altigen

MaxCS Release 9.0.1
Service Hub Guide for Administrators

January 2021

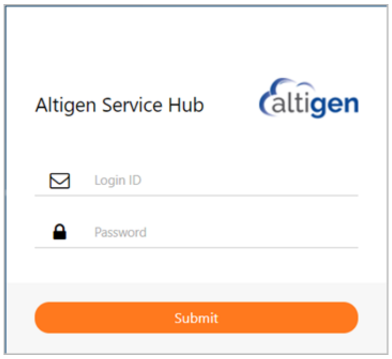
About This Guide

This guide is provided for Company administrators who will manage MaxCS 9.0.1. This release includes a new component, the *Service Hub*. The Service Hub is where you configure various aspects of your deployment, including user settings and service options.

Web application users can update their profile and password in Service Hub, if you grant them appropriate permissions.

Logging into the Service Hub

After you have completed the MaxCS installation or upgrade process, you can log into the Service Hub. The URL was defined when you deployed MaxCS; the format will be similar to https://servicehub.[system name].com. For MaxCloud users, the URL is servicehub.altigen.com.



Altigen Service Hub

Single-Sign-On

Service Hub Single-Sign-On capability allows multiple web applications to share the same login session.

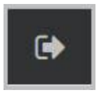
For example, a user may open the Service Hub tab and launch the AltiReport admin tab and also launch the AltiReport Client tab without requiring another login.

When a user logs out from one of these tabs, the tab opens a log-in panel.

All other tabs will also show a log-in panel. The user may log in from *any one of these log-in panels*. Afterward, the other tabs will display a message to reload the page. No additional log-in is required for the apps in the other tabs.

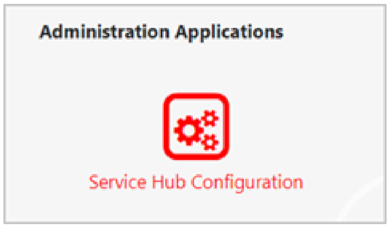
Signing out of the Service Hub

To log out of the Service Hub, just click the **Sign Out** button in the toolbar.



Getting Around

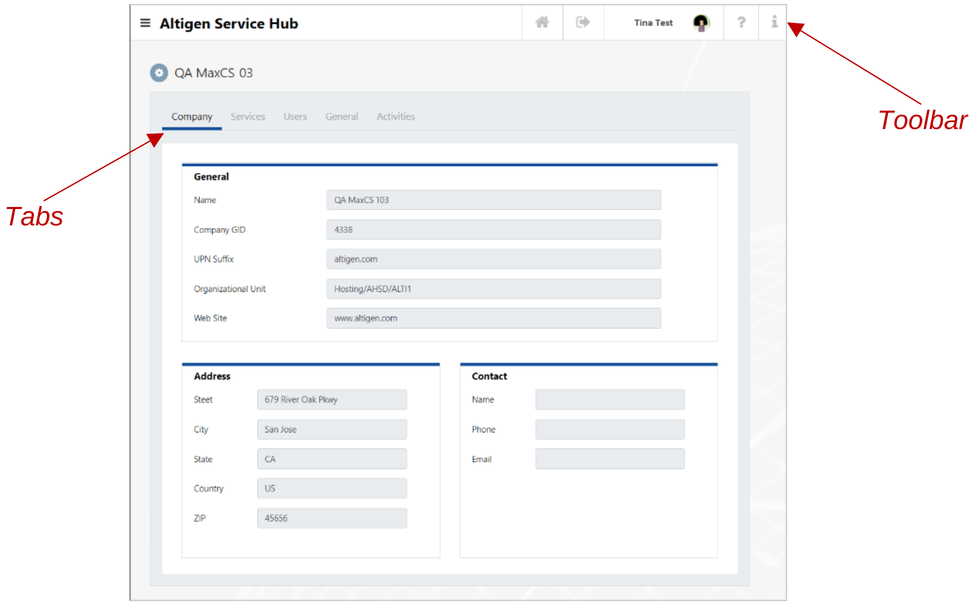
After you log in, the Service Hub opens. The main window shows you various application icons.



Administration Applications

Service Hub Configuration

Click the *Service Hub Configuration* icon. The window will look similar to the following figure.



QA MaxCS 03

Company | Services | Users | General | Activities

General

Name: QA MaxCS 103

Company GID: 4338

UPN Suffix: altigen.com

Organizational Unit: Hosting/AHSD/ALTI1

Web Site: www.altigen.com

Address

Steet: 679 River Oak Pkwy

City: San Jose

State: CA

Country: US

ZIP: 45656

Contact

Name:

Phone:

Email:

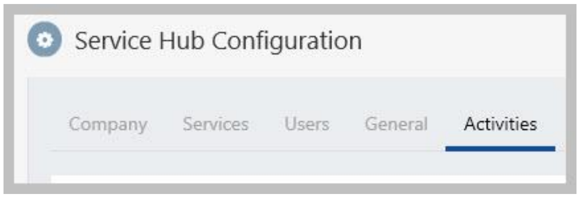
Here are the buttons you will see on the Toolbar:

🏠	The **Home** button brings you back to the main page (the page with all of the application icons).
➜	The **Sign Out** button opens a window where you can log out of the Service Hub.
admin 👤	The **Profile** button (which will show your login name) opens a window where you can change your avatar, password, and various profile options.
?	The Help button opens the *Service Hub Guide*.
i	The Information button shows you the current build of the Service Hub.

There are several tabs along the top. Each tab allows you to customize a specific aspect of your service.

Configuration Tabs

Click a tab to view or configure that aspect of your service.

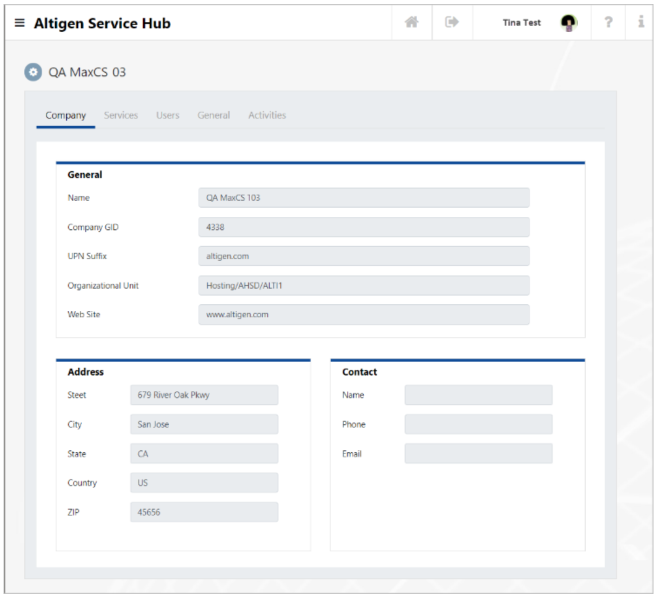


- **Company tab** – The *Company* tab is where you view various details for your organization. Most of the information on this tab came from your entries during the installation process. See The Company Tab.
- **Services tab** – On the *Services* tab, you can see the versions of various add-on applications and the server. See The Services Tab.
- **Users tab** – The *Users* tab is where you manage user account details and privileges. See Managing User Details.
- **General tab** – This tab is where you set security options for your company, set admin and user default landing pages, and import users from a CSV file. See Managing Security Options.
- **Activities tab** – This tab is where you can search a log of activities in your system.

Any fields on these tabs that appear grey or dim are fields that you cannot change in the Service Hub.

The Company Tab

The Company tab is where you view various details for your service. Most of the information on this tab came from entries during the installation process.



General

Name	QA MaxCS 103
Company GID	4338
UPN Suffix	altigen.com
Organizational Unit	Hosting/AHSD/ALTI1
Web Site	www.altigen.com

Address

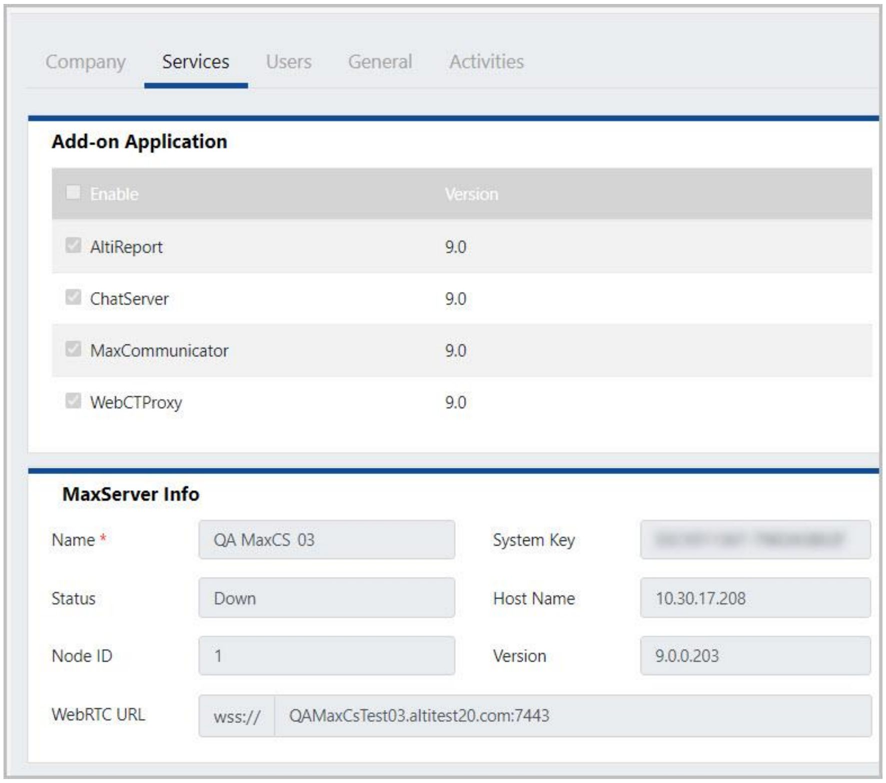
Steet	679 River Oak Pkwy
City	San Jose
State	CA
Country	US
ZIP	45656

Contact

Name	
Phone	
Email	

The Services Tab

On the *Services* tab, you see version numbers for your add-on applications and find details for the MaxCS server.



Add-on Application

□ Enable	Version
☑ AltiReport	9.0
☑ ChatServer	9.0
☑ MaxCommunicator	9.0
☑ WebCTProxy	9.0

MaxServer Info

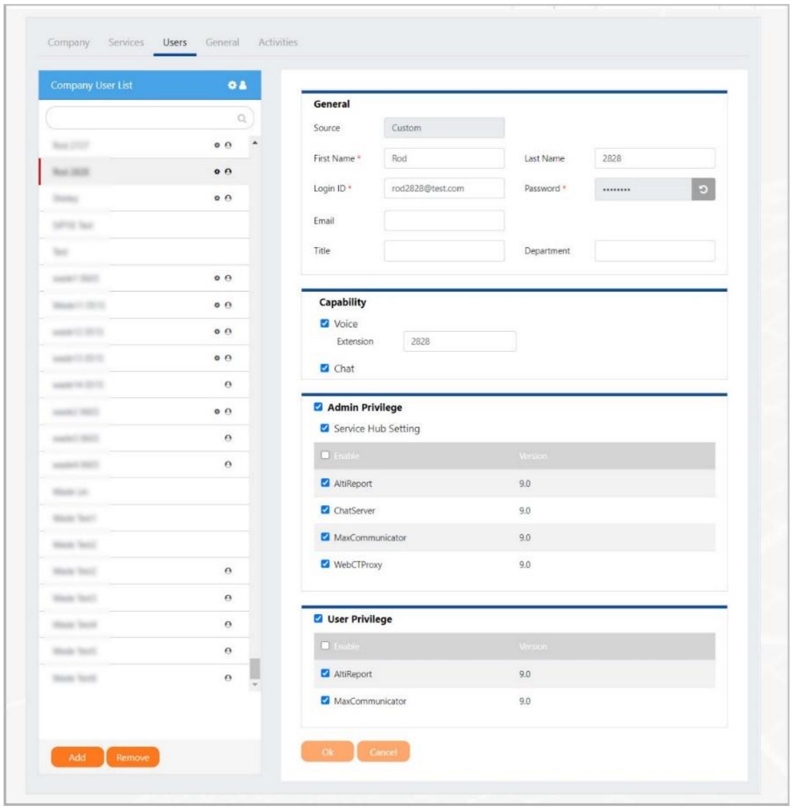
Name *	QA MaxCS 03	System Key	[redacted]
Status	Down	Host Name	10.30.17.208
Node ID	1	Version	9.0.0.203
WebRTC URL	wss:// QAMaxCsTest03.altitest20.com:7443		

The Users Tab

The users tab is where you manage user accounts.

Icons to the right of each user's name indicate whether that user is a company admin, a user, or both. You can click an icon in the heading to filter the list by user type.

For instructions on adding, updating, and removing users, refer to the section Managing User Details.



[redacted]

General

Source: Custom

First Name *: Rod | Last Name: 2828

Login ID *: rod2828@test.com | Password *: ••••••••

Email:

Title: | Department:

Capability

☑ Voice

Extension: 2828

☑ Chat

☑ **Admin Privilege**

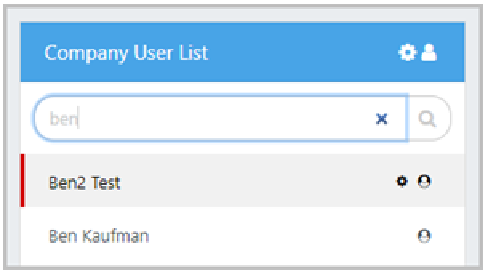
☑ Service Hub Setting

□ Enable	Version
☑ AltiReport	9.0
☑ ChatServer	9.0
☑ MaxCommunicator	9.0
☑ WebCTProxy	9.0

☑ **User Privilege**

□ Enable	Version
☑ AltiReport	9.0
☑ MaxCommunicator	9.0

You can search for a specific user by typing the name in the *Search* field at the top of the user list.



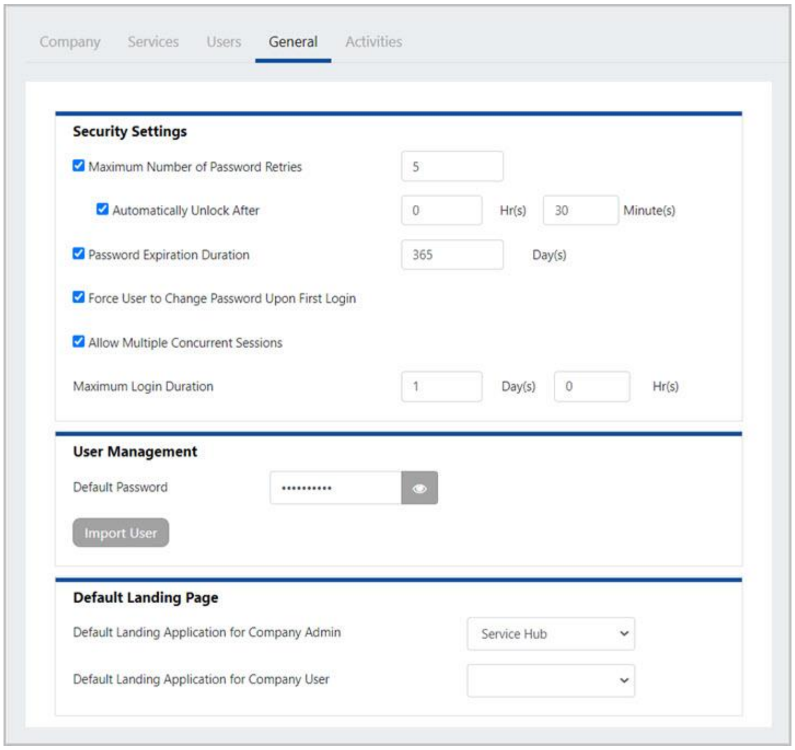
ben

Ben2 Test

Ben Kaufman

The General Tab

The General tab is where you can set password and other security options. This is also where you can upload a .CSV file of users (exported from MaxAdmin) into Service Hub.



Security Settings

☑ Maximum Number of Password Retries: 5

☑ Automatically Unlock After: 0 Hr(s) 30 Minute(s)

☑ Password Expiration Duration: 365 Day(s)

☑ Force User to Change Password Upon First Login

☑ Allow Multiple Concurrent Sessions

Maximum Login Duration: 1 Day(s) 0 Hr(s)

User Management

Default Password: ••••••••••

Default Landing Page

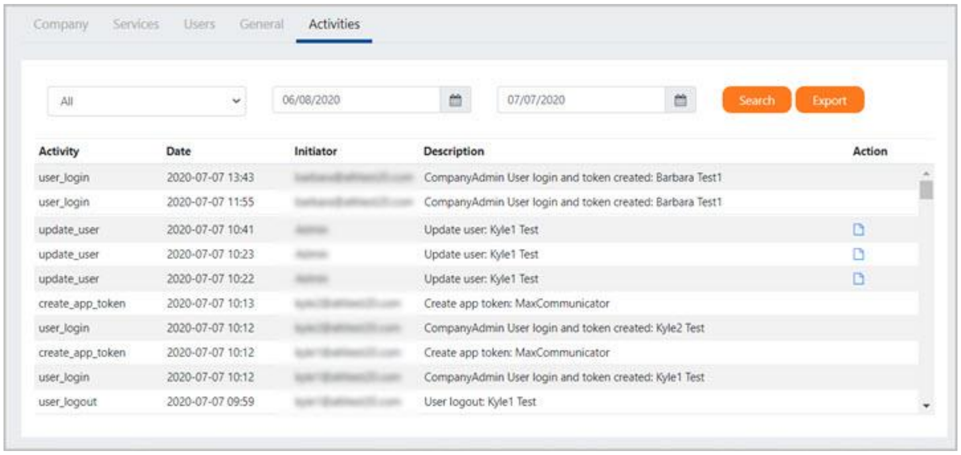
Default Landing Application for Company Admin: Service Hub

Default Landing Application for Company User:

For details, see the section Managing Security Options.

The Activities Tab

The Activities tab is where you can view a list of changes that have been made to your service.



All | 06/08/2020 | 07/07/2020

Activity	Date	Initiator	Description	Action
user_login	2020-07-07 13:43	[redacted]	CompanyAdmin User login and token created: Barbara Test1	
user_login	2020-07-07 11:55	[redacted]	CompanyAdmin User login and token created: Barbara Test1	
update_user	2020-07-07 10:41	[redacted]	Update user: Kyle1 Test	🗋
update_user	2020-07-07 10:23	[redacted]	Update user: Kyle1 Test	🗋
update_user	2020-07-07 10:22	[redacted]	Update user: Kyle1 Test	🗋
create_app_token	2020-07-07 10:13	[redacted]	Create app token: MaxCommunicator	
user_login	2020-07-07 10:12	[redacted]	CompanyAdmin User login and token created: Kyle2 Test	
create_app_token	2020-07-07 10:12	[redacted]	Create app token: MaxCommunicator	
user_login	2020-07-07 10:12	[redacted]	CompanyAdmin User login and token created: Kyle1 Test	
user_logout	2020-07-07 09:59	[redacted]	User logout: Kyle1 Test	

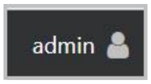
See the section Viewing Activities in your Service Hub.

Changing Your Password

If you want to sign in with your Microsoft credentials, you should not use this feature. This feature applies to users who are logging in with credentials that are separate from your Windows credentials.

To change your password,

1. In the Service Hub, click your **Profile** button in the toolbar.



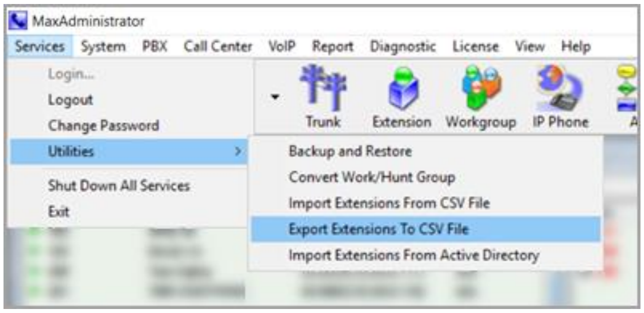
2. In the Profile panel, click **Change Password**.
3. Enter your current password, a new password, and then confirm the new password. Click **OK**.

Importing Extension Users into Service Hub

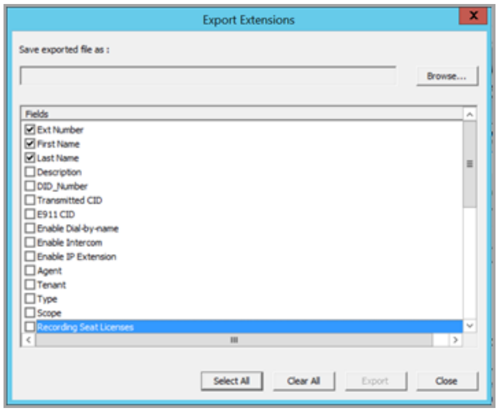
In MaxAdmin, you can export extension user properties into a .CSV file, and then import that .CSV file into Service Hub.

This “bulk upload” process avoids having to enter each user record into Service Hub individually.

1. In MaxAdmin, choose **Services** > **Utilities** > **Export Extensions to CSV File.**



Various fields are pre-selected for export. In order to create a user record in the Service Hub, you must include the *First Name, Last Name,* and *UPN* fields.

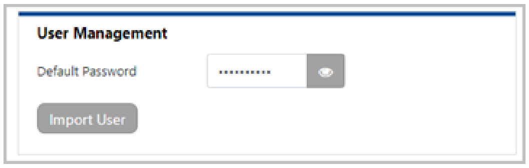


Fields

☑ Ext Number
☑ First Name
☑ Last Name
☐ Description
☐ DID_Number
☐ Transmitted CID
☐ E911 CID
☐ Enable Dial-by-name
☐ Enable Intercom
☐ Enable IP Extension
☐ Agent
☐ Tenant
☐ Type
☐ Scope
☐ Recording Seat Licenses

2. Check the options for any other fields that you want to import.
3. Click **Browse** to enter a filename and indicate a folder where you want to store the CSV file. Click **Save**.

4. Click **Export**. You will see an acknowledgment that the file was successfully created.
5. Open Service Hub and switch to the *General* tab. Click **Import Users**.



User Management

Default Password ••••••••••

6. Navigate to the CSV file that you just created.
7. Click **Open** to import the users.

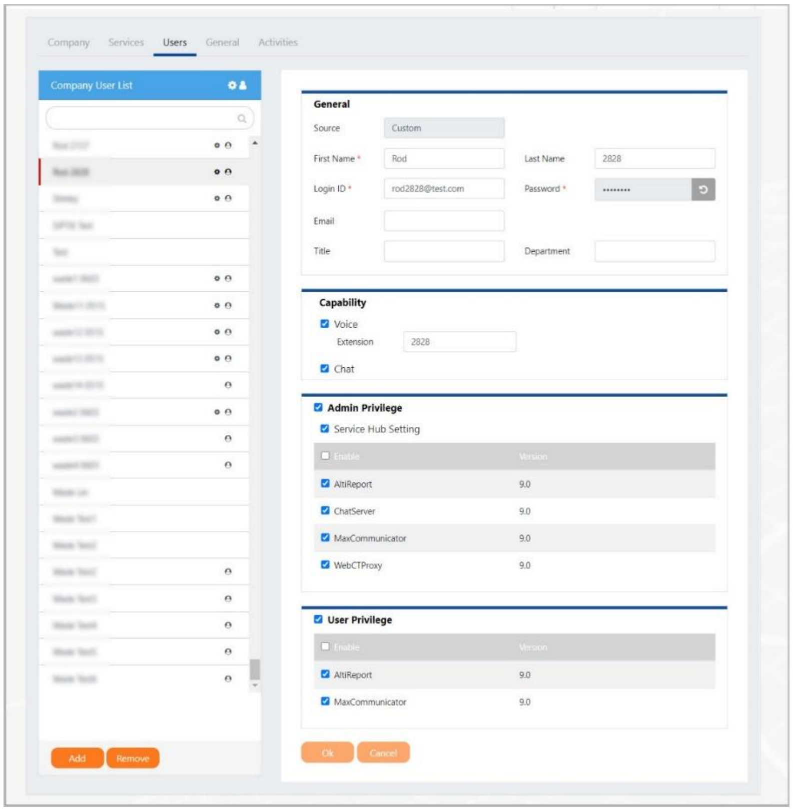
Switch to the *Users* tab to confirm that the user records were added, or switch to the *Activities* tab to search for the import activity.

Considerations

- Imported users will automatically be assigned the password that you have specified as the *Default Password* (see page 14). Users will be prompted to change their passwords the first time they log into the Service Hub or any MaxCS web application.
- If an extension user record is imported that is a duplicate of an existing Service Hub record, then the new data for the user will overwrite the existing user properties.

Managing User Details

To view or manage details about users, click the **Users** tab.



General

Source	Custom		
First Name *	Rod	Last Name	2828
Login ID *	rod2828@test.com	Password *	••••••••
Email			
Title		Department	

Capability

☑ Voice

Extension 2828

☑ Chat

☑ **Admin Privilege**

☑ Service Hub Setting

□ Enable	Version
☑ AltiReport	9.0
☑ ChatServer	9.0
☑ MaxCommunicator	9.0
☑ WebCTProxy	9.0

☑ **User Privilege**

□ Enable	Version
☑ AltiReport	9.0
☑ MaxCommunicator	9.0

Adding Individual Users

To create a custom user record,

1. On the *Users* tab, click **Add** below the current list of users.
2. Enter the details for this user and click **Add**. See User Field Descriptions for descriptions of each field.

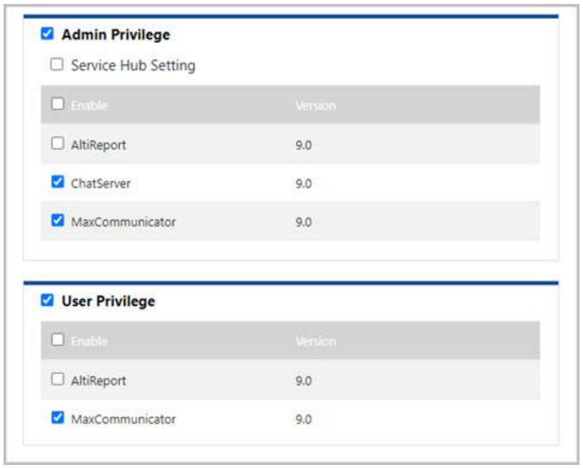
User Field Descriptions

User General Field	Description
Source	This read-only field indicates where the details for this user came from. For user records that you have added manually and for user records that were imported from a CSV file, the source will be *Custom*.
First Name, Last Name	The name of this user. You can edit this name only if this is a custom user record. If the details for this user were pulled from Active Directory, you cannot edit the user's name.
Login ID	The user's login username.
Password	The user will be assigned the Default password (see page 14) automatically, and will be prompted to change this password when the user first logs into the Service Hub or any MaxCS Web application.
Extension	The MaxCS extension of this user.
Email	The user's email address.
Title	The user's title.
Department	The user's department.

Setting Admin and User Privileges

To configure which applications a specific user can access, and whether they have user or administrator privileges to that application,

1. Click the **Users** tab.
2. Select the user in the list on the left.



☑ **Admin Privilege**

□ Service Hub Setting

□ Enable	Version
□ AltiReport	9.0
☑ ChatServer	9.0
☑ MaxCommunicator	9.0

☑ **User Privilege**

□ Enable	Version
□ AltiReport	9.0
☑ MaxCommunicator	9.0

3. In the *Admin Privilege* section, check (to enable) or clear (to disable) this user's administrator access for each application.

   Repeat this for the *User Privilege* section.

4. Click **OK**.

If you enable an application for a user, the user will see the corresponding icon in the Service Hub and will be able to click the icon to open the application.

If you disable an application for a user, the user will not see that icon.

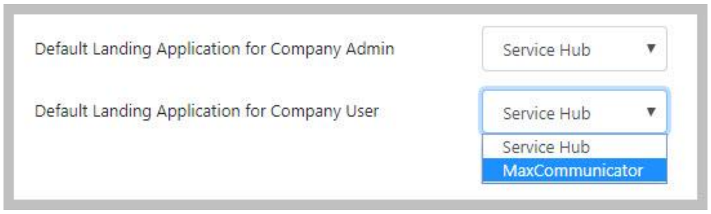
Password Requirements

- Users cannot change their passwords to a password that they have used previously.
- Requirements: Passwords must be a minimum of 9 characters, with at least one character from each of the following categories (no spaces allowed):
  - Special characters (! @ # $ % ^ & *)
  - Uppercase letters
  - Lowercase letter
  - Numbers

Configuring Default Landing Applications

On the *General* tab, you can assign a default landing application for administrators and one for web client users. This setting controls which application opens when a user logs in.

The choices will vary depending upon which components and applications your company has deployed. The options may include Service Hub, ChatServer, and MaxCommunicator.



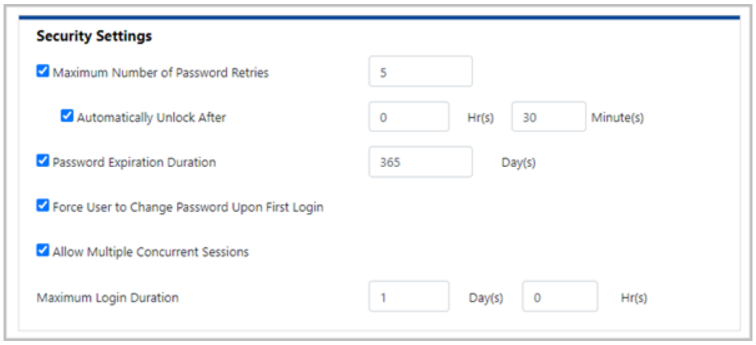
Default Landing Application for Company Admin: Service Hub ▼

Default Landing Application for Company User: Service Hub ▼

Managing Security Options

You can configure various security options for your organization, on the *General* tab.

Note that the password features apply only to “Custom” users.



Security Settings

☑ Maximum Number of Password Retries: 5

☑ Automatically Unlock After: 0 Hr(s) 30 Minute(s)

☑ Password Expiration Duration: 365 Day(s)

☑ Force User to Change Password Upon First Login

☑ Allow Multiple Concurrent Sessions

Maximum Login Duration: 1 Day(s) 0 Hr(s)

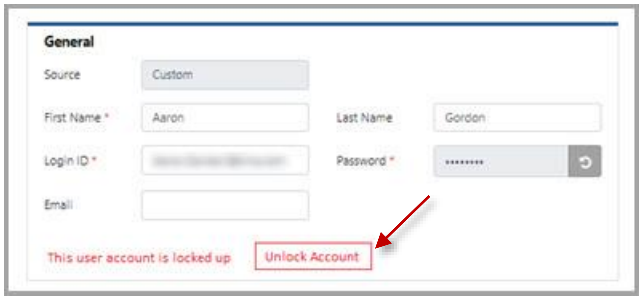
Security Field	Description
Maximum Number of Password Retries	This option specifies the maximum number of contiguous invalid password attempts that are allowed before the system locks the user’s account. You can specify a range of 1 to 20 attempts; the default value is 5. Note that if the user enters the same password sequentially, the system counts that as one attempt. • **Enabled** – The system tracks password attempts and locks the account if the user exceeds the specified number of invalid entries. When you enable this option, you can also specify an automatic unlock option (optional) ○ **Automatically Unlock After *x*** – When you enable this option, you can specify how long the user account will remain locked before the system automatically unlocks it. You can specify a range from 0–200 hours, and 0-60 for minutes. The default value is 0 hours 30 minutes. If you disable this option, then the system will not automatically unlock the user account; it must be unlocked manually by an administrator. • **Disabled** – The system does not limit the number of invalid password entries.
Password Expiration Duration	This option specifies how long (in days) user passwords remain valid, before they must be changed. • **Enabled** – User passwords expire after the duration that you specify, and users will be required to change their passwords. The default duration is 365 days. • **Disabled** – User passwords never expire.

Security Field	Description
Force User to Change Password Upon First Login	This option removes an admin's knowledge of another user's password, by forcing users to specify a new password when they first log in. • **Enabled** – (The default) Users are required to create a new password the first time they log into the Service Hub. • **Disabled** – Users are not required to create a new password the first time they log into the Service Hub.
Allow Multiple Concurrent Sessions	This option specifies whether users can log in concurrently to several different devices or browsers. For example, a user could open the Service Hub in one browser tab and open AltiReport in another tab without requiring an additional login. • **Enabled** – (The default) The system allows logging into multiple tabs or devices concurrently. • **Disabled** – (The default) The system does not allow users to log in under the same account onto different applications or devices. Users logging in to a new session will automatically be logged out of the older session.
Maximum Login Duration	The maximum length of time a user can remain logged into a single session. Specify the duration in days and hours. After the login period has elapsed, the user will be prompted to log in again.
Default password	Here, you can set a default password for new users.

Unlocking User Accounts

As a company administrator, you can unlock any user with *the same level of privileges or lower*. For example, you can unlock one of your company's user accounts or another admin account.

When a user's account is locked, the user's data on the Service hub Users tab will offer an *Unlock Account* button those with sufficient privileges. Clicking the button will unlock that user's account.



General

Source: Custom

First Name *: Aaron

Last Name: Gordon

Login ID *: [redacted]

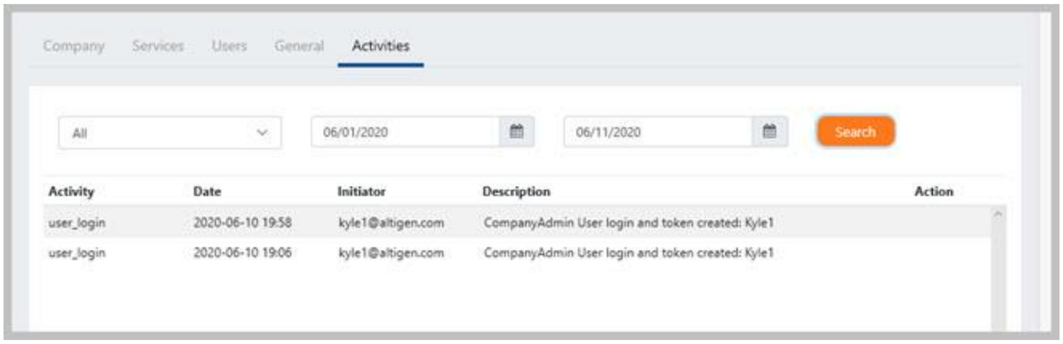
Password *: •••••••••

Email:

This user account is locked up

Viewing Activities in your Service Hub

On the Activities tab, you can search a specific time period to review the changes that were made to your configuration during that time.



06/01/2020 06/11/2020

Activity	Date	Initiator	Description	Action
user_login	2020-06-10 19:58	kyle1@altigen.com	CompanyAdmin User login and token created: Kyle1	
user_login	2020-06-10 19:06	kyle1@altigen.com	CompanyAdmin User login and token created: Kyle1	

- **Activity** – The type of activity or event that occurred.
- **Date/Time** – The date and time that the activity or event occurred.
- **Initiator** – The user who made (or in some way triggered) the change.
- **Description** – A description of the change.
- **Action** – If this column contains an icon, you can click the icon to see details of this activity. To close the Details window, click **Back to List**.

These events and actions are captured in the log:

- Service Hub Authentication successes and failures, such as log-in and log-out
  - Service Hub admin/user login/out
    - Login succeeded:
      - Privilege
      - Creator: login user GUID
    - Logout – creator: login user
  - Launch application
  - Modification to user accounts, such as changes to contact information:
    - Password change
    - Lock user account
    - Unlock user account
  - Configuration changes, showing both the old data and the new (changed) data. Note that old data and new data are encrypted.
    - Add User
    - Delete User
    - Edit User (include privilege changes)
    - Add Applications
    - Edit Applications
    - Delete Applications
    - Add Services
    - Edit Services
    - Edit General
    - Import User
    - Change Application Icon

Exporting Activity Data

To export activity data into a .PDF file,

1. Perform your search, specifying a data range.

2. Click the **Export** button.
3. Choose a path to save the file.

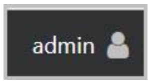
Changing Your Avatar

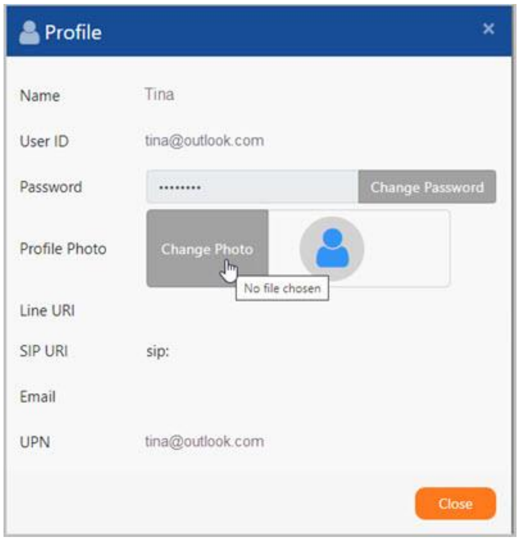
Avatars are essentially profile images that will appear beside your name in places in the Service Hub and in other applications.

Four image file formats are supported: .png, .jpg, .gif, and .bmp. The uploaded image will be reduced to maximum size of 128x128.

To upload an image file that you want to use as your avatar,

1. In the Service Hub, open your Profile panel by clicking your *Profile* button in the toolbar.



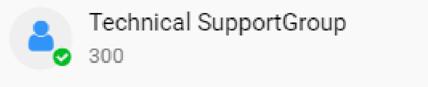


Name	Tina
User ID	tina@outlook.com
Password	••••••••
Profile Photo	
Line URI	
SIP URI	sip:
Email	
UPN	tina@outlook.com

2. Click **Change Photo**.
3. Navigate to the image you want to show as your avatar. Select the image file.
4. After you select it, the image should appear in the Profile page. Click **Close**.

About Avatar Image Files

If a user does not have an avatar image uploaded, then a default avatar image is displayed. Directory users will have a default avatar similar to the following image.



Technical SupportGroup
300

A Contact user's default avatar will show the initials of the first and last name. If neither the first name nor last name exists, a default avatar image is displayed

Operational Limitations

Please also review the readme files to learn about any limitations with this Beta release.

- There is an issue when users are running MaxCommunicator Web in a Safari browser. If the user logs out of the Service Hub, the user may remain logged into MaxCommunicator. We recommend that Safari users manually log out of MaxCommunicator in this scenario.

Altigen Technical Support

Authorized Altigen Partners and distributors may contact Altigen technical support by the following methods:

- You may request technical support on Altigen's Partner web site, at https://mspartner.altigen.com. Open a case on this site; a Technical Support representative will respond within one business day.
- Call 888-ALTIGEN, choose option 5 from the IVR, or 408-597-9000, option 5 from IVR, and follow the prompts. Your call will be answered by one of Altigen's Technical Support Representatives or routed to the Technical Support Message Center if outside of normal business hours and no one is available to answer your call.

Technical support hours are 5:00 a.m. to 5:00 p.m., PST, Monday through Friday, except holidays.

If all representatives are busy, your call will be returned in the order it was received, within four hours under normal circumstances. Outside Altigen business hours, only urgent calls will be returned on the same day (within one hour). Non-urgent calls will be returned on the next business day.

Please be ready to supply the following required information when calling in for Support:

- Partner ID.
- Altigen Certified Tech ID.
- Product serial number.
- MaxCS version number.
- Server model.
- Indicate whether this is a virtual or standalone server installation.
    - If this is a virtual installation, be prepared to identify whether you're using VMware or Hyper-V, and which version of the virtual software is installed.
- The amount of memory and the number of CPUs that are reserved for MaxCS Server use. Be aware that memory and CPU cores should always be dedicated and reserved for MaxCS Server use exclusively.
- Indicate whether SSD drives are installed. If they are not, be prepared to describe what NAS devices are installed, and whether they are shared or dedicated to MaxCS Server.
- The telephone number where you can be reached.