MAX Communication Server
Release 9.0.1

Upgrade Guide

January 2021

WARNING! Toll fraud is committed when individuals unlawfully gain access to customer telecommunication systems. This is a criminal offense. Currently, we do not know of any telecommunications system that is immune to this type of criminal activity. AltiGen® Communications, Inc. will not accept liability for any damages, including long distance charges, which result from unauthorized and/or unlawful use. Although Altigen Communications, Inc. has designed security features into its products, it is your sole responsibility to use the security features and to establish security practices within your company, including training, security awareness, and call auditing.

NOTICE: While every effort has been made to ensure accuracy, Altigen Communications, Inc., will not be liable for technical or editorial errors or omissions contained within the documentation. The information contained in this documentation is subject to change without notice.
This documentation may be used only in accordance with the terms of the Altigen Communications, Inc., License Agreement.

Altigen Communications, Inc.
670 N. McCarthy Boulevard, Suite 200
Milpitas, CA 95035 USA
Telephone: 888-Altigen (258-4436)
Fax: 408-597-9020
E-mail: info@altigen.com
Web site: www.altigen.com

Contents

Enhancement Included in This Release 4

Requirements 4

General Considerations 4

Software Upgrade Path 4

Upgrade Procedures for MaxCS Private Cloud 4

Migrating Premise Deployments to Private Cloud 6

Port Information 6

Troubleshooting 6

This document provides guidelines for upgrading from an earlier version of MaxCS to release 9.0 Upgrade 1.

Enhancement Included in This Release

For a list of new features and enhancements that are included in this release, refer to the *MaxCS 9.0.1 New Features Guide*.

Requirements

For full component requirements, refer to the *MaxCS All-Software Solution Deployment Guide*.

This release supports Softswitch SAAS and MaxCS-hosted Private Cloud.

General Considerations

- **NFR** – If you are upgrading an NFR system with MaxCS Release 8.0 or earlier, you must obtain the new license file (EXCTL.DAT) **before** you begin the upgrade process. Otherwise, your licenses will become invalid after you perform the upgrade.
- With MaxCS Private Cloud and SaaS-licensed systems, the MaxCS server will check with the AltiGen licensing server when switching starts, and will automatically retrieve the appropriate licensing.
- **MaxCall** – If you use MaxCall, you will need to copy the MaxCall phrases in the C:\PostOffice\App\MaxCall folder to a temporary folder, then copy them back to the folder after the upgrade has been completed.

Software Upgrade Path

You can upgrade MaxCS Release 8.5 and later directly to Release 9.0.1.

If your version of MaxCS is earlier than Release 8.5, follow this process:

1. Upgrade to Release 8.5 (refer to the *MaxCS 8.5 Upgrade Guide*).
2. Upgrade from Release 8.5 directly to Release 9.0.1.

Upgrade Procedures for MaxCS Private Cloud

It is critical to follow the upgrade instructions to avoid losing any configuration data.

You will need to download the Release 9.0.1 zipped files; get these from your Altigen representative or the Altigen Partner portal.

1. Review the *Exchange Integration* chapter in the *MaxCS Administration Manual,* along with the *New Features Guide*, before you begin. This will alert you to any changes that you may need to make to your configuration.
2. If there are any IP Dialing Table entries that have the Protocol set to *H.323,* update them to change the Protocol to *SIP*.

3. Log in to Windows as a domain or local user account that has local administrator privileges. If your machine is a stand-alone server, you must log in as a local administrator account. If you plan to run Exchange Integration, you must have domain administrator rights.
4. **IMPORTANT: Run the *Backup & Restore* tool** to back up the existing configuration, voice mail messages, and greetings.
5. Perform the product registration process from the MaxAdministrator *License Information* page (either online or offline registration) and obtain the EXCTL.DAT license activation file from the Altigen Product Registration portal.

   Exception: No product registration is required when upgrading directly from 8.6.x.x to 9.0.1.
6. For Softswitch deployments, install and run the MaxCS HMCP Certification tool. The instructions for running this tool are found in the *MaxCS Softswitch Deployment Guide*.
7. Run the **AltiGen Start & Stop Services** utility to stop all Altigen services.
8. Unzip the downloaded MaxCS 9.0 installation files into a temporary folder on the MaxCS server. In the folder where you extracted the zipped files, run SETUP.EXE in the MAXCS ACM folder.
9. During the installation wizard, when you are prompted whether to register. For MaxCS Private Cloud upgrades, choose **Register Later**. The MaxCS server will check with the Altigen licensing server when switching starts, and will automatically retrieve the appropriate licensing.
10. Reboot the server after the installation process has finished.
11. If you have not already imported your own certificate (in your previous release), then **request an Altigen certificate.** In MaxAdministrator, choose **System** > **Request Certificate**.

    WARNING: ***DO NOT request a certificate*** if you have already imported your own. If you do, your imported certificate will be overwritten!
12. If you downloaded an Altigen certificate in the preceding step, reboot the server again.
13. If you want your Polycom VVX phones to immediately update to any new firmware version in this release, follow these steps:
    a. Open MaxAdministrator and select **System** > **Polycom Configuration**.
    b. Check the *Enable Polycom VVX firmware automatic upgrade* option.
    c. Check each VVX phone’s extension settings, to set each phone’s enable/disable auto-update setting. This is found in **PBX** > **Altigen IP Phone Configuration** on the *Polycom* tab.
    d. If you find that your VVX phones are not updating or registering automatically, you may need to boot the server again to make sure that the phones all apply the new certificate and firmware.
14. Check your SIP Trunk configuration and make any necessary adjustments.
15. Client applications need to be upgraded to the newer version only if they are incompatible with the new MaxCS version. Note that if you do upgrade client applications for a user, then you must update **all** the MaxCS client application on a user’s desktop before the agent uses any of those applications.
16. If you plan to enforce TLS version 1.2 whenever TLS is used, upgrade your IP-705, IP-710, and IP-720 phone firmware to the latest supported version (2xB3 or later).

17. Review the information on the new features and adjust your configuration as needed, including the new password requirements.
18. For Private Cloud deployments, update all components (including External Logger, VRM, and for call centers, AltiReport), even if you are not using those components.

Note: For customers running Windows Defender: If your MaxCS server is running Windows Defender, we recommend that you add the following to Windows Defender's exclusion folder: "AltiDB", "AltiServ" and "Postoffice" (for performance reasons). If you are using VRM Pro or a voice recording feature, you may also want to add the recording folder to Windows Defender's exclusion folder.

Migrating Premise Deployments to Private Cloud

For instructions on migrating a MaxCS on-premise deployment (on a hardware chassis) to MaxCS Private Cloud, follow the steps in Article 1172, which is available from the AltiGen Knowledgebase. Click here to log in and open that document.

For any upgrade issues or questions, please contact AltiGen Technical Support.

Port Information

- When MaxCS or Softswitch is running on a non-Windows 2008/2012R2/2016/2019 system, BasePort = 49152.

  When MaxCS or Softswitch is running on a Windows 2008/2012R2/2016/2019 system, BasePort = 49664 (because those versions have some system services that use ports in the 49152 range). Check your firewall settings and reconfigure them if necessary.

- This release uses internal network port 10072 to work with the client applications. Other applications on the users’ system should not use this port. Since this is for internal use, no firewall setting should be configured for this port.

- For the MaxCommunicator Web application, additional ports are needed. Refer to the Installation Guide for MaxCommunicator Web, and to the readme file for that application.

Troubleshooting

- If during the upgrade process you see a warning message, “'Remove previous version and update first and then reboot machine to continue the installation' you will need to remove the earlier version manually.

  If you cannot find the earlier release in the Control Panel “Uninistall or Change Programs” page, follow these steps to remove the software (always follow Microsoft guidelines when editing the registry):

  1. Open the registry editor.
  2. Remove the folder *AltiGenInstallTemp*.
  3. Set this entry:
     \HKEY_LOCAL_MACHINE\SOFTWARE\AltiGenInstallTemp
  4. Save the changes.

5. Reboot the server. The MaxCS installation should run automatically.

- If you are using SNMP setting, back up the file snmpcfg.dat under altiserv\db folder. After you complete the upgrade process, if the SNMP configuration is lost:
    1. Shut down the MaxCS services using "Start & Stop All AltiGen Services."
    2. Then restore the snmpcfg.data file and restart the AltiGen services.