Mode
1st Hardware change	-	Refresh license to continue
2nd Hardware change	-	Demo Mode
License Mismatch (not an upgrade)	-	Demo Mode

Network Requirements and Specifications

Avaya IX Messaging can exist as a standalone server on a local area network which allows for network-based user and system administration.

For proper deployment, connect the Messaging server through the NIC interface and then boot up the server. A 1GB/s or better connection is recommended, but 100 kbps is acceptable.

Warning: There can be a maximum of **2** network cards installed in a single server computer.

Note: The Messaging server must be provided with sufficient administrative rights to the network so it can co-exist as another workstation on your local area network. For more information contact your LAN Administrator.

The following is an example of how Messaging can be configured within an organization's network. By having a network infrastructure as shown here, you can ensure the functionality of the Messaging server within the organization while protecting all assets through the necessary security measures (e.g. firewall) from Internet or other external connections.
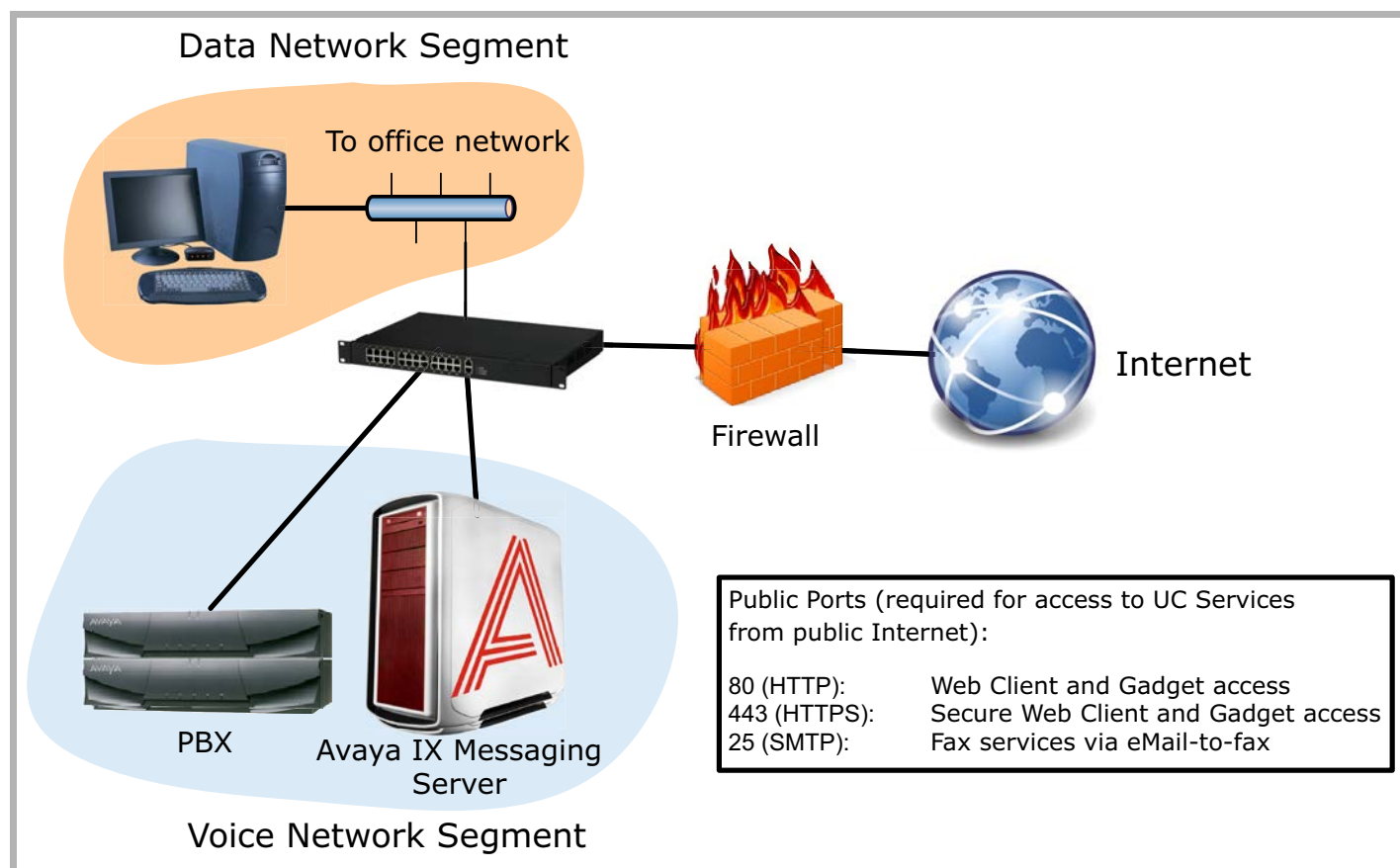
Before adding Messaging, you must have on of the following operating systems installed and fully patched:

- Windows Server 2012 or 2012 R2 - Standard Edition
- Windows Server 2016
- Windows Server 2019

Caution: The MAC operating systems is NOT supported for the voice server.

Note: It is recommended that the operating system be installed on a partition with at least 100 GB of space. This is in addition to any space requirements set aside for Avaya IX Messaging.

Note: Disable the User Access Control (**UAC**) feature of Windows to ensure proper operation of the software. Refer to the Server Install Guide for more details.

TCP/IP ports used by the application

PORT #	SERVER / CLIENT APPLICATION	SERVICE	DIRECTION	TCP/IP	UDP	SINGLE SERVER	PRIMARY SERVER	SECONDARY SERVER (S)	CONSOLIDATED SERVER	CSE SERVER	REQUIRED
25	VPIM-Smart Host Supported	Used for VM networking	Out	SMTP		●	●	●	●		1
80	Web Access		In	HTTP		●	●	●	●		●
135 *	MAPI/RPC	Contact and Calendar Synchronization	Both	MAPI/RPC		●					
389	LDAP Connector	AD Synch	Both	LDAP		●			●		2
443	Web Access	IIS Secure Services	In			●			●		●
443	Access to OEM Avaya	License Service	In	HTTPS		●	●				●
445	Microsoft File Sharing	File Sharing	Both	TCP			●	●	●	●	●
2439	Sybase Mobilink	Database Connection	Both	TCP			●	●	●		●
2638	IXM Admin Sybase	MMC Service	Both	TCP		●			●	●	●
5060	SIP Channels	Voice Application	Both	SIP	UDP 3	●	●	●			●
5061	SIP Channels	Voice Application	Both	SIP	TLS						
8201	UC Nuance Loader - Speech	Server/Client ASR	Both	TCP	UDP	●	●	●			●
10008 4	AACC	Call Center Integration	Both	TCP		●	●				
11000	UM Monitor	Local App Services	Both	TCP	UDP	●	●	●			●
12000	WebLM	License Service	Both	TCP		●	●				
13777	iLink Pro Desktop	UC Mobile	Both	TCP		●			●		●
13780	ASR Distributed	Speech Service	Both	TCP	UDP	●	●	●			●
13888	CTIClient Manager	UC CTI manager	Both	TCP	UDP	●	●	●	●		●
20002-x	RTP Media	Voice Application	Both		UDP	●	●	●			●
52233	WebLM	License Service	Both	TCP		●	●				
†	Nuance Speech Suite	Nuance Watcher Daemon	Both	TCP	UDP	●	●	●			

1 - Only required for sending messages via SMTP.

2 - Only required for LDAP synchronization.

3 - Only required for SIP with a Dialogic Media Gateway.

4 - Only required for Call Center integration with AACC environments.

* - Calendar and Contact Synchronization use MAPI, which uses RPC (Remote Procedure Call). RPC port assignment is handled dynamically, with port 135 used to locate the correct port. Both 135 and the MAPI / RPC ports must be open.

† - These port numbers are automatically assigned by the operating system. All associated traffic is local and no firewall adjustments are required.

For more information, click here: **http://technet.microsoft.com/en-us/library/cc875824.aspx**

Software Requirements

Minimum software requirements to run the Avaya IX Messaging server:

Software	Version
OS	Windows Server 2012 R2 - Standard Edition Windows Server 2016 Windows Server 2019
ASR	Nuance 10
TTS	RealSpeak 4.0 or 4.5

Media Support Requirements

If you wish to utilize additional media support within the voice server (e.g. DOC or DOCX support for fax), you must install the necessary components on the server so that the file formats can be recognized. Please refer to the chart below for requirement examples.

File Format	Application Required	Comments
DOC, DOCX	Microsoft Office	Required for additional file format support.

Note: The Remote Printer feature of Avaya IX Messaging can be used to redirect printer/fax traffic to another computer that already has the necessary licenses installed. Please refer to chapter 18 of the Feature Guide.

Note: Avaya IX Messaging versions prior to 8.2 require a separate application, such as Windows Media Player, to access MP3 files. Starting with version 8.2, Messaging supports MP3 files natively, with no additional software required.

ANTIVIRUS Software Installation

Avaya IX Messaging has only been validated with Norton Anti-virus Corporate Edition. Other anti-virus software applications that have been installed with Messaging are:

- McAfee VirusScan
- BitDefender

Note: Please ensure that, after installing your antivirus program, the UC folder and all of its subfolders are excluded from the scan. Scanning the UC folder can significantly decrease performance.

Fax Support

Messaging supports the Group 3 (G3) fax protocol, which conforms to the ITU-T specifications for T.30, T.4 and T.6.

Hardware Requirements

This table displays the recommended hardware values for different numbers of users, and the different types (single server, HA) of Avaya IX Messaging installation. Use these values to guide design and scope considerations for a new site.

For all sites:

- All processors are to be 2.0 GHz or better.
- All hard drives must be high performance, server grade drives.
- Configure the CPU for **Performance** mode in each server's BIOS settings.
- Virtual CPU's (vCPU) are shown as hyperthreaded and can be cut in half to equal physical cores.
- The same configurations can be used for both **physical** and **virtual servers**.
- Avaya IX Messaging must be installed onto servers with a RAID 10 array.
- Fragmentation management software, such as **Diskeeper**, should be installed on each server to prevent any drop in performance. This can be scheduled to run primarily during off hours.

SAN Usage

Storage Area Network (SAN) devices can be used with Messaging if they meet the necessary specifications.

- The device must provide a sustained throughput capacity of 250 requests per second, with peak traffic of up to 500 requests per second.
- This traffic is split 20% / 80% for read / write operations respectively.

Table Key

Profile: Use this tag to identify to your vendor which system configuration meets your needs.

 # CPU: The number of cores the server requires to quickly process data. All should be Intel® 2.0 GHz or better. The number of cores can be reached either through physical CPU cores, or by using Hyper-Threading Technology if available.

RAM: The amount of memory that each server must have.

Storage: This is the amount of storage space required for the hard drive where Avaya IX Messaging is installed.

Note: Running **Carbonite Availability** backup software requires additional space on the IXM Drive. Make sure that there is at least twice as much free space on the drive as is occupied by the program's files. For example, if there are 100MB of files, the IXM Drive must be at least 200MB in size. Carbonite needs this space to create the initial swap files before passing the data to the backup server. The specifications for Carbonite servers is the same as for the live voice servers.

Content Synchronization Engine (CSE): This is the server that will perform the sync with Gmail, Office 365, and MS Exchange.

Important: The **operating system** for each server must be on a different partition, or on another hard drive, than Avaya IX Messaging. The drive for the operating system must be **100 GB or greater**.

First Drive / Partition   **100GB+**   Operating System Drive (C:\ )   **+**   Messaging Install   **From the table**   Second Drive / Partition

Recommended Configurations

The listed specifications are for each instance of the application. For example, in an HA environment, a minimum of 3 servers are required (Primary, Consolidated, and 1+ Secondaries). Each server must be appropriately configured.

All systems must use a RAID 10 (RAID 1+0) configuration.

For Standalone Deployment (SA)

SEAT LICENSES	PROFILE	Stand Alone Solution		
		# CPU	RAM (GB)	Storage (GB)
1-1000	SA1	4	8	400
1001-4800	SA2	8	16	400

For High Availability Deployments (HA)

SEAT LICENSES	PROFILE	Primary / Secondary Voice Servers			Consolidated Server		
		# CPU	RAM (GB)	Storage (GB)	# CPU	RAM (GB)	Storage (GB)
1-5000	HA1	8	16	400	8	16	400
5001-10000	HA2	8	16	600	8	16	600
10001-15000	HA3	8	16	700	8	16	700
15001-20000	HA4	8	16	900	8	16	900
20001-40000	HA5	8	32	1100	8	32	1100
40001-60000	HA6	8	32	1800	8	32	1800
60001-80000 [1]	HA7	8	32	2600	8	32	2600

1 - This is 80,000 users in total, with **up to** 20,000 of those being Advanced users performing UM sync.

For Unified Messaging Sync Users (UM)

UM USERS	PROFILE	Each Content Synchronization Engine [2] [3]		
		# CPU	RAM (GB)	Storage (GB) [4]
1-3000 (SA)	N/A	CSE Running on Voice Server		
1-5000 (HA)	N/A	CSE Running on CS [5]		
5001-10000 (HA)	UM1	8	8	600
10001-15000 (HA)	UM2	8	8	700
15001-20000 (HA)	UM3	8	8	900

2 - The number of CSE Servers required depends upon the number of Advanced users that will be working on the system. One server is required for every **5,000 Advanced users**.

3 - Each Remote CSE Server supports a single email type (e.g. Exchange, Office 365, Gmail, etc.). If more than one email type is required, the Consolidated Server cannot be used for synchonization.

4 - Additional hard drive space may be required if full logging is enabled.

5 - For optional Remote CSE Server, use Profile UM1.

Note: Expanding your operation and moving from one profile to a larger one may also require changes to the system hardware (# CPU, RAM, Storage, etc.) needed to support it.

CSE Gateway Requirements

In order to use CSE, the IMAP mail server must support the following standards:

- Messaging integrates with MS Exchange 2010 / 2013, Gmail (Google Apps) and MS Office 365.

- IMAP services enabled on the email server

- IMAP services must be installed and fully operational prior to deploying Messaging with the IMAP Gateway

- MS Exchange 2010 / 2013 should be operational ahead of time if Messaging is desired

- User name and password (with permission) so UC can access user mailboxes on existing mail server

- Free IMAP TCP/IP port available between the Messaging and email server

Server Network Requirements

Networking requirements depend on what configuration and traffic load the system will bear. In most cases 100 Mbps (minimum 100BaseT) will suffice between the Messaging, IMAP CSE and the Email servers. In larger (500+ UC user) configurations a 1 GB/s network connection between the Messaging and Email servers is required. In such cases a 1GB/s layer 2-switch between all servers is also required.

The voice server can exist as a network-connected server on a LAN allowing for network-based user and system administration.

Server Email Integration Requirements

The Server can be a voicemail-only system although most deployments will involve some degree of email functionality.

Refer to **Server Messaging Type Characteristics And Deployment Scenarios on page 99** in this document for more information on the possible system deployment scenarios.

Message Compression and Storage

Depending on which deployment scenario you select, messages may be stored on the Messaging Server, on the Email Server or both.

For more information on deployment scenarios visit Deployment: Basic Unified Messaging on page 101.

It is very important that you know the message storage requirements of your particular environment. The following factors will affect this calculation:

- days to keep read messages

- days to keep unread messages

- message format used

- maximum message length

- maximum number of messages allotted per user (inbox only)

- number of Messaging users (must account for email on the Messaging Server)

The message format is the factor used to calculate storage capacity as the format determines the size of the actual messages.

File Format	KBytes/sec	KBytes/min	KB/hour	MB/hour	GB/hour
Wave A-Law 8kHz (G711)	8	480	28800	28.1	0.0275
Wave μ-Law 8kHz (G711)	8	480	28800	28.1	0.0275

In certain deployments where copies of voicemail messages are stored on the Email Server, storage capacities per email mailbox remain the same.

System Configuration Options

Messaging can be configured to support many user environments:

- Basic (Messaging)
  - Basic + ASR / TTS
  - Basic + Transcription
  - Basic + ASR / TTS + Transcription
- Advanced (Messaging & Collaboration)
  - Advanced + ASR / TTS
  - Advanced + Transcription
  - Advanced + ASR / TTS + Transcription

The following options which can be added to a license:

- SR140 Fax Ports
- ASR / TTS by user
- Transcription by user
- Upgrade the User type to Access Increased Functionality
- G.729 Support

Server Requirement Q & A

Please refer to the below Q&A article for a general understanding of the hardware requirement of the Messaging system.

What is a RAID 10 system?

RAID 10, also known as RAID 1+0 or RAID 0+1, is a RAID system where 2 drives are mirrored and then spanned with 2 other mirrored drives. This gives you the ability to lose 1 of each in the set in each mirror (1/2 of the drives) and still work at full speed. RAID 10 is required for all Avaya IX Messaging servers, physical or virtual.

How about RAID 6 or RAID 5?

RAID 5 and 6 would be an optimal choice if the Messaging system were to be a read only system. Unfortunately the act of writing burdens the RAID system since every log entry requires the entire span to be updated (parity needs to be updated with every change). If a RAID 5 or RAID 6 becomes fragmented there is a problem since small pieces of info will still take the entire stripe and parity needs to be calculated for every change once again.

What speed Hard Drives should we use?

Most typical server Hard Drives will be either 10,000 RPM or 15,000 RPM. Either one will suffice for the Messaging system. The 15,000 RPM drives are much hotter but are also 50% faster. The trade off is the electric consumption over performance. If it is a huge install base that has lots of UM with IP voice ports, we suggest the 15,000 RPM but this is not a requirement.

What can I do to increase the effectiveness of the RAID system?

An extra drive (one or more) may be configured as a hot swap spare. This is generally a good practice since it will automatically start rebuilding the RAID if one of the drives fail, removing the need for human interaction.

What is the total storage of a RAID system?

Total storage would be approximately ½ of the combined storage of all the drives.

Is there a numerical restriction on the RAID system?

The number of drives that can be used in the RAID system must be even, with 4 being the minimum (4, 6, 8 etc).

Can I install Messaging on an existing server that is already in use?

Messaging is a dedicated application which should only be installed as a **primary application** on any server. Sharing system resources with other applications may keep Messaging for working correctly.

5

PBX SPECIFICATIONS

In This Chapter:

Introduction

Avaya Messaging is a vendor neutral application which can integrate with many telephone systems. Use the information in this section as a general guideline to the kinds of integrations Messaging can support, as well as what is required from the phone system in order for specific features to work. While Messaging requires SIP for integration, media gateways provide compatibility for PBXs that use different protocols.

Multiple PBX/Node Support

Avaya Messaging is able to integrate with multiple PBXs or nodes at once, allowing you take advantage of all the capacity a site may have. This will also be a great option for legacy sites which are implementing additional PBX for higher capacity. A site can add new PBX to their legacy system and use them as one through Messaging without having worry about compatibility.

The only requirement for multi-PBX / multi-node support is that the PBX in question is compatible with Avaya Messaging. It is recommended that all PBXs/nodes utilize SIP trunks.

SIP

SIP (Session Initiation Protocol) is a set of rules that provide the basic signals used to initiate, manage, and terminate communications sessions. SIP is an open standard which allows carrier voice equipment to interoperate seamlessly with customer premise equipment. The logical voice channel established between them is a SIP Trunk. A SIP Trunk is a virtual phone line that utilizes the customer's Internet connection for access. Trunks come with unlimited local inbound minutes and long distance usage based at rates far below traditional phone service. SIP Trunking is a business-class telecommunications solution that delivers local, toll-free, domestic and international long distance service.

SIP integration is highly recommended due to reduced costs and universal compatibility. Even most legacy hardware will be able to utilize SIP through a compatible media gateway.

Tested & Verified PBX

SIP Direct

Following PBXs are integrated directly into the voice server through SIP.

Brand	Model
Alcatel	OmniPCX
Asterisk	
Avaya	IP Office 500, 6.1, 7.0, 8.0, Aura CM, Session Manager (SM), SIP Enablement Services (SES)
Broadsoft	Broadworks Release 17
Cisco	Call Manager 4.2.1 Call Manager 5.1 Call Manager 7 Call Manager Express Unified Communication Manager 8.x, 9.0
eOn	Millenium
Inter-tel	Inter-tel 500
Iwatsu*	ECS
Mitel	3300 MCD 4.2
Nortel	CS1000 (v7.5, NRS and SM) CS2000 CS2100 BCM R6
ShoreTel	ShoreGear Platform 11.1
Siemens	OpenScape Voice
Toshiba	CIX

* - Fax detection is not supported through Iwatsu ECS.

SIP Gateway

Following PBXs are integrated through a media gateway to the Messaging server.

Brand	Model
Avaya	IP Office

For specific part numbers of SIP Gateways, please refer to the Dialogic Media Gateway portions of the following sections:

- T1 on page 66
- T1 on page 66
- E1 on page 68

CTI

CTI stands for Computer Telephone Integration. CTI combines data with voice systems in order to enhance telephone services. For example, automatic number identification (ANI) allows a caller's records to be retrieved from the database while the call is forwarded to the appropriate party. An outbound example would be automatic telephone dialing from an address list.

Tested & Verified PBX

CTI Integration: Rich Presence and Call Control

Following PBXs are integrated directly into the voice server through CTI.

Brand	Model
Avaya	ACE 6.2 CM 5.2, 6.1 (AES TSAPI) IP Office 500, 6.1, 7.0, 8.0 (TAPI)
Cisco	Unified Communication Manager 8.x, 9.0 (TAPI)
Iwatsu	ECS
Mitel	MCD 4.2

Inband

Inband integration is possible on supported switches through the use of Dual Tone Multiple Frequency (DTMF) signalling. Strings of DTMF tones are transmitted on the analog voice channel after the channel connects to answer the call but before the voice is cut through.

Typically the string contains the Calling Line Identification, the Called Party Identification, reason for the call (re-direction or direct call), and will allow the following functionality among others:

- Direct Log-In in which Messaging recognizes a direct station call, identifies the internal caller's extension number and prompts the caller to enter the security code of the subscriber mailbox associated with that number.

- Call Forwarding to a personal greeting if an extension is Busy, not answered, Do Not Disturb or Forward All. Both internal and external callers can be forwarded to the subscriber's personal greeting. Depending on how the subscriber's mailbox is configured and what information is provided by the telephone system an appropriate greeting can be played for both a Busy and a Ring No Answer condition. Callers can then leave messages in the subscriber's mailbox or be presented with another list of options through voice menus.

- Call Routing based on the trunk number, DNIS number or forwarded PBX extension number. These types of calls can be routed to a specific mailboxes, ACD agent or call center. The time frame (when the voicemail is waiting for signaling) is configurable so that it can be adjusted regardless of the PBX.

T1

SUPPORTED PROTOCOLS

Robbed Bit Signaling

Channel Associated Signaling (CAS), also referred to as Robbed Bit Signaling, is a method of signaling each traffic channel rather than having a dedicated signaling channel (like ISDN). In other words, the signaling for a particular traffic circuit is permanently associated with that circuit.

The most common forms of CAS signaling are loopstart, groundstart, Equal Access North American (EANA) and E&M. The biggest disadvantage of CAS signaling is its use of user bandwidth to perform signaling functions. In addition to receiving and placing calls, CAS signaling also processes the receipt of Dialed Number Identification Service (DNIS) and automatic number identification (ANI) information which is used to support authentication and other functions.

Each T1 channel carries a sequence of frames. These frames consist of 192 bits and an additional bit designated as the framing bit, for a total of 193 bits per frame. Super Frame (SF) groups 12 of these 193 bit frames together and designates the framing bits of the even numbered frames as signalling bits. CAS looks specifically at every sixth frame for the timeslot's or channel's associated signaling information. These bits are commonly referred to as A- and B-bits. Extended super frame (ESF), due to grouping the frames in sets of twenty-four, has four signaling bits per channel or timeslot. These occur in frames 6, 12, 18, and 24 and are called the A-, B-, C-, and D-bits respectively.

ISDN Signaling Concepts

The Integrated Services Digital Network (ISDN) is a digital communications network capable of carrying all forms (voice, computer and facsimile) of digitized data between switched end points. This network is a digital-switched system that makes a connection only when requested.

Control over switched connections is provided by a protocol of messages that pass between the two ends of the digital link. Any type of equipment can be connected to an ISDN provided the equipment is capable of generating a digital bit stream that conforms to ISDN standards.

ISDN technology offers the benefits inherent in digital connectivity such as fast connection (setup and tear down), fast Direct Dialing In service (DDI) and fast Automatic Number Identification (ANI) acquisition.

ISDN protocols use an out-of-band signaling method carrying signaling data on a channel or channels separate from user data channels. This means that one signaling channel (D channel) carries signaling data for more than one bearer channel (B channel). This signaling technique is referred to as common channel signaling (CCS). Signaling data carries information such as the current state of the channel (for example, whether the telephone is on-hook or off-hook). Common channel signaling allows the transmission of additional information, such as ANI and DNIS digits, over the signaling channel.

An ISDN Primary Rate Interface (PRI) trunk provides a digital link that carries some number of TDM (Time Division Multiplexed) channels:

- a T-1 trunk carries 24 64 Kbit channels, 23 voice/data channels (B channels) and one signaling channel (D channel) on a single 1.544 MHz digital link

- an E-1 trunk carries 32 64 Kbit channels, 30 voice/data channels and two additional channels: one signaling channel (D channel) and one framing channel to handle synchronization on a single 2.048 MHz digital link.

The ISDN digital data stream contains two kinds of information: user data and signaling data used to control the communication process. For example, in telephony applications user data is digitally encoded voice data. Voice data from each time slot is routed to a separate B channel. Signaling data carries information such as the current state of the channel (for example, whether the telephone is on-hook or off-hook). The signaling information for all B channel information is routed to the D channel of the device.

Dialogic Media Gateway

SIP

The Dialogic® 2000 Media Gateway Series is a turnkey appliance that seamlessly merges traditional PSTN technology with IP networks. This economical gateway helps consolidate typically separate voice and data networks and provides new and differentiated communications services. Without making radical, disruptive, and expensive upgrades to existing PBX equipment, service providers and enterprises can realize the benefits of a converged voice and data network.

Dialogic Media Gateway Part Numbers for T1	
DMG2030DTIQ	Single T1 Integration Gateway
DMG2060DTIQ	Dual T1 Integration Gateway
DMG2120DTIQ	Quad T1 Integration Gateway

Note: For detailed information regarding Dialogic Media Gateway, please refer to:
http://www.dialogic.com/products/gateways/DMG2000.htm

For integration notes regarding Dialogic Media Gateway, or to check your current hardware for compatibility, please refer to:
http://www.dialogic.com/support/helpweb/mg/iw1904.aspx

E1

QSIG is the European association for Standardising Information And Communication Systems. QSIG has a long history of producing standards related to the interworking of communications equipment within Private Integrated Services Networks (PISNs). PISN standardisation is undertaken by the various task groups of its technical committee: TC32. Much of their effort is put towards the definition of the intraPISN signalling system commonly referred to as "QSIG".

QSIG is an ISDN based protocol for signalling between nodes of a Private Integrated Services Network (PISN)

Dialogic Media Gateway

SIP

The Dialogic® 2000 Media Gateway Series is a turnkey appliance that seamlessly merges traditional PSTN technology with IP networks. This economical gateway helps consolidate typically separate voice and data networks and provides new and differentiated communications services. Without making radical, disruptive, and expensive upgrades to existing PBX equipment, service providers and enterprises can realize the benefits of a converged voice and data network.

Dialogic Media Gateway Part Numbers for E1	
DMG2030DTIQ	Single E1 Integration Gateway
DMG2060DTIQ	Dual E1 Integration Gateway
DMG2120DTIQ	Quad E1 Integration Gateway

Note: For detailed information regarding Dialogic Media Gateway, please refer to:
http://www.dialogic.com/products/gateways/DMG2000.htm

For integration notes regarding Dialogic Media Gateway, or to check your current hardware for compatibility, please refer to:
http://www.dialogic.com/support/helpweb/mg/iw1904.aspx

6

HIGH AVAILABILITY ENVIRONMENT

In This Chapter:

High Availability Description

Vulnerability of the Single Server System

The High Availability system is designed to deliver a redundancy solution to environments where uptime is critical. The HA system achieves redundancy through Secondary servers that are constantly online along with the Primary server. In a traditional single server environment as shown below, the system is vulnerable to downtime which can be caused by the malfunction of the single Voice Server computer.
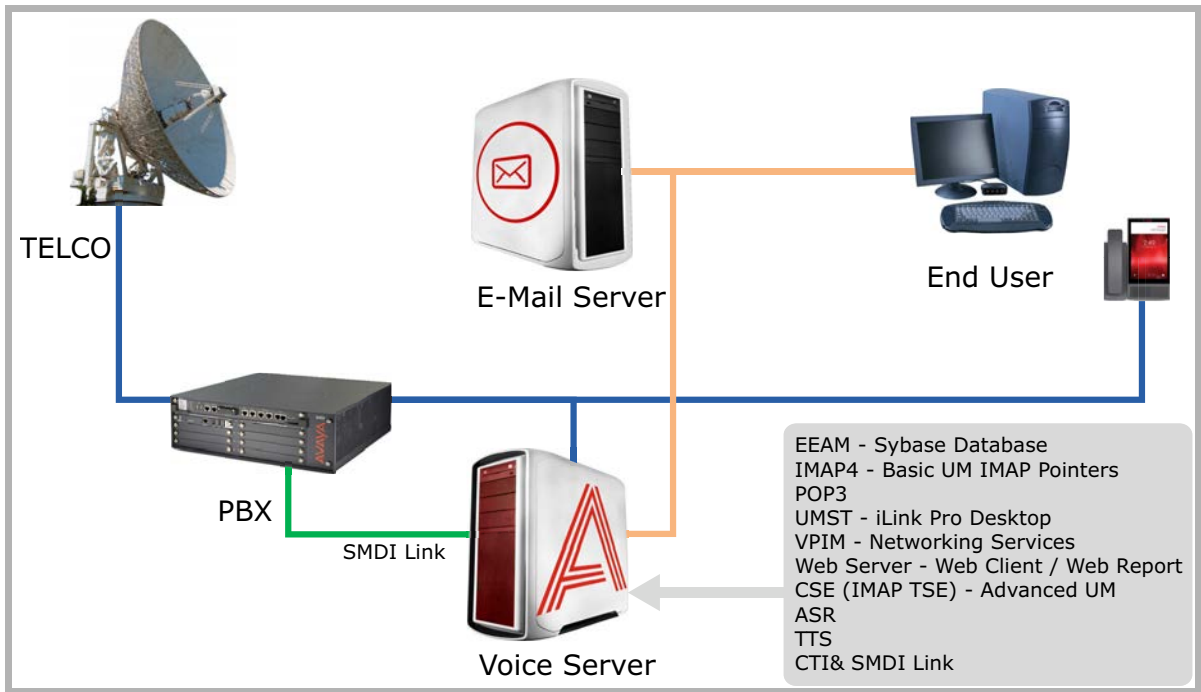
Since only one Voice Server is operating, any failure of the voice server equates to downtime. Even regular tasks such as regular maintenance, or a simple reboot will cause the system to be offline in single server configurations.

Reliability of the Multi-Server System

In the multiple server environment illustrated below, the Primary server is supported by the Secondary server(s) at all times. This means that a site can remain functional even if one of the voice servers fail. When the Primary server stops working, a Secondary server will take over until the Primary is back online.

The Primary and Secondary servers are able to work in unison with the help of the Consolidated (DB/File) server, also refereed to as the Common server. The Consolidated server manages the flow of data between all servers, and ensures proper synchronization of files. For a detailed explanation on database synchronization, please refer to Database Management on page 73, Failure Scenario on page 74 and Recovery Scenario on page 75.
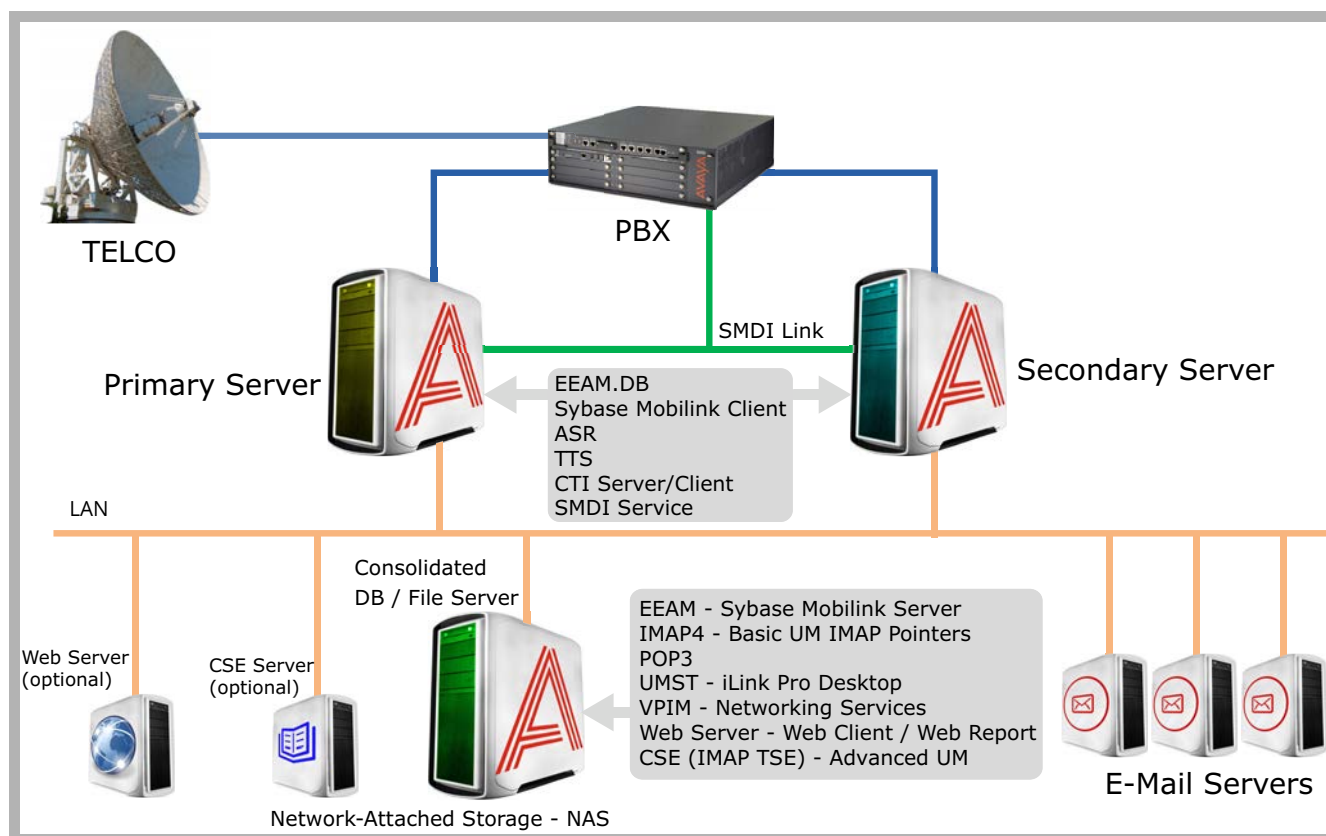
While the Multi-Server installation guarantees uptime for the voice servers, there may be scenarios in which the PBX itself is out of service.

Multiple Server Multiple PBX System

The multiple server system combined with multiple PBXs provides the most reliable configuration. In this scenario, maximum uptime is guaranteed even if the PBX fails along with the Primary server. The secondary PBX and the Secondary server will continue to accept calls while the Primary voice server and the primary PBX are offline.
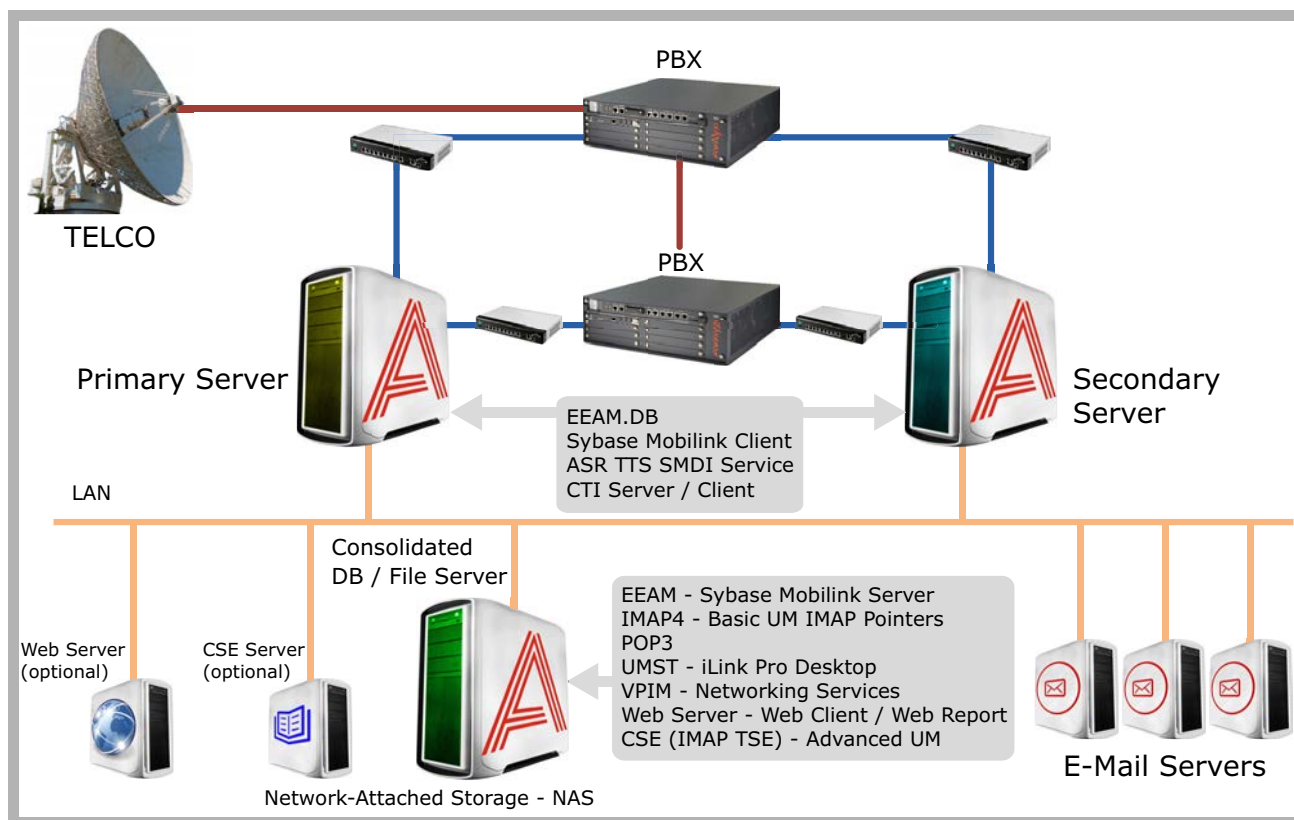
Database Management

In a High Availability environment, the databases in all the servers are synchronized through the Sybase Mobilink system. The Consolidated (Common) server acts as the Mobilink Server and manages the database for all of the Primaries and Secondaries.

This architecture gives sites full message access at all times, not just full uptime for all Voice server functions. Whenever a change (new message, deleted message, etc.) is made in either the Primary or Secondary servers, the Consolidated server copies these change to all databases in the system, allowing end users to maintain their messages and greetings even when one of the servers become unavailable.
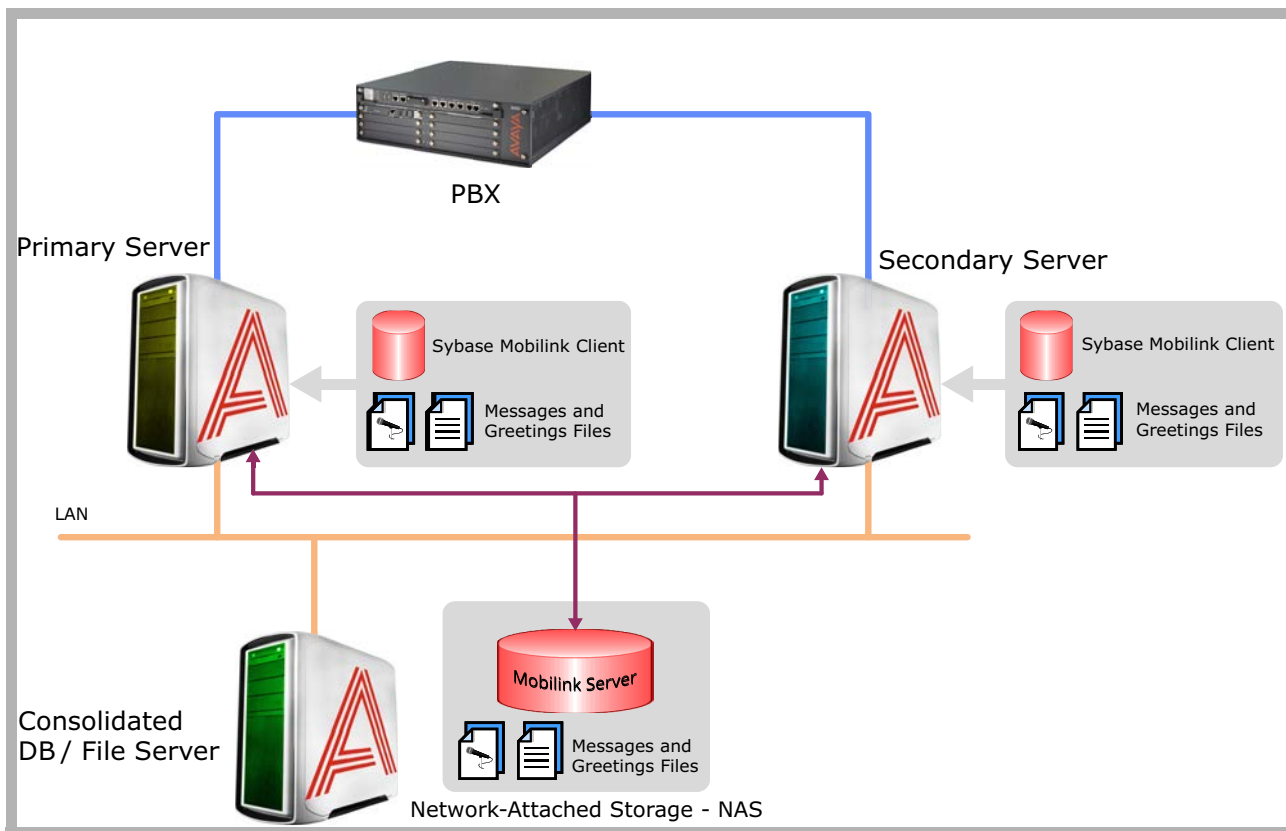
Failure Scenario

In this scenario, the Secondary server is unavailable due to a malfunction, severing the tie between the databases. The new messages received in the Primary server will continuously be synchronized with the Consolidated server but the Secondary server will be left behind during the down time.

Any messages received by the Secondary server are still accessible by the users since the database has already been synchronized before the Secondary server crash. There is also no disruption in regular service since the Primary server is still fully functional. All traffic is handled by the Primary server in the meantime.
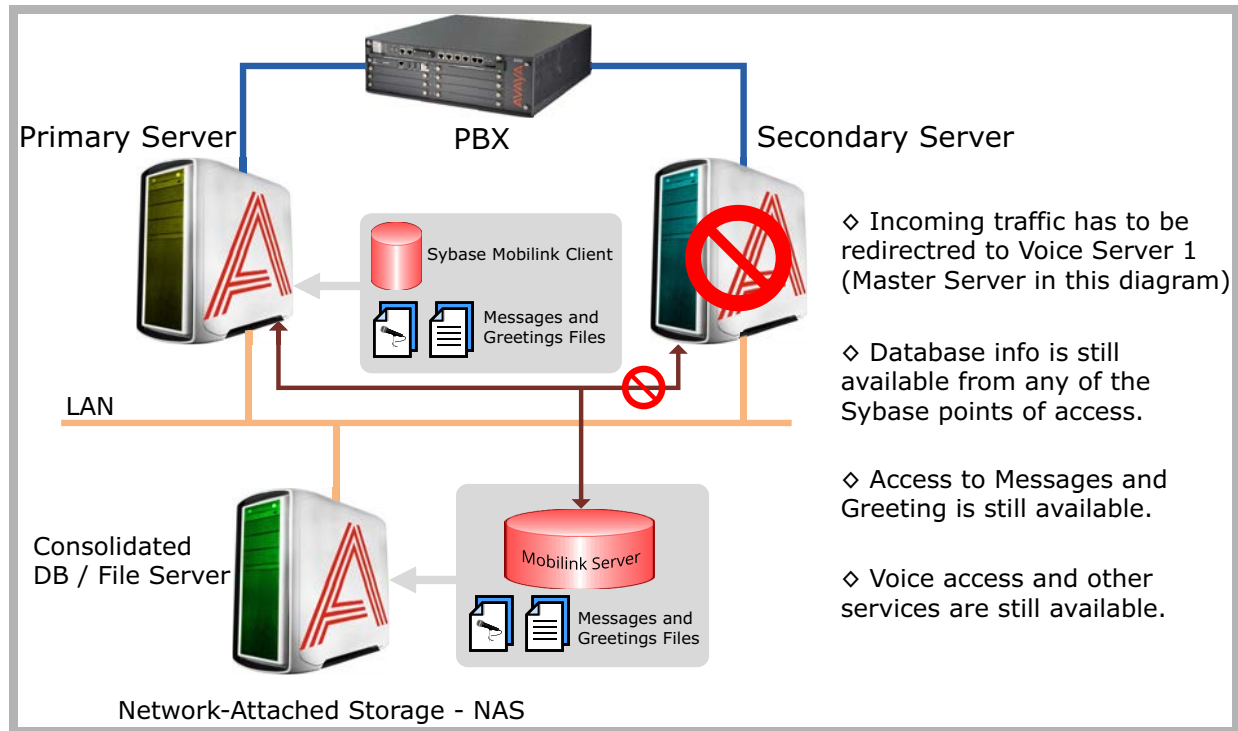
Recovery Scenario

In this scenario, the Secondary server that was down in the previous example has recovered. Soon after the Secondary server comes back online, the Consolidated server will start to synchronize the data between all the servers again, allowing the Secondary server to catch-up to the current database.

All messages and greetings will become automatically up to date on the secondary system soon after it comes online, which means that recovery will be a virtually invisible process that takes place in the background during regular operation.
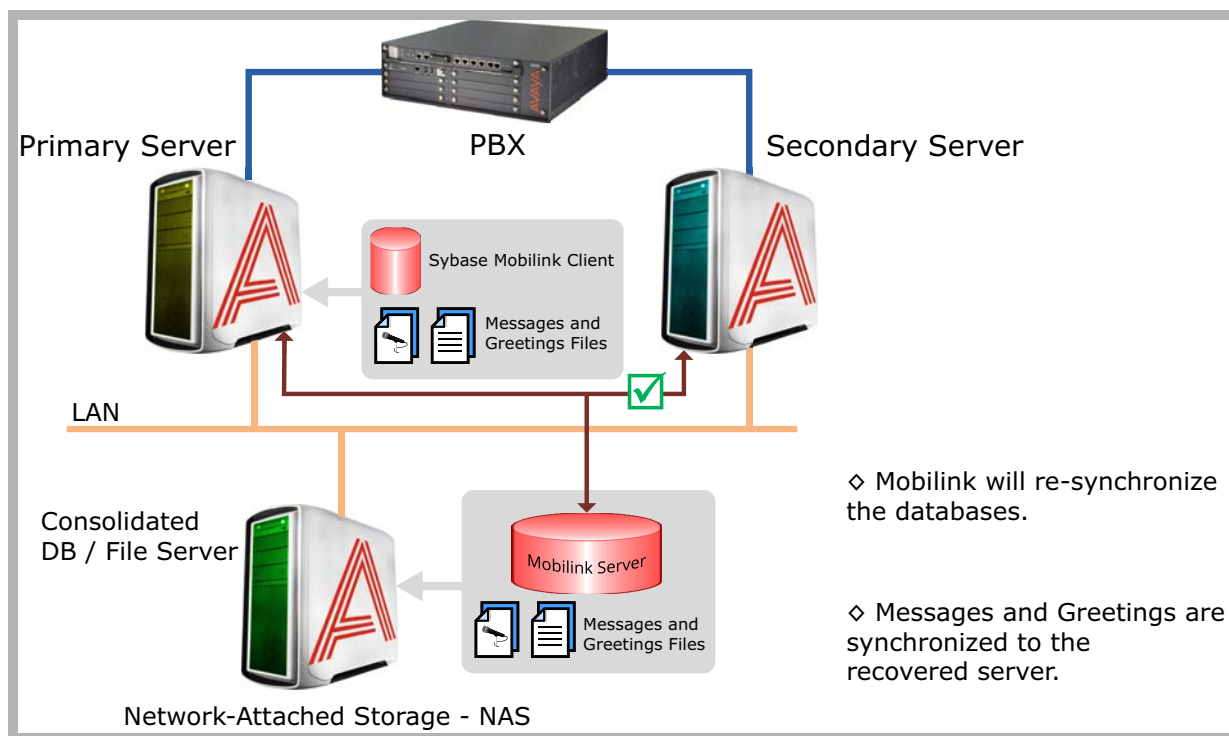
License Management

The High Availability system utilizes a unique licensing feature that allows full functionality of service while only one server holds the Sentinel key. In all cases, the Primary server will hold the USB Sentinel and becomes the primary holder of the license. However, the license file will be copied to all servers in the system through the database synchronization performed by Sybase Mobilink.

The copied license files will allow other servers (other than the Primary) to maintain full functionality even when they don't have individual license available to them. This system also allows for easier license management since only the Primary server has to be updated, should there be any type of addition or modification to the license.

However, the copied license files are time stamped to expire after a certain period. The time stamps are constantly updated by the Primary server, so it will not have any effect during regular operation.
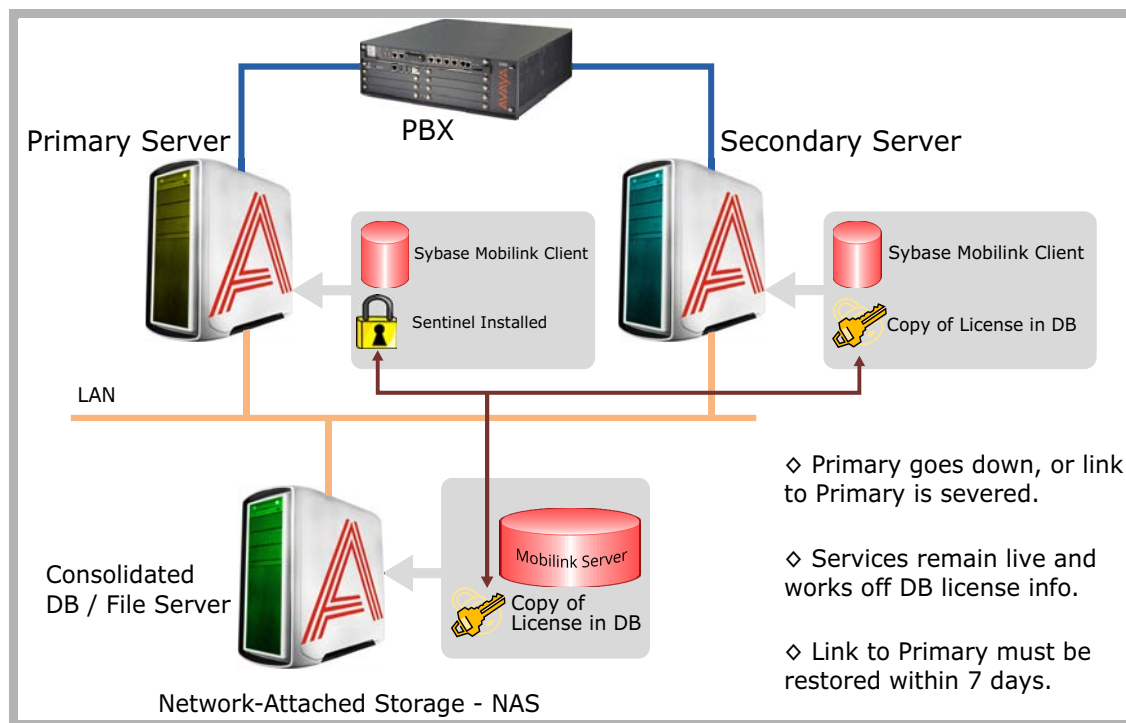
License Management During Primary Server Down Time

When the Primary server becomes unavailable, it will also stop updating the time stamps on the copied license files that exist on the Secondary server and the Consolidated server. When this happens, the Primary server has to be recovered within 7 days. If the Primary server isn't brought back online within the 7 days, the copied license files will expire and the system will cease to function due to invalid license status.

Since 7 days is a generous time period for recovery, most sites will not even notice such architecture in licensing. They will experience no problems as long as the Primary server is recovered in a timely manner.
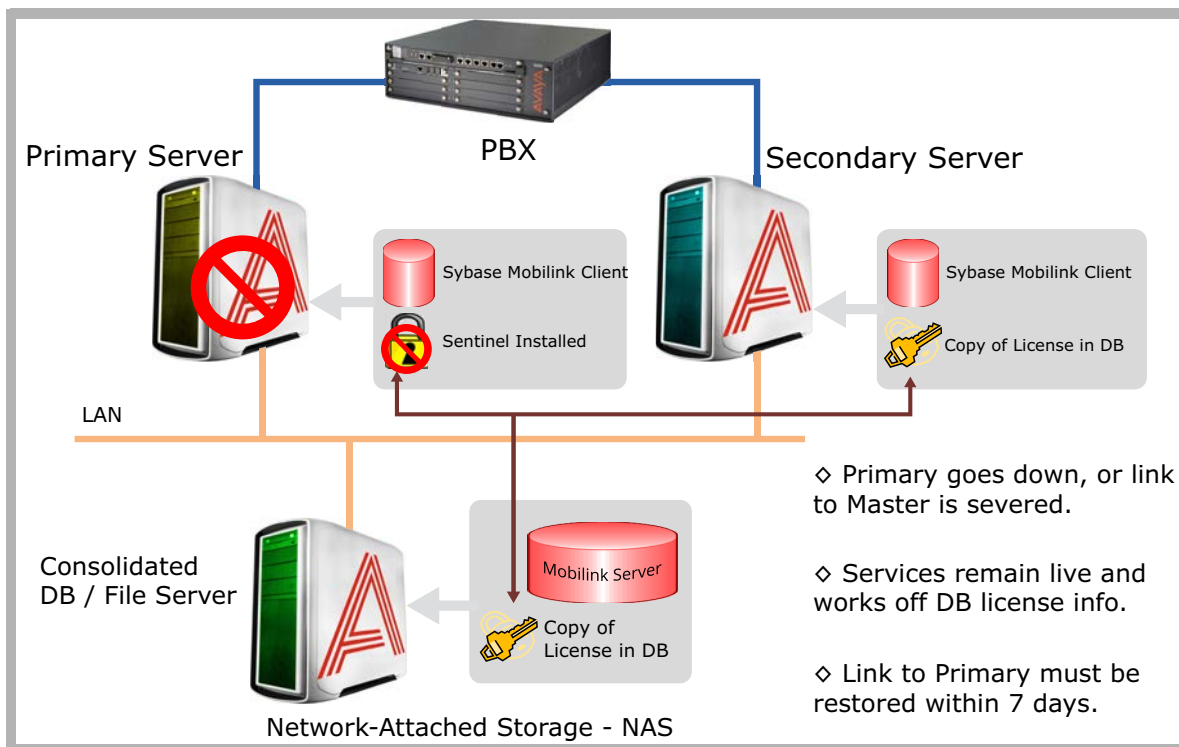
High Availability Redundancy & Scalability

Server Specification

The minimum configuration for a High Availability system is three servers, Primary, Secondary and Consolidated.

As of now, the High Availability system is able to support up to 20 voice servers maximum. This means that a site can maintain 1 Primary server and 19 Secondary servers in a single High Availability environment.

Configuration Limitation

Each voice server is designed to support up to 120 ports (SIP).

A single High Availability environment can support up to 20,000 user accounts (business rules apply).

Single Web server can support up to 10,000 users.

Single CSE server can support up to 5,000 users.

Other Rules and Limitations

The system is high availability rather than fully redundant.

The MWI function is only available for Voice and Fax messages.

Warning: Avaya Messaging is not compatible with Windows Remote Desktop Services (**Server Manager > Server Roles**). If Remote Desktop Services exists on the server, it must be removed or Messaging will not work or install properly.
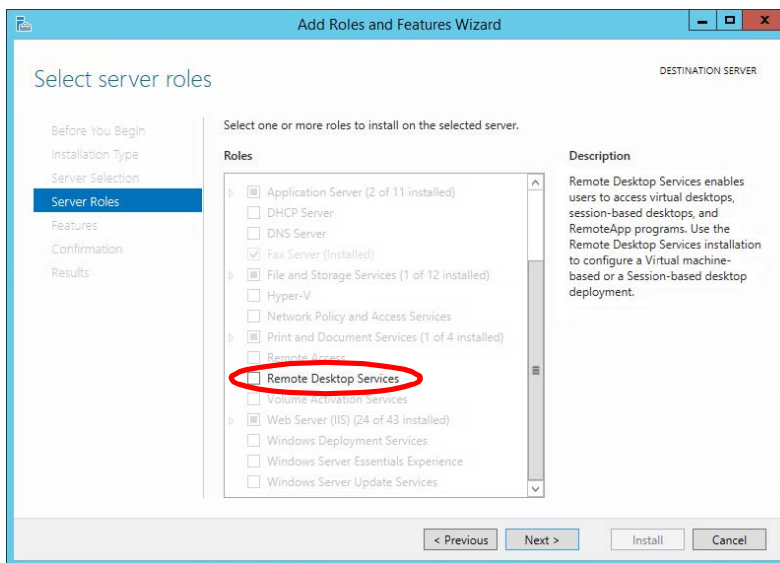
High Availability Configuration Flow

General Configuration Logic

Most configurations within an HA system will take place on the Consolidated server. While all servers have access to Messaging admin console, only the Consolidated server has the ability to change the fields for Company, Feature Group and Mailbox settings. Any changes made on these fields from the consolidated server will be pushed to all voice servers, which synchronizes configuration settings on all servers.

Secondary Servers

Primary Server

Company, **Feature Group** and **Mailbox** settings are all pushed from the **Consolidated** server to the others, synchronizing all changes between all servers.

Consolidated Server
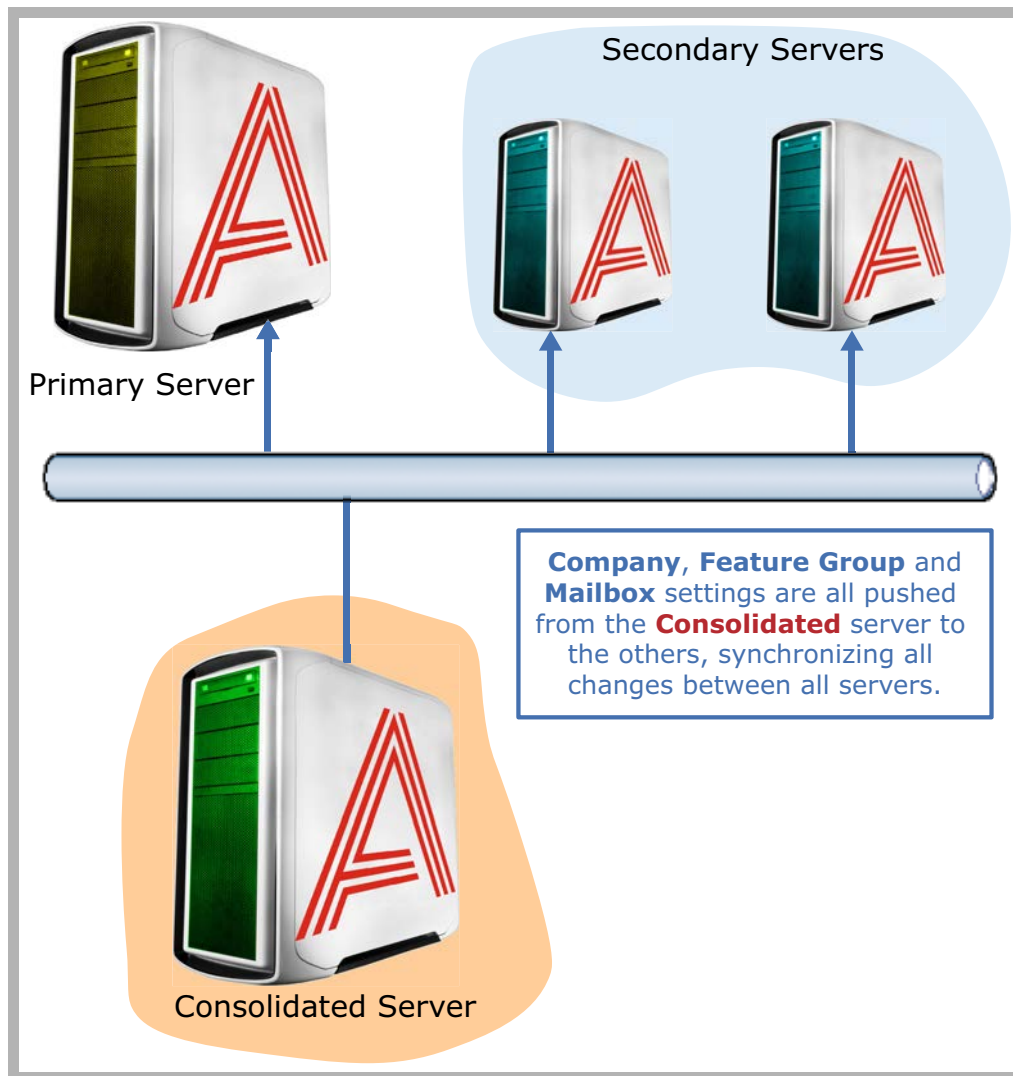
Server Specific Configuration

PBX properties and **Configuration** section within Messaging admin console is managed individually. Since each voice server may integrate into a different PBX, it is necessary for voice servers to be in control of their PBX related settings. However, **Configuration > Advanced > Consolidated Path** will be synchronized between all servers. This is the path which defines the location of the Consolidated server, so all servers must have an identical entry to correctly synchronize. The same goes for the Voicemail Channel list within the PBX. This list will be a compilation of all channels allocated on all voice servers. Defining individual extensions or channels within a voice server is done through the **SIP Configuration Tool**, which manages each voice server separately.
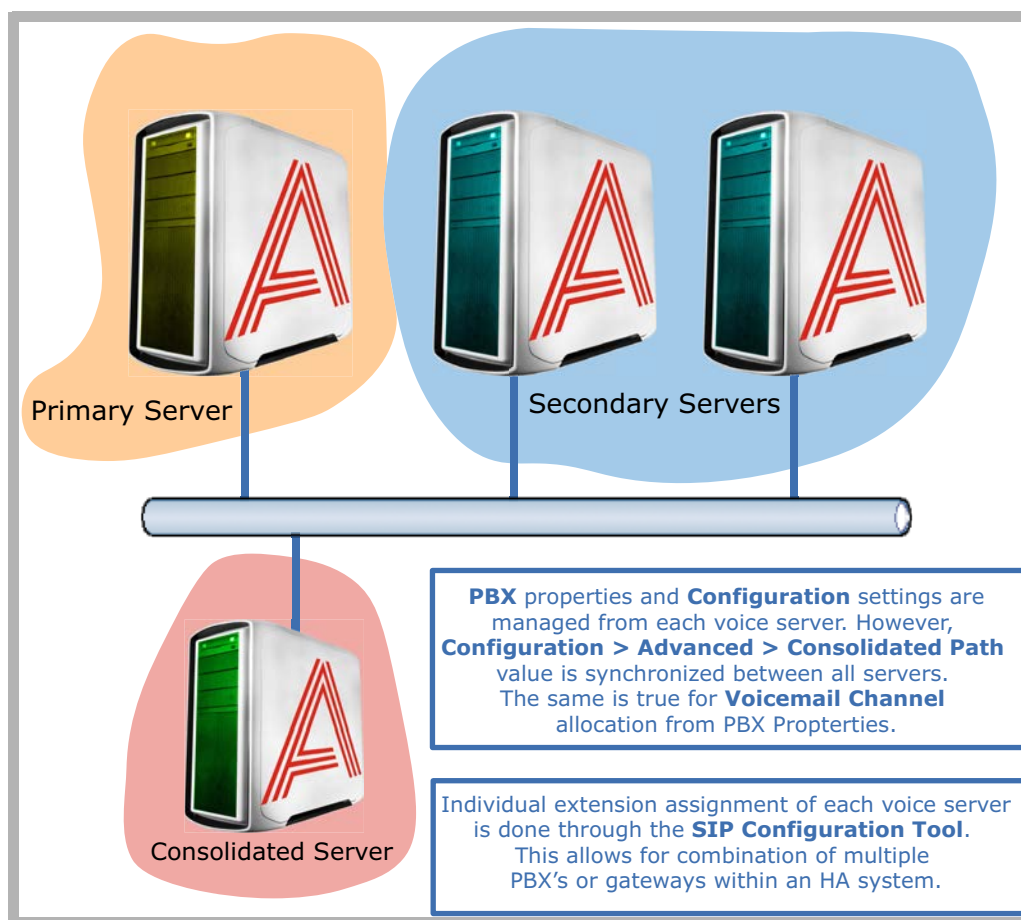
Primary Server

Secondary Servers

Consolidated Server

PBX properties and **Configuration** settings are managed from each voice server. However, **Configuration > Advanced > Consolidated Path** value is synchronized between all servers. The same is true for **Voicemail Channel** allocation from PBX Propterties.

Individual extension assignment of each voice server is done through the **SIP Configuration Tool**. This allows for combination of multiple PBX's or gateways within an HA system.

Requirements for High Availability Installations

In addition to all of the normal specifications, High Availability installations have several other requirements that must be met:

- All servers must be part of the same domain.
- All servers must have a minimum 1 GB/s connection to the network.
- The maximum round-trip latency between the servers must be no more than 10 ms.
- The maximum round-trip latency between the voice servers and the PBX must not exceed 200 ms. Optimal round-trip latency is less than 150 ms.
- The path of connectivity must have 1.5 MB/s guaranteed bandwidth with no steady-state congestion.

Voice Server Settings and Primary Server Selection

While many of the settings are controlled by Consolidated server, **Voice Server** settings within Messaging admin console is managed by the **Primary Server**. Each Voice Server, including the Primary and all Secondary Servers, will have its own entry within the Voice Server settings section. Only the Primary Server will be able to modify the fields within Voice Server settings, which is then pushed and synchronized to all other servers. However, all servers are able to change a single field labeled Primary within the Voice Server settings. This field can be used to designate any Voice Server as the Primary Server. If your Primary Server is unavailable for any reason (e.g. taken offline for maintenance), you will be able to assign another Voice Server as a Primary should the need arise.

Secondary Servers

Primary Server

Consolidated Server

Voice Server settings are pushed from the **Primary** server, and then synchronized to the other servers. However, all servers have the ability to be either Primary or Secondary, allowing you to change the Primary server even if the original Primary has crashed.
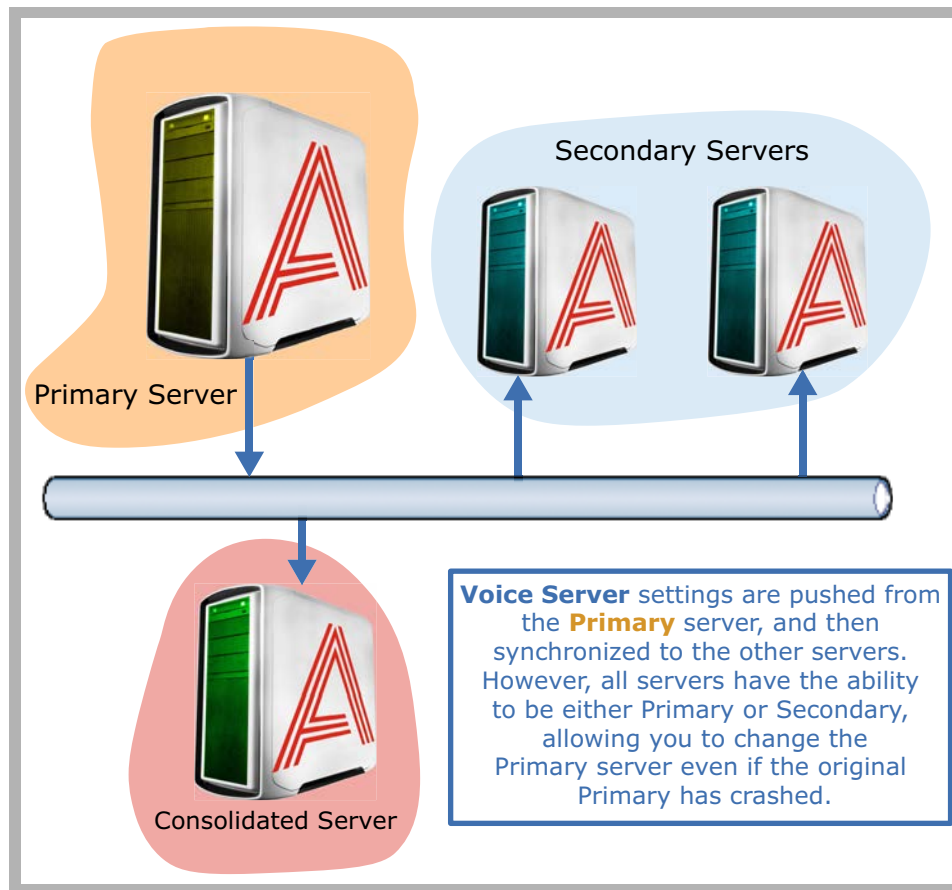
Logs and Reports

When it comes to voice traffic, each Voice Server will store activities which have occurred on that server, which means that logs related to a call will only be available on the specific server that the call took place (both incoming and outgoing). All message related logs (including voice messages) will be stored on the Consolidated server since it is the Consolidated server's task to maintain synchronization of messages.

If you wish to create a Web Report of server activities, the necessary information will be pulled by the Consolidated server from the Voice servers. For most purposes, all you have to do is connect to Web Report services within the Consolidated server to obtain comprehensive information regarding the usage and status of your server. Individual log files are mostly used for troubleshooting purposes, so you will not have to track them from each servers separately.
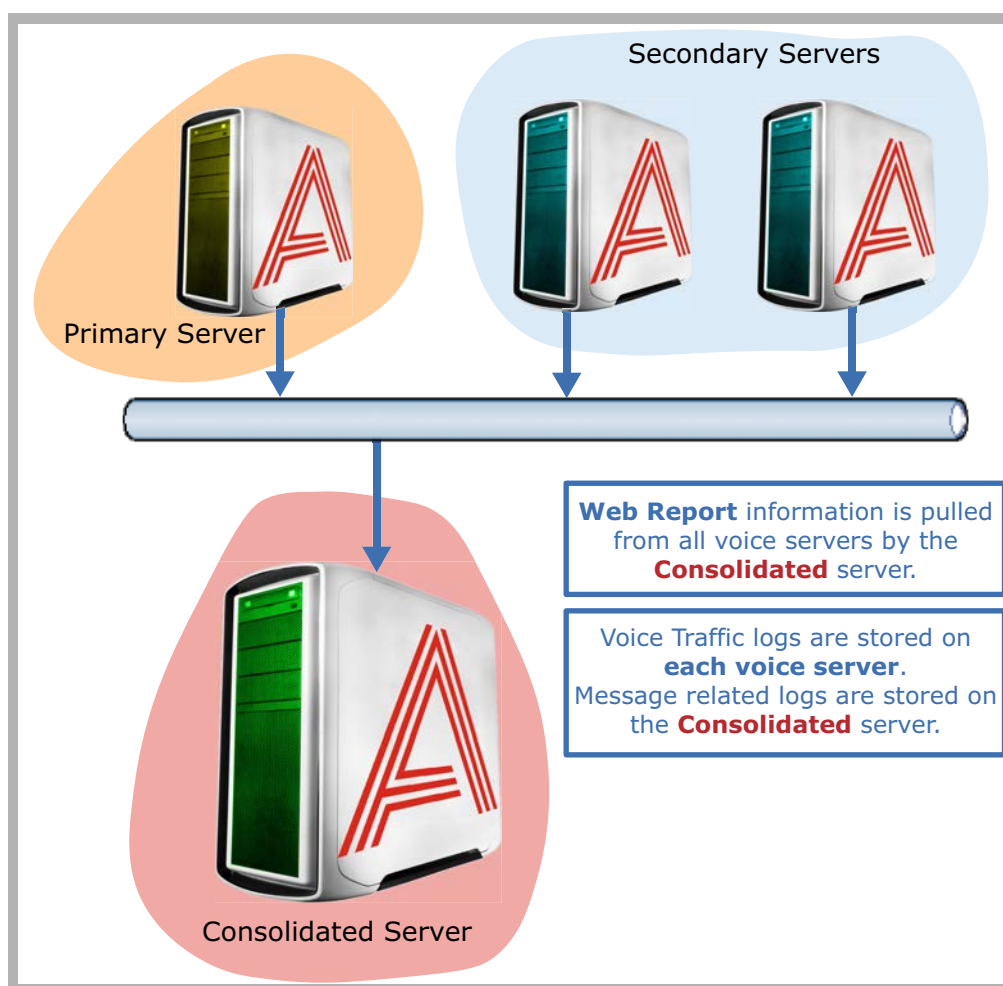
Geo Redundancy

An Avaya Messaging HA installation can be spread across a geographically distributed network. Geo Redundancy allows a section of the network in one part of the world to go offline without affecting the remaining elements.

Installing Messaging with Geo Redundancy proceeds the same way as it does with any other HA install, but with some of the servers existing in other locations.

Geo Redundancy has the following network connection requirements to operate properly.

- All Messaging servers must be on the same network as the PBX.
- All servers must have a minimum 1Gbps connection to the network.
- The maximum round-trip latency for optimum performance is 10ms between servers, with an acceptable tolerance up to 60ms.
- The maximum round-trip latency between the voice servers and the PBX must be no more than 200 ms.
- Optimal round-trip latency is a maximum of 150 ms.
- The path of connectivity must have 20Mbps guaranteed bandwidth with no steady-state congestion.
- At all times, the LAN network connection must provide a min guaranteed 20Mbps upload / download speed.

Contact your dealer if you have any further questions.

7

VMWARE SUPPORT

In This Chapter:

Introduction

Many organizations are turning to virtual environments for their server needs due to their cost and efficiency. Instead of a room full of servers, virtual servers on hosted or in-house environments can perform the functions of multiple computers.

Avaya IX Messaging can be installed on a virtual environment enabling you to reuse the equipment you already have. Instead of buying a new computer to host the voice server, upgrades to existing hardware may be sufficient through virtualization.

Pre-Requisites

Software	Version
VM Software	VMware ESXi 4.x / 5.0 / 5.1 / 5.5 / 6.0 / 6.5 / 6.7 Hyper-V Server 2012 Windows Terminal Services[1]
OS for Messaging	Server 2012 or 2012 R2 Server 2016 Server 2019

Note: ESXi has been tested on versions 4.x / 5.0 / 5.1 / 5.5 / 6.0 / 6.7. Hyper-V Server 2012 has also been tested.

Hardware	
CPU	Requires Intel® CPU which meets or exceeds the requirements of ESXi 4+

1 - Windows Terminal Services only supports the installation of the client software. The Messaging server cannot be installed here.

Virtual Environment Limitations

Migrating data from a virtual machine environment is not supported.

Migrating data to a virtual machine from an existing physical environment is supported, but only if AM is installed first. Move an existing server onto a virtual machine by migrating the database using the utilities provided with the Messaging installation package. You can transfer both 7.x and 8.x systems to an 10.8 virtual environment. Messaging must be installed on a new virtual machine with a clean operating system.

Warning: Importing an existing Avaya IX Messaging environment to a virtual image is not supported.

Messaging installed on a virtual environment requires the same hardware resource as non-virtual machine environments.

Note: The fax capability of Messaging within a virtual environment is limited to **24 ports**.

Warning: **Do Not take snapshots** while the servers are in operation as this can lead to serious corruption in the database. System performance may also be heavily compromised. To take a snapshot, shutdown the server first, then take the snapshot while the system is down.

This table shows the list of VMWare features supported.

FEATURE	AVAYA MESSAGING 10.8	AVAYA MESSAGING 11.0
Support for ESXi 6.0	Yes	No
Support for ESXi 6.5	Yes	Yes
Support for ESXi 6.7	Yes	Yes
Support for ESXi 7.0	No	Yes
VMware vMotion	No	No
VMware Snapshot	No	No (Only temporary snapshots prior to upgrade can be created and should be removed after upgrade)
VMware HA	Yes	Yes
VMware DRS	No	No
VMware FT	No	No
vSphere Standard Switch	Yes	Yes
vSphere Distributed Switch	Yes	Yes
Reservation Required	No	No
VSAN Support	Yes	Yes
Thin Provisioning	No	No

Virtual Machine Environment Hardware Requirements

The hardware requirements for setting up Messaging within a virtual environment are the same as for a physical machine. See the <u>System Requirements and Capacity</u> chapter of this guide for more information.

The configuration of the virtual environment does create other considerations for server installation.

For further details on Hardware Requirements, see page 53.

VMware Technology Guidelines

VMware offers wide range of technologies which may be implemented on a virtual machine for greater redundancy and ease of maintenance. This section explains which features are compatible with the Messaging server application and how to utilize VMware solutions with Messaging in mind.

- **High Availability**: VMware also offers its own High Availability solution, which should not be confused with Messaging HA. VMware's HA model is initiated in 2 ways: one is hardware (machine) failure and the other is software (Operating System) failure. When the ESXi hardware fails on a system monitored by HA, VMware will automatically restart the Virtual Machine image on another ESXi host. If the OS becomes unresponsive, VMware HA will start the virtual machine on another ESXi host and bring the server back online. This will lead to down time while VMware moves operations onto another host. Messaging will be down during the recovery period and will not be able to answer calls until the secondary virtual image is fully up and running. The recovery occurs automatically, but it must be 'hard coded' to a specific recovery ESXi server. If there are no available resources on the recovery server, Messaging may fail to restart.

- **Distributed Resource Scheduler**: Distributed Resource Scheduler is intended for sites with multiple physical ESXi servers available. DRS keeps track of hardware resources, and is able to see the current availability of CPUs, RAM, etc. on all servers. When the main server crashes, DRS will automatically allocate the necessary resources and restart the virtual machine in a suitable environment. This means that Messaging will be guaranteed a minimum level of resources upon recovery to ensure there is no reduction in service. This is an advantage offered by DRS when compared to HA alone since HA does not consider hardware requirements when allocating space for a new virtual machine to replace the crashed server.

- **Fault Tolerance**: Fault Tolerance offers a higher level of protection than HA by eliminating of downtime. A virtual machine being monitored by an FT system will have a shadow image created that is identical to the monitored virtual machine. When the main server becomes unavailable for any reason, the shadow image which has been reproducing all activity on the main server will become active, instantly replacing the crashed server. This reduces the chance of an interruption or data loss in most active environments. However, due to the extensive nature of FT's monitoring, FT can only support virtual machines with a single core CPU. This does not meet Messaging Voice Server's minimum hardware requirements, so Messaging will remain incompatible with FT until the algorithm is changed to support the resources required.

VM Environment Feature Comparison Chart

	HA	DRS	FT
Active Migration	N	N	N
Recovery from Hardware Crash	Y	Y	Y
Recovery from Software Crash	Y	Y	Y
0 Down Time during Crash	N	N	Y
Smart Allocation of Hardware Resources	N	Y	N
Messaging Support	Y	Y	N*
Known Behaviors:			
Voice Traffic	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
iLink Pro Desktop	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
Messaging	Interrupted until HA recovers	Interrupted until HA recovers	N/A*
CTI	Interrupted until HA recovers	Interrupted until HA recovers	N/A*

***** Due to the way in which Fault Tolerance is designed, Avaya IX Messaging cannot function within the FT model. FT is limited with regard to computer resources (e.g. single core processor) while Messaging has specific minimum resource requirements to function properly. Until VMware upgrades the FT system to support higher amounts of resources, Messaging cannot be deployed under the FT model.

VMware: HA for the Consolidated Server

In a High Availability environment, the Primary and all Secondaries act as backups for each other. If one server fails, the Consolidated server redirects traffic through the remaining operational units preventing any service interruptions. However, the Consolidated server has no such protection. If the Consolidated server fails, the entire system will fail.

VMware includes an HA option for its Hosts, providing failover support for the Consolidated server. Both the Consolidated and Primary voice servers can backed up this way. The Secondary voice servers cannot.

1. The site admin must install and configure VMware vSphere on the network. There should also be an external SAN for data storage.
2. Create a Cluster within vSphere.
   - When configuring the Cluster, under **vSphere Availability**, ensure that **Turn ON vSphere HA** is enabled.
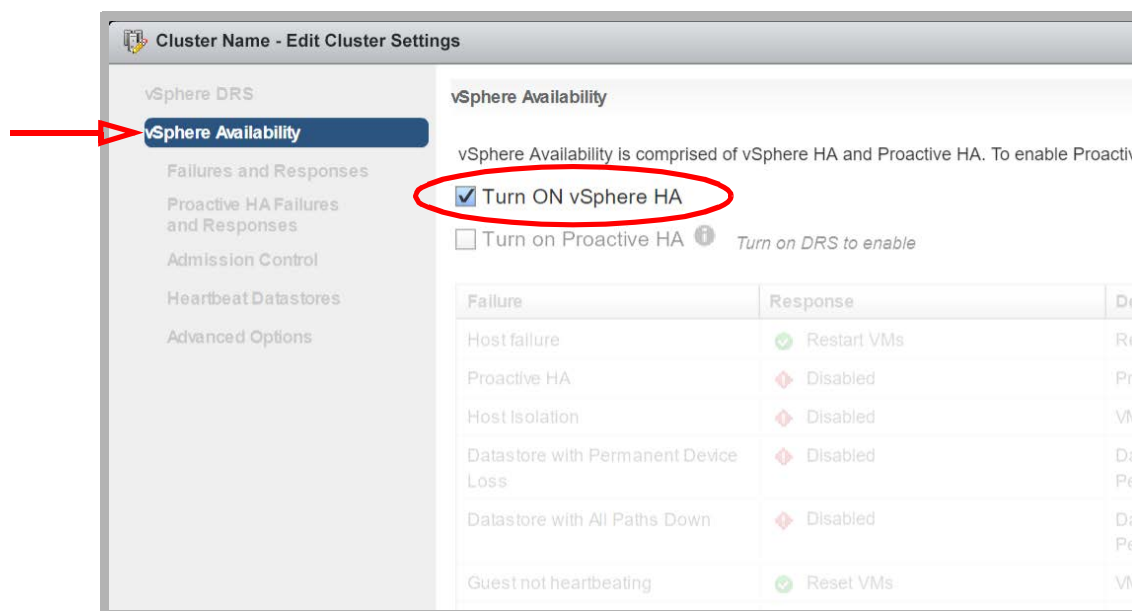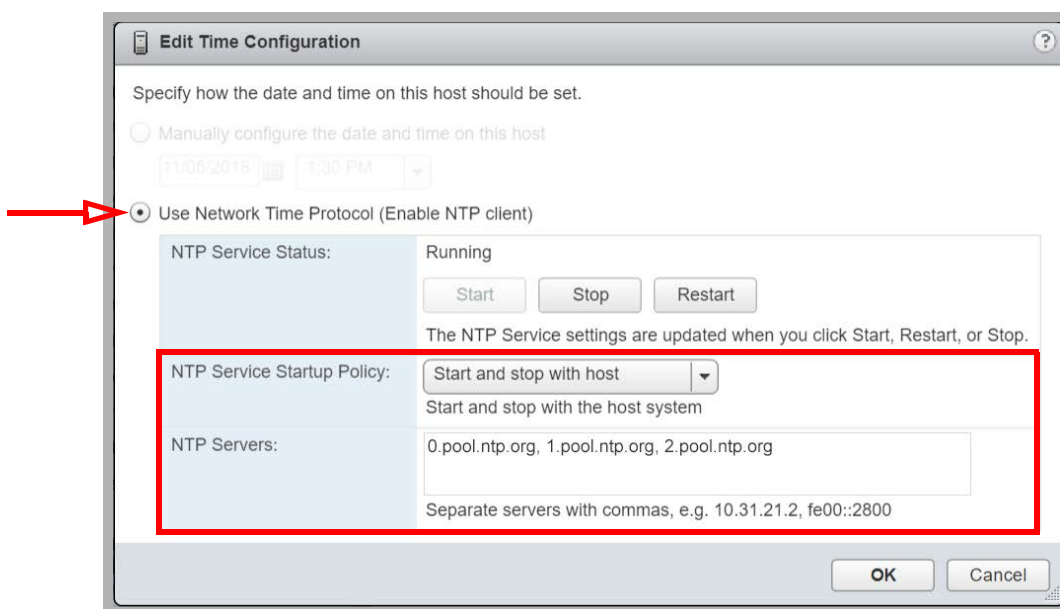

3. Add 2 or more Hosts within the Cluster. One Host contains the virtual machine that houses the Consolidated server, while the others are available should the active Host fail.

Important: It is essential that all of the Host servers (Consolidated, Primary, and backups) have their clocks synchronized. Certain critical functions within Messaging are time sensitive and will fail if the Hosts are not coordinated.

---

4. For each Host, open the Configuration tab and go to **System > Time Configuration**.
   - Enable **Use Network Time Protocol (Enable NTP client)**.
   - Set the **NTP Service Startup Policy** to **Start and stop with host**.
   - Enter one or more NTP servers in the space provided. The time signals will be synchronized with these sites.

- **Start / Restart** the NTP Service to activate the changes.

5. Create virtual machines and choose the SAN as the data storage location.
6. Edit the settings for each virtual machine.
Under **VM Options > VMware Tools > Time**, enable **Synchronize guest time with host**.

7. Install the Avaya IX Messaging Consolidated server onto one of the virtual machines.

If the Host with the virtual machine running the Consolidated server fails, VMware will automatically move the server to another Host within the Cluster and restart the virtual machine.

Important: The Messaging system will be unavailable during the changeover and reboot process.

VMware: HA for the Primary Voice Server

In a High Availability environment, the Primary and all Secondaries act as backups for each other. If one server fails, the Consolidated server redirects traffic through the remaining operational units preventing any service interruptions.

VMware includes an HA option for its Hosts, providing failover support for the Primary voice server. Both the Consolidated and Primary voice servers can backed up this way. The Secondary voice servers cannot.

1. The site admin must install and configure VMware vSphere on the network. There should also be an external SAN for data storage.
2. Create a Cluster within vSphere.
   - When configuring the Cluster, under **vSphere Availability**, ensure that **Turn ON vSphere HA** is enabled.
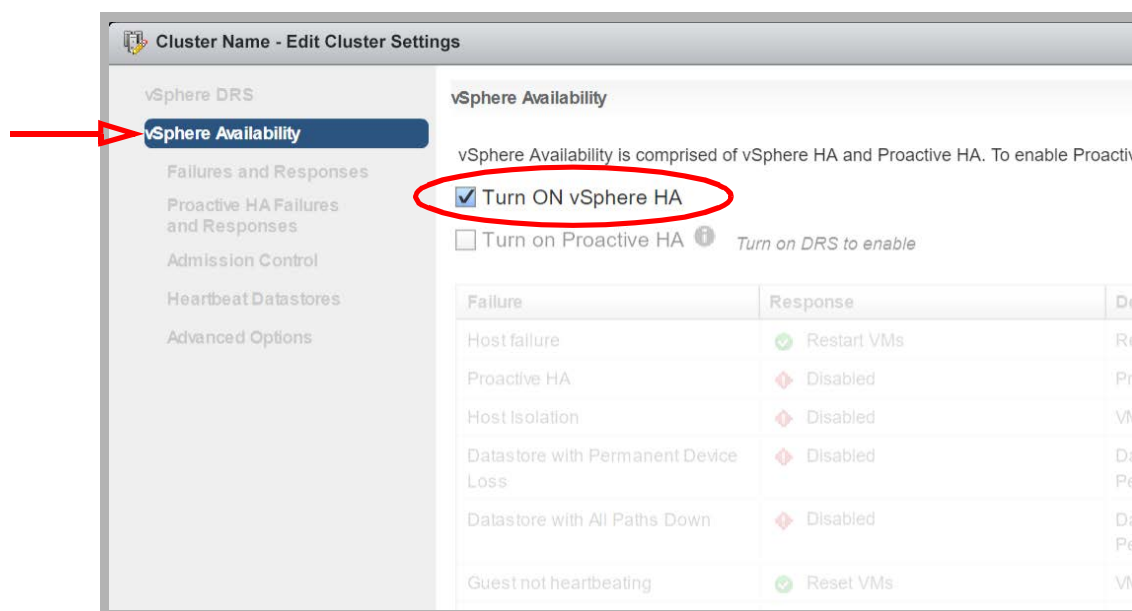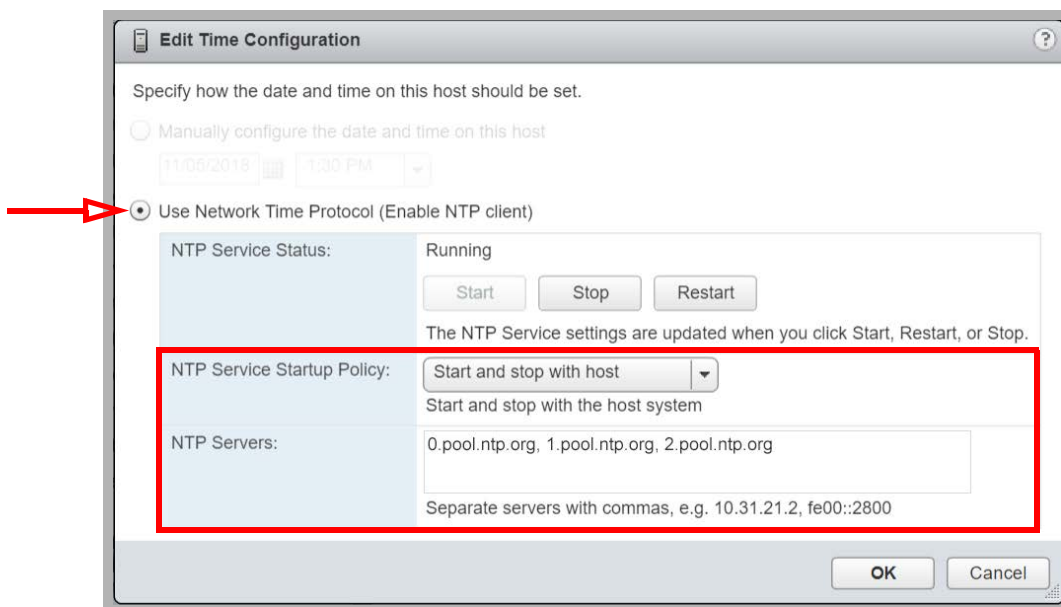

3. Add 2 or more Hosts within the Cluster. One Host contains the virtual machine that houses the Primary voice server, while the others are available should the active Host fail.

Important: It is essential that all of the Host servers (Consolidated, Primary, and backups) have their clocks synchronized. Certain critical functions within Messaging are time sensitive and will fail if the Hosts are not coordinated.

---

4. For each Host, open the Configuration tab and go to **System > Time Configuration**.
   - Enable **Use Network Time Protocol (Enable NTP client)**.
   - Set the **NTP Service Startup Policy** to **Start and stop with host**.
   - Enter one or more NTP servers in the space provided. The time signals will be synchronized with these sites.

- **Start** / **Restart** the NTP Service to activate the changes.

5. Create virtual machines and choose the SAN as the data storage location.
6. Edit the settings for each virtual machine.
Under **VM Options > VMware Tools > Time**, enable **Synchronize guest time with host**.

7. Install the Avaya IX Messaging Primary voice server onto one of the virtual machines.

If the Host with the virtual machine running the Primary voice server fails, VMware will automatically move the server to another Host within the Cluster and restart the virtual machine.

> **Important**: The Messaging system will be unavailable during the changeover and reboot process.

Additional Considerations for AACC Users

There are additional conditions for sites that are integrating with Avaya Aura Contact Center.

- The IX Messaging virtual machine must use the same network interface card (NIC) for both ELAN and CLAN
- On the CS1000, configure the parameter **Set Type = 2008** for the DMG ports.
- Configure the following 2 services for **Automatic (Delayed Start)**:
  UC Voice Server
  UC Service Recovery Manager (found on the Consolidated Server)

Virtual Environment Deployment Example

The following are performance results from a virtualized Avaya IX Messaging system running 100 active voice ports with 1,000 users registered under the system. Please keep in mind that this is a limited test run to showcase how a typical operation may perform under a virtual environment. This example does not guarantee an identical level of performance on every virtual environment, but rather serves as a guideline with regards to Messaging's behavior under virtual environments.

CPU Usage

Avaya IX Messaging used an average of 58.945% of the CPU capacity, which equates to 5,643.95 MHz. When considering the Maximum requirement, providing at least 6.8 GHz of CPU resources to Messaging will guarantee a consistent level of performance.

Datastore Latency
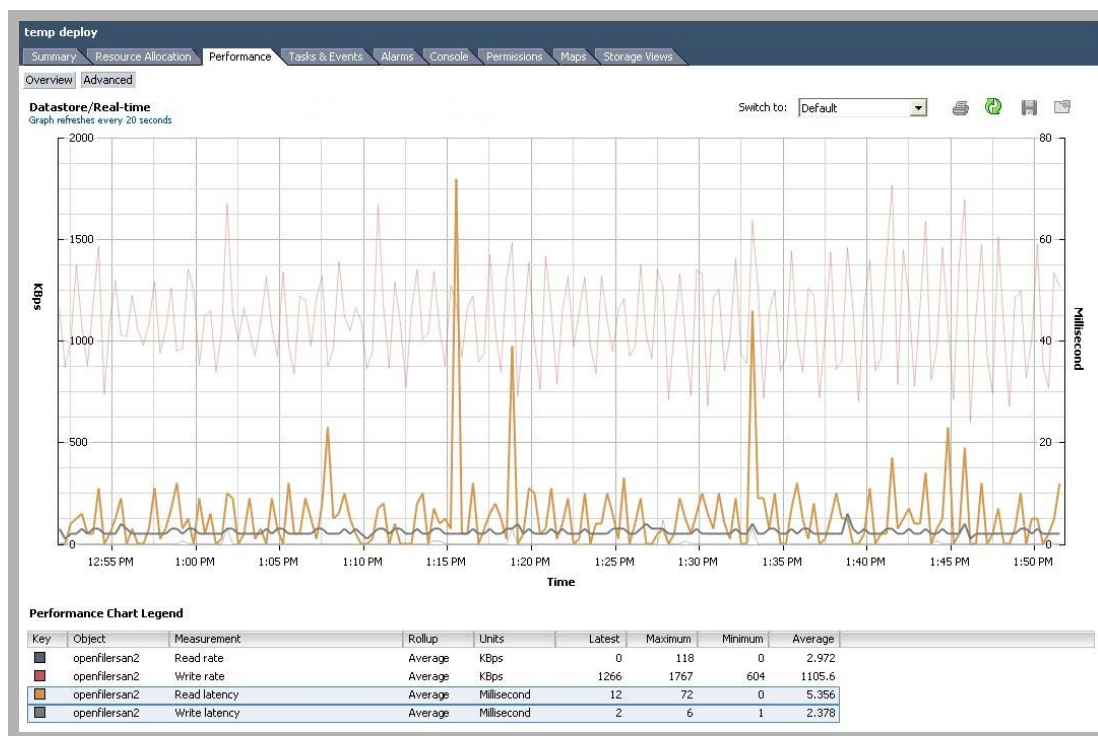
Avaya IX Messaging achieved a low average latency of 5.356ms for reading and 2.378ms for writing.

Disk Usage Rate
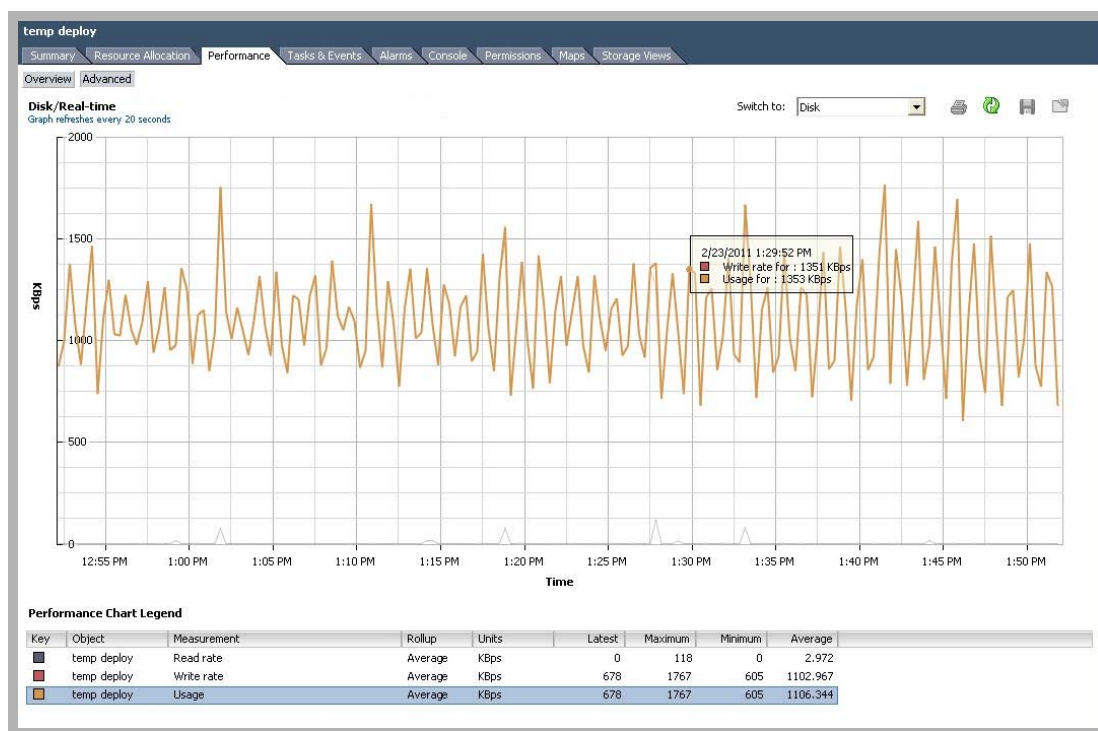
Avaya IX Messaging had an average disk usage rate of 1,106.344 KBps with a peak of 1,767 KBps. Ensuring a data transfer

rate of 1,800 KBps to Messaging will guarantee a consistent level of performance.

Network Usage Rate
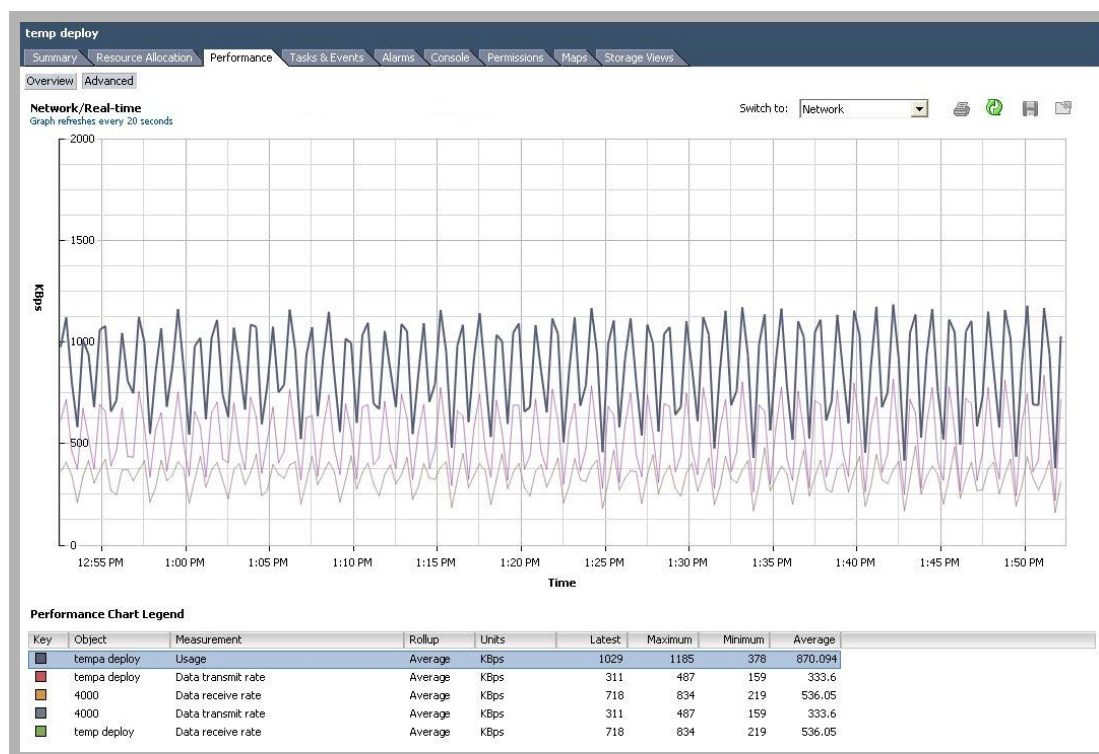
Avaya IX Messaging had an average network usage rate of 870.094 KB/s with a peak of 1,185 KB/s. Providing 1,500 KB/s of network bandwidth to Messaging will guarantee a consistent level of performance.

Conclusion

Since Avaya IX Messaging is designed to be the sole application running on a given Virtual Machine, it is easy to assign the necessary resources for Messaging. By ensuring that Messaging always has access to the required resources, you will be able to guarantee the level of performance required by your site.

8 SERVER MESSAGING TYPE CHARACTERISTICS AND DEPLOYMENT SCENARIOS

In This Chapter:

E-mail Server Synchronization (CSE)

Unified Messaging Deployment Email Requirements

Deployment of Unified Messaging into an email system is limited to tested and verified email server environments. Please refer to the chart below to determine if a site is compatible for UM deployment.

Email Server	Requirements	Contact Sync	Calendar Sync	Comments
Exchange 2010 / 2013	Configure to be compatible with Messaging, enable IMAP4	Y	Y	
Google Apps Gmail	Configure to be compatible with Messaging, enable IMAP4	Y	Y	OAuth performs Super User function

Note: CSE is based on IMAP4 standards. Other email servers with this same capability may function correctly but take note that they have not been validated by Avaya.

Avaya Messaging's CSE gateway can now utilize high performance pace (HPP) mode when connecting to an Exchange server. The HPP mode uses an event-driven model to communicate information changes between the Messaging Server and the Exchange server. This is in contrast to the polling model used in previous releases which continues to be used in the current release with non-Exchange servers. The default setting for HPP mode is "enabled". To turn it off it is necessary to go to the IMAP Tester utility. The benefit of using HPP mode is a significant reduction in CPU usage on the voice Server.

When a voicemail message is received by the Messaging Server the MWI on the user's telephone is extinguished. When the message from the phone or Web Client is read the MWI is no longer lit.

Unified users with access to all their phone and email messages may notice a slight delay before their MWI is extinguished when accessing their messages via their email client (Outlook, etc). This delay is very short and can be modified based on individual user priorities and on how many users are in the feature group.

The following tables indicate MWI behavior in a **controlled** environment. The following data reflects traffic with inbox-only synchronization with a maximum message count of 250 messages in the inbox. Keep in mind that using HPP mode ignores the priority assigned to mailboxes, which means that the following information does not apply to HPP systems.

Unified Messaging Capacity

The following chart illustrates the capacity of CSE server on a UM environment.

Capacity	
Maximum number of total users on system	20,000
Maximum number of M+C user on system	10,000
Maximum Number of users for 1 CSE Server	5,000
Maximum Number of users for 2 CSE Servers	10,000
Maximum Number of users for 3 CSE Servers	15,000
Maximum Number of users for 4 CSE Servers	20,000

MS Exchange Performance Considerations

Microsoft advises that a large numbers of items in folders can decrease the speed of operations in Exchange. For details on MS Exchange 2010, refer to the following link:

http://technet.microsoft.com/en-us/library/ee832791.aspx

Deployment: Basic Unified Messaging

Integrated Messaging is a unified view of all messages in a user's email client.

There are two methods of deploying Basic Unified Messaging (UM):

Deployment 1 - Basic UM via SMTP Forwarding

In this deployment Avaya Messaging forwards received voice and fax messages to an SMTP* compliant email server. All message types are stored on the email server and the user is given a single view in their email client.

Note: Simple Mail Transfer Protocol (SMTP) is a TCP/IP protocol used to send and receive email.

You can record voice mail responses from your PC desktop and either have these responses sent via email or forwarded to others. You also have the option of responding to a voice mail with a simple email.

Note: As the reply destination would be the user's mailbox and not that of the original sender the 'Reply' feature is not available.

You respond to a voice message from Outlook via the 'Forward' feature, by keying in your response and selecting a recipient from the Global Address List. By this method both the original voice message and the email response is sent back to the original sender.

Note: The Avaya Messaging toolbar plug-in (Outlook only) is required to enable the recording of voice replies to voice messages from email.
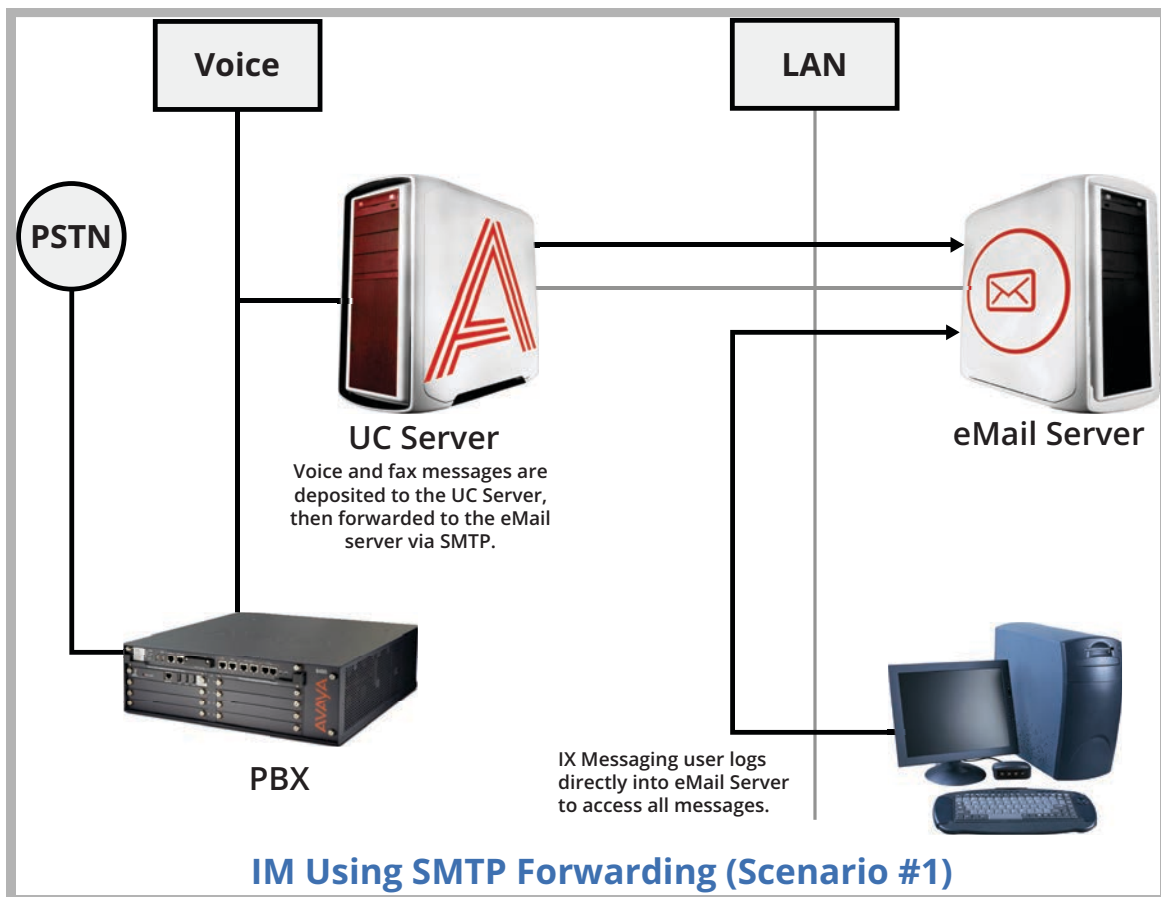
Deployment 1 is ideal for PC-centric desktop users who want to retrieve their messages via their email client. Such users do not typically need to check their voice messages by telephone. They may access this option if the voice messages are copied and sent to the email server rather than deleted from the voice Server.

SMTP forwarding may be deployed in the following email environments:

- Exchange 2010/2013
- Gmail (Google Apps)
- Office 365

The email server must be configured to accept attachments (WAV attachments specifically) and the client PC must have a media player installed that can play GSM compressed WAV files (i.e. Windows Media Player).

Warning: Users of SMTP forwarding should make careful use of the Delete after Forward option. If this option is selected messages are permanently deleted immediately after being forwarded to the designated email address. In the event of a failure to deliver the message (receiving server is down, mailbox is full, invalid address, etc), an "undeliverable mail" message will be received in the inbox on the Messaging Server. Although the forwarded message will still be accessible from the Sent folder the Web Client application must be used to access this folder (by the user or the System Administrator) and retrieve the message.
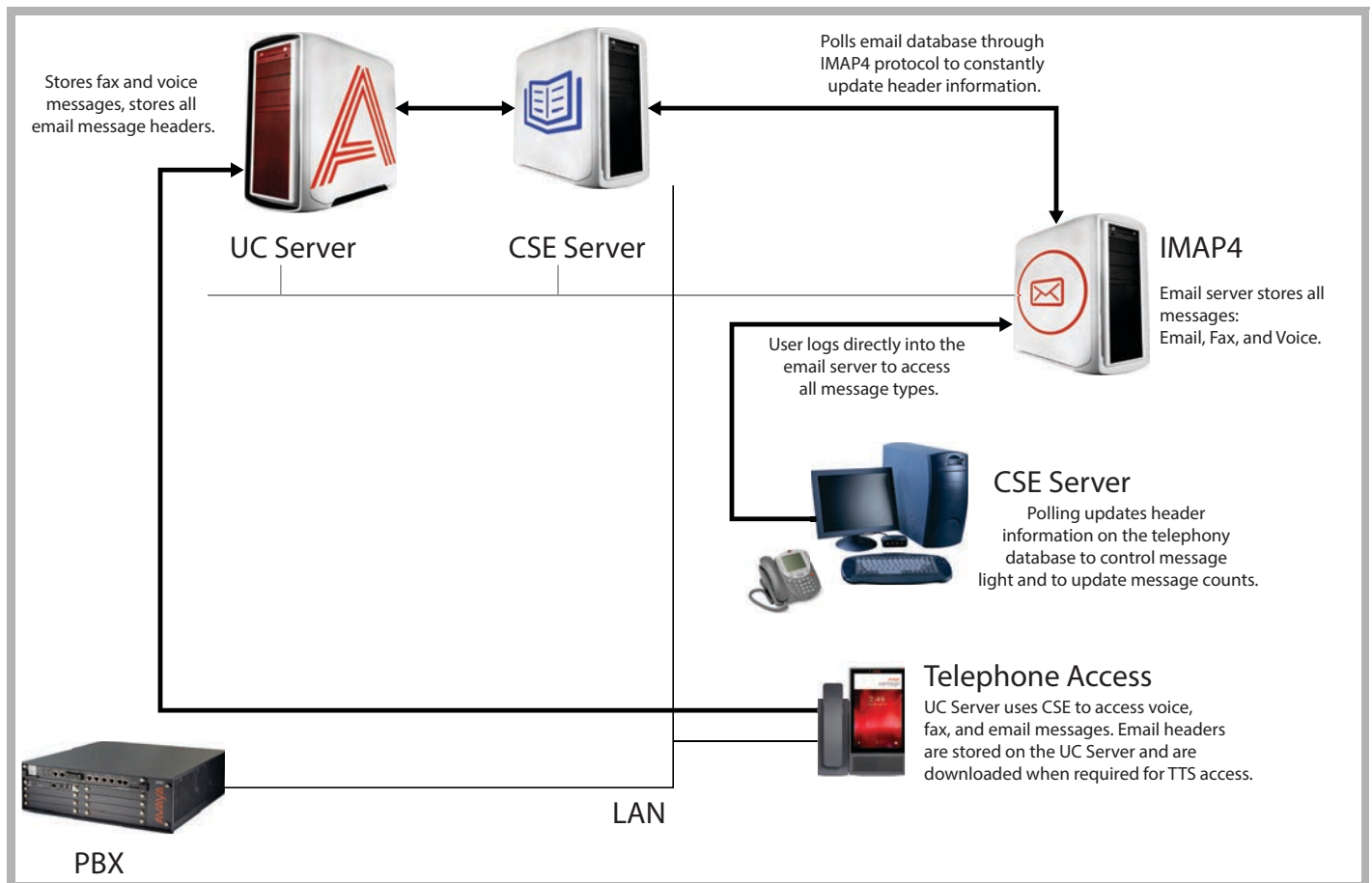

Voice

LAN

PSTN

UC Server

Voice and fax messages are deposited to the UC Server, then forwarded to the eMail server via SMTP.

eMail Server

PBX

IX Messaging user logs directly into eMail Server to access all messages.

IM Using SMTP Forwarding (Scenario #1)

Deployment: Advanced Unified Messaging

Unified Messaging is a unified view and single point of management for phone, web, and email messages.

CSE (Content Synchronization Engine) / CSE Gateway

The CSE gateway connects directly to the current email server for synchronized message access. Email servers currently supported include Exchange 2010 / 2013, and Gmail (Google Apps).

CSE polls the messaging servers on a schedule determined by the System Administrator. At the time of the poll, actions and changes are synchronized. Although polling activity on the Messaging Server does use a lot of CPU resources the service is low priority and uses CPU resources only as they become available. Any time another service or process requires CPU resources the polling service releases the needed resources. This applies to Gmail. For Exchange 2003/ 2007/2010 please refer to CSE/Email Server Contact Synchronization.

Stores fax and voice messages, stores all email message headers.

UC Server

CSE Server

Polls email database through IMAP4 protocol to constantly update header information.

IMAP4
Email server stores all messages:
Email, Fax, and Voice.

User logs directly into the email server to access all message types.

CSE Server
Polling updates header information on the telephony database to control message light and to update message counts.

Telephone Access
UC Server uses CSE to access voice, fax, and email messages. Email headers are stored on the UC Server and are downloaded when required for TTS access.

LAN

PBX

CSE Deployment

Microsoft Exchange Configurations

- Although Exchange can be in Mixed mode, an additional CSE Gateway must be purchased for each separate Exchange Server (i.e. non-clustered).

- Active Directory in Mixed mode is supported.

- UC deployments cause a considerable increase in transaction log activity on the Exchange Server. Make sure you have enough available hard disk storage space for additional logging. The general rule (how much space required for logging after UC implementation) is twice your current logging storage requirements.

- In order to perform synchronization with the mail store the CSE Gateway will connect to the Exchange server which will increase overall system traffic. This in turn can cause an increase in the amount of transaction logs generated by Exchange. In addition the CSE Gateway will increase the size of the message store within Exchange. This, in combination of with the above, results in a higher growth rate of transaction logs. These increases are discussed at the following online links:

  http://technet.microsoft.com/en-us/library/aa996118.aspx#TheStmFile
  http://forums.msexchange.org/m_1800422107/mpage_1/tm.htm#1800422251

- The structure of the .STM and set of operations recorded into the transaction logs while working with the .STM might be different from operations with the .EDB (standard part of the message store).

Make sure your Exchange Server meets Microsoft's recommended minimum specifications prior to deploying UC.

9 FREQUENTLY ASKED QUESTIONS

Included are the 10 most viewed solutions, and the 10 with the highest customer ratings.

Top Viewed

A Best practices for installing Windows Updates.

A How to setup Message Waiting Indicators for Mitel integration.

A Transfer not working on SIP systems.

A Set up CSE server in IXM Admin to synch with Google Gmail.

A SMTP Forwarding not working.

A How to setup up remote admin.

A Call voicemail and the system asks for MBX number not password.

A iLink Pro Desktop does not login.

A Say date and time or caller ID.

Top Rated

A Does iLink Pro Desktop work with Outlook 2007?

A Notification to cell.

A Setting a custom TUI to play message count.

A Faxing out of Avaya Messaging and back to the same system fails.

A iLink Pro Desktop does not login.

A The UC License is not available on the voicemail server.

A Web Access cannot be displayed.

A Say date and time or caller ID.

A What operating systems are supported by Messaging?

A After adding a PDF license, incoming faxes are still TIFF files.

Top Viewed Solutions

◇ Best practices for installing Windows Updates.

In order to prevent unexpected down time, Avaya recommends that Windows Updates be set to Download updates but let me choose whether to install them. With this setting the user can schedule an appropriate time to install the upgrades with a minimum of disruption since a system reboot is usually required.

Avaya tests all windows updates as they are released and if any cause conflicts with our software, a technical bulletin will be released and a knowledge base article is created. Contact Avaya Customer Support for further information.

Ⓐ Back to top

◇ How to setup Message Waiting Indicators for Mitel integration.

Setting up MWI lights requires Host Command Interface (**HCI**) on the 3300. Messaging 7.1+ requires a Mitel 3300 Integrated Communications Platform (**ICP**) using Direct SIP.

1. In the Mitai Configuration wizard, define HCI.

2. In the SIP Configuration wizard, on the General tab, the Voice Port Alias must have HCI defined.

3. In IXM Admin, go to Configuration > Device Management Settings > CTI Settings. Enable CTI Installed. Set CTI Mode to Mitai and enable CTI Multiple Message Lights.

4. In IXM Admin, go to PBX Properties. On the Message Light tab, enable CTI.

Ⓐ Back to top

◇ Transfer not working on SIP systems.

Transfers to any number are not working on SIP systems when you call into the auto attendant and transfer to an internal or external number. The voicemail seems to perform the transfer but then the call is dropped.

For a call to be transferred, the system must put the call on hold. If the call gives Anonymous@anonymous.invalid as contact info, then the system cannot put this call on hold since there is no specific call information to pass to the PBX. This can be seen by running a Wireshark trace and using a SIP filter. The Invite packet of the call contains a From field with Anonymous@anonymous.invalid.

Ⓐ Back to top

◇ SMTP Forwarding not working.

SMTP Forwarding is not working. When checking the VPIM log, voicemail does connect to the email server but the message is rejected. The log shows **Client Not Authenticated** because the email server is looking for SMTP authentication which is not supported.

STMP Authentication must be disabled on the email server.

Ⓐ Back to top

◇ How to setup up remote admin.

Remote Admin allows system administrators and support personnel to remotely access IXM Admin from a workstation. However, using Remote Admin means that more than one person can be modifying the database at one time. If two or more people make changes to the same entry, some changes may be overwritten without notification. The maximum number of people that can connect through Remote Admin is 5. IXM Admin must be installed on each workstation where Remote Admin is to be used.

1. Insert the Messaging installation DVD. Browse to the root folder and double-click **TOLEE_Admin.exe**.

2. Click Next to continue with the installation.

3. Select the drive where Remote Admin will be installed. Click Next.

4. Confirm the selection, and then click Next to begin copying the files.

5. Click Finish when completed.

Remote Admin is now ready to be used. A shortcut has been placed on the Windows desktop for convenience.

A Back to top

◇ Call voicemail and the system asks for MBX number not password.

When calling into the voicemail server to retrieve messages, the system should prompt for the mailbox password, but it is asking for the mailbox number instead. This occurs when more than one mailbox has the same extension.

In IXM Admin, go to the Mailbox Structure > Addresses tab. Review all listed addresses to find one with the same extension. Remove the extension from the other mailbox.

A Back to top

◇ iLink Pro Desktop does not login.

iLink Pro Desktop is not logging in, even when right-clicking and selecting Login.

Ensure that the IP address entered in Settings correctly points to the voicemail server, then restart the **UC Unified Messaging System Tasks Service**.

A Back to top

◇ Say date and time or caller ID.

Starting with Messaging 8.x, caller ID and message delivery information are not heard. Users do not hear the date, time or caller ID of a message even when pressing the key for Envelope Information in the TUI.

In 8.X, Caller ID, date, time and delivery flags (i.e. urgent, important, etc.) for a message are part of the **Message Envelope**. To activate the function, open the TUI associated with the mailbox and in sub menu 2, open **Envelope Information** and enable the options you want to include in the playback.

A Back to top

Top Rated Solutions

◇ Does iLink Pro Desktop work with Outlook 2007?

Avaya Messaging version 7.1+ will integrate with Outlook 2007.

A Back to top

◇ Notification to cell.

Set up a mailbox to outcall to a cellphone for notifications. After leaving a message, the cell does not ring, and the ports are not making an outcall.

Make sure that Notification has a schedule setup, and the schedule has a Default Address. If the notification is to a single cellphone, do not enable Cascade Notification on the Options tab.

A Back to top

◇ Setting a custom TUI to play message count.

Calling into a mailbox does not play the new message count.

To play, it must be enabled on the Custom TUI. On the Custom TUI, click on **Announcements**, enable **Play message count** and select **Read** and **Unread**.

Save the TUI.

A Back to top

◇ Faxing out of Avaya Messaging and back to the same system fails.

Faxing a doc to another employee on the same voicemail system does not work. The fax is sent out on one port and comes in on another, taking 2 ports of the voicemail fax setup.

However, faxing to another address on the same voicemail system is not supported. Internal users can only send a fax to a fax machine internally. Faxing to external numbers is not affected.

A Back to top

◇ iLink Pro Desktop does not login.

iLink Pro Desktop is not logging in, even when right-clicking and selecting Login.

Ensure that the IP address entered in Settings correctly points to the voicemail server, then restart the **UC Unified Messaging System Tasks Service**.

A Back to top

◇ The UC License is not available on the voicemail server.

When going to **Start > Programs > Office-LinX > UCLicenseUpgrade**, the system displays **Error 70. Cannot read license**.

This will occur when connecting to the voice server using Remote Desktop. Sign in on the server machine itself, or access it remotely through another a remote client application, such as Logmein or VNC.

A Back to top

◇ Web Access cannot be displayed.

When attempting to launch Web Access through a browser, the screen does not load and there is an error message saying **The page cannot be displayed** or **Not authorized to view the page**.

On the voice server (Windows Server O/S): Go to Administrative Tools > Computer Management > Local Users and Groups, select **UCIISUser** and click **Reset Password**. Then go to Computer Management > Services and Applications > Internet Information Services (IIS) > Web Sites > Default Web Site > UC. Right-click **Properties** and select **Directory Security**. Choose Edit under Authentication and Access Control. Make sure the user UCIISUser has the necessary rights and click Reset Password.

Restart the World Wide Web Service.

A Back to top

◇ Say date and time or caller ID.

Starting with Messaging 8.x, caller ID and message delivery information are not heard. Users do not hear the date, time or caller ID of a message even when pressing the key for Envelope Information in the TUI.

In 8.X, Caller ID, date, time and delivery flags (i.e. urgent, important, etc.) for a message are part of the **Message Envelope**. To activate the function, open the TUI associated with the mailbox and in sub menu 2, open **Envelope Information** and enable the options you want to include in the playback.

A Back to top

◇ What operating systems are supported by Messaging?

All versions between >=8.0 and <9.0 support XP and WIN 7, Windows Server 2003 and 2008 (32 and 64-bit). OL versions **9.0+** support **Windows 7 and 8**, and **Windows Server 2008**, **2012**, **2016** and **2019**.

A Back to top

◇ After adding a PDF license, incoming faxes are still TIFF files.

After applying the PDF license and rebooting, incoming faxes are still TIFF files even though the VPIM is set to PDF. This is a voicemail issue where the VPIM server version and PDF library are not installed. Please call support for assistance with replacing the VPIM server and adding the PDF library.

A Back to top

APPENDIX A: REVISION HISTORY

Date	Issue	Change Summary
3 October, 2019	1	Initial document release.
31 October, 2019	2	Updated list of ports.
6 November, 2019	3	Modified Maximum System Capacity requirements.
11 November, 2019	4	Clean-up of some out-of-date information (e.g. supported O/S, CPU requirements, etc.).
14 November, 2019	5	Since support has been added for IPv6, removed the note saying otherwise.
20 February, 2020	6	Modified VMWare Chapter to include HA functions for the Primary as well as the Consolidated servers.
25 February, 2020	7	Changed Ch4 title to System Requirements and Capacity to make it clear what is inside. Added subtitle to main page.
25 March, 2020	8	Made changes to the Feature Comparison table to synch with other sources.
9 April, 2020	9	Removed references to Lotus Notes, Mercury Mail, SLMail, Infolink, IMail, First Class and Domino.
14 May,2020	10	Removed leftover references to TSE in favor of CSE.
24 June, 2020	11	Added specifications for HA Geo Redundancy.
28 October, 2020	12a	Included a note that each Remote CSE Server can only support a single email type.
4 January, 2021	13	Updated O/S requirements including Windows Server 2019 throughout.
6 July, 2021	14	Included requirement for all installations to include RAID 10 hard drive array.
28 July, 2021	15	Removed support for vMotion.
30 July, 2021	16	Emphasized restrictions on migrating to a virtual machine, and moving from a VM environment.
01 October, 2021	17	Added Nuance Watcher Daemon to the TCP/IP port usage table.
20 October, 2021	18	Removed table of virtual hardware requirements that applied only to Avaya Aura Messaging. Removed IMAP4 and POP3 references as they are no longer supported.
6 January, 2022	19	Removed TCP/IP port requirement for SMTP VPIM.