

# MaxCS 9.0.1 Service Hub and Web Apps Deployment Guide

May 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.

MAX Communication Server, MaxAdministrator, MaxCommunicator, MaxAgent, MaxSupervisor, MaxOutlook, MaxInSight, MaxCall, Altiserv®, Altalink, Alticonsole, VRPlayer, Zoomerang, IPTalk, Alt-Mobile Extension, InTouch Dialer, and Altireport are trademarks or registered trademarks of Altigen Communications, Inc. All other brand names mentioned are trademarks or registered trademarks of their respective manufacturers.

Altigen's products are protected under one or more of the following U.S. patents, with other U.S. patents pending: 6532230; 6192344; 6292549; 6493439; 6909780; 6738465; 6754202; 6766006; 6928078; 6909709; 6956848; 7058047; 7013007; 7027578; 7280649; 7308092.

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](mailto:info@altigen.com)  
Web site: [www.altigen.com](http://www.altigen.com)

Copyright © Altigen Communications, Inc. 2021. All rights reserved.

# Contents

About This Guide .....	4
Web Server Public IP Address and FQDN .....	4
Create Application Database .....	5
Deploying the Service Hub.....	5
Step 1. Run the InstallShield Wizard.....	5
Step 2. Install a certificate for the Service Hub to support HTTPS connection.....	11
Step3. Login to the Service Hub via HTTPS. ....	12
Opening Firewall Ports .....	13
Deploying WebApps .....	13
Adding Service Hub Users.....	17
Appendix A: Manually Assigned Certificates .....	19

## About This Guide

This guide describes how to install and deploy the MaxCS Service Hub and MaxCS WebApps.

MaxCS Service Hub and MaxCS WebApps are intended for on-premise MaxCS installation. We recommend you install both applications on the same server as MaxCS and use the same database for both applications.

WebApps is a web application suite. In 9.0 Update1, WebApps includes MaxCommunicator Web and Chat.

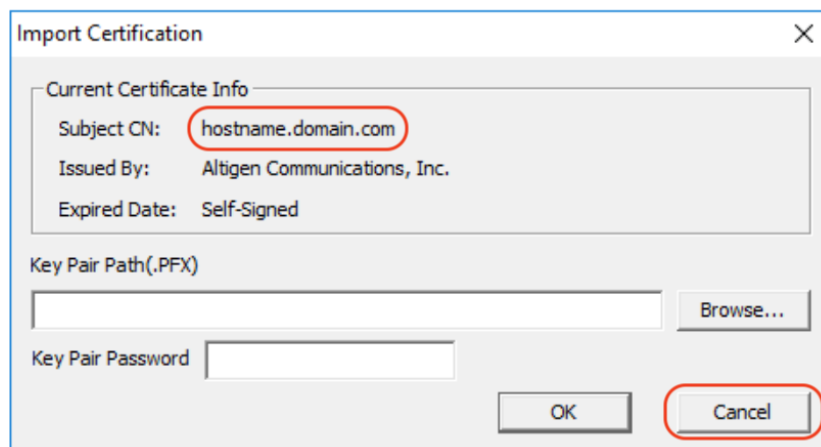
## Web Server Public IP Address and FQDN

If users need to access Service Hub or WebApps from the internet, a public IP address for the servers should be assigned. Also, set up web server's FQDN for Service Hub and WebApps URL access.

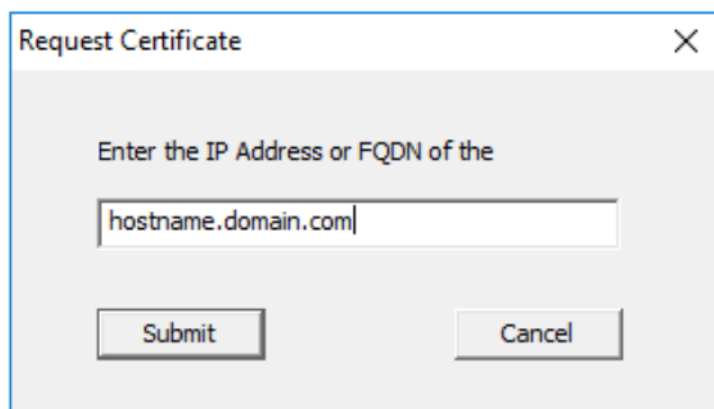
If the MaxCS server is using Polycom Corporate Directory or Recording functionality, two different fully qualified domain names (FQDNs) are required: one for Polycom phones users and the other for WebApps. Both FQDNs need to map to the same MaxCS IP address but must be different FQDNs. For example, hostname.domain.com is the FQDN for Polycom phone and web-hostname.domain.com is for Service Hub and WebApps.

To check if the Polycom service is using an IP address or FQDN, go to **MaxAdmin-> System-> Import Certificate**, check **Subject CN**. Press Cancel after checking.

This screen shows that the Polycom Service is using an FQDN, hostname.domain.com.



1. If your Polycom service is using a FQDN, talk to your IT/ISP to get a second FQDN to deploy Service Hub and WebApps. For example, the existing FQDN for Polycom phones is hostname.domain.com and the WebApps FQDN will be web-hostname.domain.com. You will not need to request a Polycom phone certificate or reconfigure Polycom phones again.
2. If the Polycom service is using an IP address, you need to reconfigure your Polycom phone setting. Talk to your IT/ISP to get Polycom and WebApps FQDNs. To request your certificate, go to **MaxAdmin-> System-> Request Certificate** and type in your Polycom service FQDN.



3. Make sure all the Polycom phones' directory are working correctly before you start to deploy WebApps. Also, make some test calls on your Polycom phones.

---

## Create Application Database

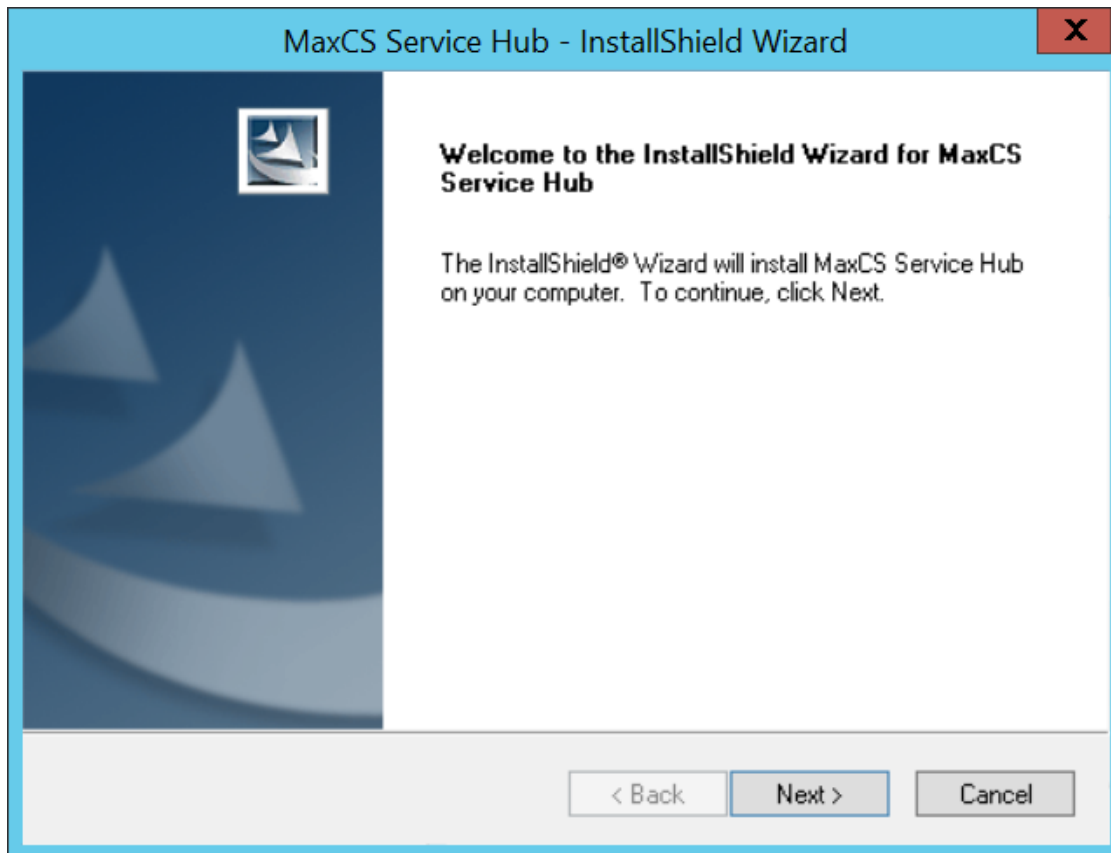
On a Microsoft SQL server, create an Application Database for Service Hub and WebApps and access account.

---

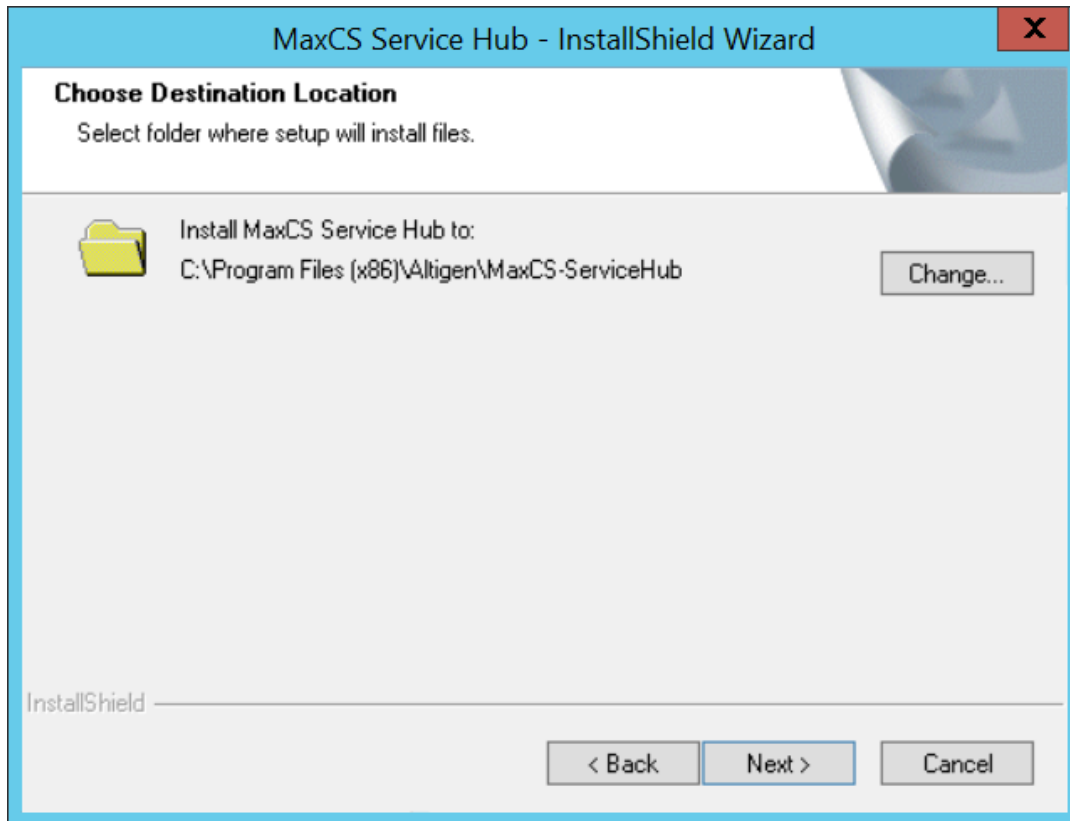
## Deploying the Service Hub

### Step 1. Run the InstallShield Wizard

- 1 In the MaxCSServiceHub folder, run setup.exe to install the on-premise Service Hub. The InstallShield Wizard appears.



- 2 Follow the prompts.



- 3 Select the Web Site. By default, the web site is "Default Web Site".



- 4 Input Application Database access credential information.



MaxCS Service Hub - InstallShield Wizard

**Enter application data database login credential.**

ALTIGEN COMMUNICATIONS

SQL Server Address: 10.40.1.45

SQL Instance: sqlexpress

SQL DB Name: SH1030

SQL DB Account: sa

SQL DB Password: ●●●●●●●●●●

InstallShield

< Back Next > Cancel

MaxCS Service Hub - InstallShield Wizard

**Ready to Install the Program**

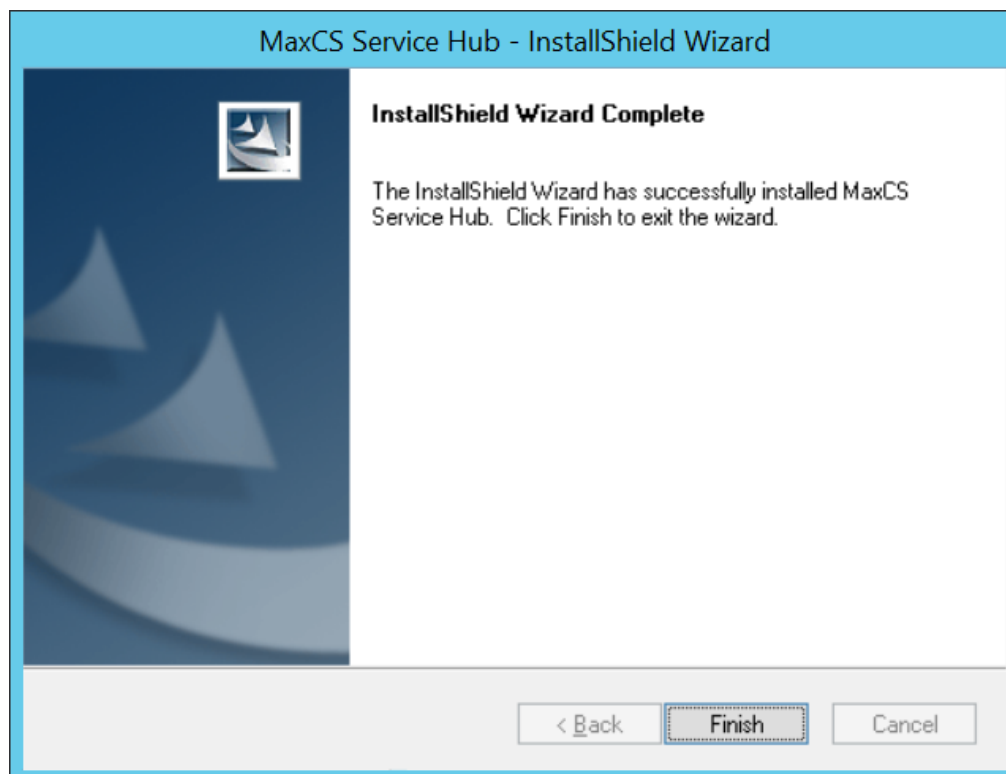
The wizard is ready to begin installation.

Click Install to begin the installation.

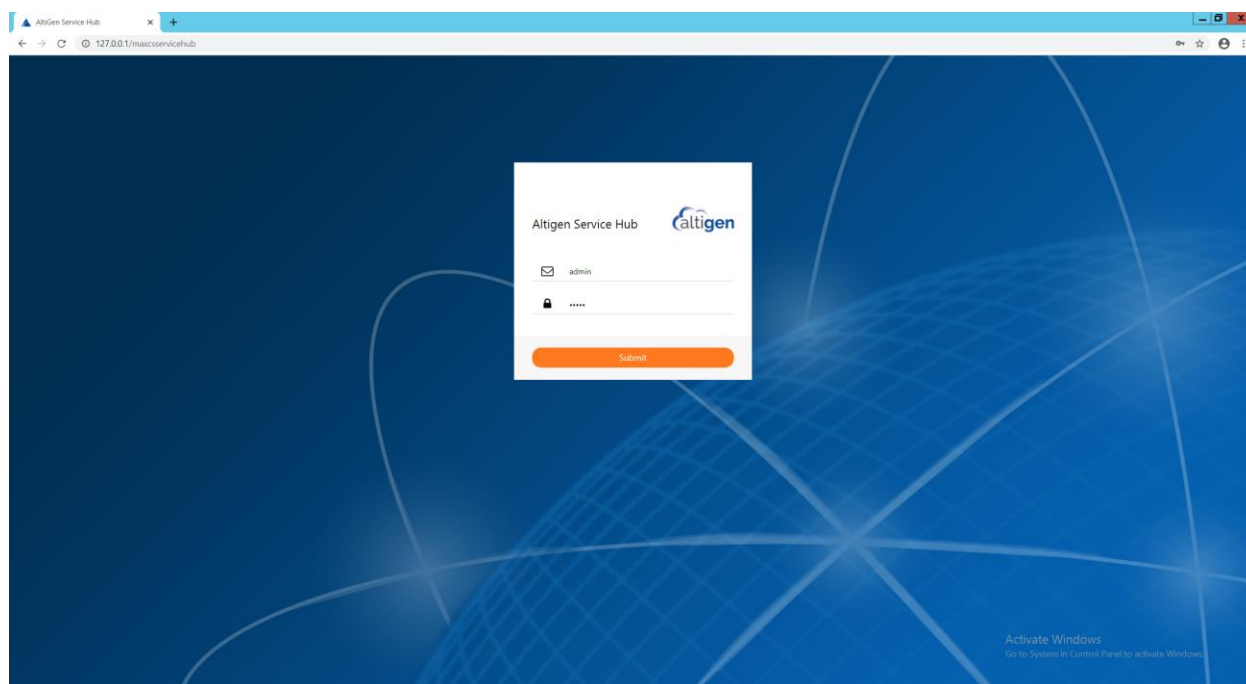
If you want to review or change any of your installation settings, click Back. Click Cancel to exit the wizard.

InstallShield

< Back Install Cancel

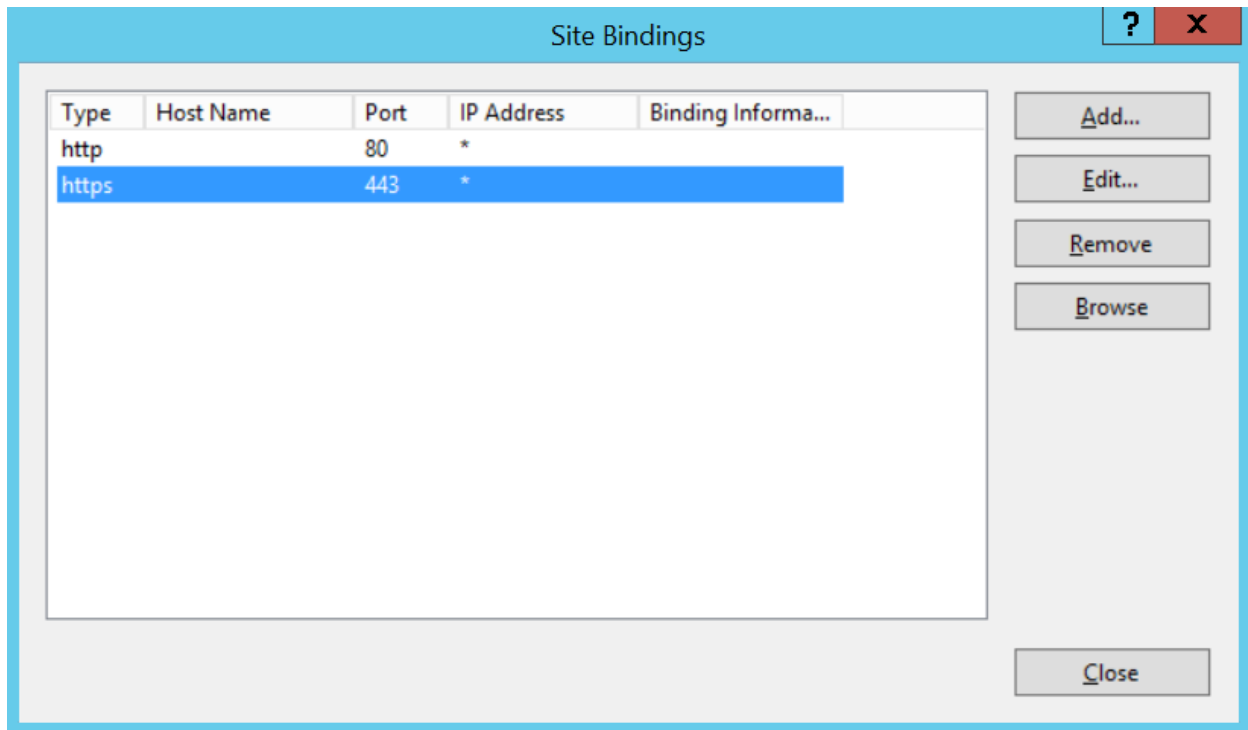


After you've installed the Service Hub successfully, you can access the Service Hub login page from the local server using URL <http://127.0.0.1/maxcsservicehub>.

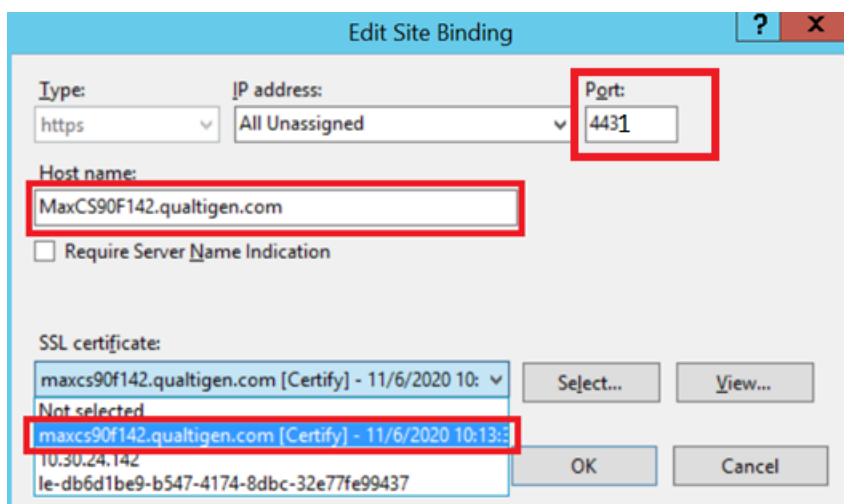


## Step 2. Install a certificate for the Service Hub to support HTTPS connection.

- 1 Obtain a certificate for Service Hub server's FQDN.
- 2 From IIS Manager, edit the Site Bindings (Default Web Site).

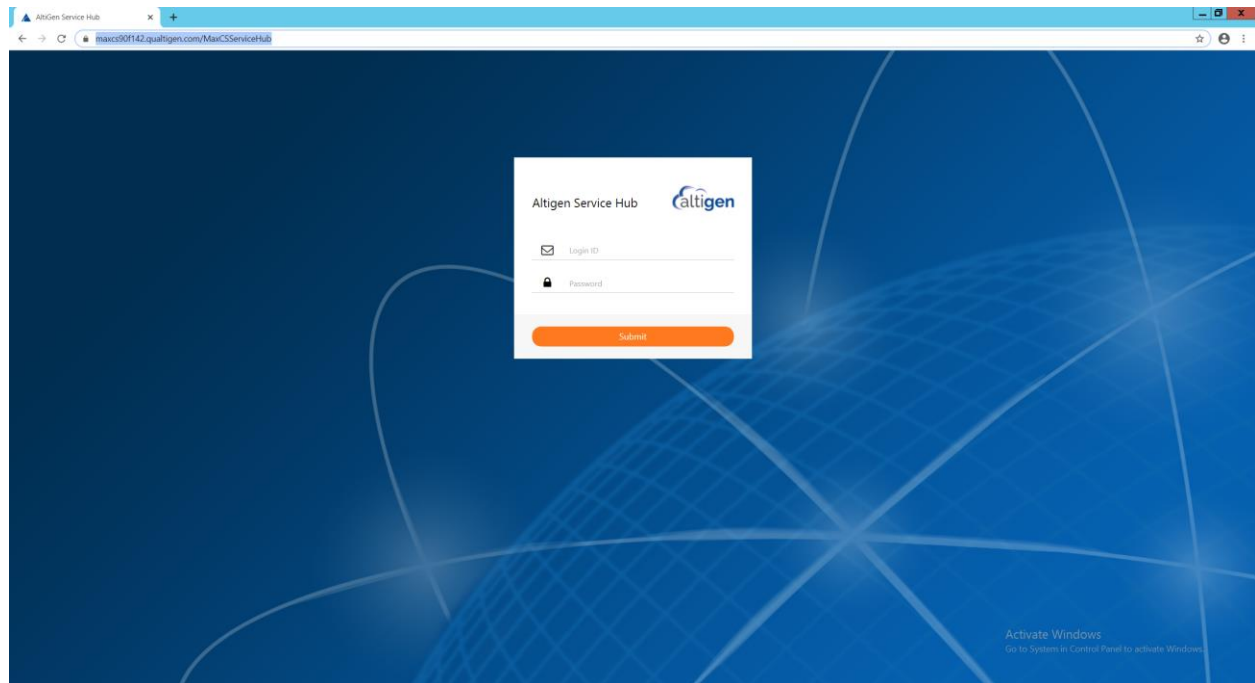


- 3 Assign the certificate just created. Also change the default https port to others, for example: 4431. The default https port 443 will be used by WebApps later.

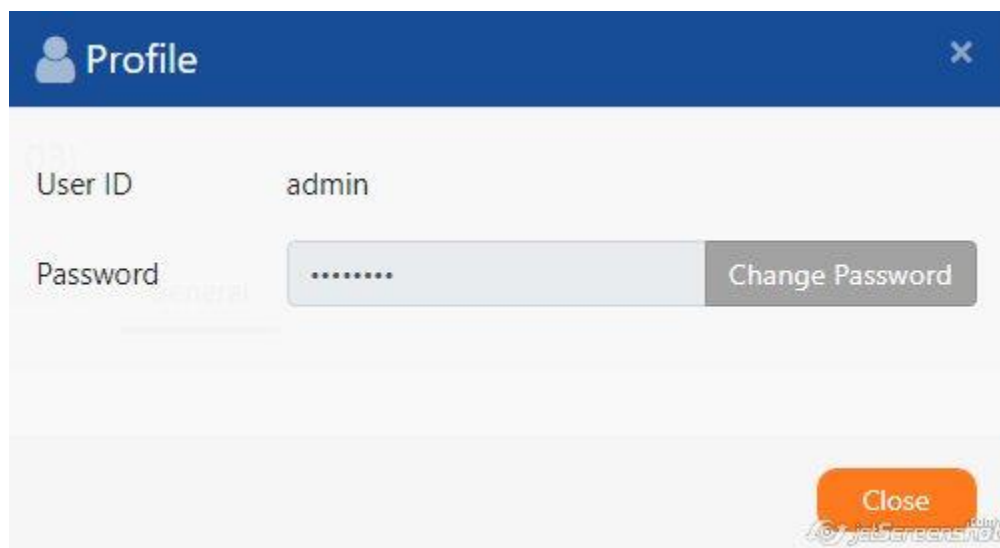


### Step3. Login to the Service Hub via HTTPS.

- 1 In this example we'll access the Service Hub through this URL: <https://maxcs90f142.qualti-gen.com:4431/MaxCSServiceHub>.



- 2 Login using default admin User ID/Password credentials: admin/22222.
- 3 Display the Invoke Profile page and change the admin password.



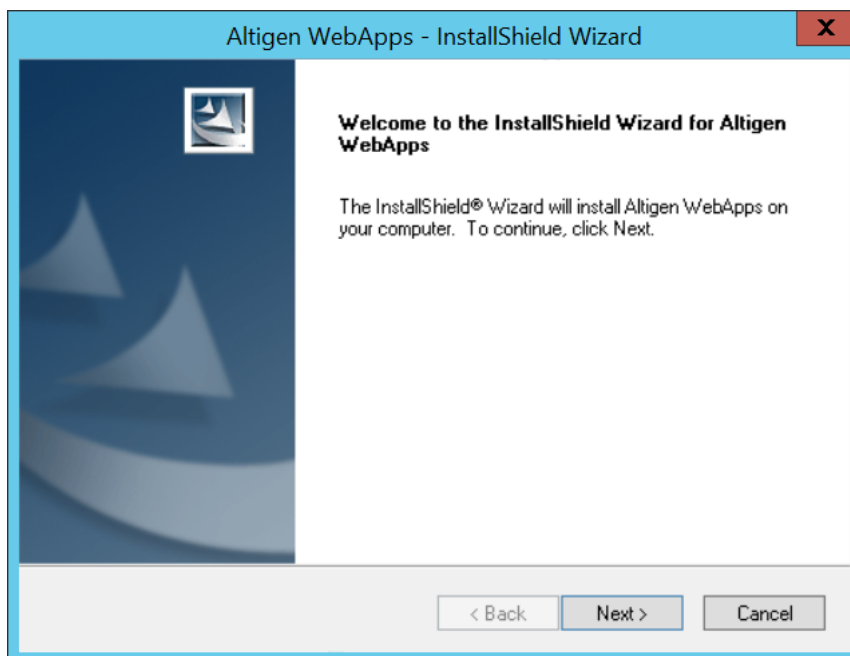
## Opening Firewall Ports

Open the following firewall ports for Service Hub and MaxCommunicator Web applications:

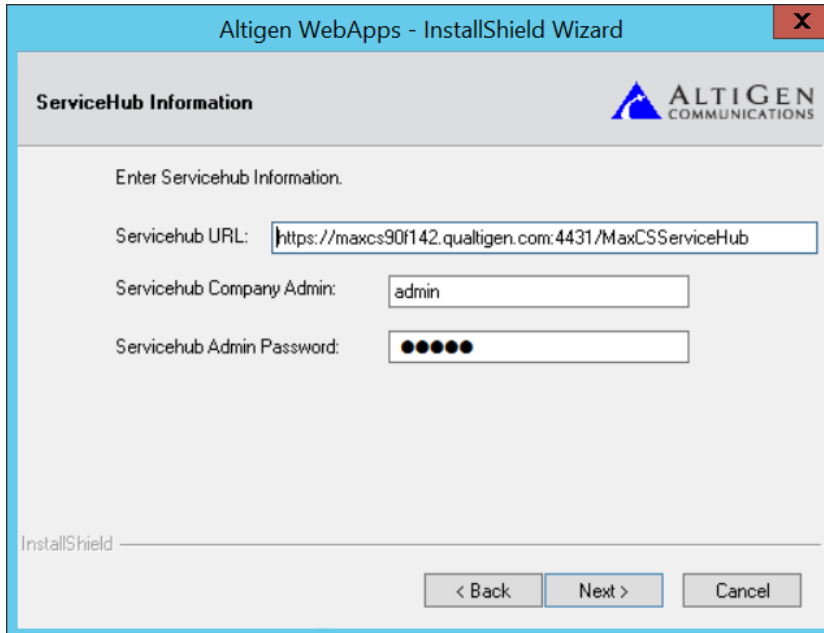
- 4431 – Service Hub (the port is specified by admin during Service Hub installation)
- 8065 – MaxCommunicator Web Chat Server
- 7443 – MaxCommunicator Web
- 443 - MaxCommunicator Web

## Deploying WebApps

- 1 Run setup.exe from the MaxCSWebApps folder.



- 2 Enter the Service Hub URL and login credential information.



**Altigen WebApps - InstallShield Wizard**

**ServiceHub Information**

Enter Servicehub Information.

Servicehub URL:

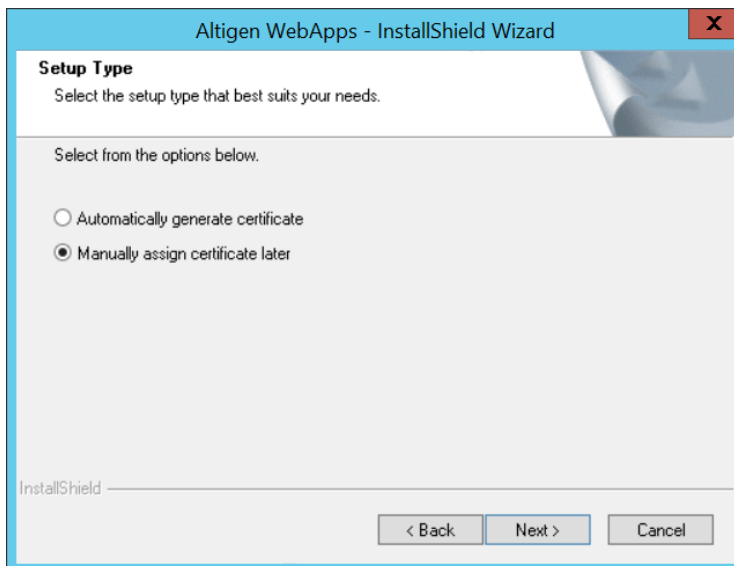
Servicehub Company Admin:

Servicehub Admin Password:

InstallShield

< Back   Next >   Cancel

- 3 You can choose to generate and load the certificate either automatically or manually. If you choose to assign the certificate manually, refer to the Manually Assign Certificate section.



**Altigen WebApps - InstallShield Wizard**

**Setup Type**

Select the setup type that best suits your needs.

Select from the options below.

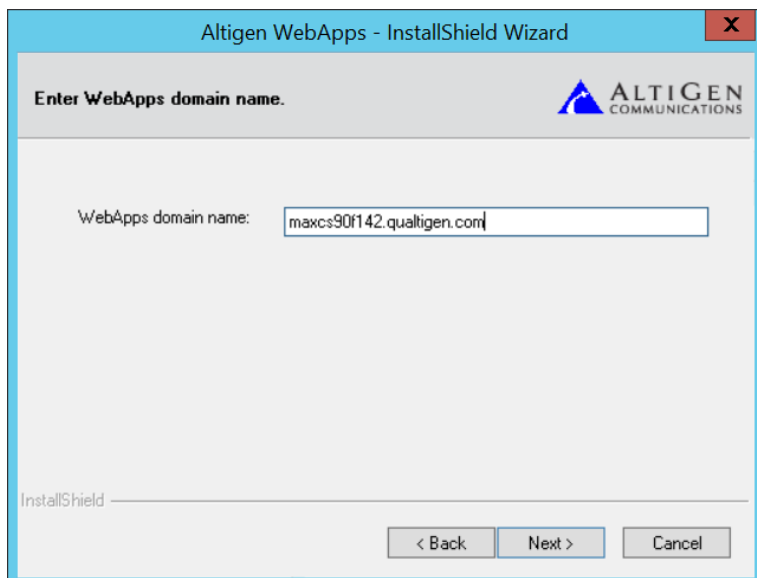
☐ Automatically generate certificate

☒ Manually assign certificate later

InstallShield

< Back   Next >   Cancel

- 4 Enter WebApps server FQDN.



Altigen WebApps - InstallShield Wizard

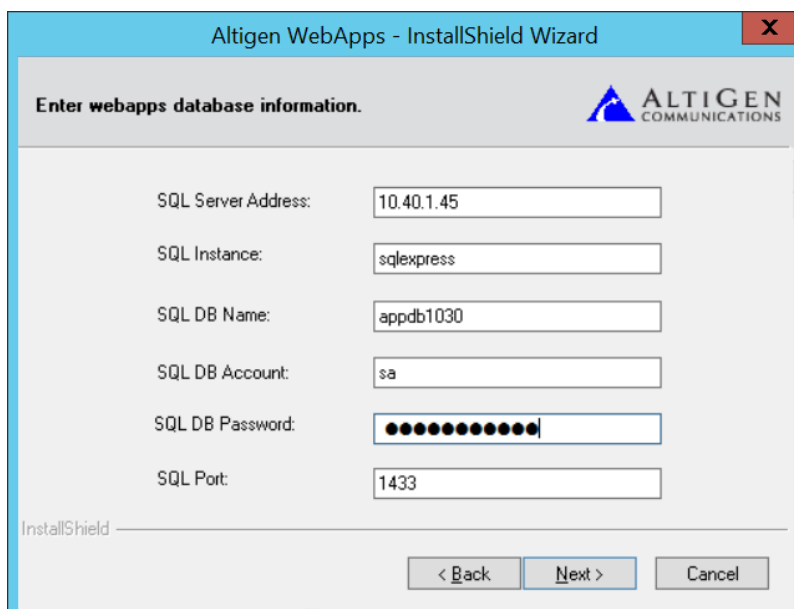
Enter WebApps domain name.

WebApps domain name: maxcs90f142.qualigen.com

InstallShield

< Back Next > Cancel

- 5 Enter Application Database access credential. This should be the same as Service Hub's.



Altigen WebApps - InstallShield Wizard

Enter webapps database information.

SQL Server Address: 10.40.1.45

SQL Instance: sqlexpress

SQL DB Name: appdb1030

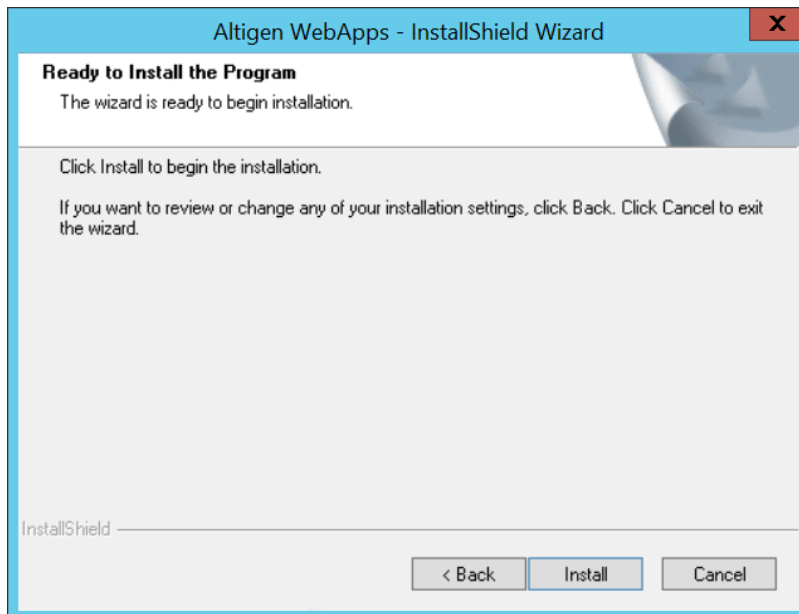
SQL DB Account: sa

SQL DB Password: ●●●●●●●●

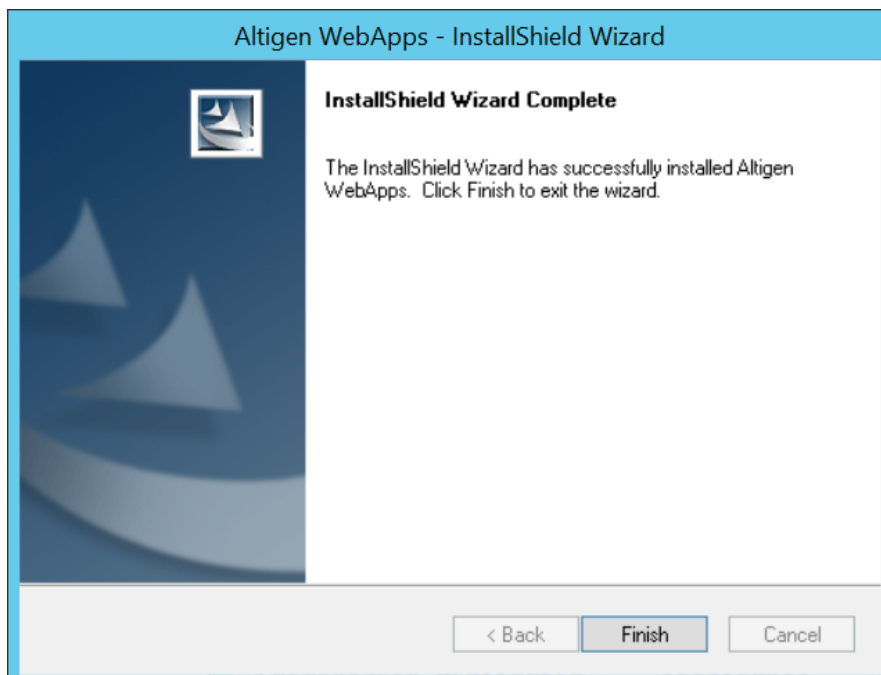
SQL Port: 1433

InstallShield

< Back Next > Cancel



It may take up to 10 minutes to install.

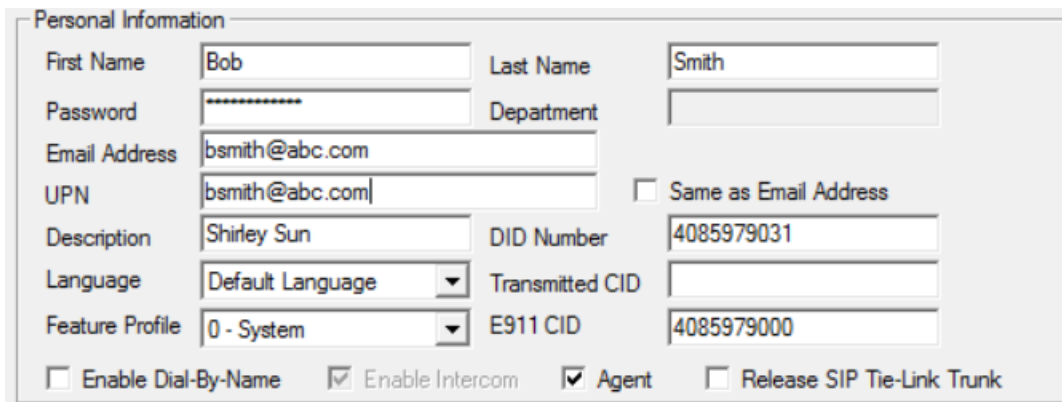




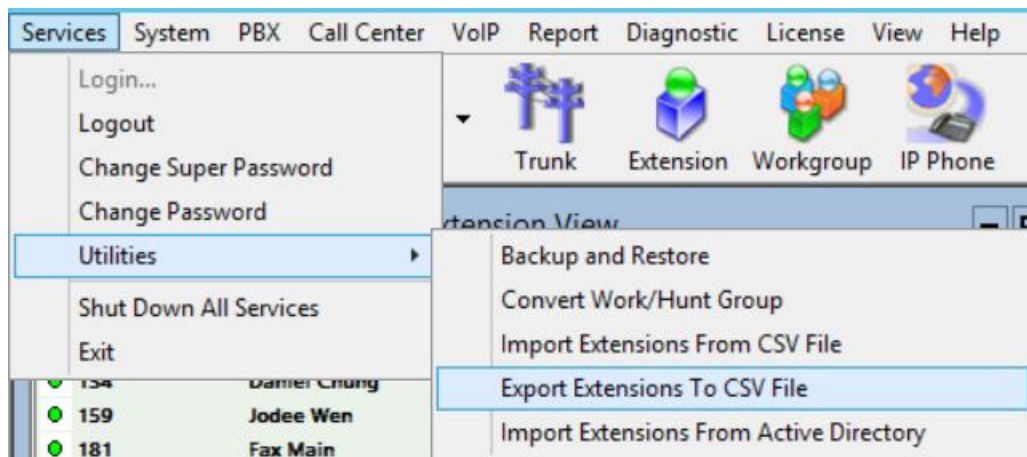
## Adding Service Hub Users

You can import MaxCS extensions to create Service Hub users.

- 1 Go to **Extension > General** in MaxAdmin and set up UPN and Email Address field for the extensions to be imported to Service Hub.
  - UPN is used for Service Hub Login ID.
  - Email Address is used for obtaining contacts and meeting presence from Exchange.



- 2 Export the extensions to a CSV file.



- 3 From Service Hub Settings > General page, import users from this CSV file.

### User Management

Default Password

Import Users

- 4 Set up Service Hub user access for MaxCommunicator Web.

### Capability

☒ Voice

Extension

☒ Chat

### ☒ Admin Privilege

☐ MaxCloud Service Hub Setting

<input type="checkbox"/> Enable	Version	
<input checked="" type="checkbox"/> MaxCommunicator	9.0	<a href="#">View Users</a>

### ☒ User Privilege

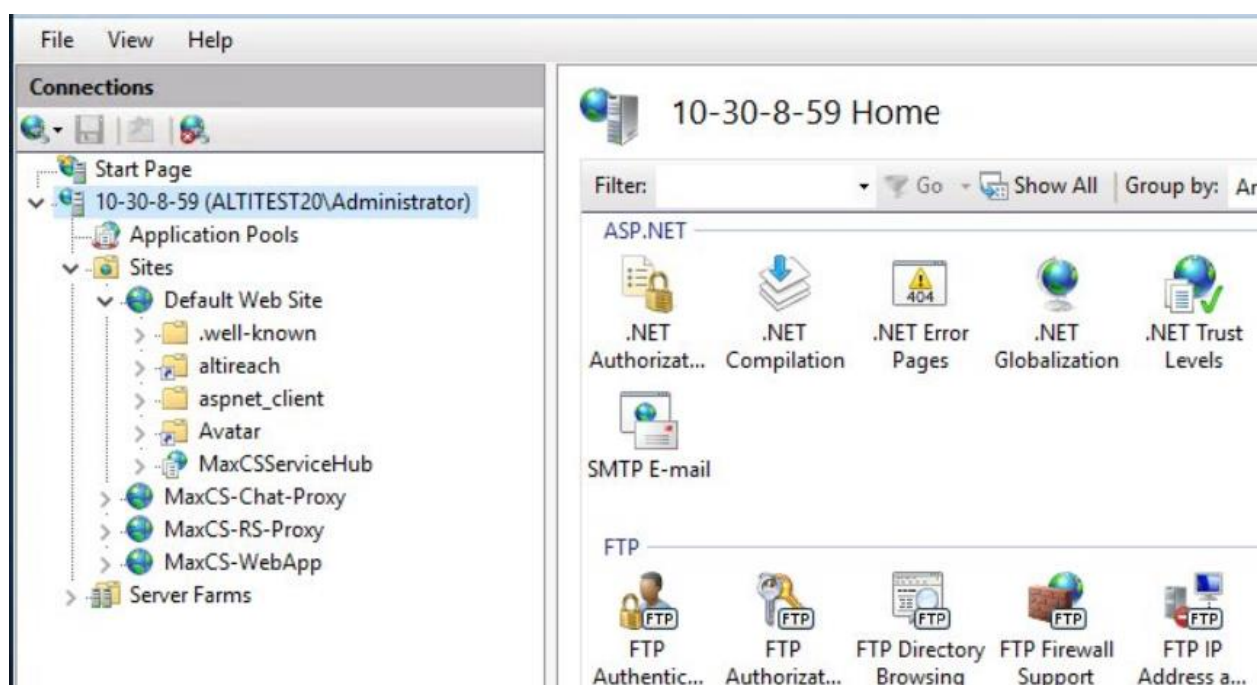
<input type="checkbox"/> Enable	Version	
<input checked="" type="checkbox"/> MaxCommunicator	9.0	<a href="#">View Users</a>

- 5 The admin or user can log into Service Hub to access MaxCommunicator applications.
  - Log into Service Hub using the URL set up for Service Hub deployment: `https://<Service Hub server FQDN>:<port>/MaxCSServiceHub`.
  - Click the MaxCommunicator icon in the Home page to access the application.

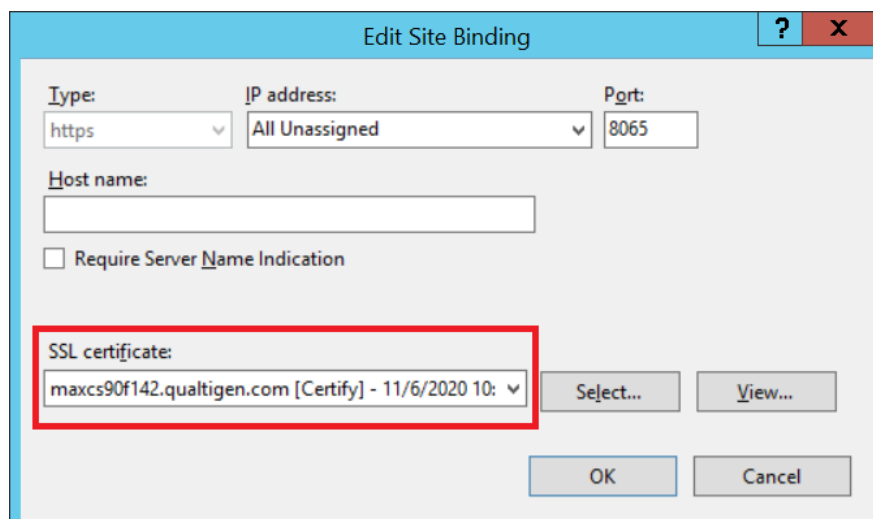
## Appendix A: Manually Assigned Certificates

If you manually assign a certificate to Service Hub and WebApps during installation, here is the information you'll need to obtain the certificate required for the Service Hub and WebApps FQDNs and load it into IIS.

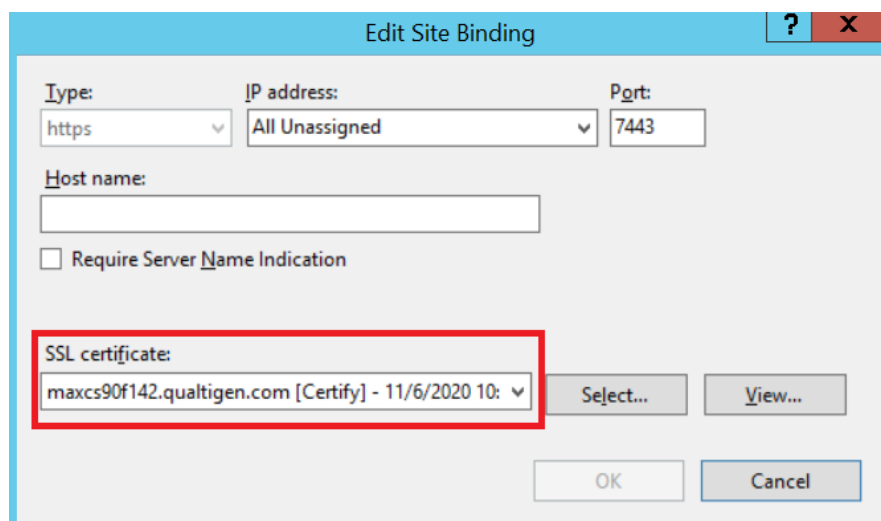
- 1 Go to IIS, select the websites, then right click to choose Edit Binding to load the certificate:
  - For MaxCSServiceHub under Default Web Site, use the specified port during Service Hub installation.
  - For MaxCS-Chat-Proxy, use Port 8065.
  - For MaxCS-RS-Proxy, use Port 7443.
  - For MaxCS-WebApp, use Port 433.



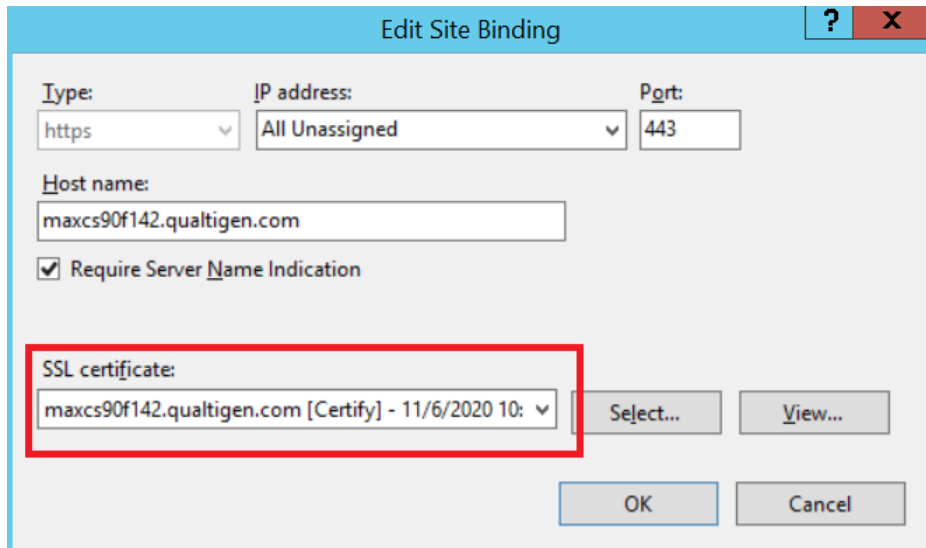
Here is an Edit Binding example for website MaxCS-Chat-Proxy:



Here is an example of Edit Binding for website MaxCS-RS-Proxy.



Here is an example of Edit Binding for MaxCS-WebApp.



Edit Site Binding

Type:  IP address:  Port:

Host name:

☒ Require Server Name Indication

SSL certificate:

- 2 Reboot Windows, then it is ready to go.