ScreenBeam CMS Enterprise Deployment Guide

For CMS version 4.4.15.0

Document and Software Copyrights

This ScreenBeam Document and all software offered through or used on this ScreenBeam Document are our property or the property of our suppliers, sponsors, licensors or affiliates (collectively, "Business Partners"), and are protected by United States and international copyright law, trademark law, and trade secret law, as well as other laws, rules and regulations.

We own a copyright in this ScreenBeam Document and in the selection, coordination and arrangement of the content available through this ScreenBeam Document. Except as expressly provided herein, neither we nor our Business Partners grant any rights to you under any patents, copyrights, trademarks or trade secret information. Accordingly, unauthorized use of this ScreenBeam Document or any content available on this ScreenBeam Document may violate patent laws, copyright laws, trademark laws, trade secret laws, and laws pertaining to privacy and publicity rights or other laws or regulations.

Copyright © 2025 ScreenBeam Inc. All Rights Reserved. ScreenBeam, and the ScreenBeam logo and all page headers, custom graphics and button icons are the service marks, trademarks, and/or trade dress of ScreenBeam ("Trademarks"). All other service marks, trademarks, product names and company names or logos displayed in this ScreenBeam Document are the property of their respective owners. You may not use, copy, reproduce, republish, upload, post, transmit, distribute or modify any of the Trademarks in any way, including in advertising or publicity pertaining to distribution of materials on this ScreenBeam Document, without our prior written consent.

Table of Contents

Part I Planning 1
1.1 Basic 1
1.2 Sites 2
1.3 Administrative Users (Roles) 3
1.4 Deployment Flow 5
1.5 Compatible ScreenBeam Receivers 6
Part II Deploying CMS Server and Companion Servers 7
2.1 CMS Server 7
2.1.1 System Requirements 7
2.1.2 Install ScreenBeam CMS 9
2.1.3 Check CMS Service Status 21
2.1.4 Uninstall ScreenBeam CMS 23
2.2 DNS Server and DHCP Server 24
2.3 HTTP Server 24
Part III Provisioning ScreenBeam Receivers 25
3.1 Connecting ScreenBeam Receivers to Network 25
3.2 Provisioning Receivers Using DNS Discovery Method 26
3.3 Provisioning Receivers using Static IP Discovery - USB Method 27
Part IV Manage ScreenBeam Receivers with CMS 30
4.1 Login 30
4.2 Basic Functions 32
4.3 Connecting CMS to ScreenBeam Cloud 33
4.3.1 Signing up for ScreenBeam Cloud 33
4.3.2 Connecting CMS to ScreenBeam Cloud 38
4.3.3 Activating Licenses on ScreenBeam Cloud 40
4.3.4 (Optional) Inviting Users to ScreenBeam Cloud 44
4.3.5 Resetting Password 51
4.4 Managing CMS Users 53
4.4.1 Add a New User 53
4.4.2 Re-assign Roles 55
4.4.3 Edit User Info and/or Change User Password 60
4.4.4 Delete a User 62
4.5 Managing Receivers 64
4.5.1 Add a New Site 64
4.5.2 Rename a Site 67
4.5.3 Delete a Site 69
4.5.4 Add Receivers to a Site 71
4.5.5 Release Receivers from a Site 73
4.5.6 Add Users to a Site 75
4.5.7 Release a User from a Site 77
4.5.8 Configure Receiver Remotely 79

4.5.9 Save / Load Settings for Batch Configuration 81
4.5.10 Configure Receiver with a USB Flash Drive 85
4.5.11 Update Receiver Firmware 88
4.5.12 Connect Receiver to RADIUS Authenticated AP/LAN 90
4.5.13 Switch CMS Server for Receivers 94
4.5.14 Update Receiver Background Image 96
4.5.15 Update Receiver Screensaver Image 98
4.5.16 Reboot Receivers 100
4.5.17 Reset Receivers 102
4.5.18 Delete Offline Receivers 104
4.5.19 Edit Receiver Descriptions 106
4.5.20 Clear All Unlicensed Legacy Receivers 108
4.5.21 Clear Feedback 110
4.5.22 Clear Debug Logs 112
4.5.23 Assign Licenses to Receivers 114
4.5.24 Push an Alert to Receivers 117
4.6 Managing Scheduled Tasks 121
4.6.1 Schedule a Task 121
4.6.2 Add Receiver to Task 125
4.6.3 Remove Receivers from a Task 127
4.6.4 Edit a Task 130
4.6.5 Delete a Task 132
4.7 Managing Logs 134
4.7.1 Upload Receiver Log 134
4.7.2 View Receiver Logs 138
4.7.3 Export Receiver Logs 140
4.7.4 View Scheduler Log 142
4.7.5 Export Scheduler Log 144
Appendix I Using Azure AD for User Management 146
Prerequisite 146
Setting up Azure AD and ScreenBeam CMS 147
Appendix II Backing up and Restoring ScreenBeam CMS 168
Backing up ScreenBeam CMS 169
Restoring ScreenBeam CMS 171

Part I Planning

ScreenBeam Central Management System (CMS) Enterprise is a robust tool that enables administrators to remotely access and manage ScreenBeam receivers distributed over multiple geographic locations and across networks with ease. Administrators can monitor receiver status, apply security policies, troubleshoot problems, perform device resets, update receivers, and more.
ScreenBeam Cloud provides premium features and license management, and it enables multiple CMS systems to work together in an organization.

Careful and comprehensive planning can help you better deploy CMS and ScreenBeam receivers.

1.1 Basic

To plan CMS deployment, follow these guidelines:

- Designate an x86-based Windows device to host the ScreenBeam CMS server.

- Ensure that firewall allows the following CMS ports (default: 7237 / 7238 / 5001 / 8890), the web server access port (default: 8888), the Service Platform ports (default: 8889 / 6388) or the SQL server port (default: 1433).
  Note: The Service Platform Port is used for communication between ScreenBeam receivers (versions 11.x.14.x and older). It is not required for versions 11.x.15.x and newer.

- It is highly recommended that the device hosting the ScreenBeam CMS server has a fixed IP address.

- Designate a HTTP server to host the firmware and miscellaneous files used for upgrading or customizing ScreenBeam receivers. The server should be of commercial grade capable of handling large number of simultaneous connections and bandwidth. Scheduling smaller groups of receivers to upgrade firmware can reduce system load.

- Ensure that the policies allow TCP traffic on the CMS ports across the network routers and port forwarded accordingly.

- Note the ScreenBeam CMS server address. This is generally the IP address (or FQDN) of the CMS server. If the PC is behind a NATed router, then the CMS IP Address is the WAN IP address to which the PC is mapped to. Use this IP (or FQDN) to provision ScreenBeam receivers.

- Determine which parameters must be globally changed and which need to be modified on individual receivers. Tracking inventory of ScreenBeams and mapping them to their locations (sites) should be planned in advance.

1.2 Sites

ScreenBeam CMS uses sites to group receivers according to their locations or other criteria which help admins manage receivers efficiently. Admins can manage up to nine levels of sites hierarchically. It is recommended to create sites that correspond to actual locations. Assign receivers to sites, and then assign users to sites to manage the receivers.

CMS users should plan appropriate naming conventions for the sites and define the hierarchy.

Example:

HQ
- Building 1
  - - Floor 1
  - - Lab
- Building 2

Seattle Office
- Building 1

1.3 Administrative Users (Roles)

CMS Enterprise has several types of user (roles), the users differ in their ability to interact with CMS Enterprise and their ability to interact with ScreenBeam receivers.

- CMS SysAdmin (CMS System administrator)
  This account type is an administrator over the CMS Enterprise program and an administrator over all ScreenBeam receivers. It can create, delete, and modify user accounts, set up Sites and assign ScreenBeam receivers to them, and assign CMS Users as ScreenBeam Admins or ScreenBeam Monitors for particular sites.

- CMS User - CMS Admin
  This account type is an administrator over ScreenBeam receivers assigned to the Site(s) that the ScreenBeam Admin has access to. A CMS SysAdmin must create a CMS User account and then assign that account to be a ScreenBeam Admin for one or more Sites. A CMS User does not have administrator privileges within CMS Enterprise to create or modify other users.

- CMS User - CMS Monitor
  This account type is an observer of ScreenBeam receivers assigned to the Site(s) that the ScreenBeam Monitor has access to. A CMS SysAdmin must create a CMS User account and then assign that account to be a ScreenBeam Monitor for one or more Sites. A CMS User does not have administrator privileges within CMS Enterprise to create or modify other users.

- Default Administrator (default user)
  The default account in CMS Enterprise is named Administrator. This account is for the IT person that installs and configures the PC or VM. The Administrator account is not used to manage ScreenBeam receivers and is only used to create additional accounts for CMS Enterprise.

The following table shows the functions that different administrative users can access:

Roles / Function	CMS SysAdmin	CMS Admin	CMS Monitor	Default Administrator
Dashboard (Total/Idle/Busy count)	All receivers	Only assigned receiver	Only assigned receiver	No
Sites Pane	All Sites	Only assigned Sites	Only assigned Sites	No
Edit / Rename / Delete Site	Yes	No	No	No
Join / Release receivers to site	Yes	No	No	No
Add / Remove Users to site	Yes	No	No	No
Users Table	Yes	No	No	No
Receivers Table	All receivers	Only assigned receiver	Only assigned receiver	No
Show Hide column	Yes	Yes	Yes	No
Sort by columns	Yes	Yes	Yes	No
Search	Yes	Yes	Yes	No
Filter (idle/busy/offline)	Yes	Yes	Yes	No
Actions	Yes	Yes	No	No
Delete receiver	Yes	No	No	No
Modify receiver description	Yes	Yes	No	No
Export receiver list	Yes	Only assigned receiver	Only assigned receiver	No
Schedule Tasks	Yes	Only assigned receiver	No	No
View Tasks	Yes	Yes	Yes	No
Create Tasks	All tasks	Only tasks user created	No	No
Edit Tasks	All tasks	Only tasks user created	No	No
Delete Tasks	All tasks	Only tasks user created	No	No
Scheduler Logs	Yes	No	No	No
Receiver Logs	Yes	No	No	No
USB Provisioning	Yes	No	No	No
Assign Licenses	Yes	No	No	No
User Management	Yes	No	No	Yes
ScreenBeam Cloud log on	Yes	No	No	No
ScreenBeam Cloud log off	Yes	Yes	Yes	No
Unregister CMS	Yes	Yes	Yes	No

1.4 Deployment Flow

The following is a typical deployment flow:

1. Default Administrator installs CMS.
2. Default Administrator logs in using default username/password **Administrator** / **Screenbeam**.
3. Default Administrator changes default Administrator Password.
4. Default Administrator creates the **CMS SysAdmin** user.
5. CMS SysAdmin logs in to https://<CMS-server_address>:8888.
6. CMS SysAdmin signs up and creates an account on ScreenBeam Cloud. This is the Account Owner on the Cloud.
7. CMS SysAdmin provisions receivers to connect to CMS.
8. ScreenBeam receivers are installed and connected to the same network.
9. CMS SysAdmin goes to **User Management** page and adds CMS members, specifying them as CMS Users (CMS Admin or CMS Monitor) or CMS SysAdmin (for backup).
10. CMS SysAdmin navigates to the Receivers page.
11. CMS SysAdmin adds sites if required.
    Note: When creating sites, CMS SysAdmin manages level 1 sites and below.
12. CMS SysAdmin adds ScreenBeam receivers to sites.
13. CMS SysAdmin adds users to sites and specifies their roles.
14. CMS Admin and CMS Monitor users can log in with their credentials and manage / monitor their receivers.

Notes:

- If multiple users will be managing the same sites, it is recommended to allow those users to share the same login to allow the site admin and backup site admin to edit each other's tasks (which is tied to user), and for one administrator to take over from another that leaves the organization.
- Actions are displayed for CMS Monitor users even though CMS Monitor users cannot make modifications. Receivers that a user cannot configure are greyed out.

1.5 Compatible ScreenBeam Receivers

The following ScreenBeam receivers are compatible with ScreenBeam CMS Enterprise:

- ScreenBeam 1100P
- ScreenBeam 1100F
- ScreenBeam 1100 EDU Gen2
- ScreenBeam 1000 EDU
- ScreenBeam 1100
- ScreenBeam 960B (license required)
- ScreenBeam 960A (license required)
- ScreenBeam 750A (license required)

Part II Deploying CMS Server and Companion Servers

2.1 CMS Server

ScreenBeam CMS Enterprise can be deployed directly on an X86 Windows device.

2.1.1 System Requirements

Designate an x86-based Windows device to host the CMS server. The device that hosts the CMS server should meet the following requirements:

Minimum Requirements

- Windows 10/11 (64-bit) Pro/Enterprise build 17763 or higher
- 2 Core i5 2 GHz or higher
- 8 GB Memory
- 30 GB available Hard Disk Space
- Network connectivity

Recommended Requirements

- Windows Server 2019 build 17763 or higher
- 4 Core Xeon 2 GHz or higher
- 16 GB Memory or higher
- 100 GB available Hard Disk Space
- Network connectivity

This device is to be configured based on the number of receivers deployed.

Ensure the following ports are opened on the PC hosting ScreenBeam CMS:

- CMS communication port: TCP 7237 (or the port specified during CMS installation), used to communicate with ScreenBeam receivers.
- Receiver log upload port: TCP 7238 (or the port specified during CMS installation), used for uploading receiver logs to the CMS server.
- CMS WebApp port: TCP 8888 (or the port specified during CMS installation), used for accessing CMS via a web browser.
- CMS Hub port: TCP 5001 (or the port specified during CMS installation), used for communication between web app and the CMS server.

- CMS Identity Server port: TCP 8890 (or the port specified during CMS installation), used for communication between the Identity server and CMS server.
- SQL server port: TCP 1433 (or the port specified during CMS installation), used for communication between SQL server and the CMS server.

Ensure that network policies allow TCP traffic on the CMS ports across the network routers and port forwarded accordingly.

Service	**Port** (default)	**Protocol**
CMS communication	7237	TCP
CMS Receiver logging	7238	TCP
CMS WebApp	8888	TCP
CMS Hub	5001	TCP
CMS Identity Server	8890	TCP
SQL server	1433	TCP

Note the IP address, hostname, or fully qualified domain name belonging to the device hosting CMS server.

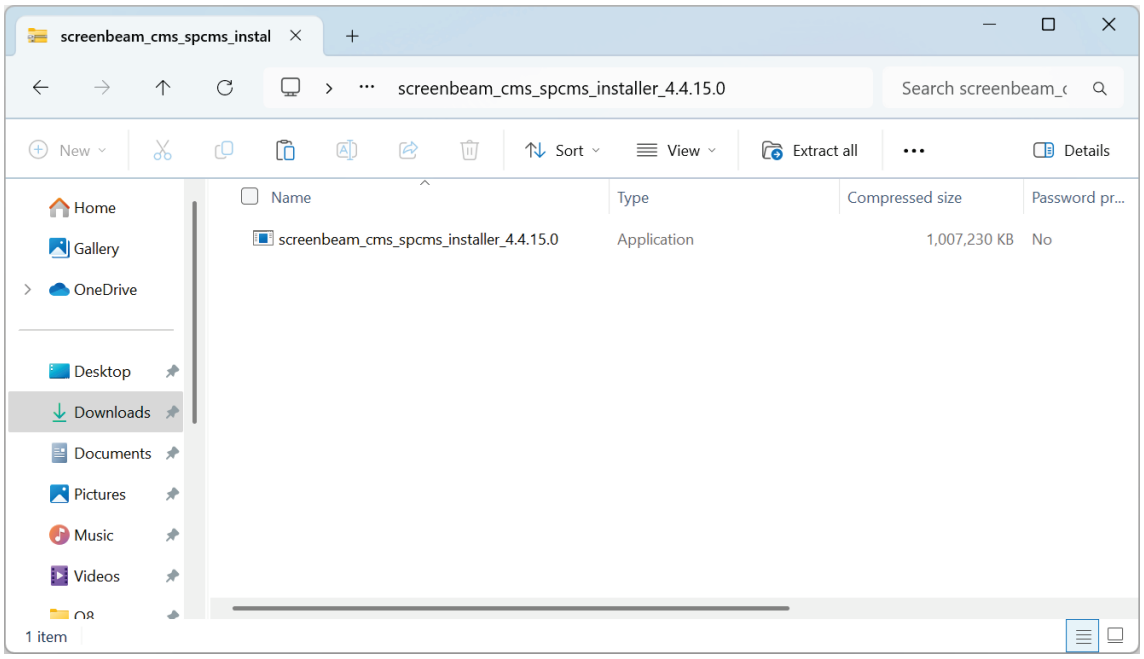
2.1.2 Install ScreenBeam CMS

ScreenBeam CMS Enterprise Installer version is a replacement for CMS Enterprise Docker 4.0 version or CMS V2.x. Therefore, if any of these versions is installed on the machine, be sure to remove it first. If Docker and Hyper-V are not used by other programs, uninstall them, as well.

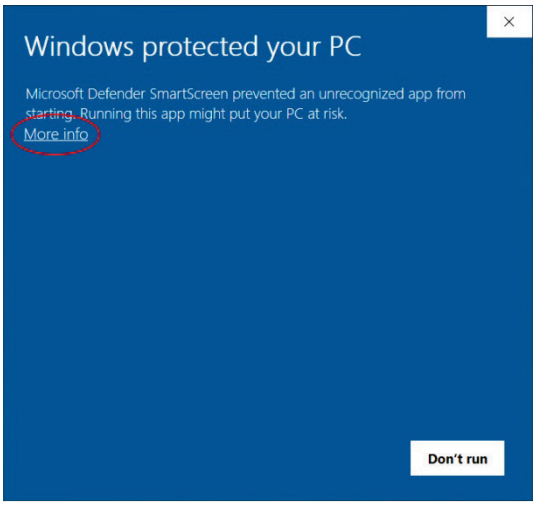
To install ScreenBeam CMS, follow this procedure:

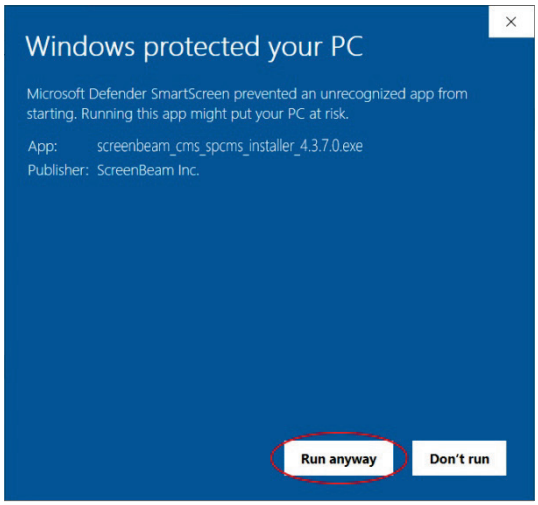
1. Go to https://support.screenbeam.com/cms and download the latest version of ScreenBeam CMS Enterprise software.

2. Extract the downloaded software package and run the ScreenBeam CMS installer.
   Note: A user with Administrator privilege is required to run the ScreenBeam CMS installer.

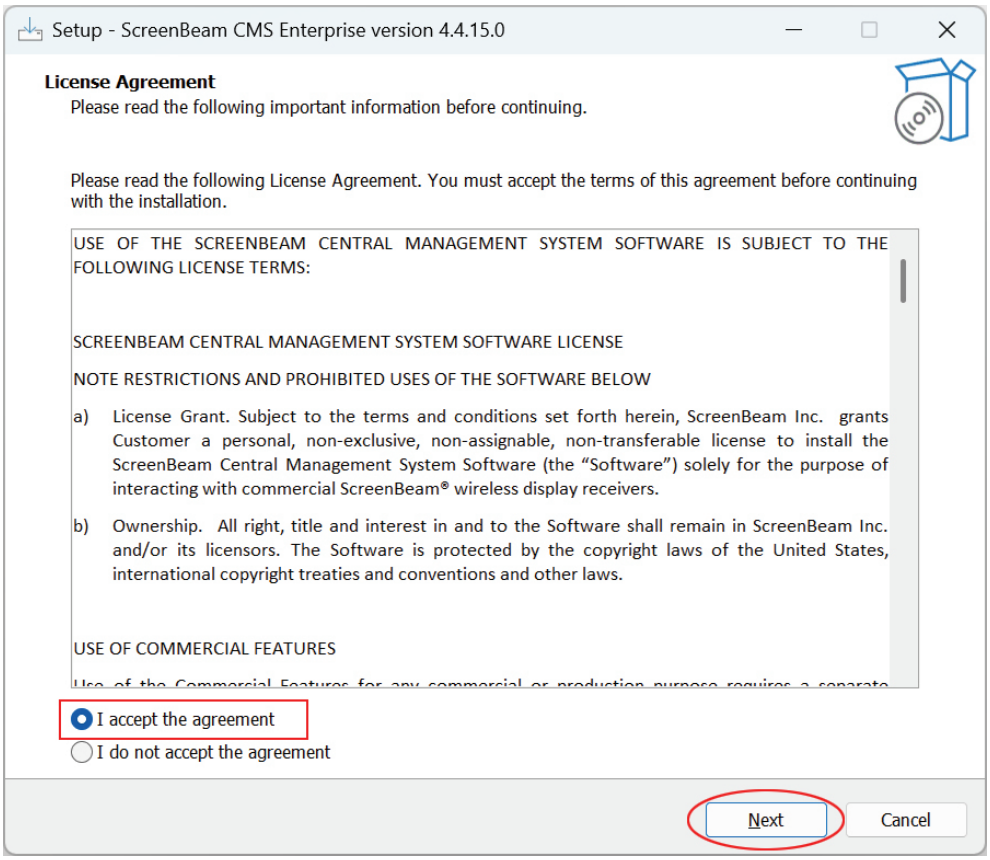


3. The Microsoft Defender Smartscreen window may appear. Click **More Info** and then click **Run Anyway** to continue.

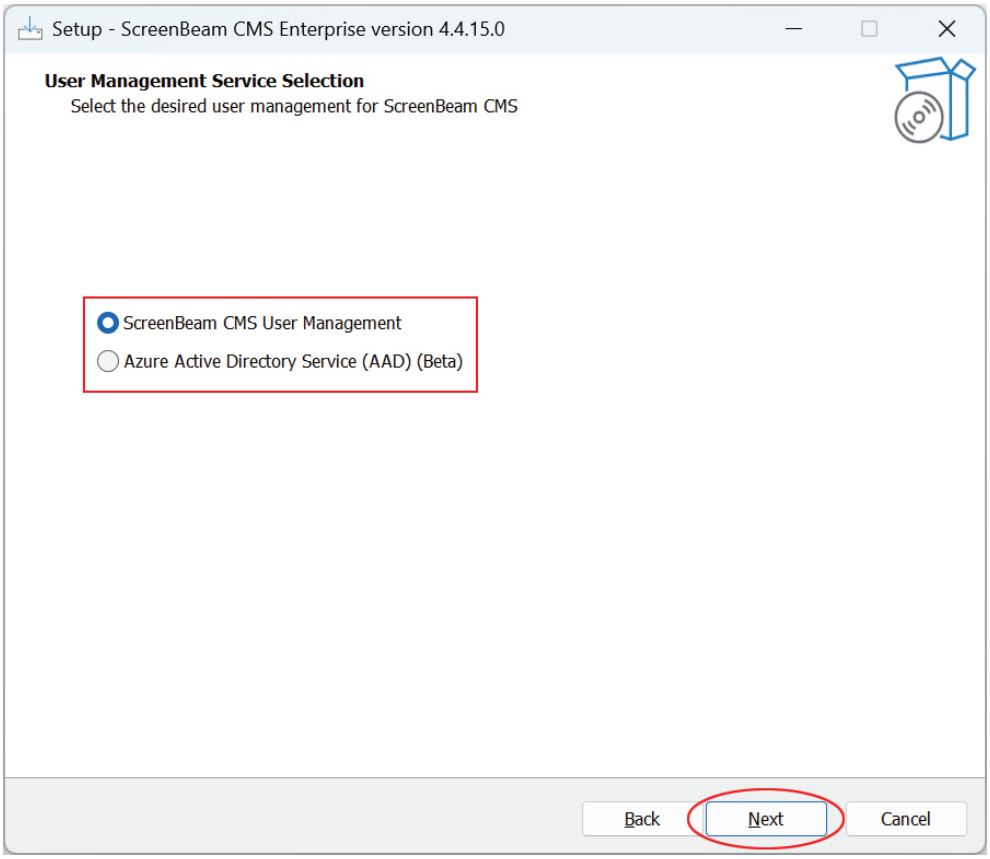




4. During the installation, the software license agreement appears first. Read the agreement carefully. Select **I accept the agreement** and click **Next** to continue.

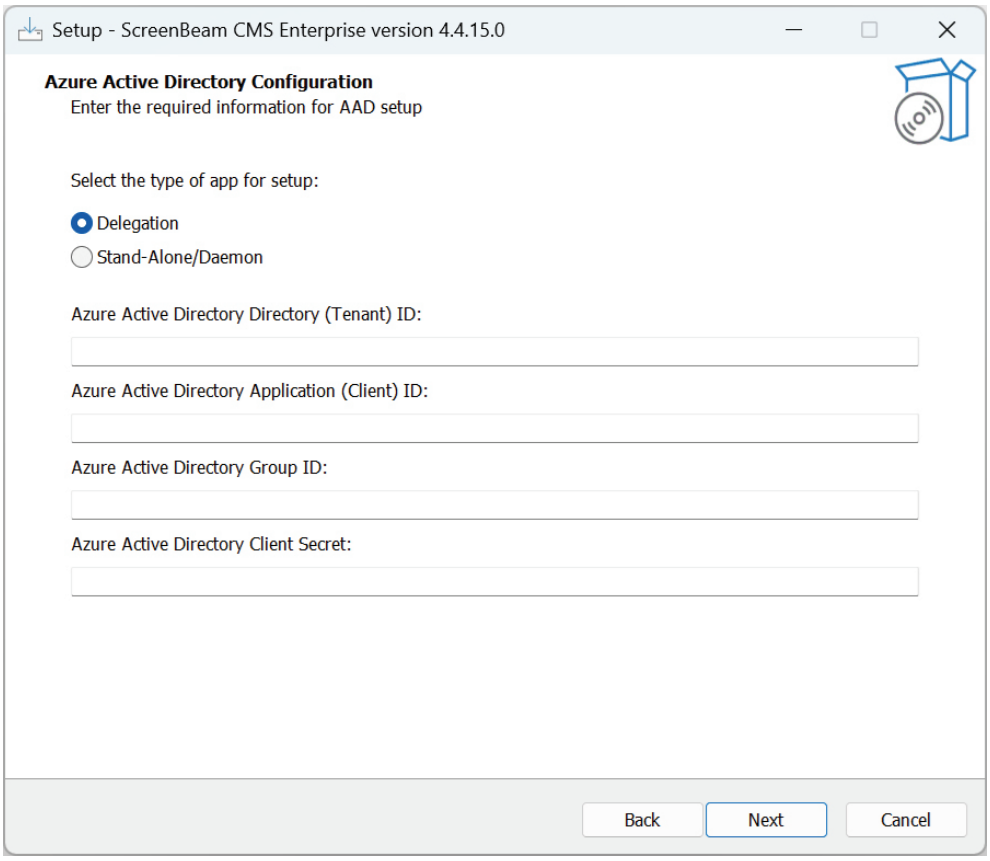


5. The **User Management Service Selection** window appears. Select **ScreenBeam CMS User Management** and click **Next**.
   - **ScreenBeam CMS User Management**. ScreenBeam CMS users will be managed locally with the Identity server.
   - **Azure Active Directory Service (AAD) (Beta)**. ScreenBeam CMS users will be managed using Azure Active Directory.

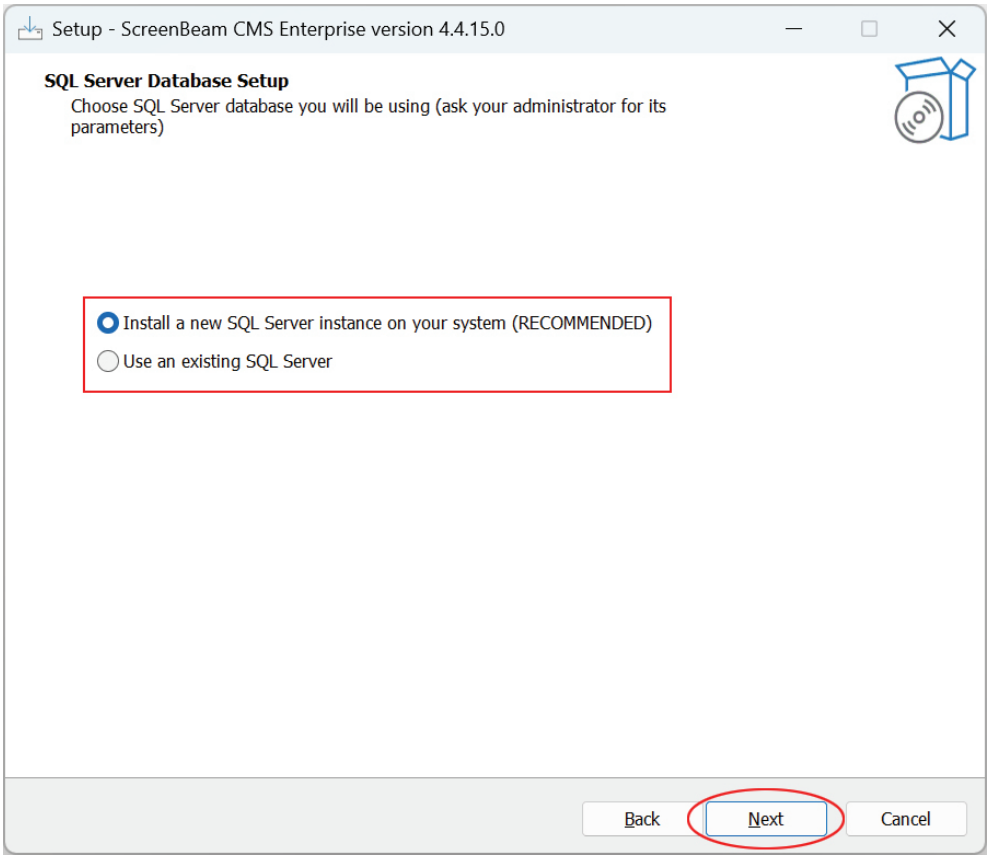


6. (Optional) If you choose **Azure Directory Service (AAD) (Beta)**, you need to specify the following parameters on the **Azure Active Directory Configuration** page that appears:
   - Delegation: CMS needs a signed-in user to request data from AAD.
   - Stand-Alone/Daemon: CMS can request permitted data without a signed-in user.
   - Azure Active Directory (Tenant) ID: The ID of the tenant used to manage ScreenBeam CMS.
   - Azure Active Directory Application (client) ID: It is the ID of the registered app for ScreenBeam CMS.
   - Azure Active Directory Group ID: It is the ID of the Security group that is assigned to manage ScreenBeam CMS.
   - Azure Active Directory Client Secret: It is the secret of the registered application for ScreenBeam CMS.

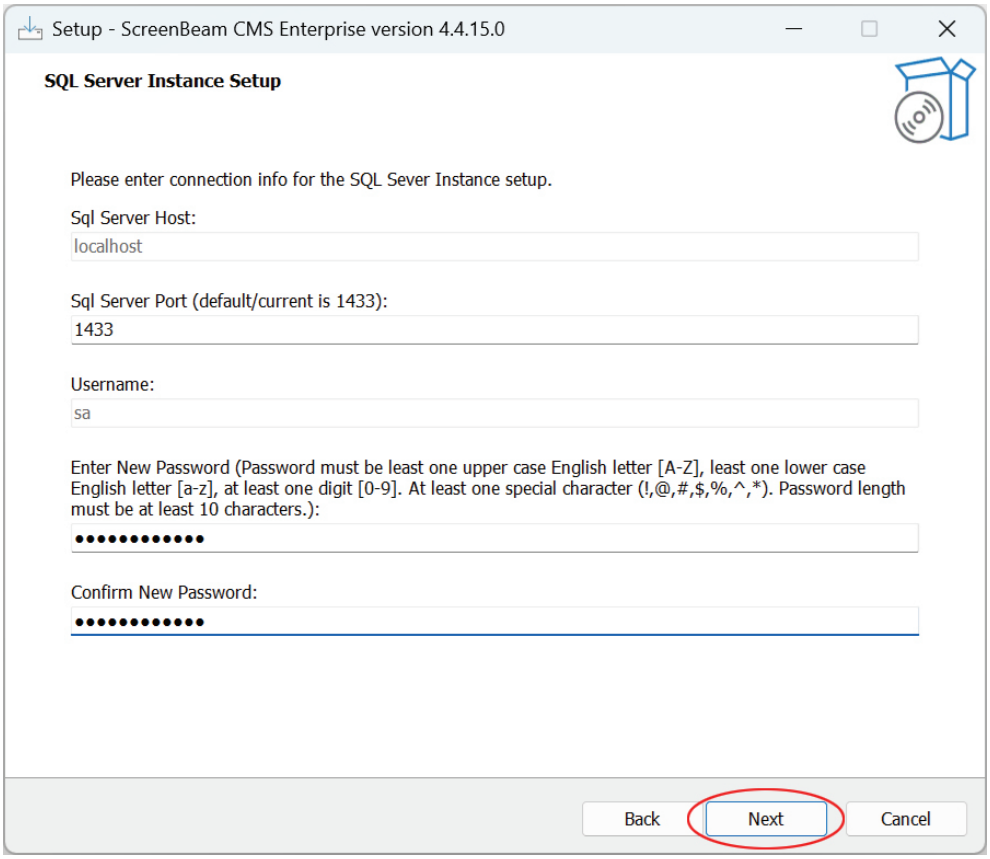
   Note: For detailed setups about Azure AD and ScreenBeam CMS, refer to Appendix I.



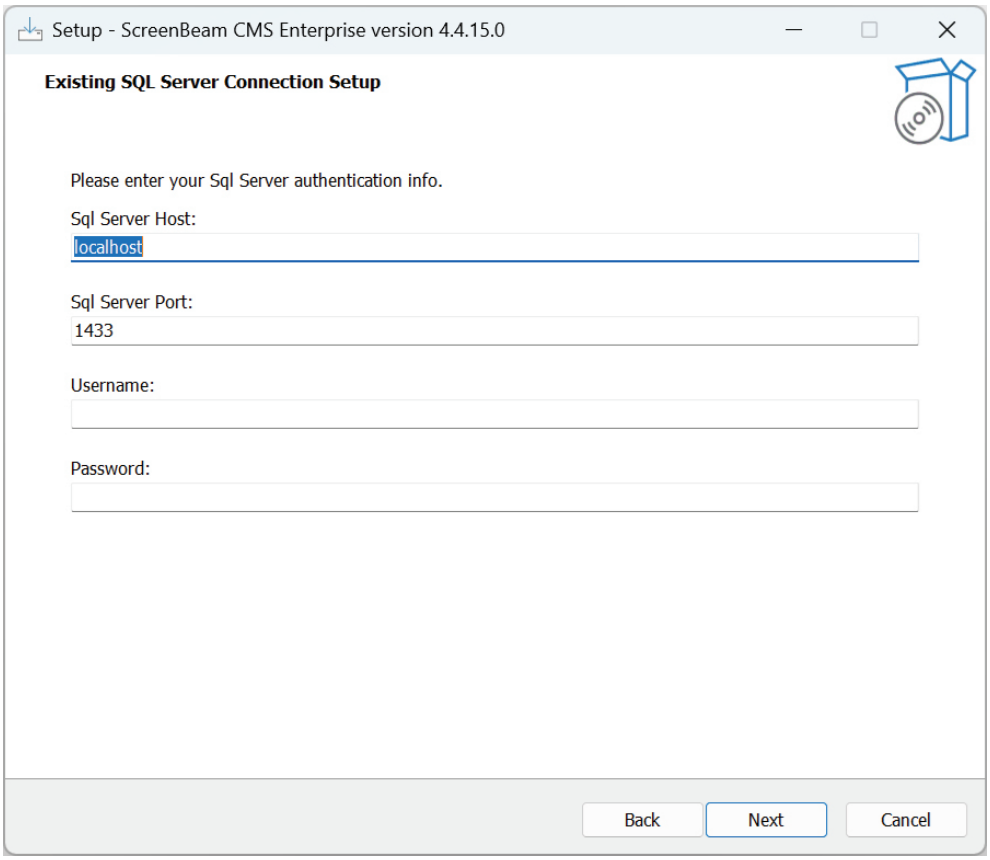
7. The SQL Server Database Setup window appears. Users are allowed to use an existing SQL server or install a new SQL Server instance.
   It is highly recommended to install an SQL Server instance on the same machine. As an existing SQL server on a separate machine can result in network latency, which will slow down CMS functions.
   Select **Install a new SQL Server instance on your system (RECOMMENDED)** and click **Next**.



8. The SQL Server Instance Setup page appears. A new SQL Server instance will be installed on your system, and you must define an SQL Server port and a password. Microsoft SQL 2017 Express will be installed.
   Define these parameters and click **Next** to continue.



If you choose to use an existing SQL server, you must set up the following parameters: SQL server host, SQL server port, username and password.

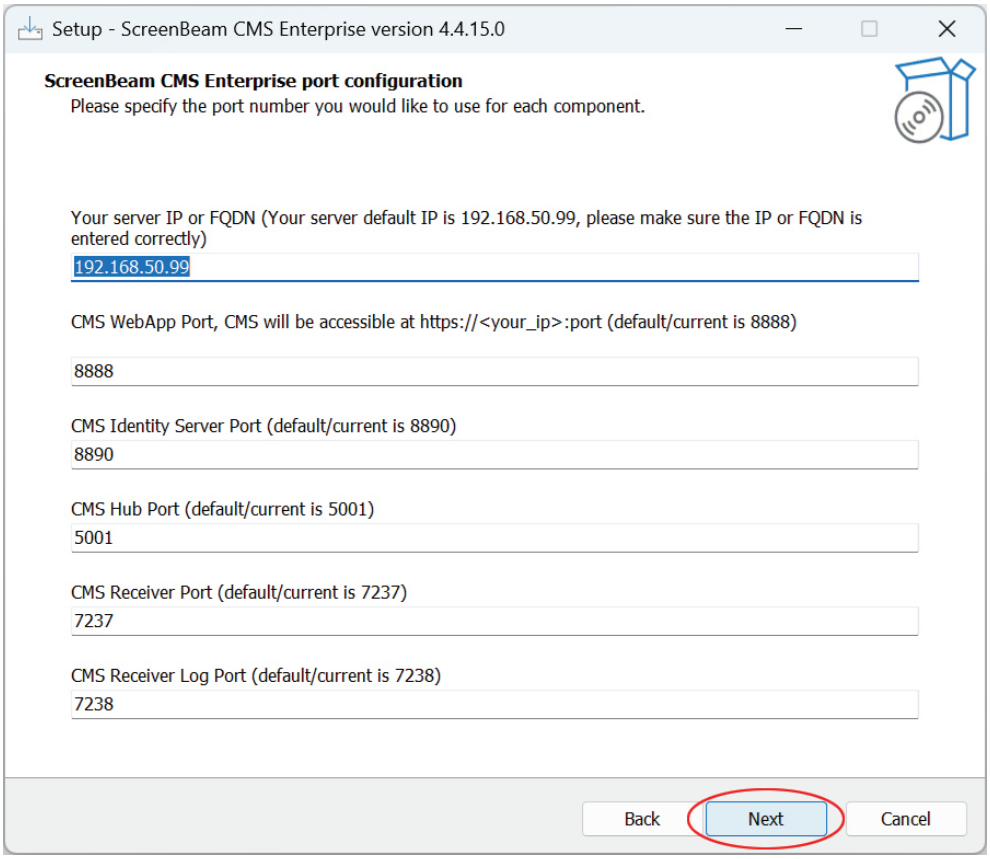


9. The ScreenBeam CMSv4 port configuration window appears.
   - **Your server IP or FQDN**: The CMS installer will get the IP address of your server automatically. If not, type the IP address of your server in this field. Note: You must enter the FQDN of your server in this field if you plan to access the CMS using an FQDN.
   - **CMS WebApp port**: This port is for accessing the CMS server via a web browser. The default port is 8888. If this port is already in use, specify a new one.
   - **CMS Identity Server Port**: This port is for communication between the CMS and the Identity server. The default port is 8890. If this port is already in use, specify a new one.
   - **CMS Hub port**: This port is for communication between the web app and the CMS server. The default port is 5001. If this port is already in use, specify a new one.
   - **CMS receiver port**: This port is for communication between receivers and the CMS server. The default port is 7237. If this port is already in use, specify a new one.
   - **CMS receiver log port**: This port is for uploading receiver logs to the CMS server. The default port is 7238. If this port is already in use, specify a new one.

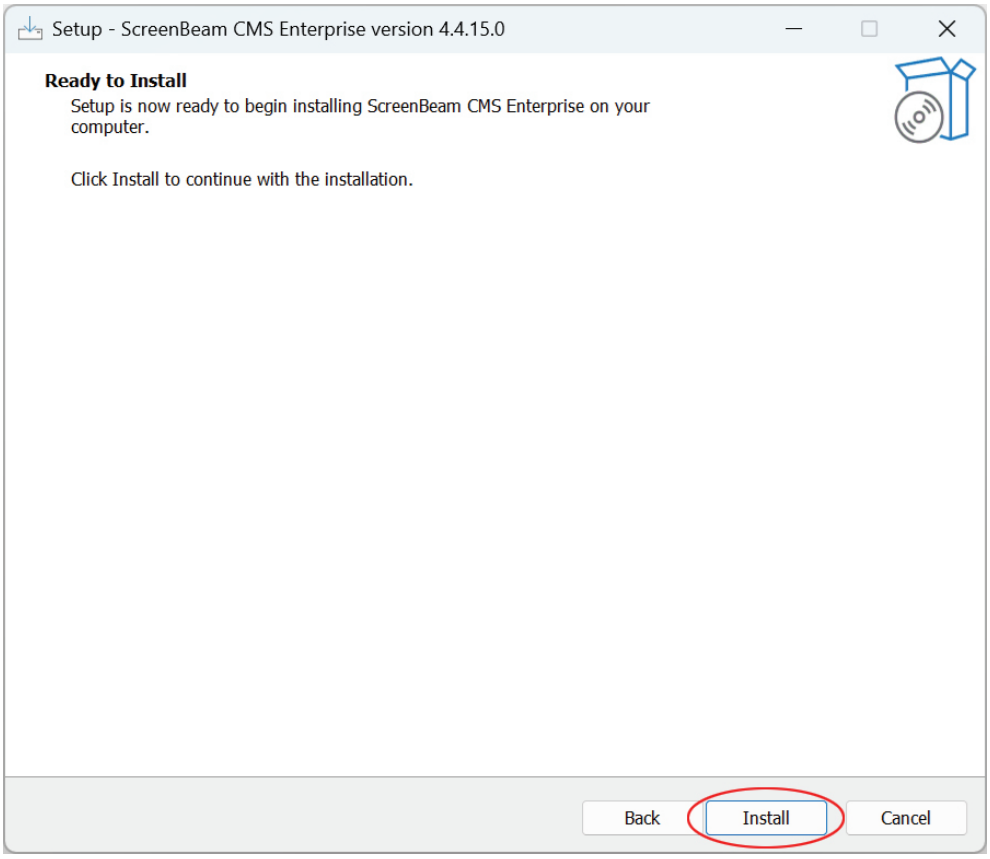
   Note: Valid port ranges from 1024 to 65535, provided these ports are not used by other devices on the network.

   Ensure that any custom port numbers are noted for future reference.

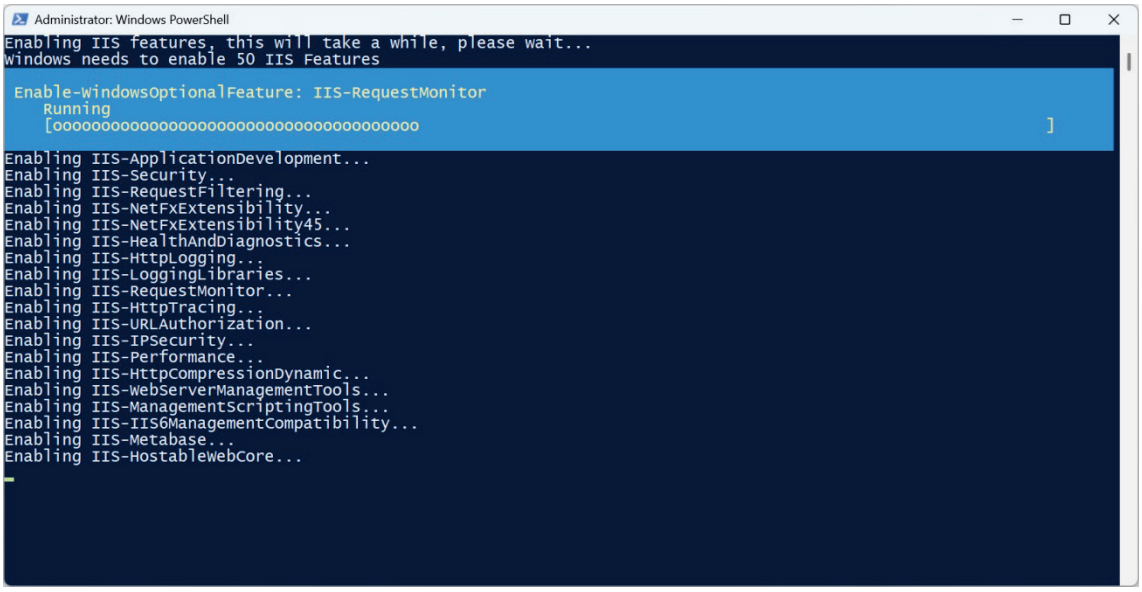
   Define these parameters and click **Next** to continue.



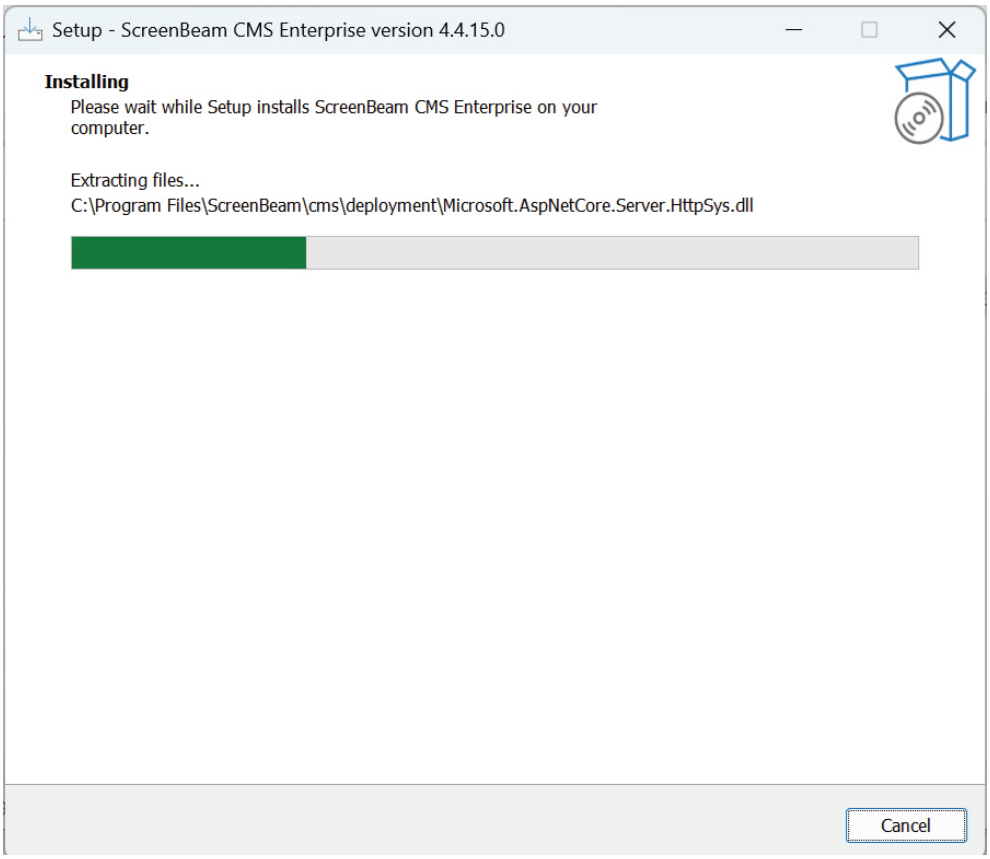
10. The **Ready to Install** window appears. Click **Install** to continue.
    The remaining installation process is automated. It may take some time to complete the installation.



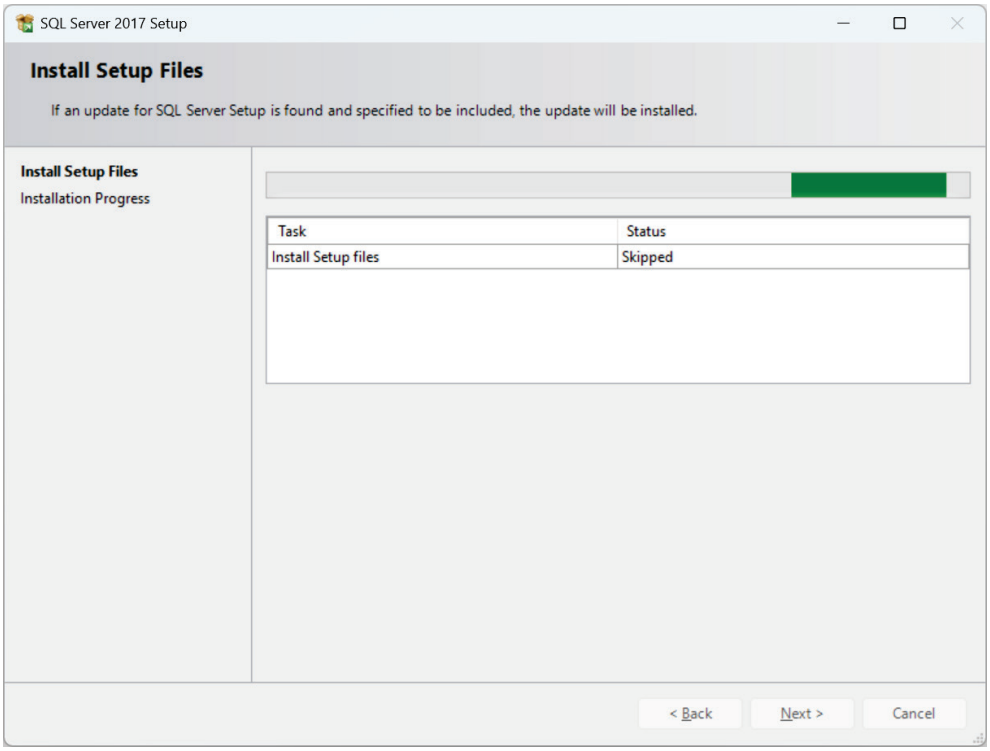
Enable IIS features.



Install ScreenBeam CMS Enterprise.

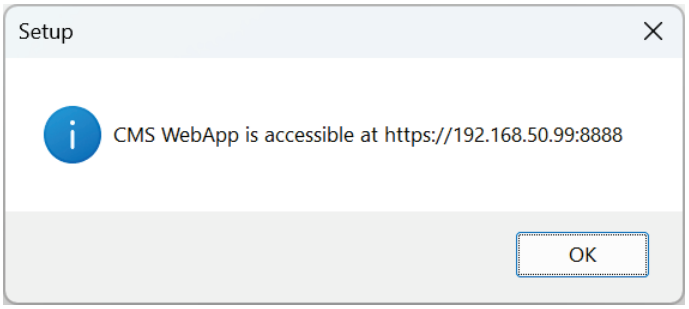


Install SQL server, if you choose to install a new SQL server instance.

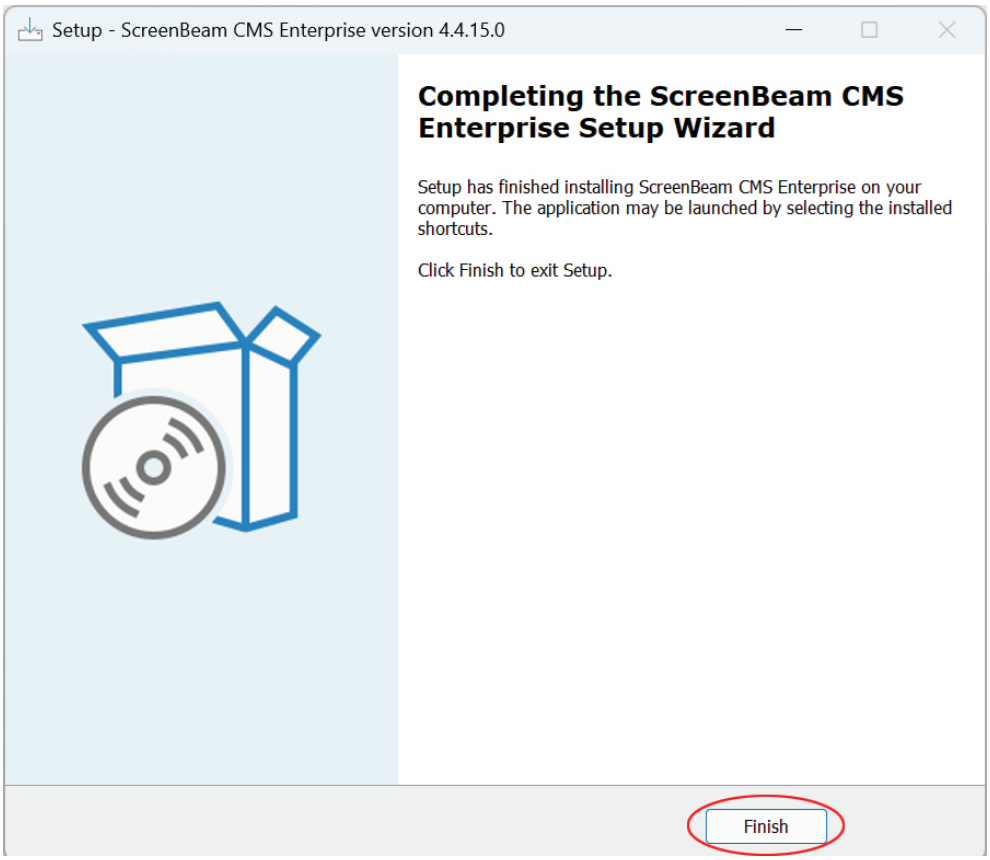


Note: Don’t click in the Windows PowerShell window during the installation. If you have done it, the installation may pause. In this case, you can press Enter to resume.

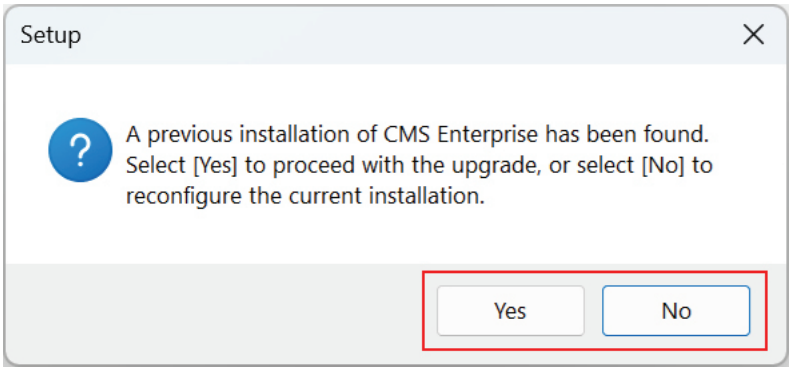
A message box that shows how to access the CMS WebApp appears. The CMS WebApp can be accessed via *https://<your_server_ip>:WebApp_port*



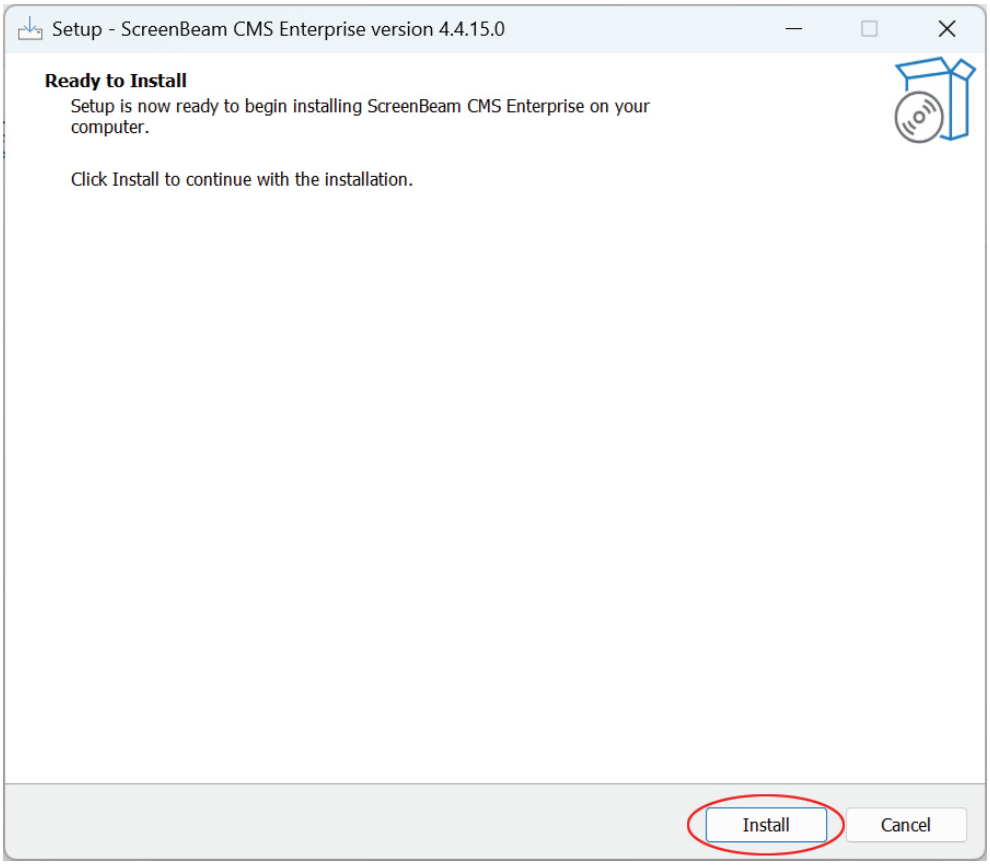
11. ScreenBeam CMS Enterprise is successfully installed when the installation completion window appears. Click **Finish**.



If there is an existing CMS installation, then the message box below will appear. Select **YES** to upgrade CMS or **NO** to reconfigure settings in your current installation.



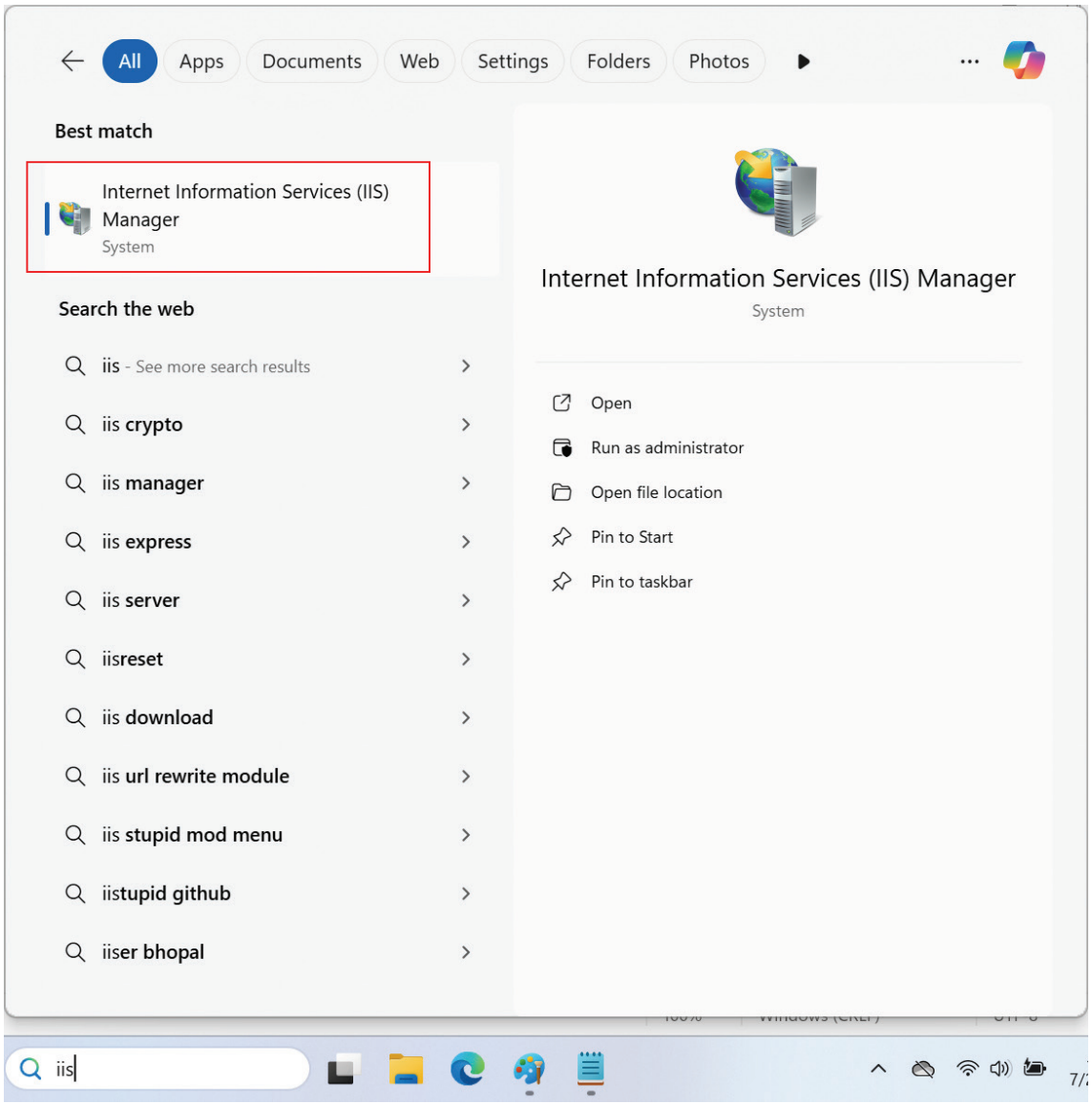
The **Ready to Install** window appears. Click **Install**. The remaining installation process is automated.



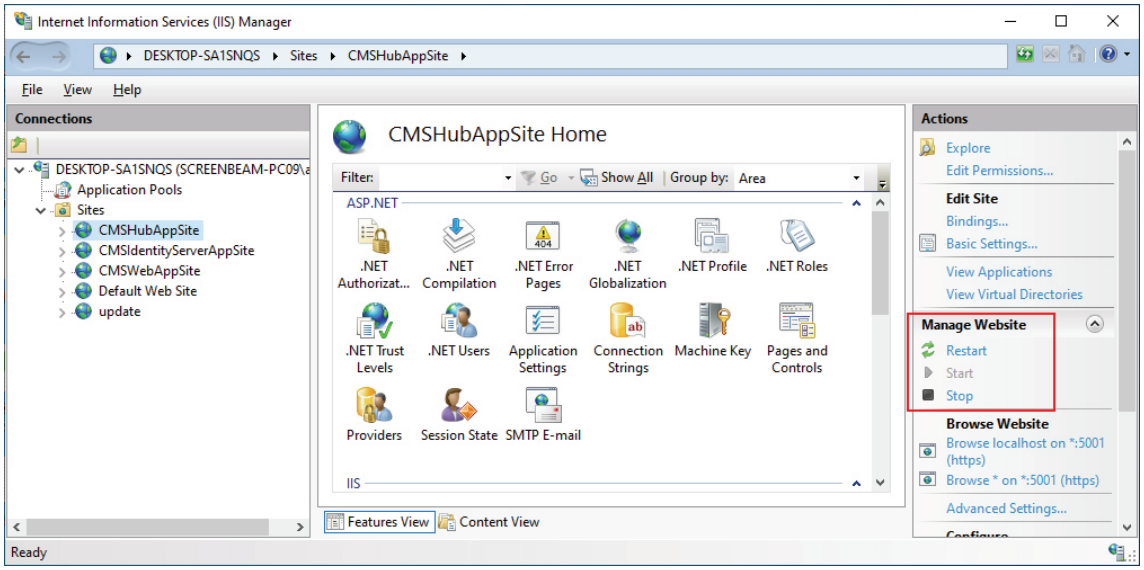
2.1.3 Check CMS Service Status

After the CMS is installed, you can check if the CMS services are running.
To check the CMS service status, follow this procedure:

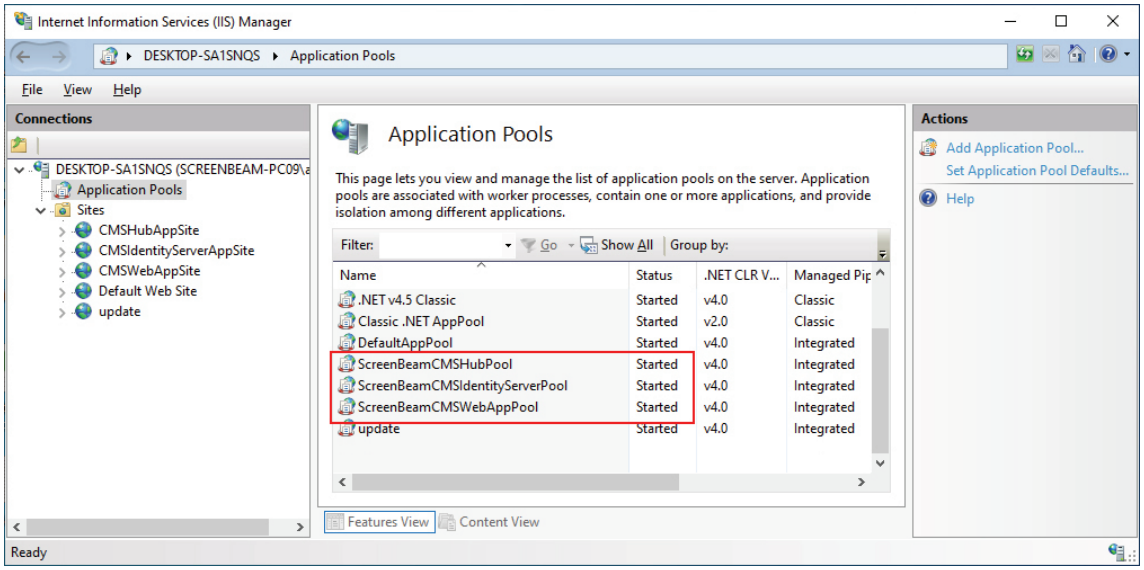
1. Open Internet Information Services (IIS) Manager on your server.



2. On the **Connections** pane, navigate to **Sites**, and check the status of the following sites: **CMSHubAppSite**, **CMSIdentityServerAppSite**, and **CMSWebAppSite**.
   - When these sites are started, the CMS is running.
   - When one of these sites is stopped, the CMS is out of service.



3. On the **Connections** pane, select **Application Pools**, and check the status of the following pools: **ScreenBeamCMSHubPool**, **ScreenBeamCMSIdentityServerPool**, and **ScreenBeamCMSWebAppPool**.
   - When these pools are started, the CMS is running.
   - When one of these sites is stopped, the CMS is out of service.

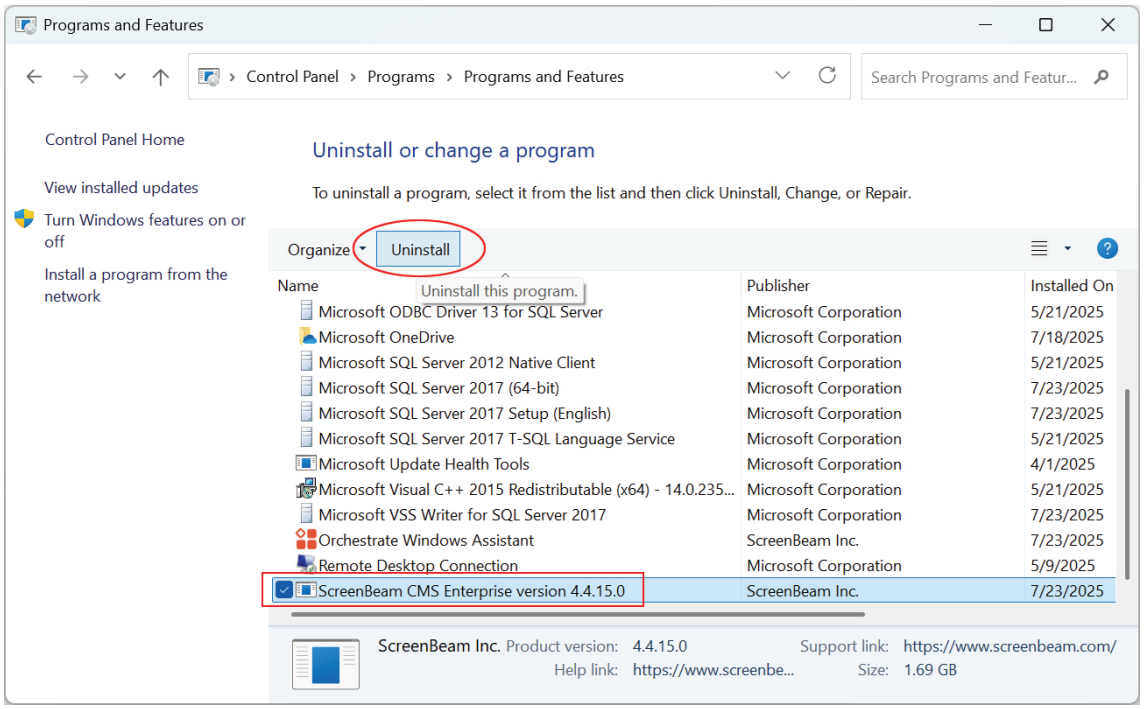


2.1.4 Uninstall ScreenBeam CMS

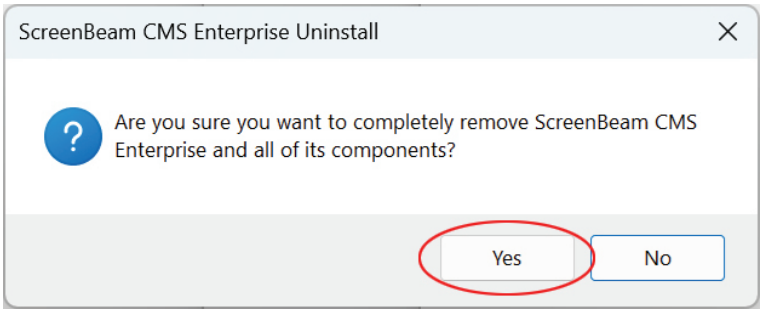
Note: Ensure that all receivers are switched to the new CMS server before starting the uninstallation process. You may back up your CMS data before you uninstall your CMSE. Refer to Appendix II for details.

To uninstall ScreenBeam CMS, follow this procedure:

1. Go to **Control Panel** > **All Control Panel Items** > **Programs and Features**, select **ScreenBeam CMS Enterprise version 4.x.x.x** and click **Uninstall**.



2. The **ScreenBeam CMS Enterprise Uninstall** message box appears. Click **Yes** to uninstall ScreenBeam CMS Enterprise.



2.2 DNS Server and DHCP Server

A DNS server, while technically optional, is strongly recommended for discovery of ScreenBeam receivers. DNS Discovery allows all ScreenBeam receivers discovered by the CMS server, requiring very little user interaction once the network is configured properly. Additional details on this method can be found in **Section 3.2 Provisioning Receivers Using DNS Discovery Method**.

2.3 HTTP Server

An HTTP server should be deployed in parallel with CMS to host the firmware files and other miscellaneous files used for upgrading or customizing ScreenBeam Receivers.

For a large ScreenBeam deployment, the HTTP server should be of commercial-grade, capable of handling a large number of simultaneous connections and bandwidth as policy and network capabilities shall permit.

Generally, the HTTP server should meet these requirements:

Minimum Requirements (for 100 or less receivers):

- OS: Windows 10 Pro
- CPU: 1.4 GHz 64-bit Processor
- RAM: 8 GB
- Disk space: 40 GB of free space
- Network: PCI-E Ethernet adapter capable of at least 1 Gbps throughput

Recommended Requirements (for 1000 or more receivers):

- OS: Linux Server NGINX or equivalent Windows server 2019
- CPU: 8-Core @ 2.4 GHz or faster
- RAM: 16 GB or more
- Disk space: 100 GB of free disk space
- Network: PCI-E Ethernet adapter capable of 1 Gbps throughput or faster

Note: While the same CMS host can technically be used to host a web server, this may result in unpredictable CMS and/or HTTP server behavior. Use of a different server is highly recommended to ensure optimal performance.

Part III Provisioning ScreenBeam Receivers

ScreenBeam receivers can connect to ScreenBeam CMS by DNS or by USB provisioning. Details on this process are provided below.

3.1 Connecting ScreenBeam Receivers to Network

CMS supports ScreenBeam models SBWD960A, SBWD960B, SBWD1000EDU, SBWD1000EDU Gen2, SBWD1100, SBWD1100F, and SBWD1100P. These receivers provide both LAN and WLAN connectivity. For LAN connection, use an Ethernet cable to connect the receiver's Ethernet port to a LAN port. For WLAN connection, configure wireless connection parameters using the receiver's Local Management Interface or CMS' USB Provisioning to connect the device to a Wi-Fi Access Point. Refer to the corresponding receiver's user manual for details.

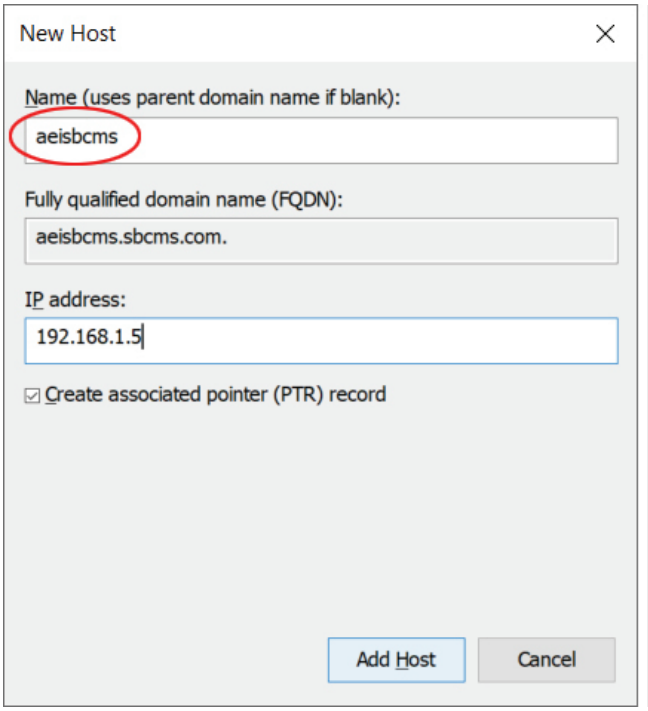
When first deploying receivers, verify that an IP address is assigned to the receiver at the default Ready to Connect screen on the front-of-room display. ScreenBeam receivers are set to obtain IP addresses from the DHCP server automatically by default.

3.2 Provisioning Receivers Using DNS Discovery Method

DNS Discovery of ScreenBeam receivers can be used if access to a Corporate DNS Server is available. Ensure DHCP servers advertise the corporate domain (e.g. mycompanyname.com).

To provision receivers using DNS discovery, follow the procedure below:

1. Add the CMS's default hostname (aeisbcms) to an A-record of the corporate DNS server. Point this entry to the CMS IP address. Ensure that all the DHCP Servers connected to the ScreenBeam receivers assign this DNS to its clients.



2. Power the receiver on and connect it to the network.
3. Access the CMS web app in a browser and verify that the receiver appears on the list and is online.
4. Manage the ScreenBeam receivers using the CMS as usual.

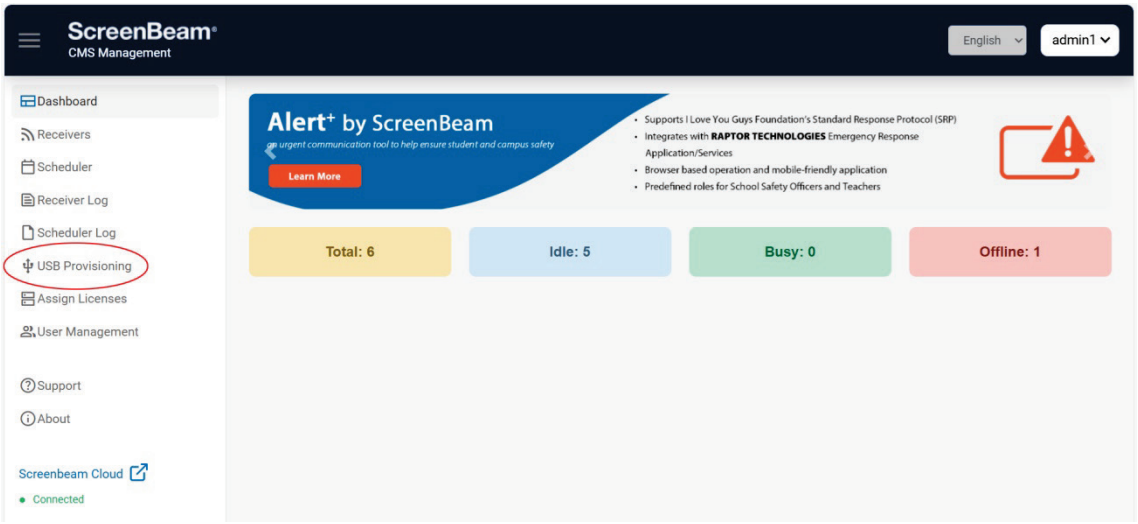
ScreenBeam receivers can also be configured to use the CMS IP address instead of domain name if a static IP exists. Please refer to the corresponding receiver User Guide for details.

3.3 Provisioning Receivers using Static IP Discovery - USB Method

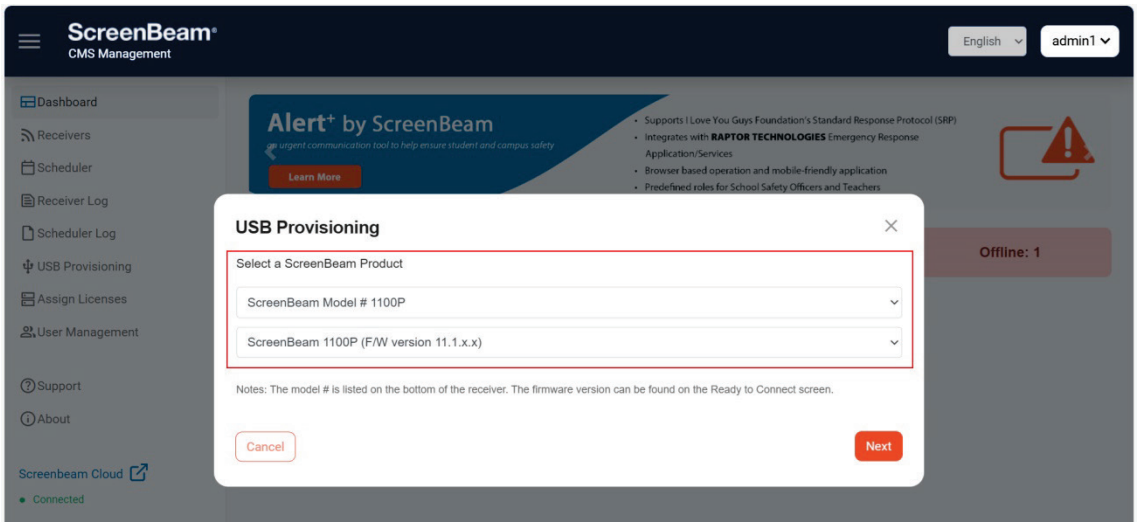
If DNS is unavailable, the following method can be used to provision receivers using Static IP discovery using a USB flash drive.

Initial login and user creation is required before creating the USB configuration file. Instructions can be found in **Section 4.1 Login**.

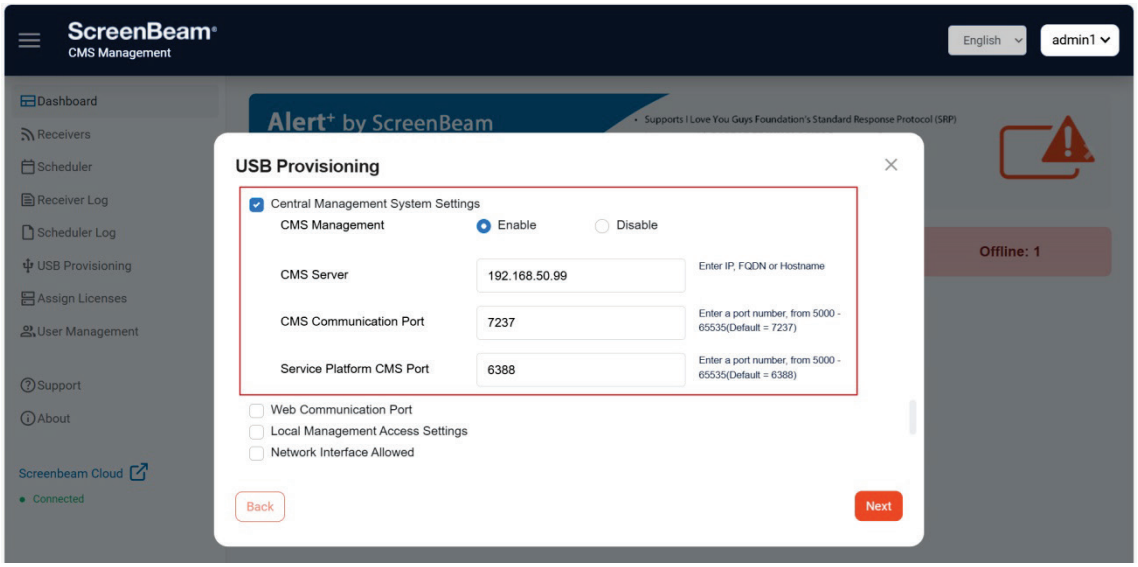
1. Launch a web browser and access the CMS server's IP address (https://CMS_server_IP:8888).
2. Select **USB Provisioning** from the left pane.



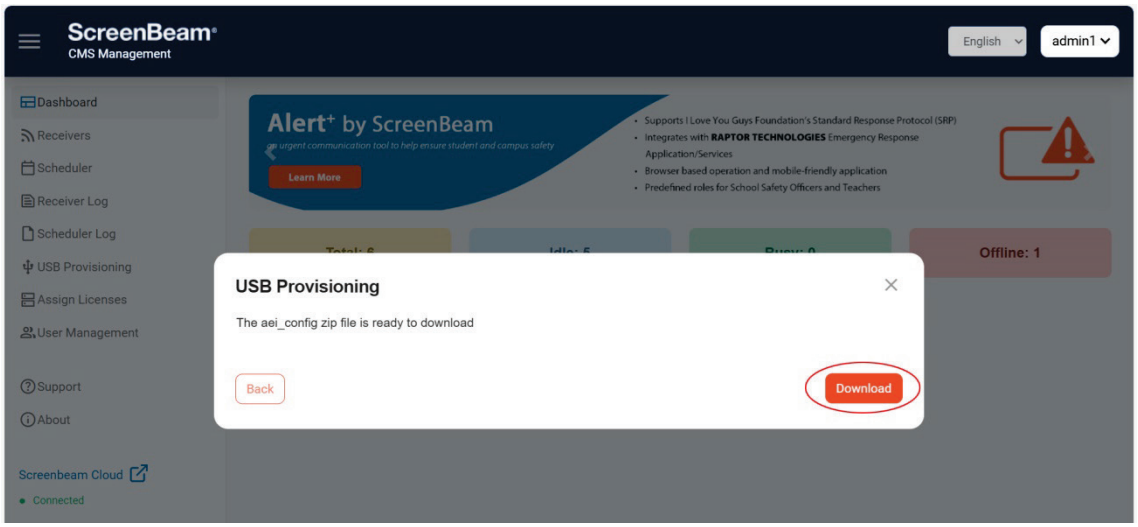
3. The **USB Provisioning** window appears. Select a ScreenBeam product and its firmware. Click **Next**.



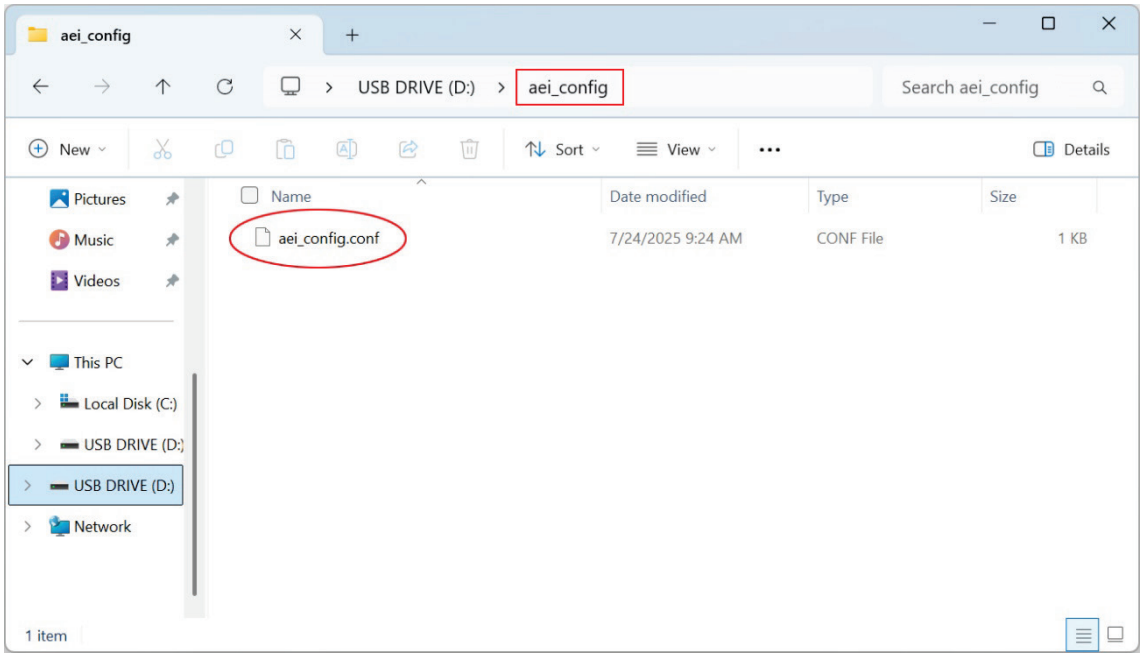
4. Select **Central Management System Settings** on the configuration item list and set **CMS Management** to **Enable**, enter the CMS IP address (or FQDN / hostname) in the **CMS Server** box, the CMS port number in the **CMS Communication Port** box and the service platform port in the **Service Platform Port** box, then click **Next**.
   Note: The Service Platform Port is used for communication between ScreenBeam receivers and ScreenBeam CMSE 4.3.10.13 or older.



5. The download page appears. Click **Download** and save the receiver configuration file (**aei_config.zip**).



6. Unzip the downloaded receiver configuration file (**aei_config.zip**) and copy the “aei_config” folder to the root directory of a FAT32 formatted USB flash drive. Ensure that the receiver configuration file (aei_config.conf) is in the **aei_config** folder, and no modifications to the name or file contents are made.



7. Power on the ScreenBeam receiver. When the Ready to Connect screen appears, plug in the USB flash drive. After the receiver has rebooted, it is provisioned and ready for deployment.

8. Power off the ScreenBeam receiver and deploy it in its final location, then power it back on. At the Ready to Connect screen, verify that an IP address is assigned to the receiver and that it is connected to the CMS.

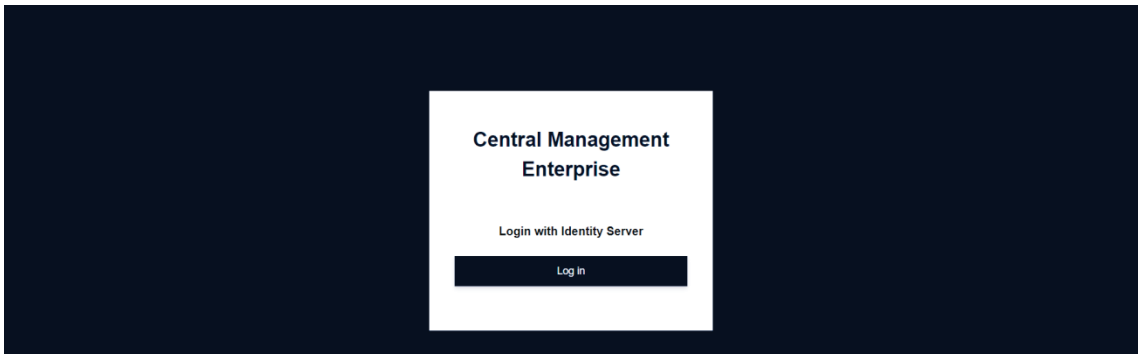
9. In CMS, verify that the ScreenBeam receiver appears on the list and is online. This will verify that the ScreenBeam receiver can now be provisioned and monitored using CMS.

Part IV Manage ScreenBeam Receivers with CMS

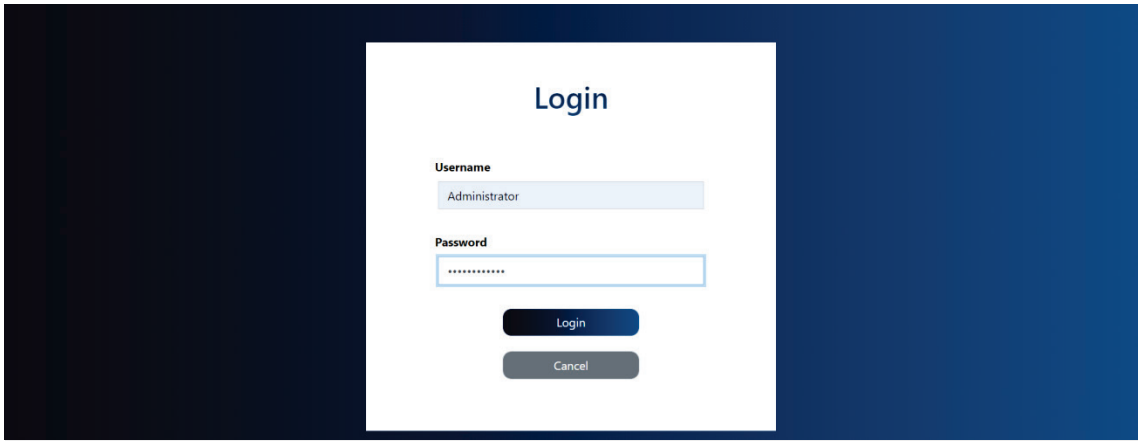
After ScreenBeam CMS server and companion servers are deployed and ScreenBeam receivers are provisioned, the ScreenBeam receivers can then be managed using CMS. The capabilities of ScreenBeam CMS are shown below.

4.1 Login

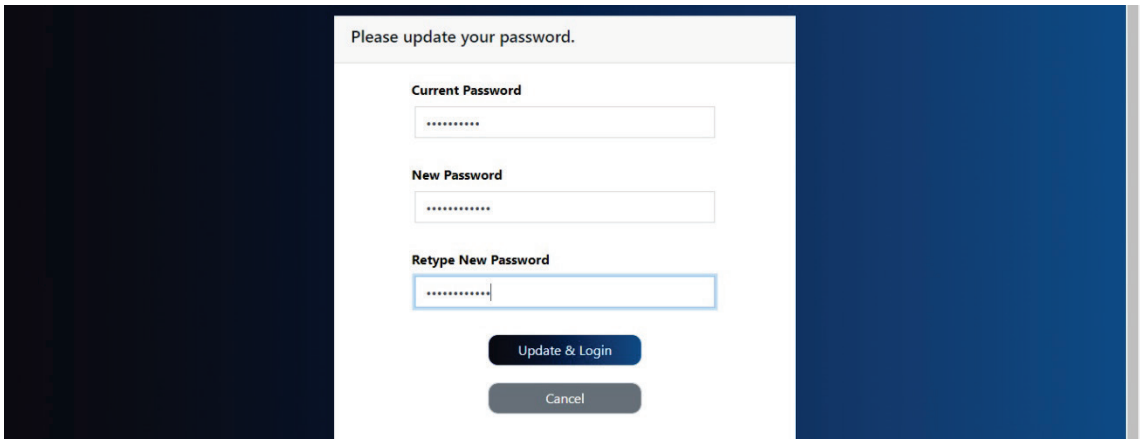
ScreenBeam CMS uses a multi-user web-based user interface, meaning that multiple users can use CMS simultaneously to monitor and manage ScreenBeam receivers. The CMS web interface can be accessed using the hostname or IP at a port of 8888 (or the port of choice during CMS configuration), e.g. https://<CMS_Address>:8888.



The default Administrator role username and password are **Administrator** and **Screenbeam**, respectively. All other user logins will use the credentials provided by the Administrator.



If this is the first time you log in as Administrator or any other CMS user, you are required to change the password for the CMS user.

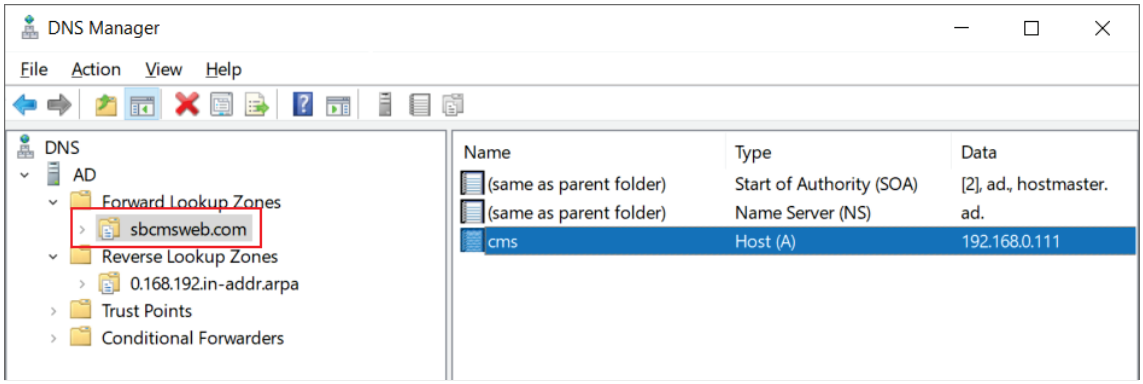


The browser may give an error stating “The connection or site is not secure or private.” Manually accept the connection as follows:

- Chrome browser: click **Advanced**, and then click **Proceed to ….**
- Edge browser: click **Advanced**, and then click **Continue to ….**
- Firefox browser: click **Advanced**, then click **Accept the Risk and Continue**.

To avoid the certificate warning page, follow this procedure:

1. Create a forward lookup zone on your DNS, and name it "**sbcmsweb.com**".



2. Add an A record to this zone, e.g. **cms.sbcmsweb.com**, and point it to the IP address of the CMS machine.
3. Ensure the PC running the browser can resolve the CMS IP address.
4. Type the URL e.g. https://cms.sbcmsweb.com:8888

4.2 Basic Functions

The primary functional areas available in a ScreenBeam CMS session are:

- Dashboard – provides a general overview and statistics of the CMS.
- Receivers – provides information on all receivers managed by a CMS user through the Sites pane, Receivers pane and Users pane.
  - Site pane – displays the sites where ScreenBeam receivers are located.
  - Receivers pane – displays receivers' basic information, allows users to configure receivers, update receiver firmware, reboot/reset receivers
  - Users pane – allows CMS SysAdmin to view users assigned to site, and re-assign roles or delete roles.
- Scheduler – creates scheduled tasks for managing receivers.
- Receiver Log – gives access to receiver logs.
- Scheduler Log – gives access to scheduler logs.
- USB Provisioning – allows receiver configuration using a USB flash drive.
- License Management – allows users to manage licenses for management of ScreenBeam 960 and ScreenBeam 750 receivers, Orchestrate by ScreenBeam, ScreenBeam Alert Plus, ScreenBeam Message Manager, etc..
- User Management – allows the CMS system administrator to add, delete, and edit users and roles.
- Alert – allows CMS administrators to push alert to ScreenBeam receivers.

These items will be discussed in additional detail below.

4.3 Connecting CMS to ScreenBeam Cloud

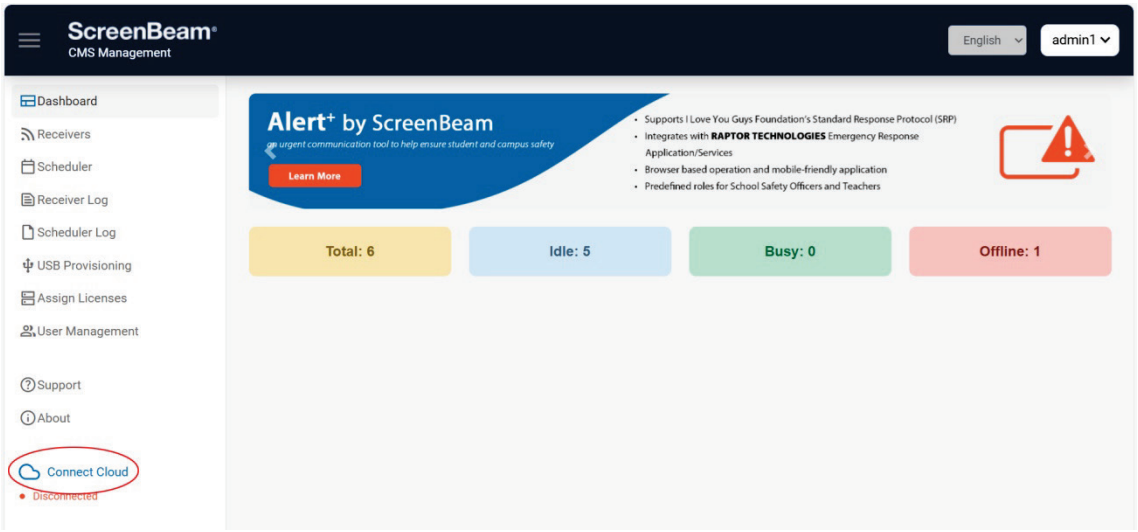
The ScreenBeam license service is managed on ScreenBeam Cloud. ScreenBeam CMS is required to connect to ScreenBeam Cloud to access this service and many others. This section describes some ScreenBeam Cloud features that are related to the use of ScreenBeam CMS.

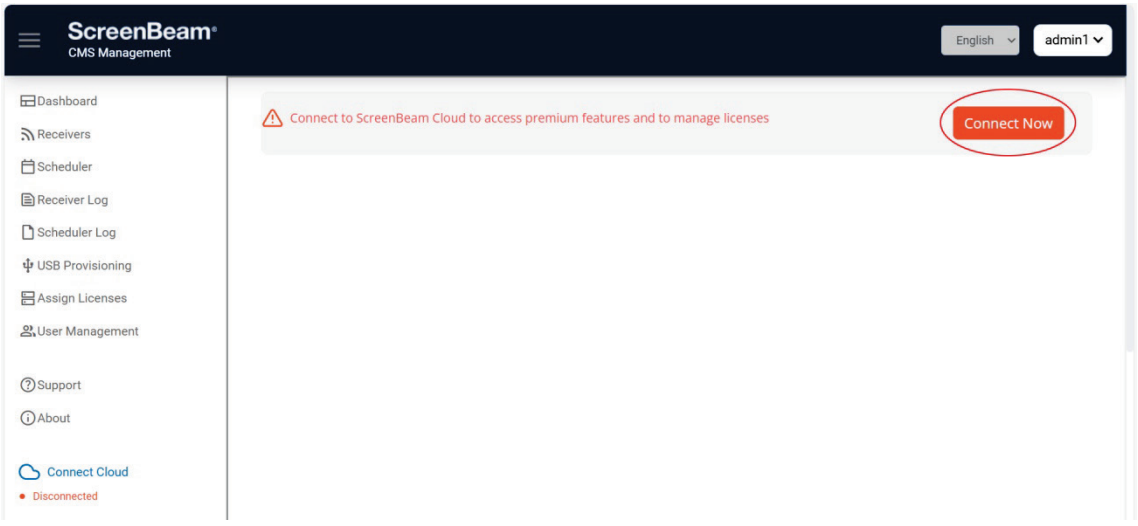
Note: Internet access is required for using services on ScreenBeam Cloud.

4.3.1 Signing up for ScreenBeam Cloud

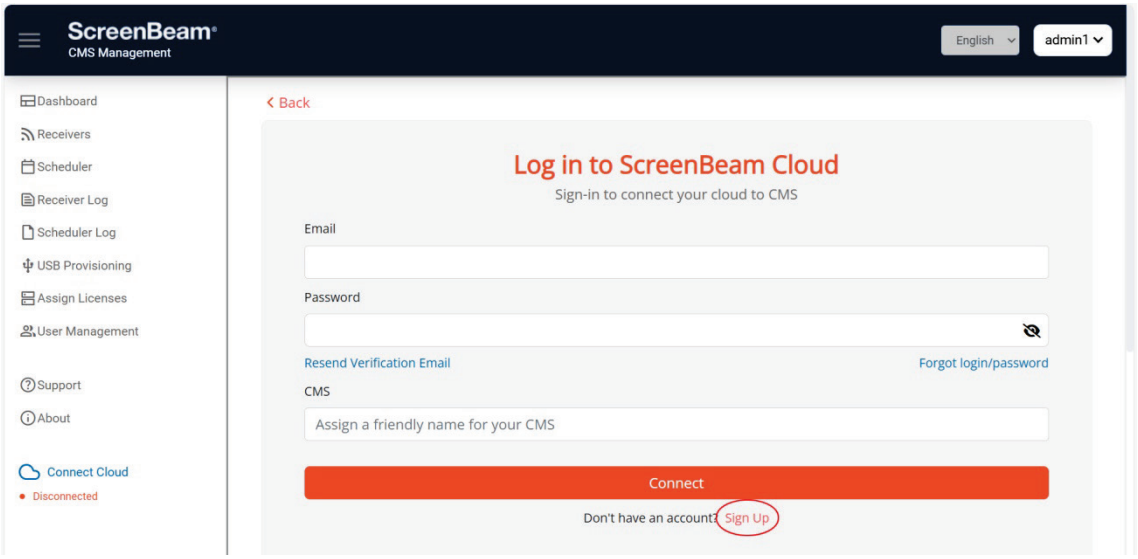
If you are new to ScreenBeam Cloud, sign up first. Follow the procedure below to sign you up:

1. Log into ScreenBeam CMS with a CMS SysAdmin user.
2. Click the **Connect Cloud** button in the bottom of the left menu, and then click the **Connect Now** button on the page that appears.

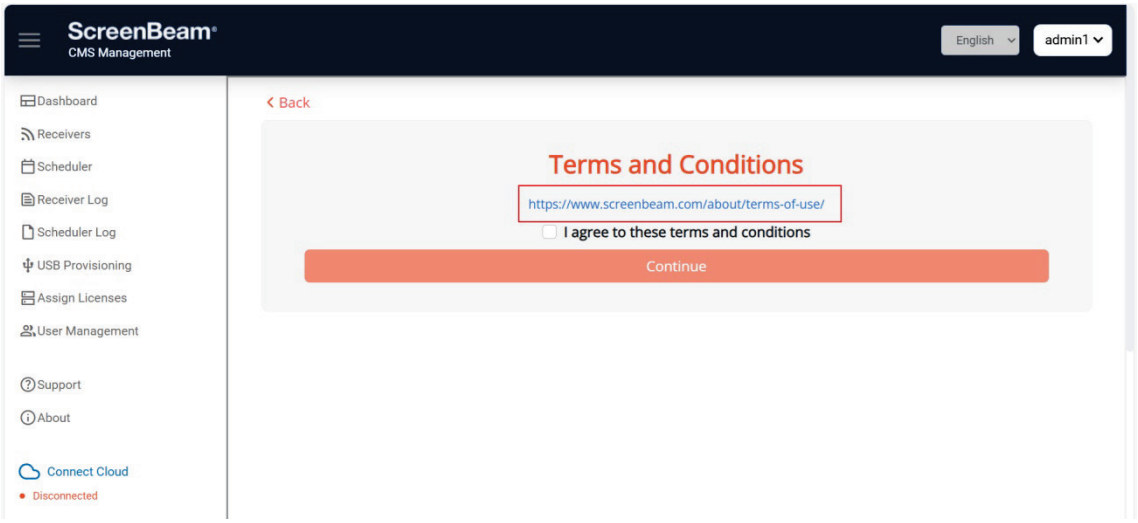




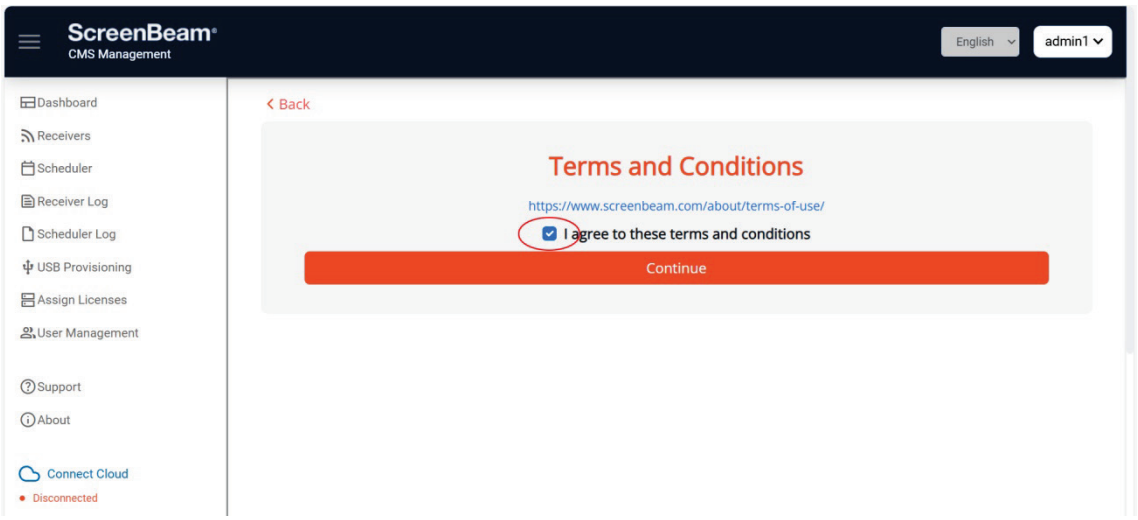
3. The **Log in to ScreenBeam Cloud** page appears. Click **Sign Up** at the lower part of the page.



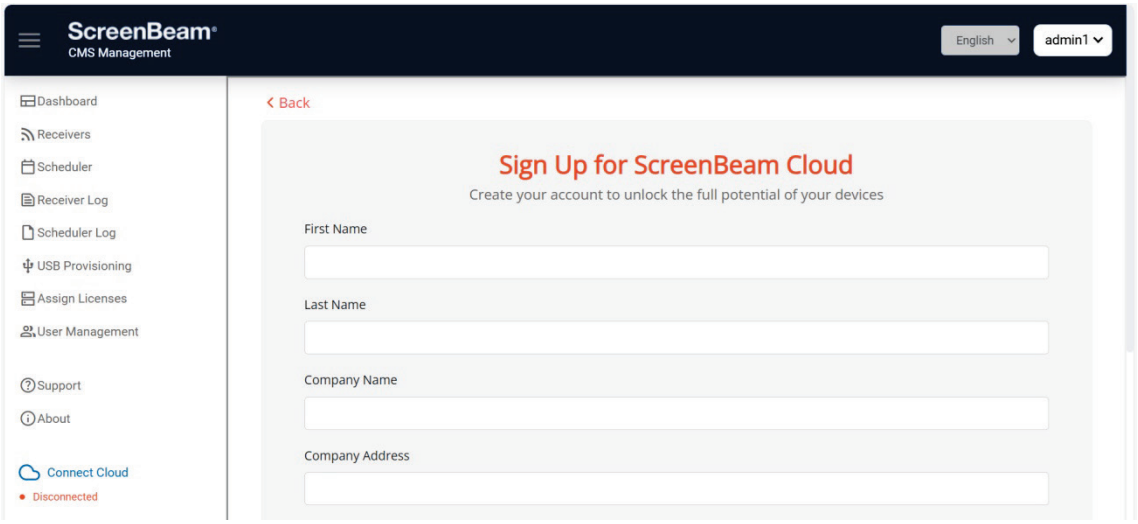
4. The Terms and Conditions page appears. Click the Terms and Conditions link (**https://www.screenbeam.com/about/terms-of-use**) to read the Terms and Conditions of ScreenBeam Cloud carefully.



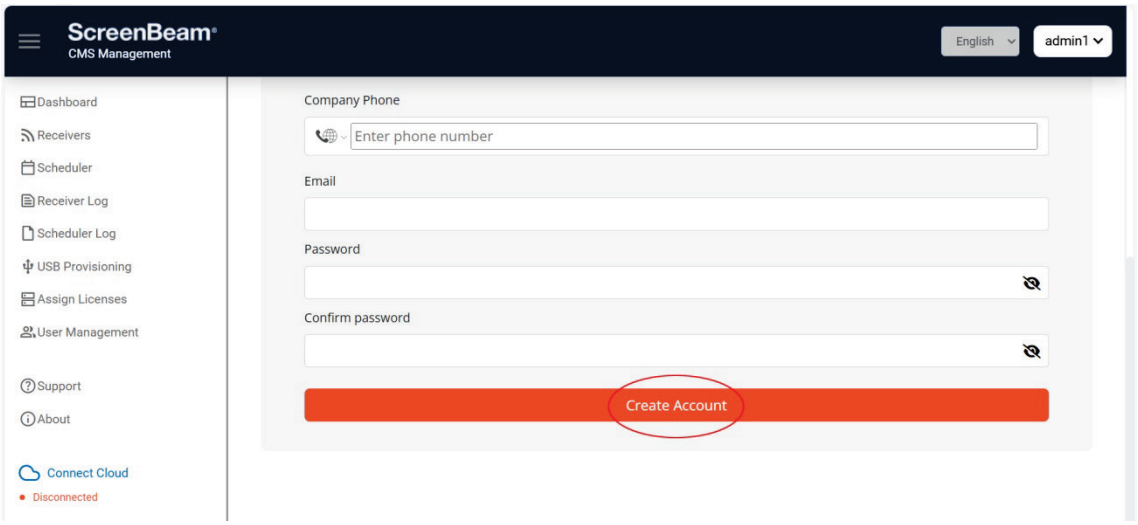
5. Check the **I agree to these terms and conditions** box. Then click the **Continue** button.



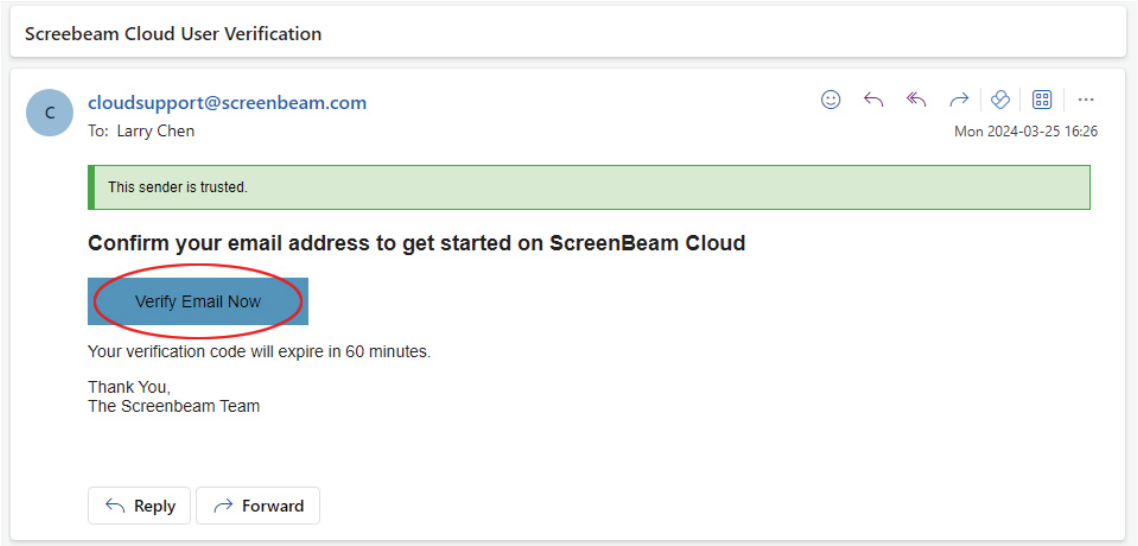
6. The **Sign Up for ScreenBeam Cloud** page appears. Fill out all fields on this page.
   Note: The password must include at least one upper case English letter [A-Z], one lower case English letter [a-z], one digit [0-9], and one special character. And the length of password must be 9-64 characters.
   The top 50 email domains in this list (https://www.gmass.co/domains) are not supported.



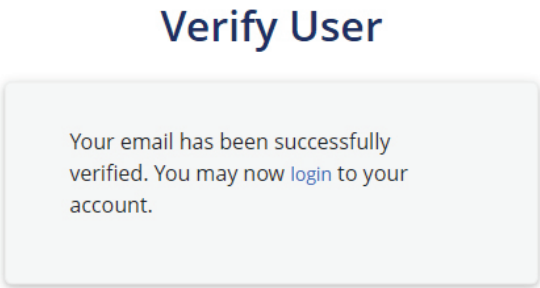
7. Click the **Create Account** button. ScreenBeam Cloud will create an account, and a verification email will be sent to the email address you have filled in the **Email** box in the **Sign Up for ScreenBeam Cloud** page.



8. Go to your email box and look for the email titled “Screenbeam Cloud User Verification”, which is sent by **cloudsupport@screenbeam.com**. Open this email and click **Verify Email Now**.



9. Your account will be activated successfully when the **Your email has been successfully verified. You may now login to your account.** shows.

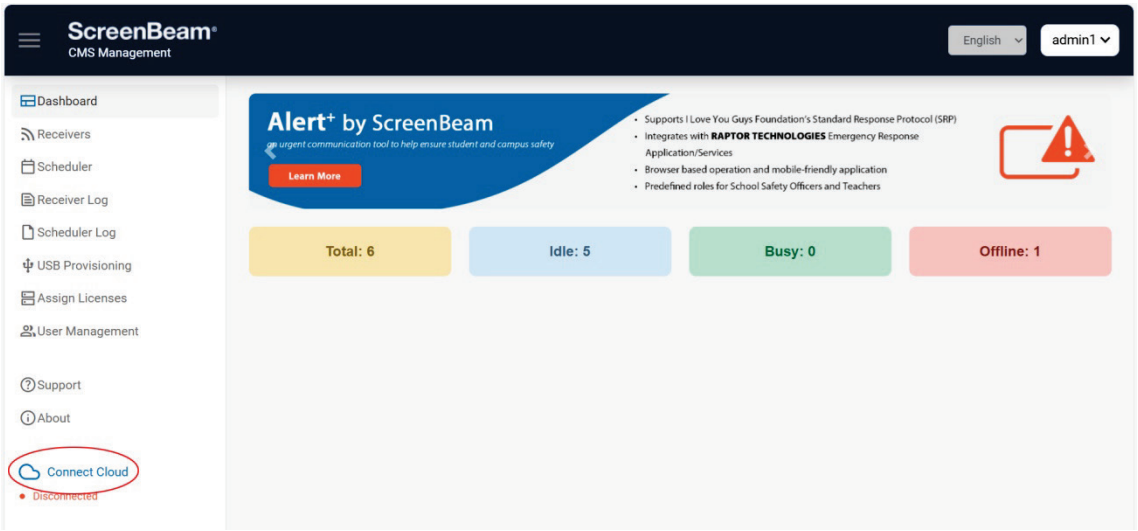


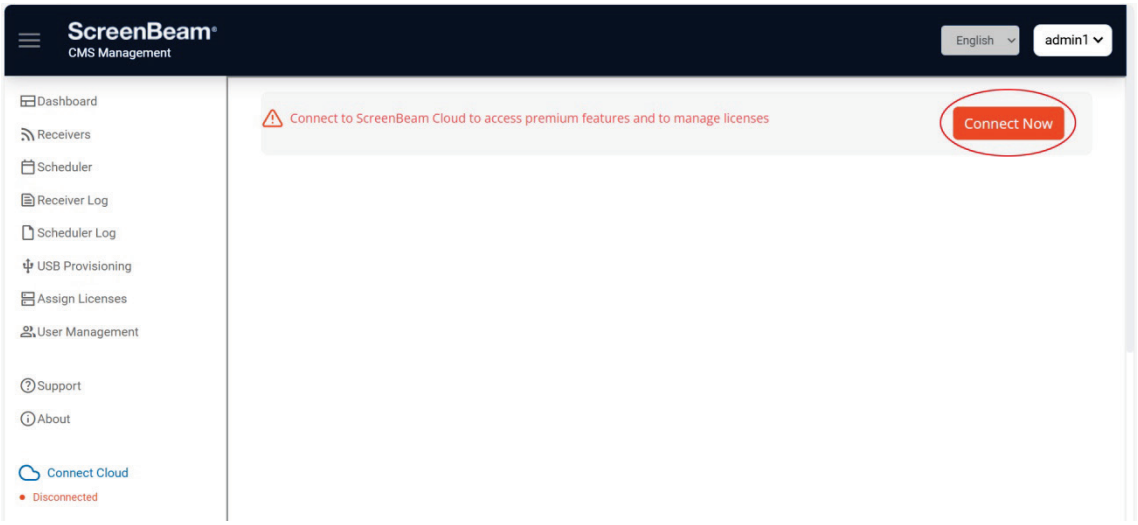
Note: ScreenBeam Cloud will create a tenant for the signed-up user. This user is the account owner of the tenant. If the organization needs more users for management purposes, the account owner can invite other users in the organization to ScreenBeam Cloud. In this way, the account owner has more control over the invited users' privileges.

4.3.2 Connecting CMS to ScreenBeam Cloud

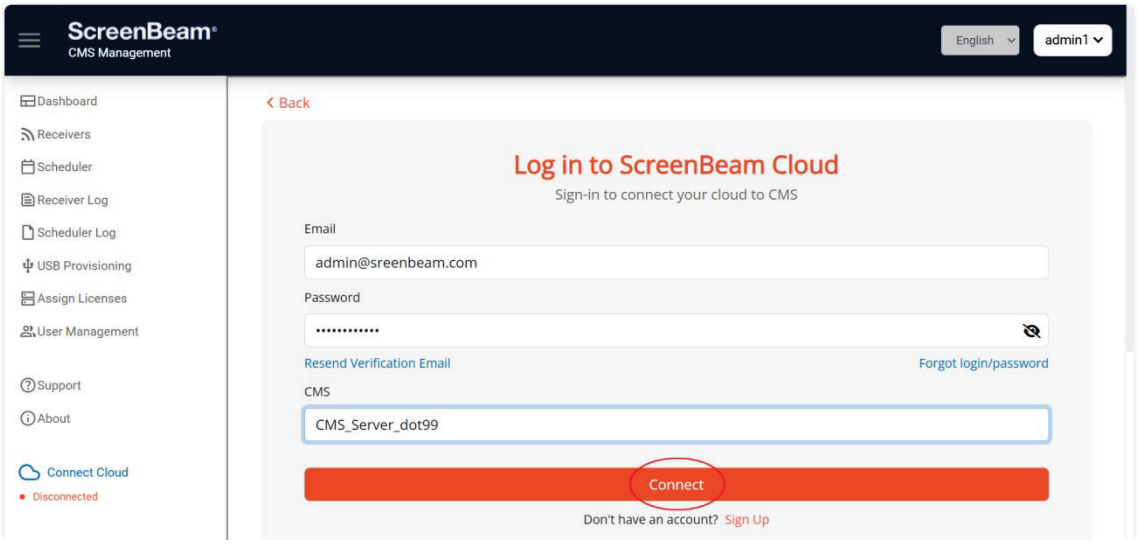
Follow the procedure below to connect your CMS to ScreenBeam Cloud:

1. Log into ScreenBeam CMS with a CMS SysAdmin user.
2. Click the **Connect Cloud** button in the bottom of the left menu, and then click the **Connect Now** button on the page that appears.

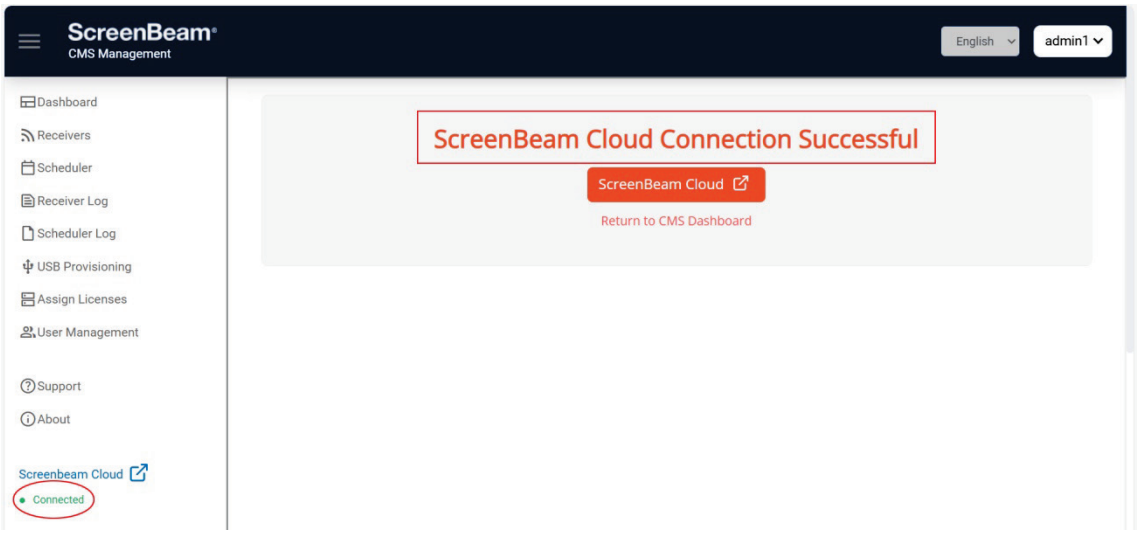




3. The **Log in to ScreenBeam Cloud** page appears. Type the email that you have registered in section **4.3.1 Signing up for ScreenBeam Cloud** in the **Email** box, and your password in the **Password** box. And give your CMS a friendly name in the **CMS** box. Click **Connect**.



4. Your CMS will connect to ScreenBeam Cloud.



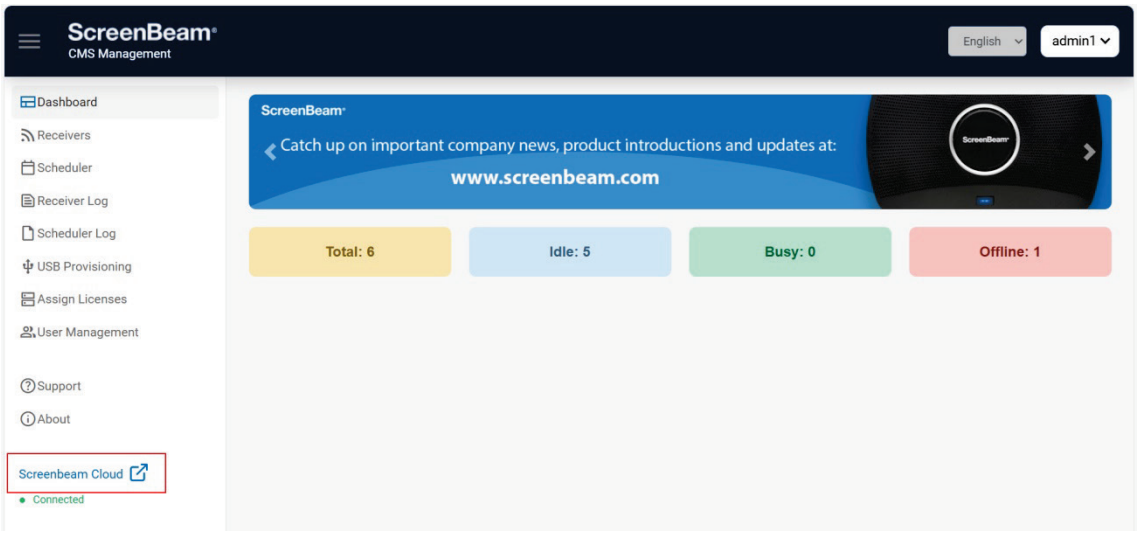
4.3.3 Activating Licenses on ScreenBeam Cloud

ScreenBeam provides licenses for the following services:

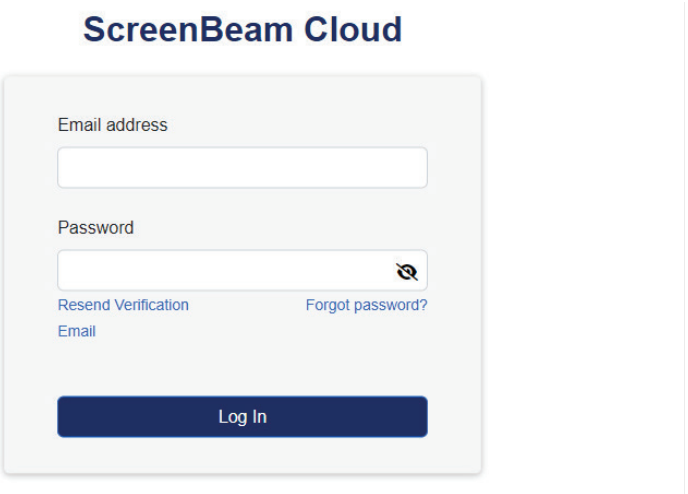
- Management of ScreenBeam 960/750 receivers: As ScreenBeam 960/750 receivers are sold with ScreenBeam CMS Classic (v2.x), they are not supported by CMS Enterprise (v4.x) natively. To manage these receivers in ScreenBeam CMS Enterprise, a license is required.
- INSTRUCTIONAL TOOLS: the classroom orchestration solution for schools by ScreenBeam.
- ADMINISTRATIVE TOOLS: sends alerts or messages to ScreenBeam receivers via mobile devices (iOS / Android) or a web browser.

Follow the procedure below to activate a ScreenBeam license on ScreenBeam Cloud:

1. Ensure that a ScreenBeam license key is available.
   Note: Contact your sales representatives for more information about ScreenBeam licenses.
2. Log into ScreenBeam CMS and click the **ScreenBeam Cloud** link in the bottom of the left menu.
   Note: You can also access ScreenBeam Cloud via cloud.screenbeam.com.

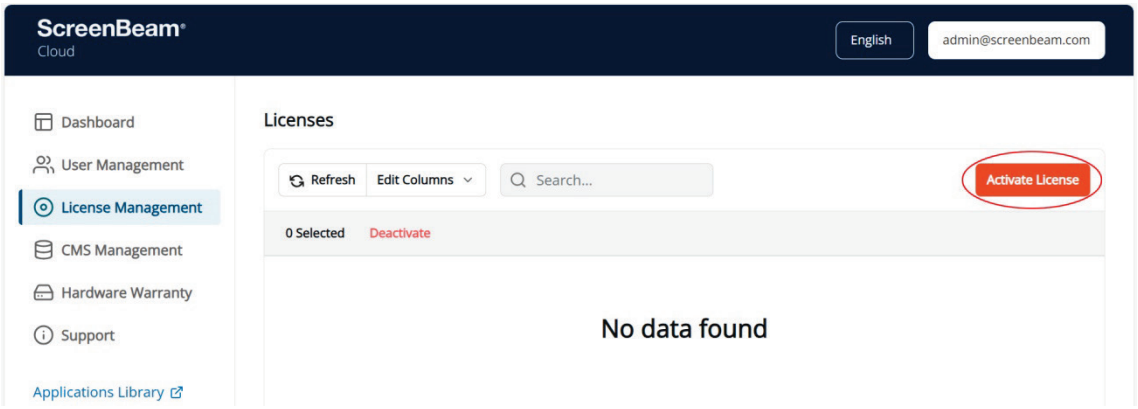


3. The ScreenBeam Cloud website will open in a new tap. You will be required to enter your registered email and password.

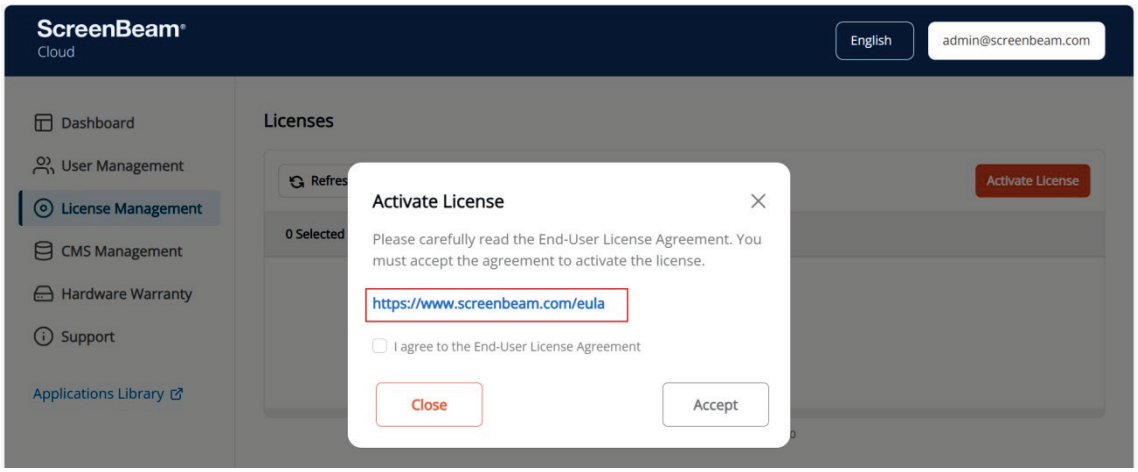


4. Click **License Management** on the left menu to go to the **Licesnses** page.

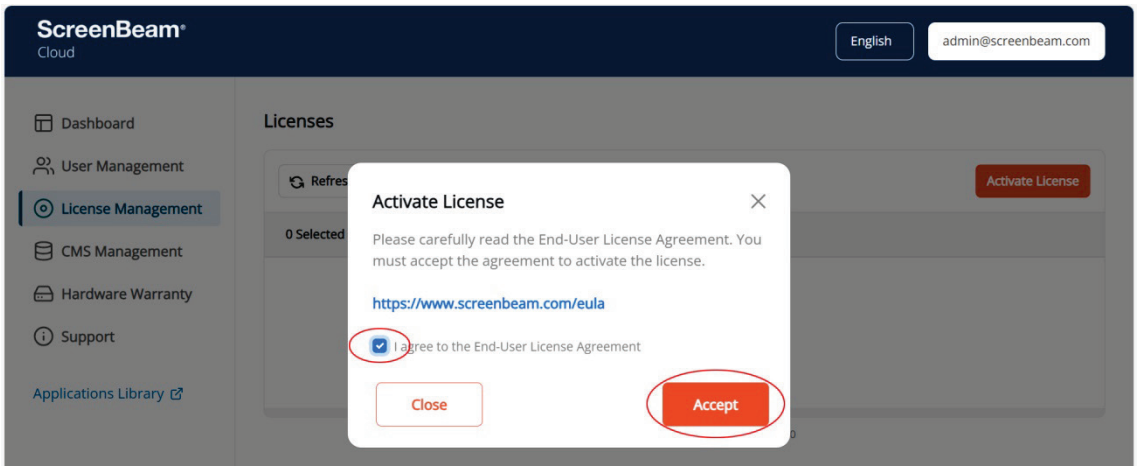
5. Click the **Activate** button on the **Licenses** page.



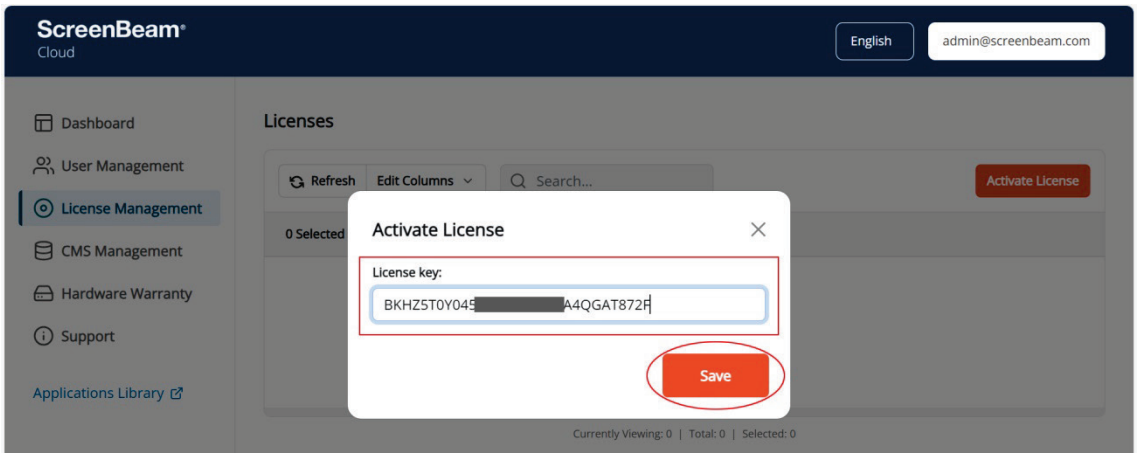
6. The **Activate License** dialog box appears. Click the end user license agreement link to read the ScreenBeam End User License Agreement carefully.



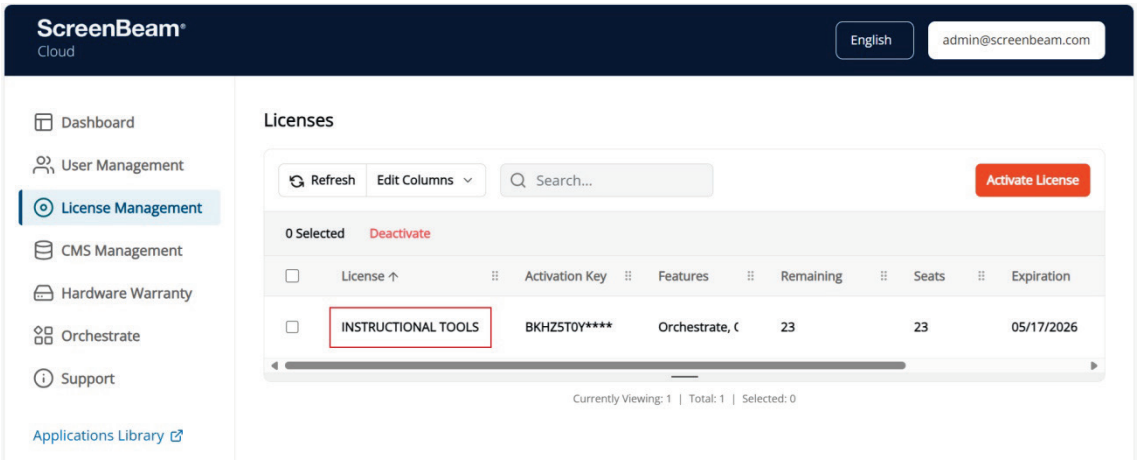
7. Check the **I agree to the End-User License Agreement** box and click **Accept** on the **Activate License** dialog box to continue.



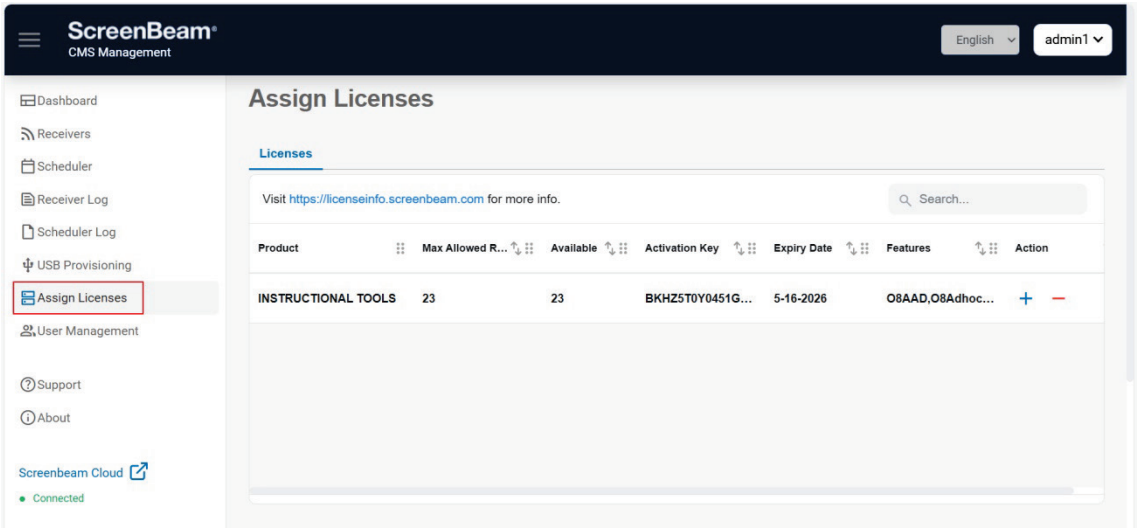
8. Type your license key in the **License key** box. Click **Save**.



9. Your license will be activated in a short while.



10. The activated license is also shown in the **Assign Licenses** page of your CMS if your CMS is connected to ScreenBeam Cloud.

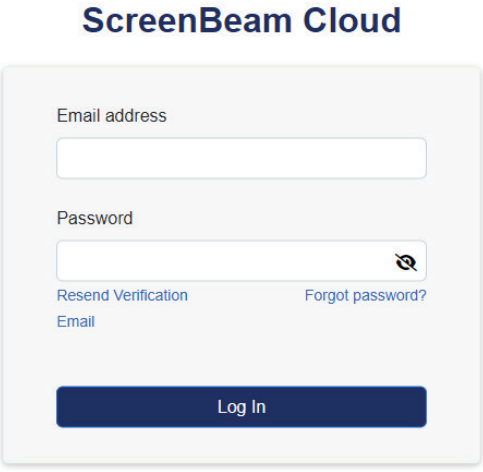


4.3.4 (Optional) Inviting Users to ScreenBeam Cloud

Note: The setup in this section is optional.
If you have activated multiple services on ScreenBeam Cloud, you may want to invite your workmates to help manage these services together.
Follow the procedure below to invite users to ScreenBeam Cloud:

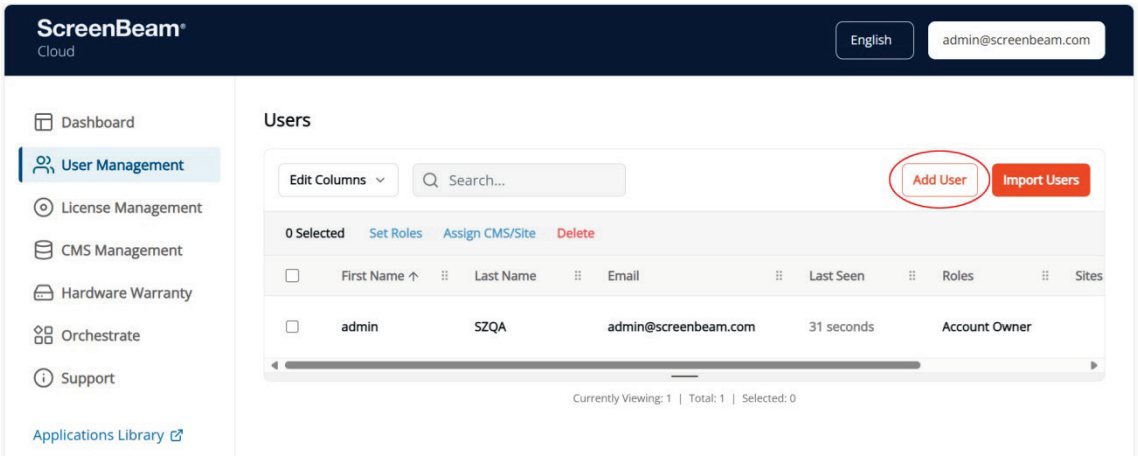
1. Log into ScreenBeam CMS and click the **ScreenBeam Cloud** link in the bottom of the left menu.
   Note: You can also access ScreenBeam Cloud via cloud.screenbeam.com.

2. The ScreenBeam Cloud website will open in a new tab. You will be required to enter your registered email and password.

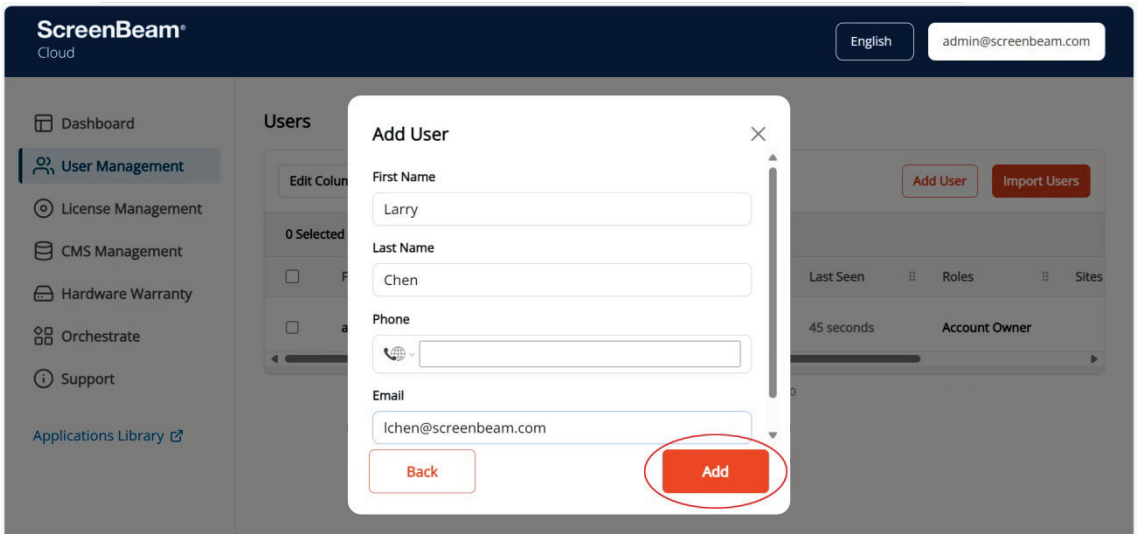


3. Click **User Management** on the left menu to go to the **Users** page.

4. Click the **Add User** button on the **Users** page.



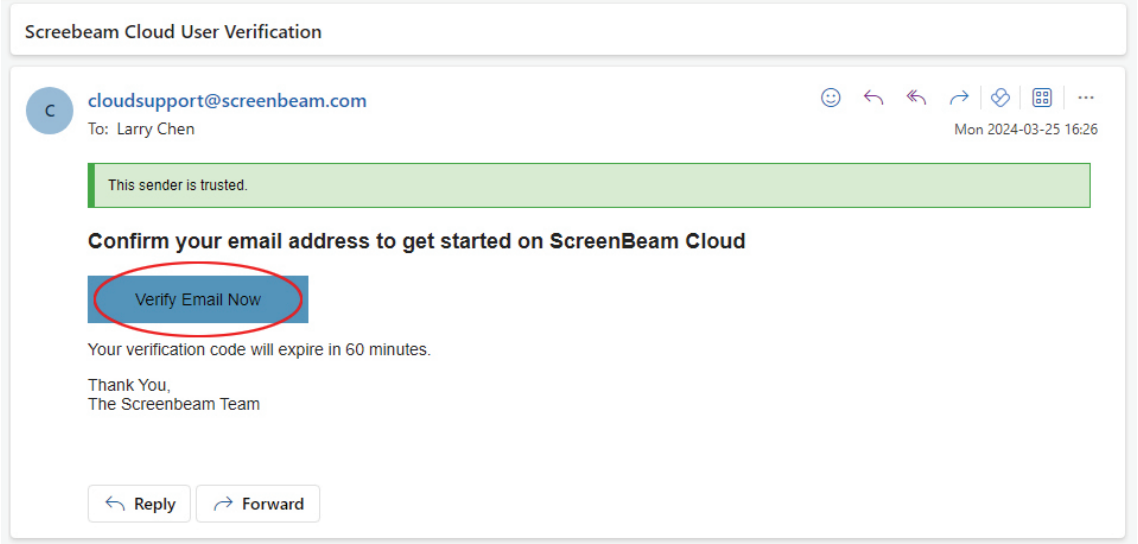
5. The **Add User** dialog box appears. Fill out all fields and click **Add**.
   Note: First Name and Phone are optional. The top 50 email domains in this list (https://www.gmass.co/domains) are not supported.



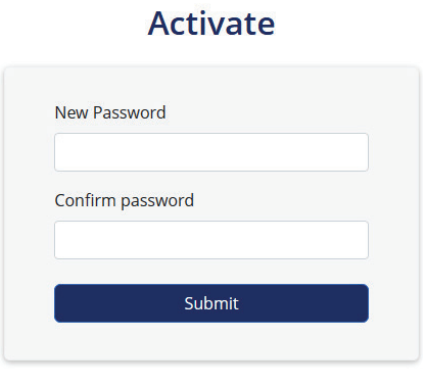
6. A user account will be created with the invited user's email and a verification email will be sent to that email as well.

Note: The user account verification link in the email is valid for 60 minutes.

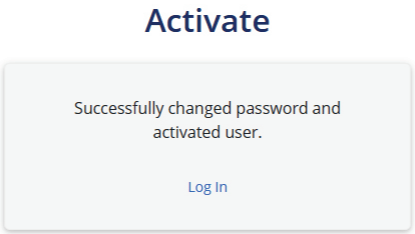
7. Assign the newly added user a role.
   Note: The invited user is not allowed to log into ScreenBeam Cloud if it is not assigned a role.
8. The invited user opens his/her email box and looks for the email titled “Screenbeam Cloud User Verification”, which is sent by **cloudsupport@screenbeam.com**. Open this email and click **Verify Email Now**.



9. The ScreenBeam account activation page will open in a new tab. Fill out the **New Password** and **Confirm password** boxes and click **Submit**.
   Note: The password must include at least one upper case English letter [A-Z], one lower case English letter [a-z], one digit [0-9], and one special character. And the length of password must be 9-64 characters.

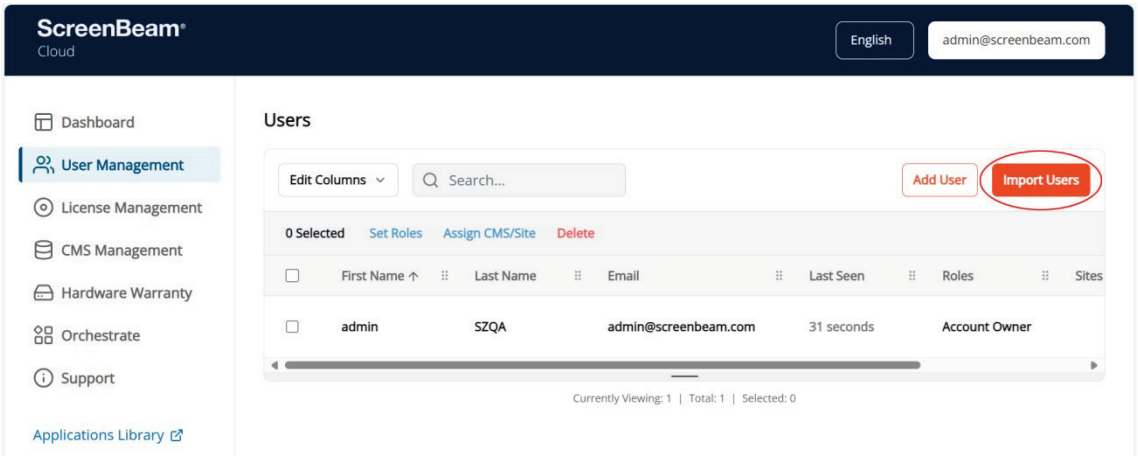


10. The invited user's account will be activated successfully when the **Successfully changed password and activated user** message shows.
    Note: If the invited user doesn't complete email verification within 60 minutes, then account activation will fail. The user can click **Resend** to trigger the email verification again.

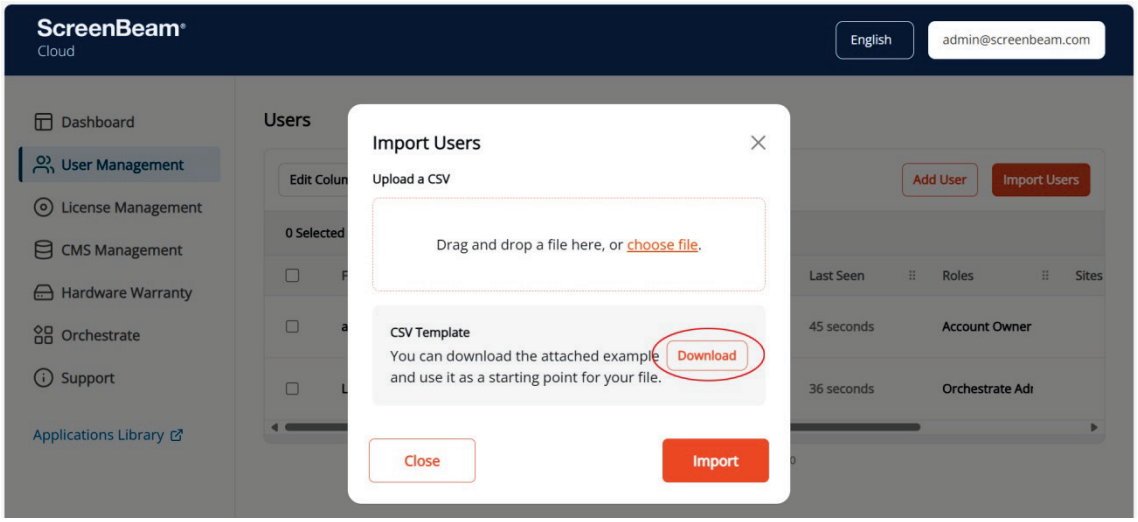


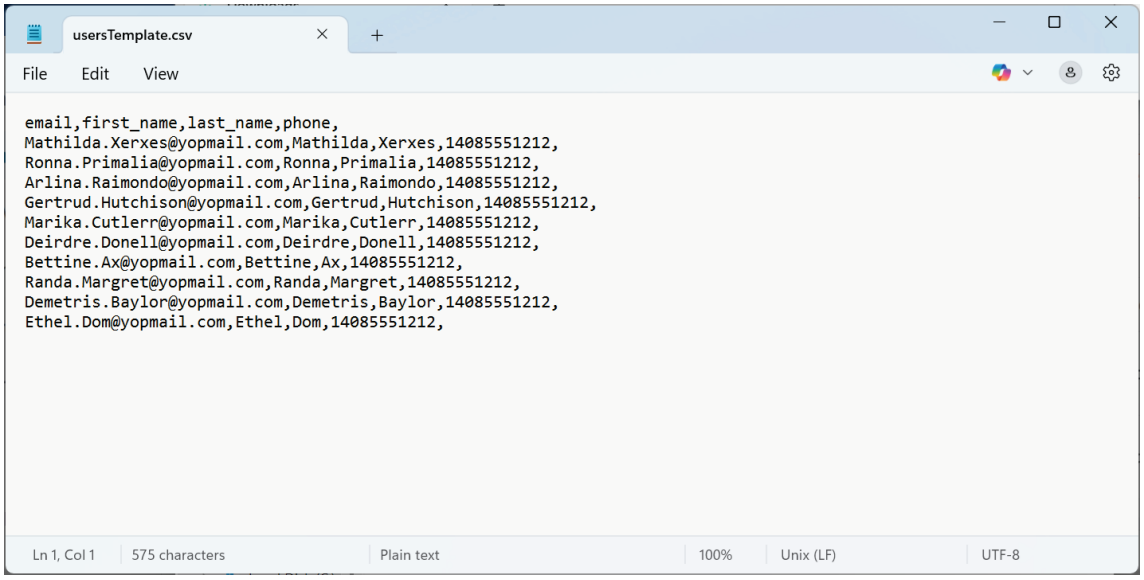
You can also add multiple users at a time using the **Import Users** feature. Follow the procedure below to invite multiple users at a time:

1. Go to ScreenBeam Cloud -> **User Management**, and then click **Import Users**.

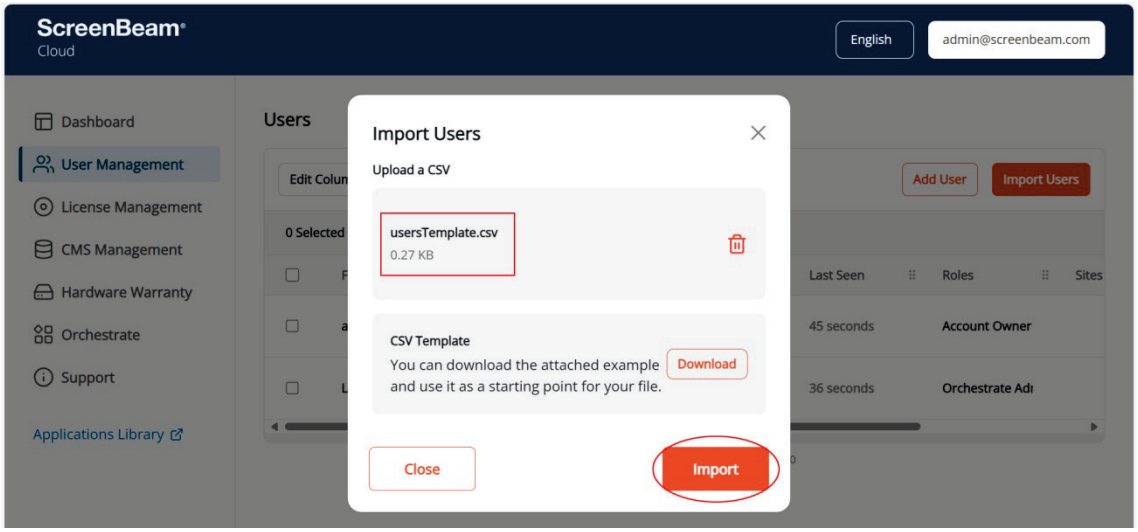


2. The **Import Users** dialog box appears. Download the example file for importing users. And follow the example to prepare a .csv file.
   Note: The top 50 email domains in this list (https://www.gmass.co/domains) are not supported.

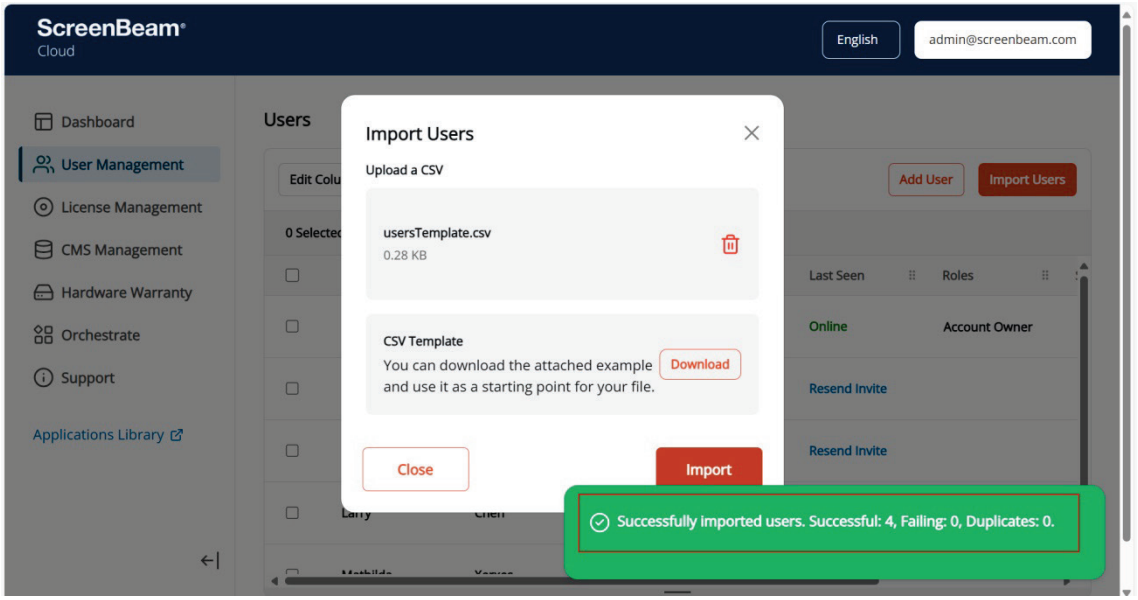




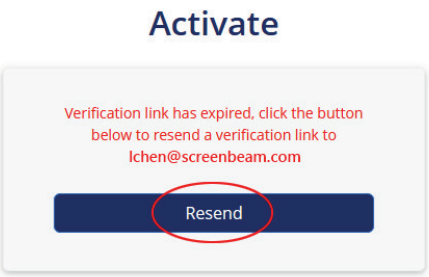
3. Click **Choose File** and then choose the .csv file that you have prepared. And click **Import**.



4. The users in the .csv file will be imported.



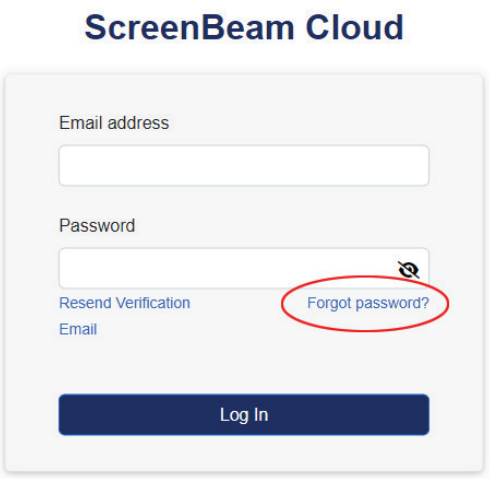
5. Assign the newly added users a role.
   Note: The invited users are not allowed to log into ScreenBeam Cloud if they are not assigned any role.
6. The invited users must complete email verification to activate their accounts.
   Note: If the user account verification link has expired, you can click **Resend**, and then ScreenBeam Cloud will send you a new verification email.



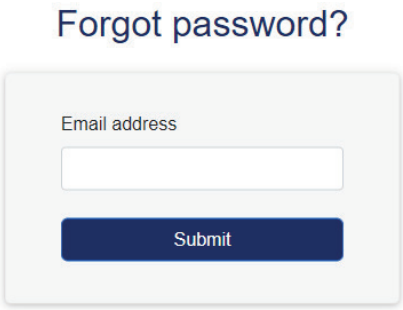
4.3.5 Resetting Password

If you have lost or forgotten your ScreenBeam Cloud account's password, you can reset your password with this procedure.

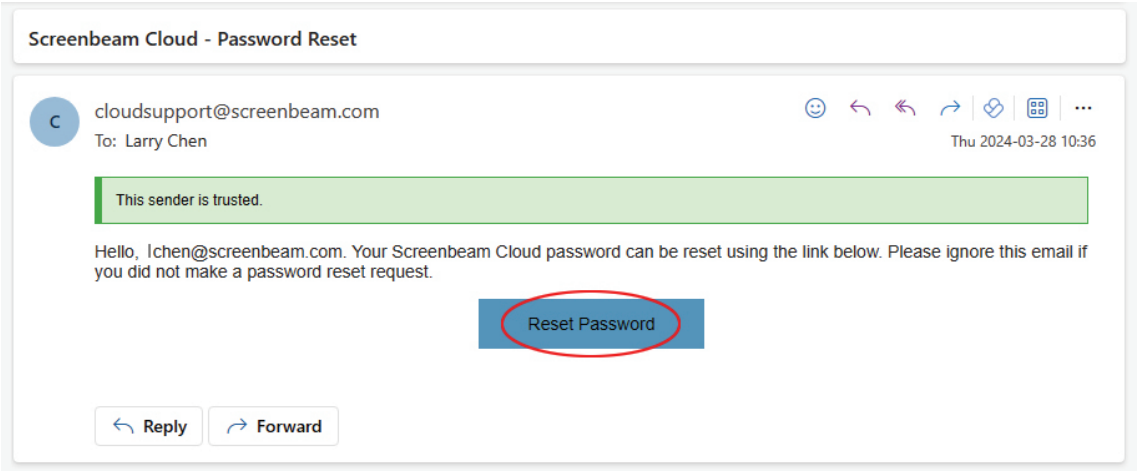
1. Access ScreenBeam Cloud via cloud.screenbeam.com/login.
2. On the ScreenBeam Cloud Login page, click **Forgot password**.



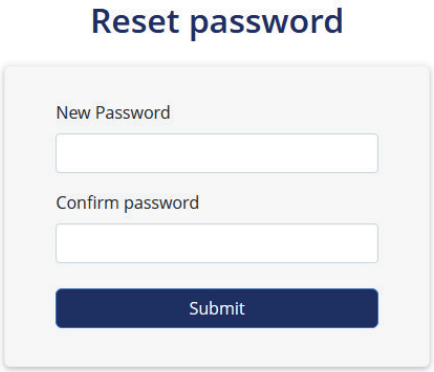
3. On the **Forgot password?** page, enter your email address in the **Email address** box. Click **Submit**.



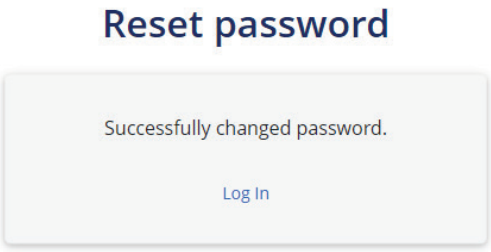
4. Open your email box and look for the email titled "Screenbeam Cloud - Password Reset", which is sent by **cloudsupport@screenbeam.com**. Open this email and click the **Reset Password** link.



5. The **Reset Password** page will open in a new tab. Type your new password in the **New Password** and **Confirm password** boxes. Click **Submit**.



6. The new password will be set successfully when the page shows **Successfully changed password**.



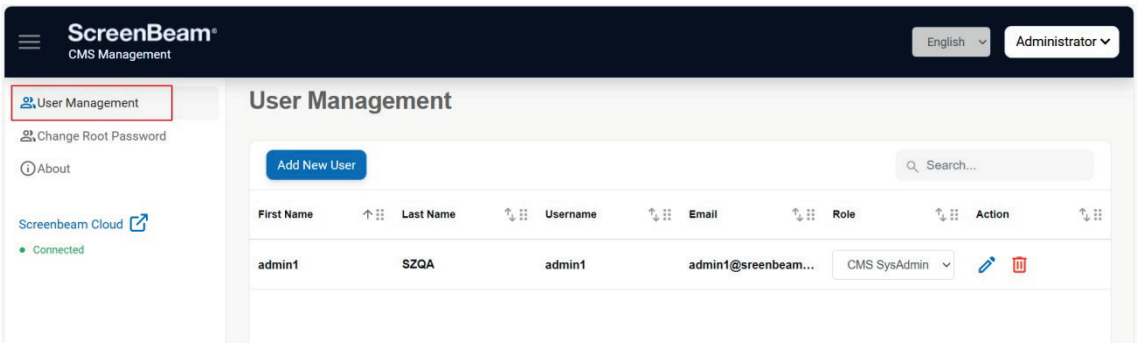
4.4 Managing CMS Users

Access to different CMS functions depends on the type of CMS user. CMS user management should first be configured before deployment.

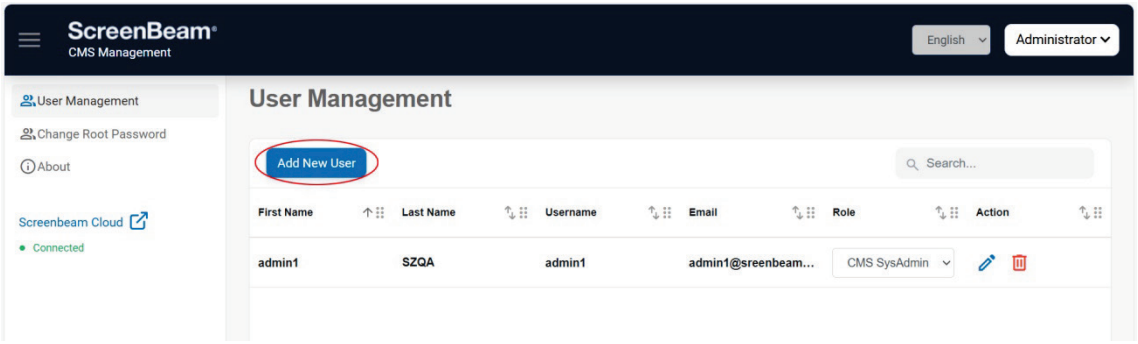
4.4.1 Add a New User

To add a new user of any type:

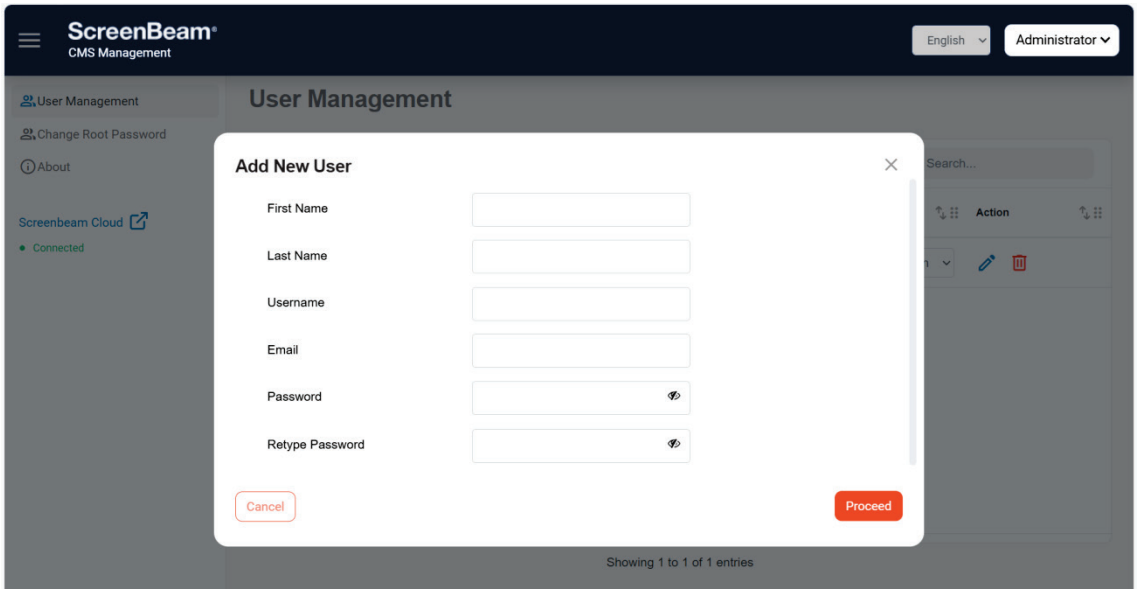
1. Go to the **User Management** page by clicking **User Management** on the left pane.



2. Click on **Add New User** on the **User Management** page.



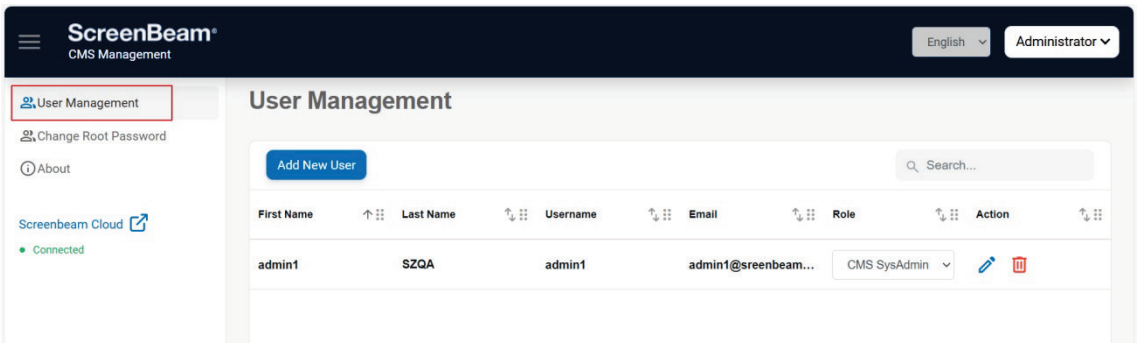
3. The **Add New User** window appears. Fill in the required information and click **Proceed**.
   - First Name must be 2-20 alphanumeric characters.
   - Last Name must be 2-20 alphanumeric characters.
   - Username must be 4-20 characters. It can contain alphanumeric characters and any of the following symbols ' . - _ ! # ^ ~
   - Password must be 6-256 characters in length, and must contain at least one of each: upper-case letter, lower-case letter, number and one of the following symbols ! @ # $ % ^ & *



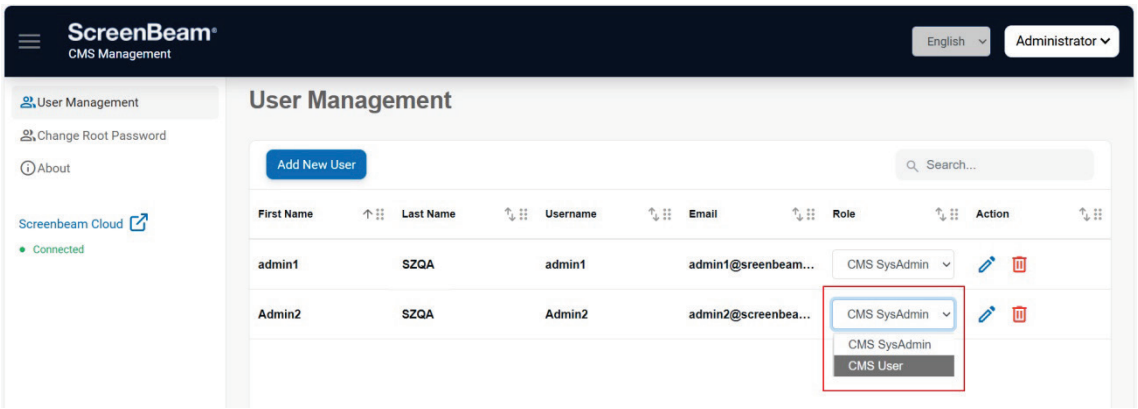
4.4.2 Re-assign Roles

The user's role can be changed by a CMS System Administrator by following the procedure below:

1. Go to the **User Management** page by clicking **User Management** on the left pane.

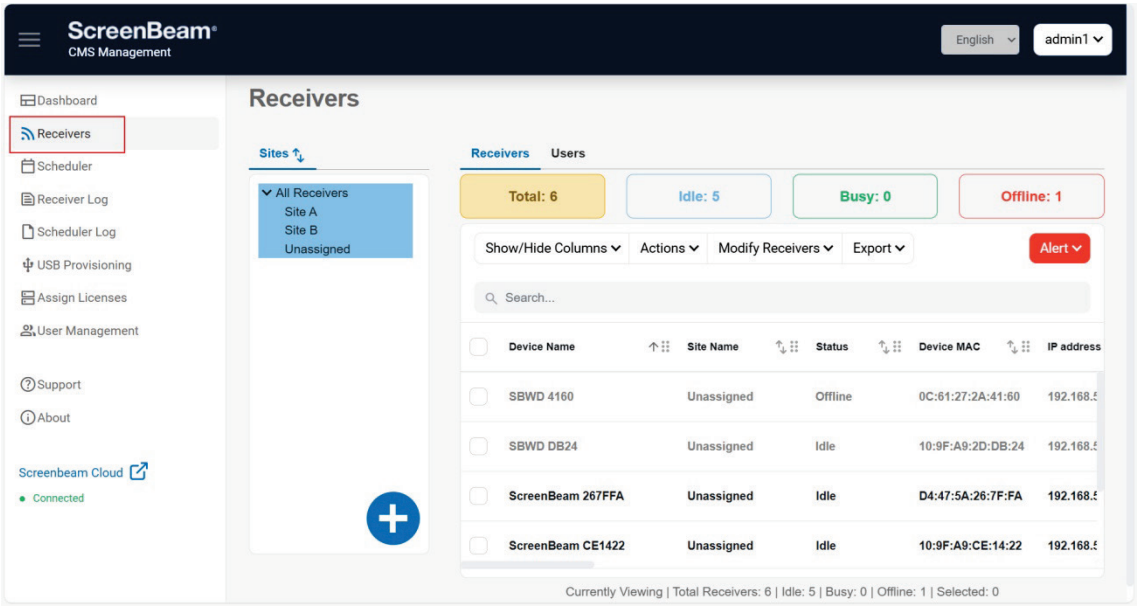


2. Select **CMS SysAdmin** or **CMS User** from the **Role** box of the user's entry.

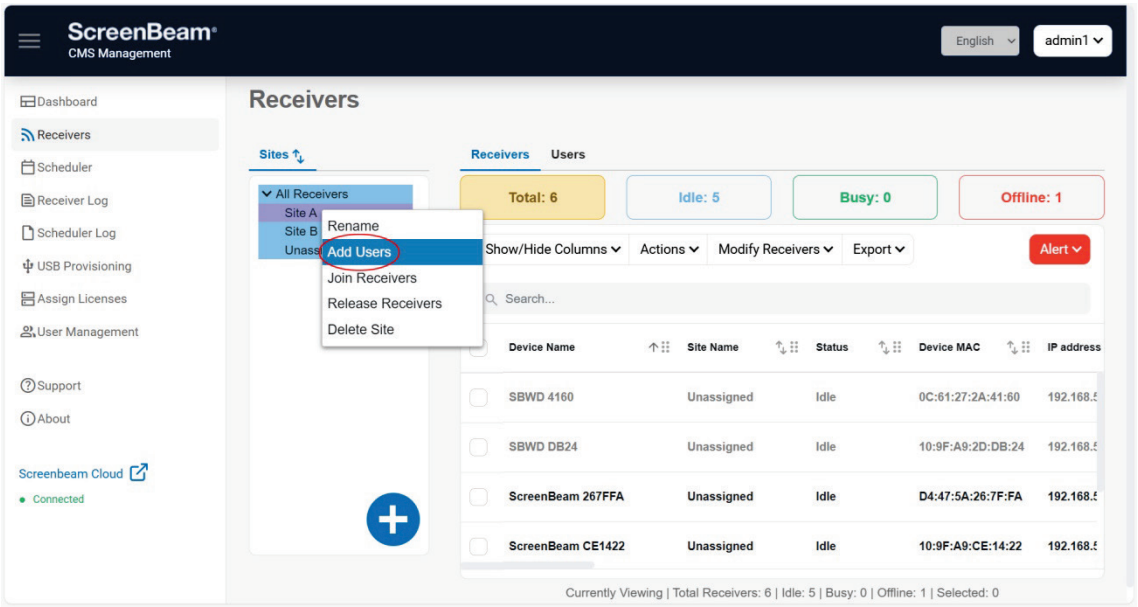


There are two kinds of standard CMS users: CMS Admin users and CMS Monitor users. These roles can be assigned to CMS users when adding users to sites as follows:

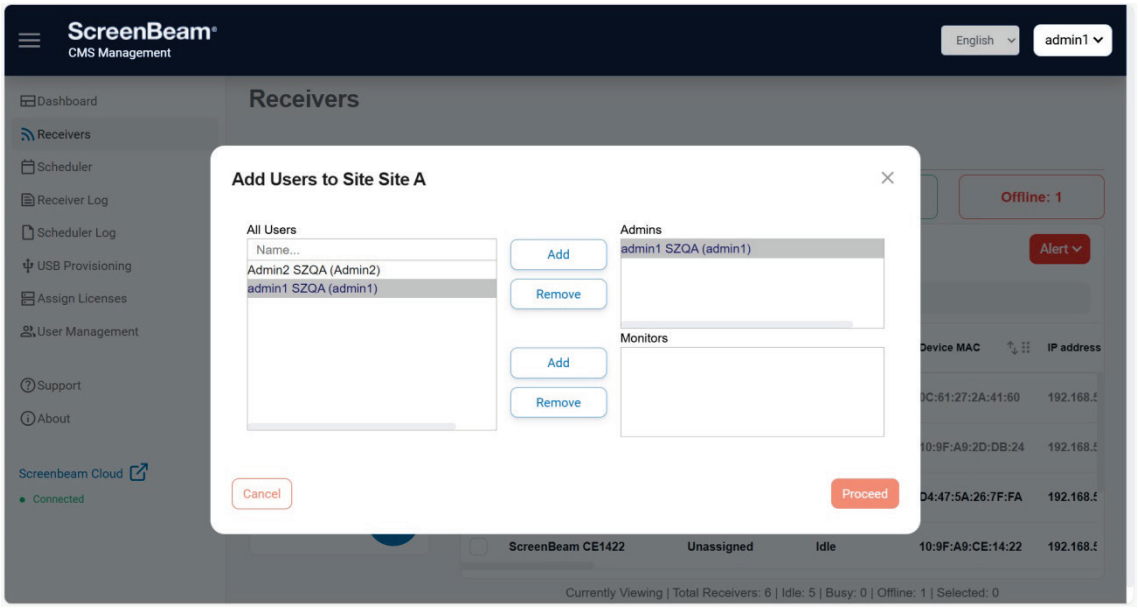
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



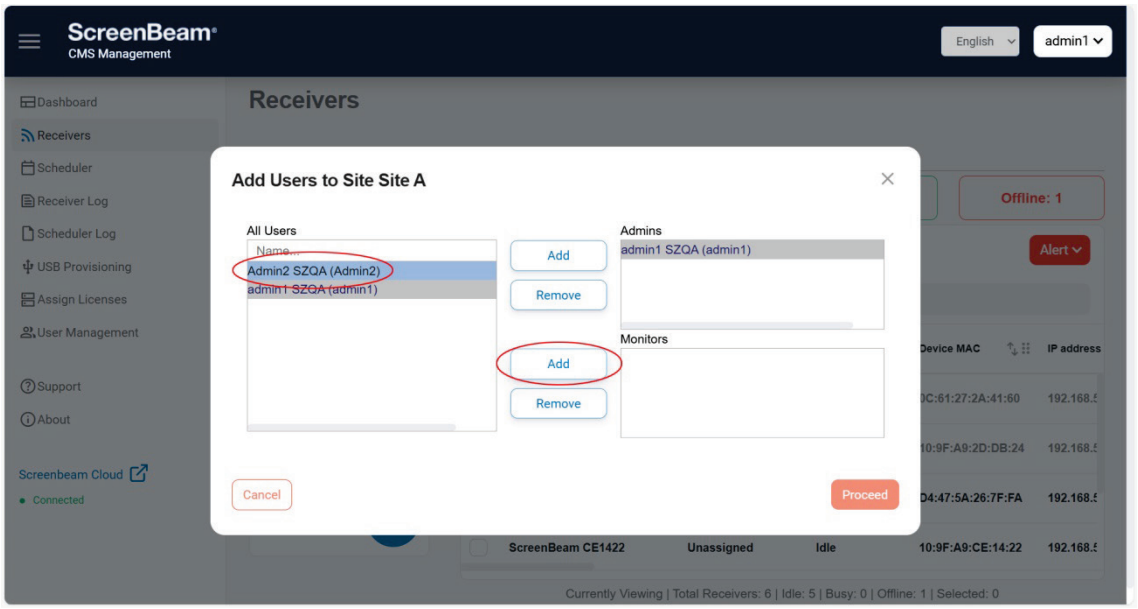
2. Right-click a site on the **Sites** pane and select **Add User** from the short-cut menu.



3. The **Add Users to Site xxx** window appears.

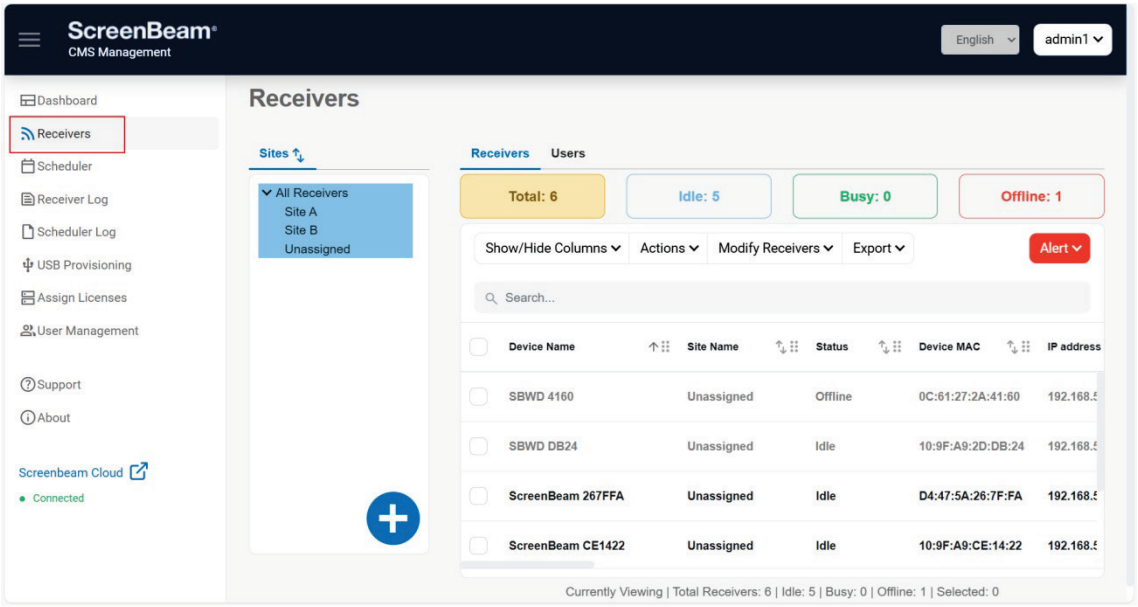


4. Select a user from the **All Users** box, and then click **Add** to add the selected user to the Admins box or the Monitors box.

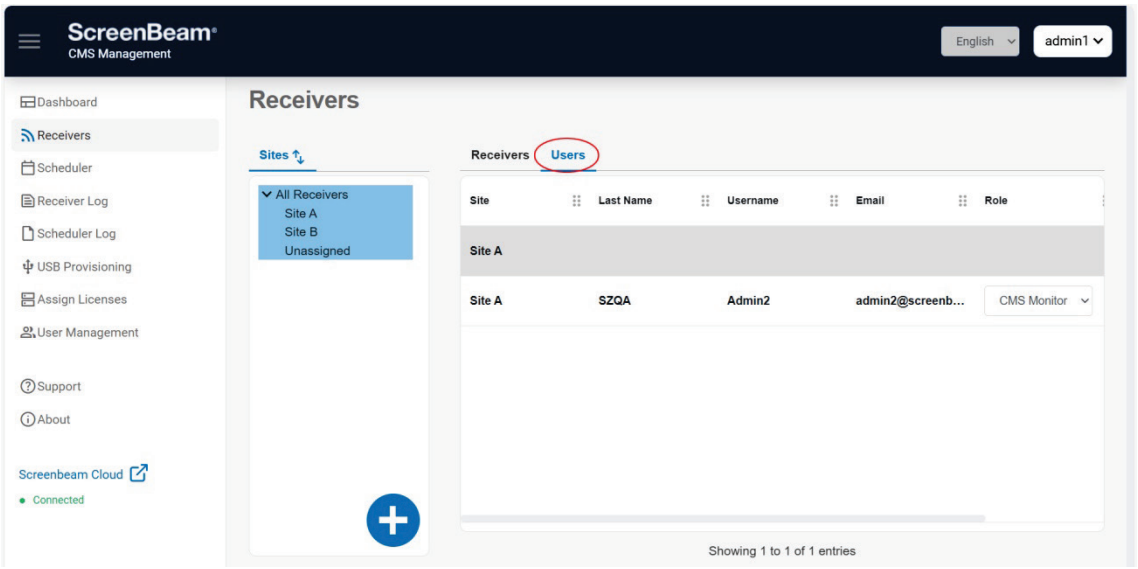


Different roles can be assigned to a CMS user in the Users pane as follows:

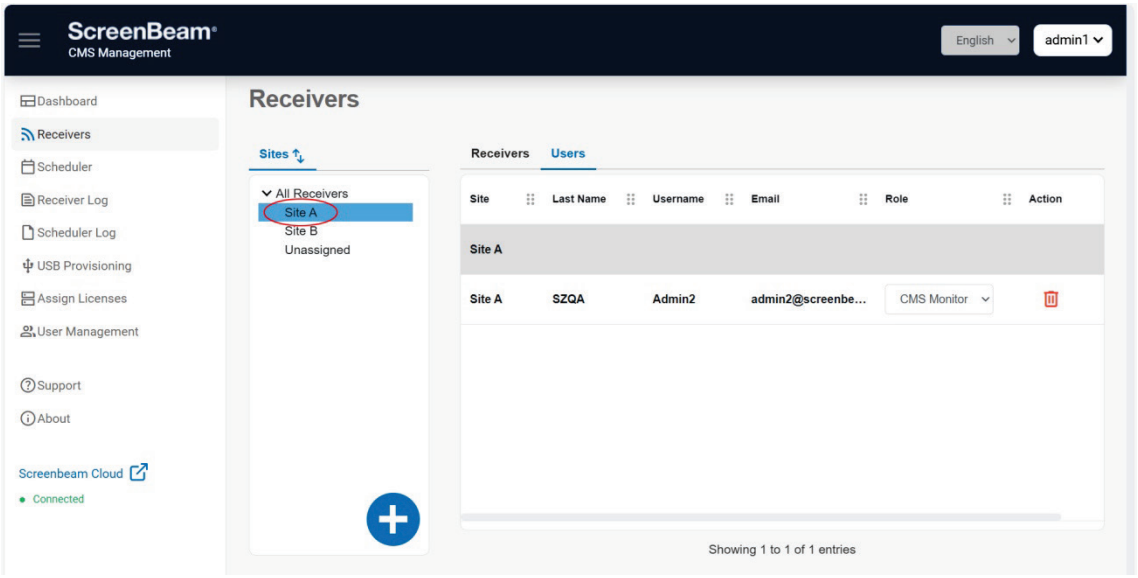
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



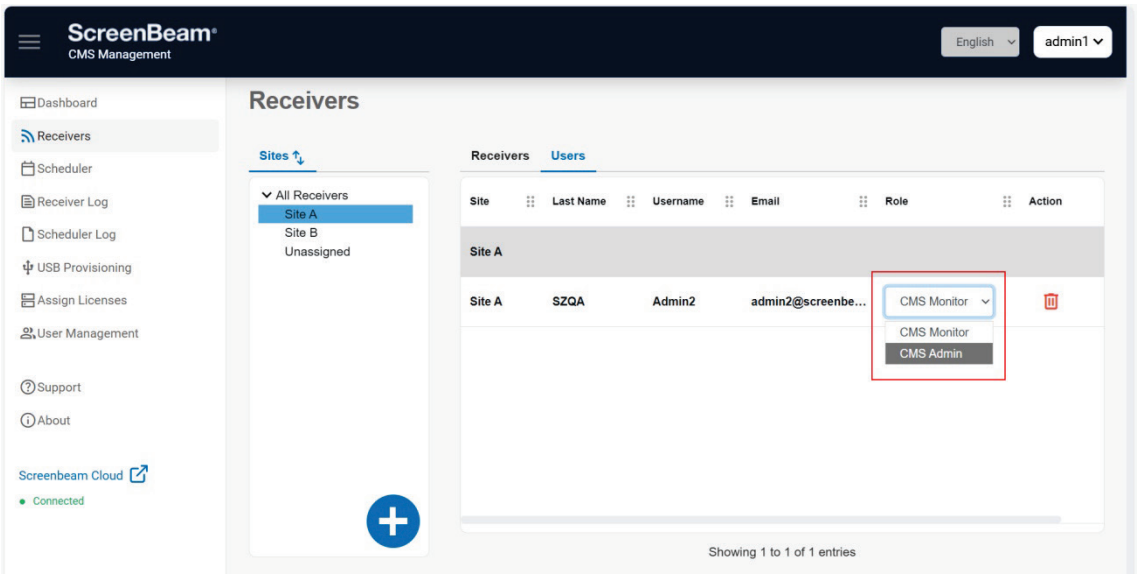
2. Go to the **Users** pane by clicking on the **Users** tab.



3. Select a site on the **Sites** pane to display the users that manage this site.



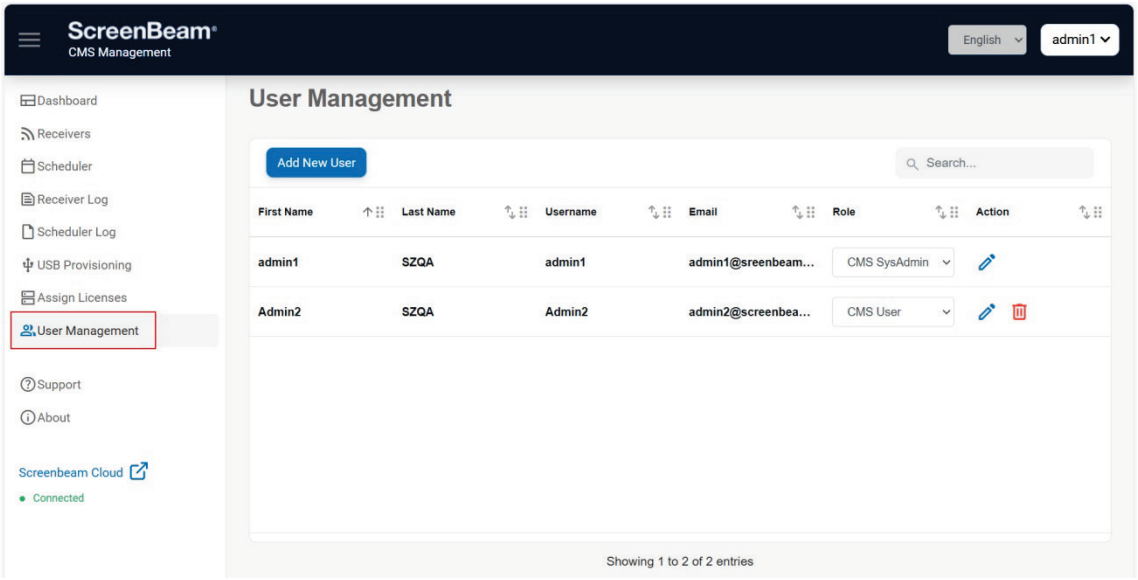
4. Select **CMS Admin** or **CMS Monitor** from the **Role** box of the user's entry.



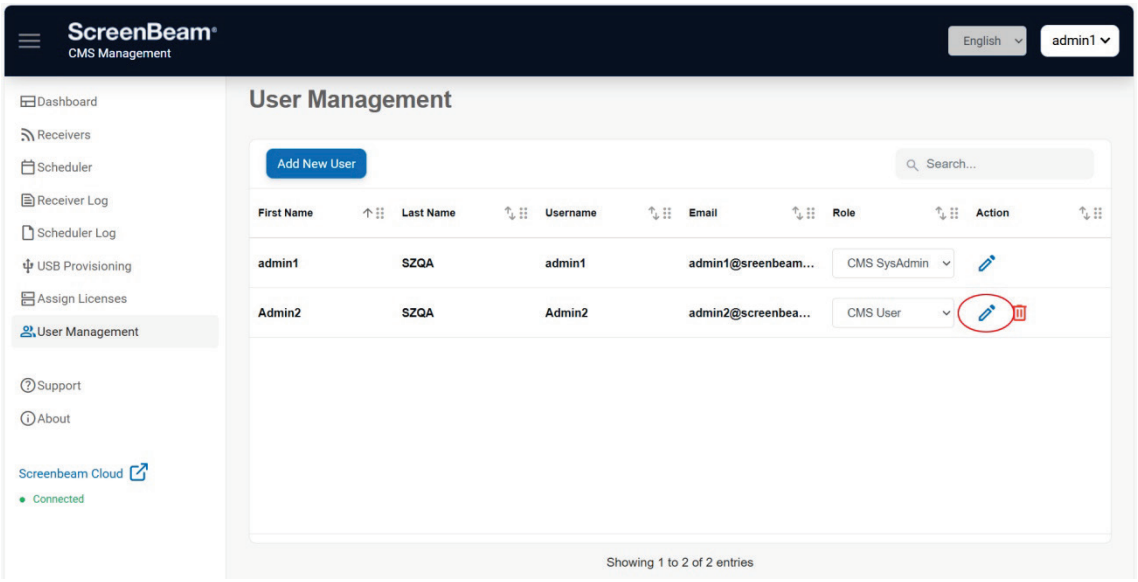
4.4.3 Edit User Info and/or Change User Password

To edit a user's info and/or change a user's password, follow this procedure:

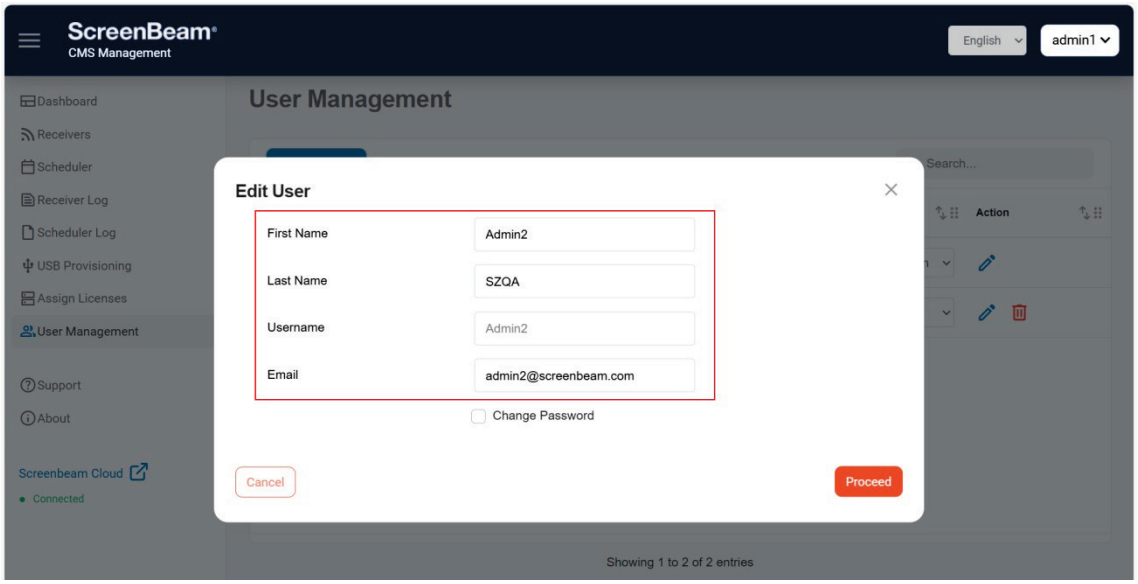
1. Go to the **User Management** page by clicking **User Management** on the left pane.



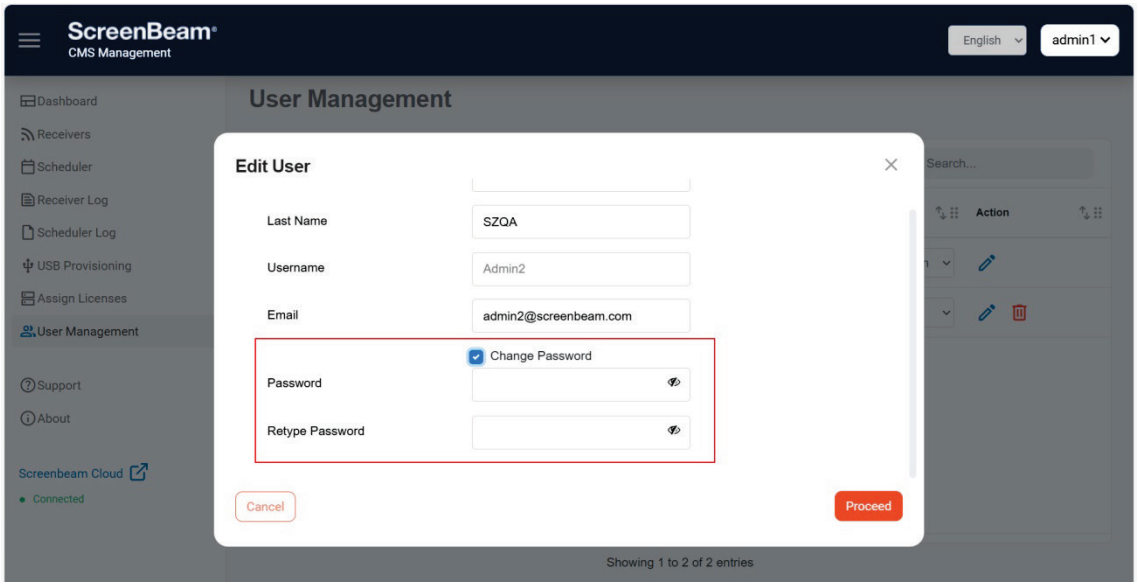
2. Click the Edit button (the pen icon) in the Action column of a user entry.



3. The **Edit User** window appears. Edit user information such as First name, Last name, and Email address.



4. Check the **Change Password** box. Password options appear. Enter a new password and retype it to confirm.

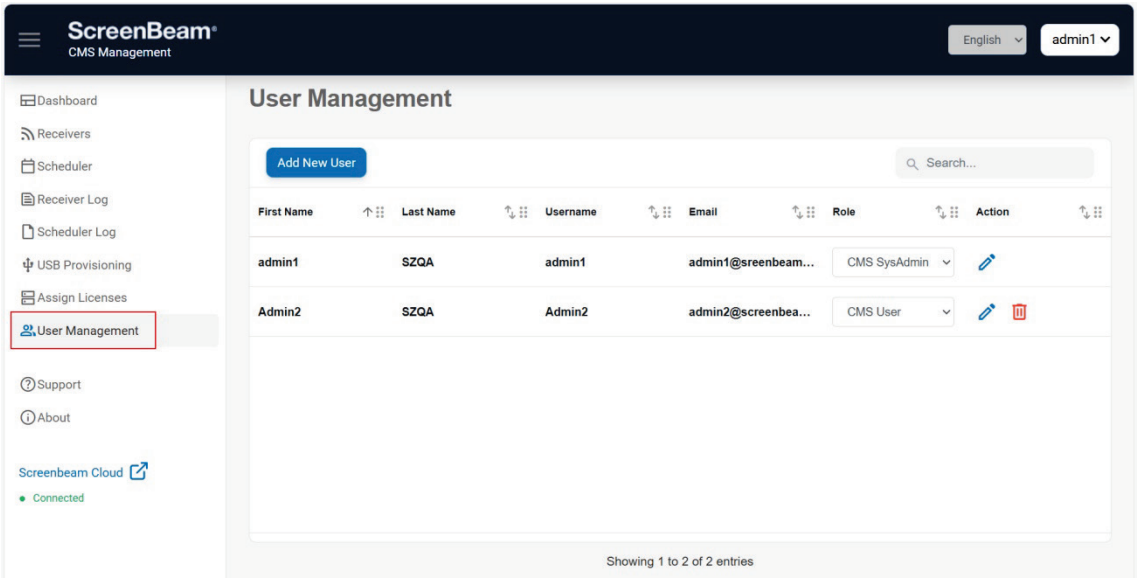


5. Click the **Proceed** button to confirm.

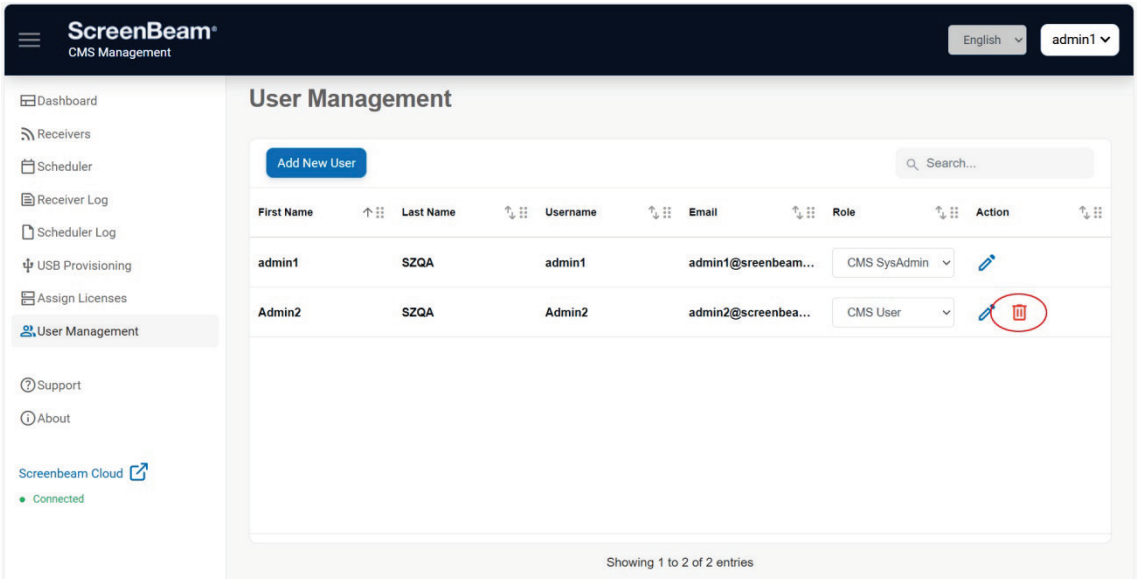
4.4.4 Delete a User

To delete a user, follow this procedure:

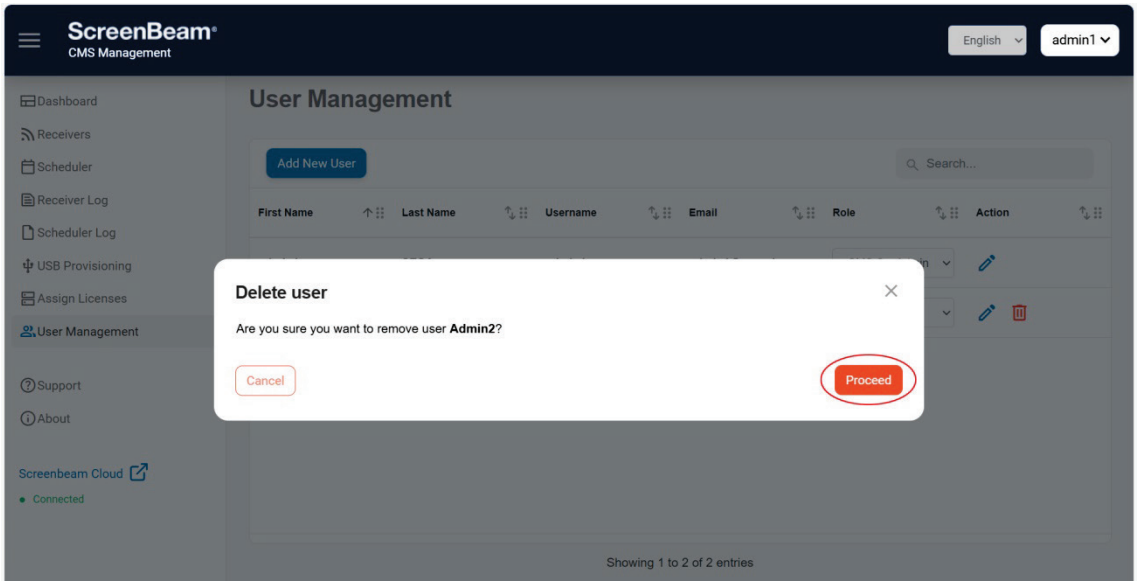
1. Go to the **User Management** page by clicking **User Management** on the left pane.



2. Click the Delete button (the red trash bin icon) in the Action column of a user entry to delete the corresponding user.



3. The **Delete user** box appears. Click **Proceed** to delete the user.



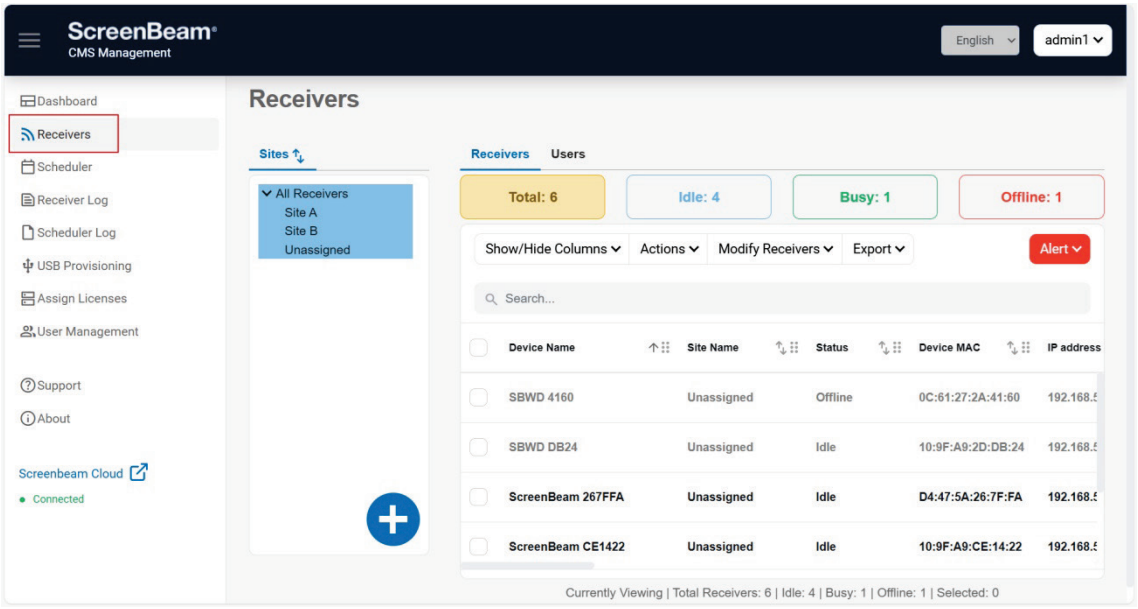
4.5 Managing Receivers

A CMS system administrator can add new sites, add receivers to sites, add users to sites, etc. Operations in this section are available to CMS system administrator (CMS SysAdmin) only.

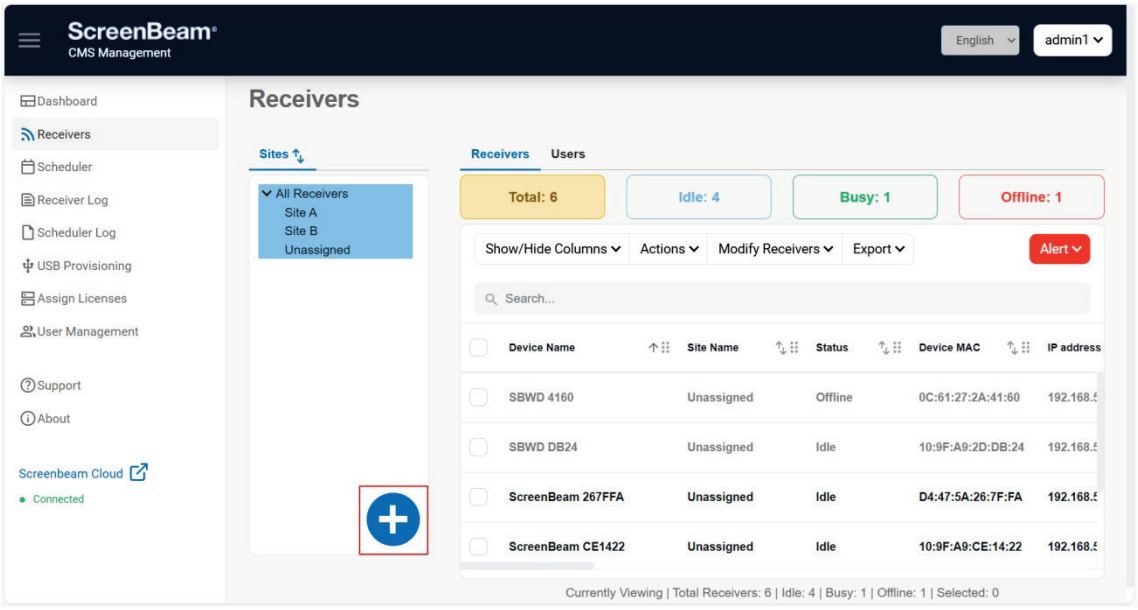
4.5.1 Add a New Site

To add a new site, follow this procedure:

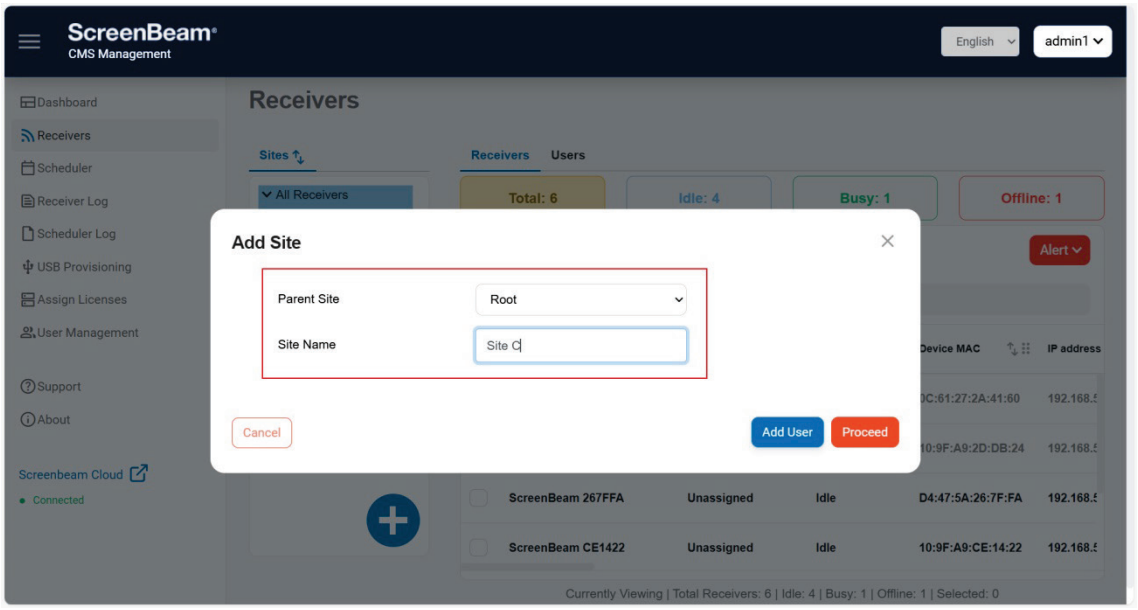
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



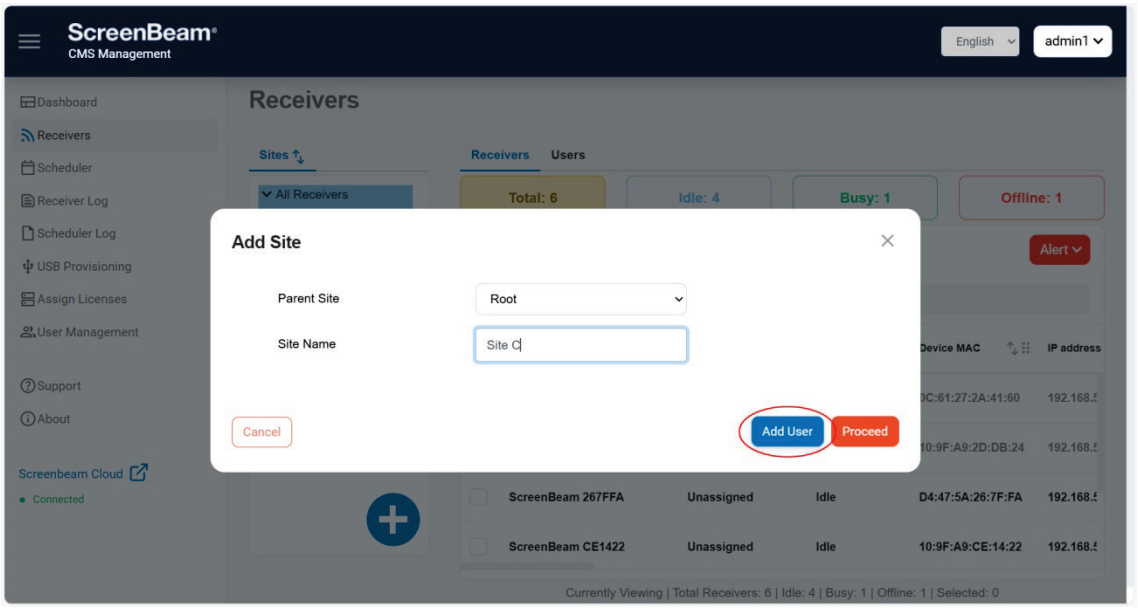
2. Click the plus sign on the bottom right corner of the **Sites** pane.

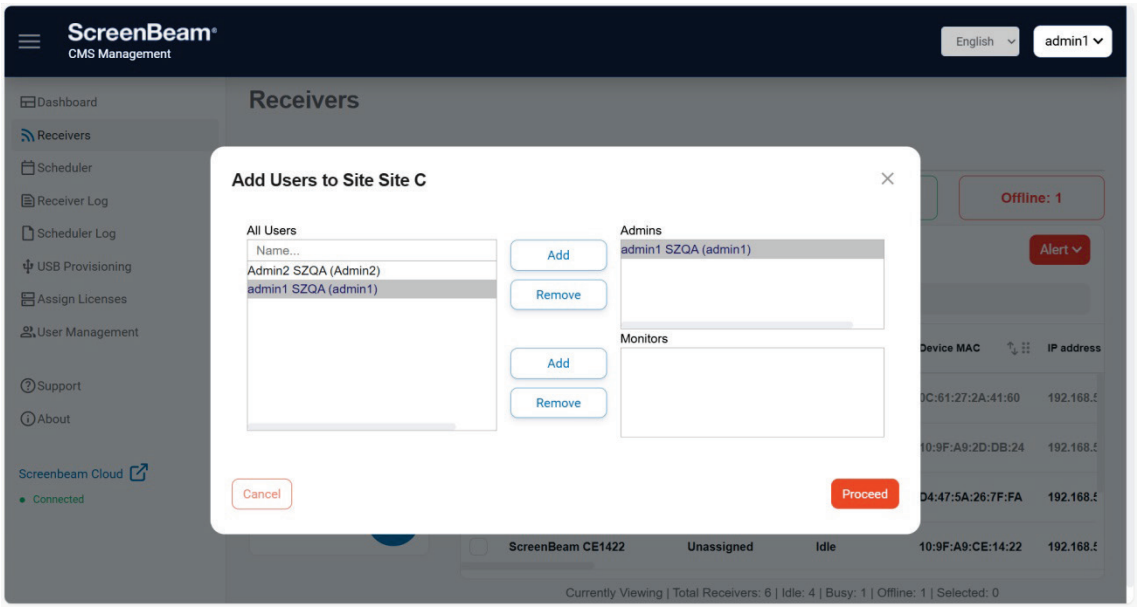


3. The **Add Site** window appears. Select a parent site and enter a name for the new site in the **Site Name** box.

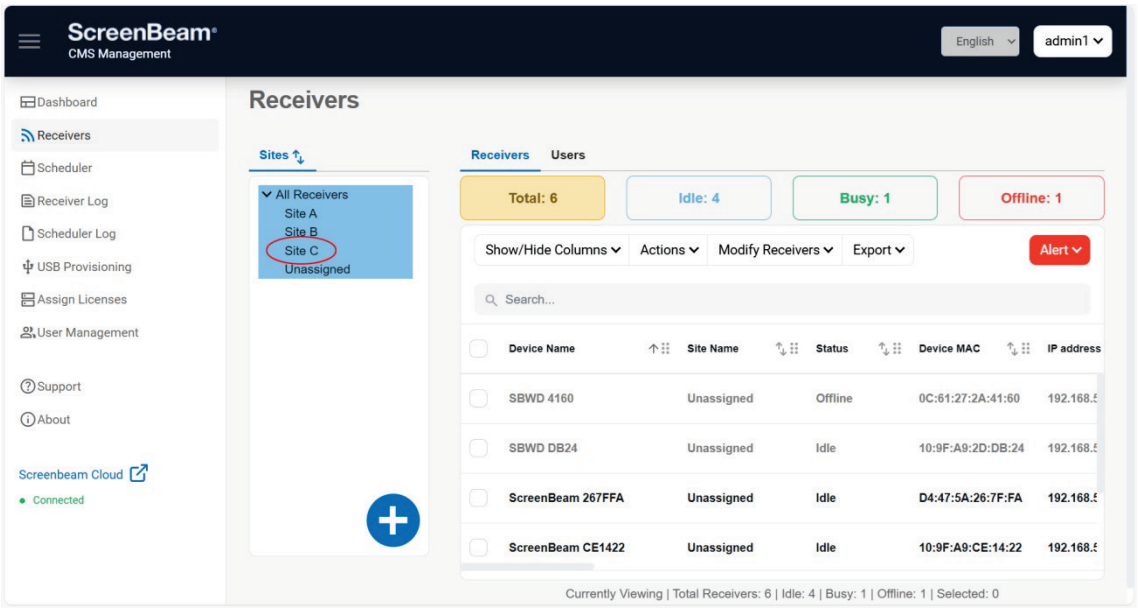


4. (optional) Click **Add User** to open the **Add Users to Site xxx** window. Select users from the **All Users** box, and then click **Add** to add the selected users to the **Admins** box or the **Monitors** box.





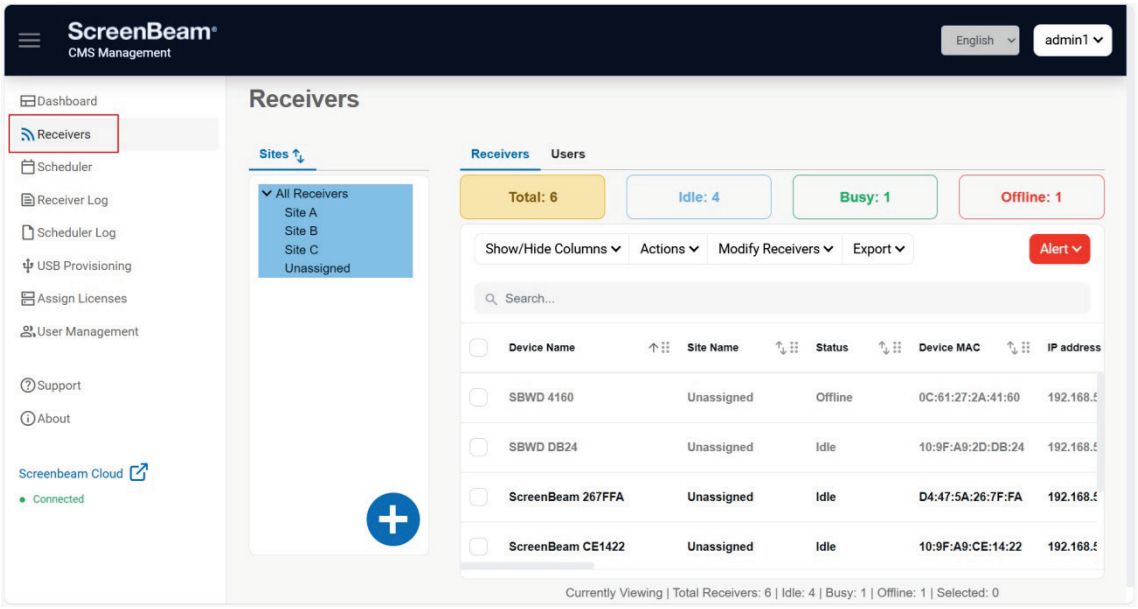
5. Click **Proceed** to create a new site.



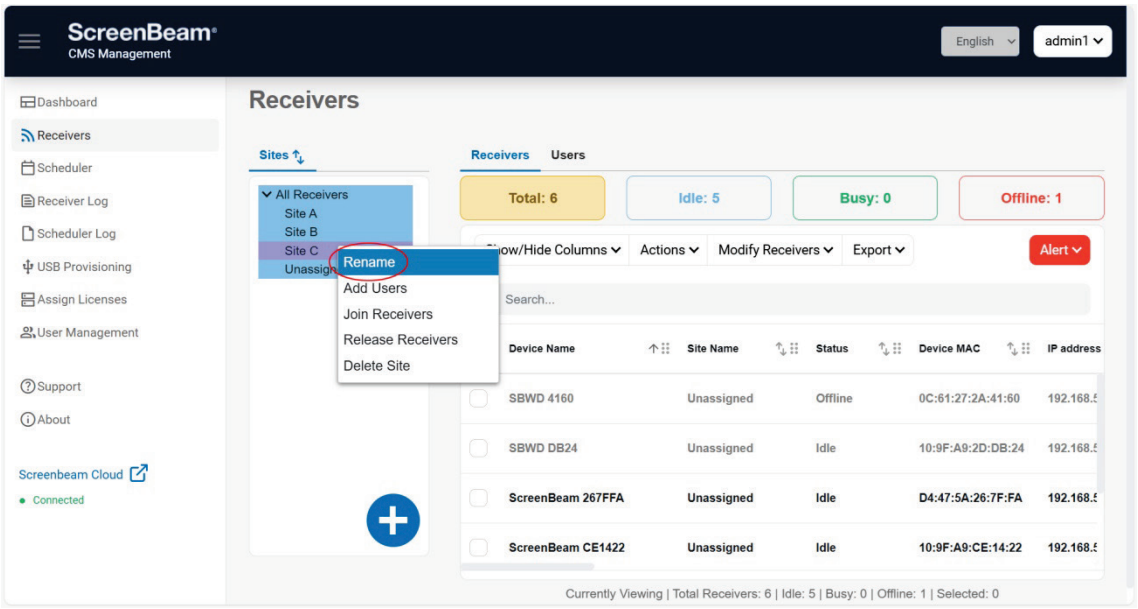
4.5.2 Rename a Site

To rename a site, follow this procedure:

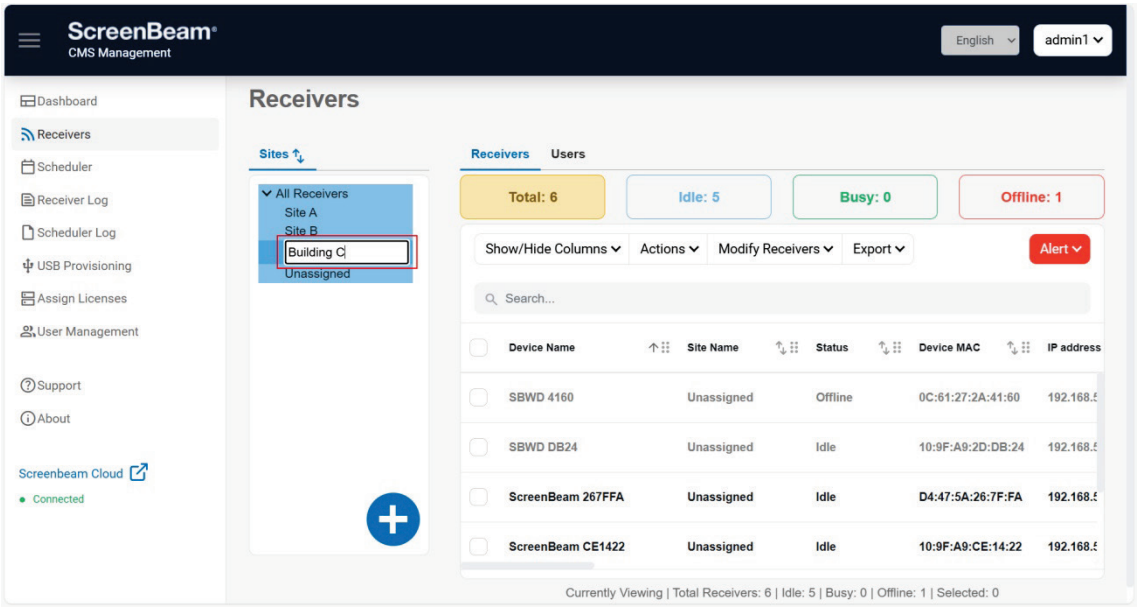
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Right-click the site that you want to rename in the **Site** pane and select **Rename** from the shortcut menu.



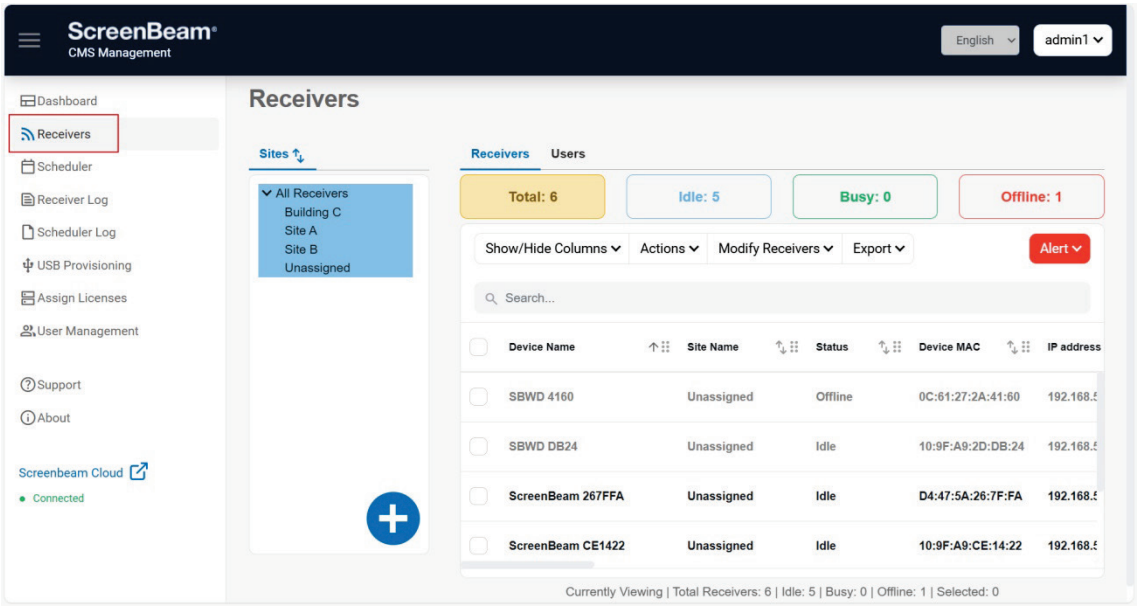
3. Type a new name and press Enter to confirm.



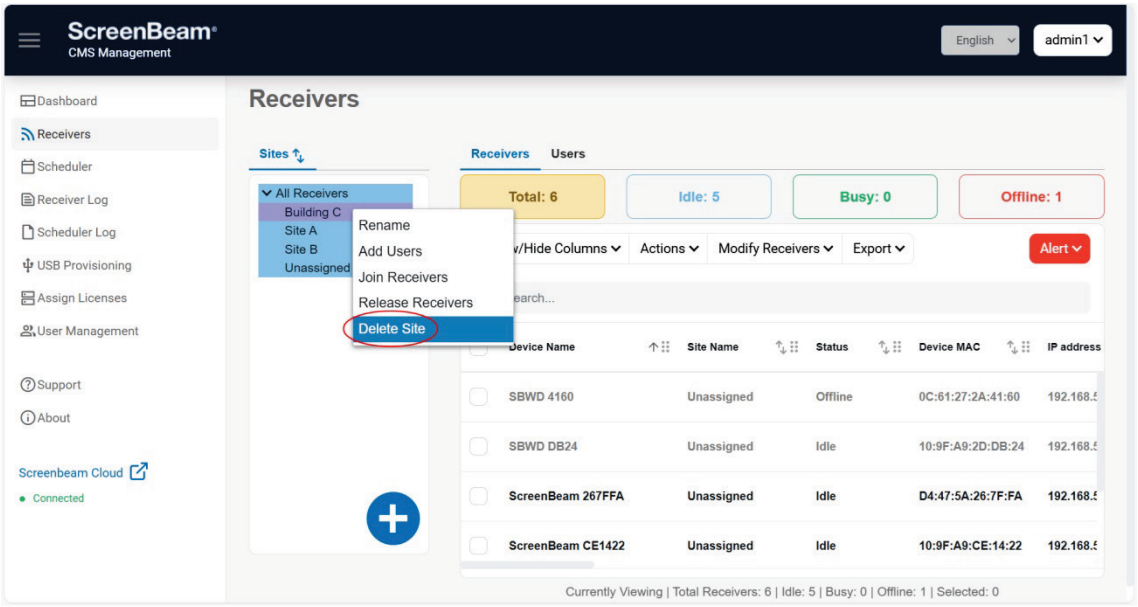
4.5.3 Delete a Site

To delete a site, follow this procedure:

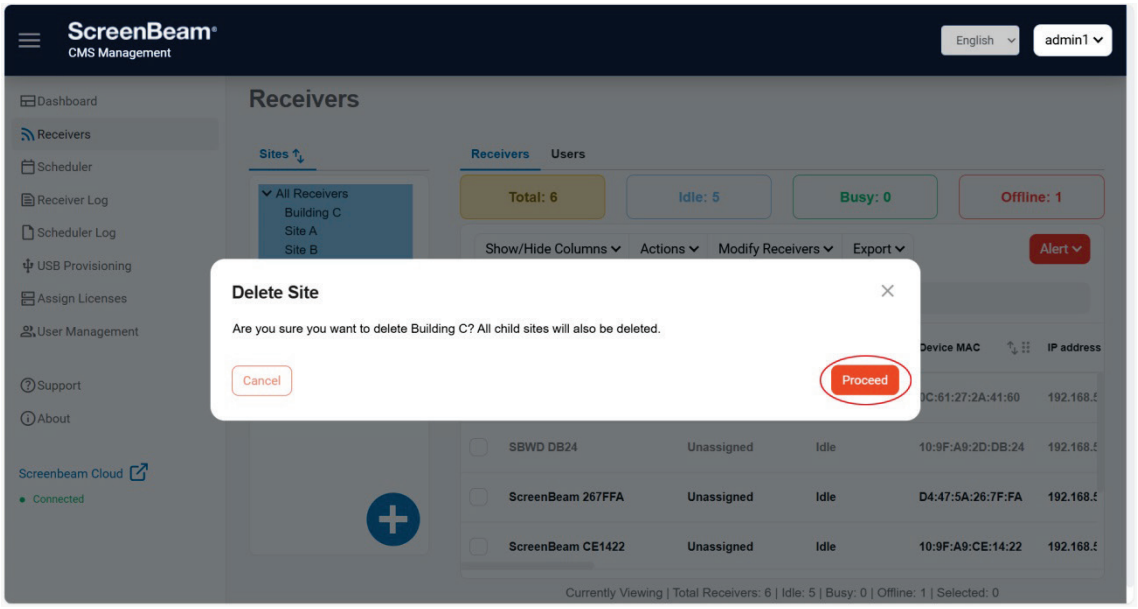
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Right-click the site that you want to delete in the **Site** pane and select **Delete Site** from the shortcut menu.



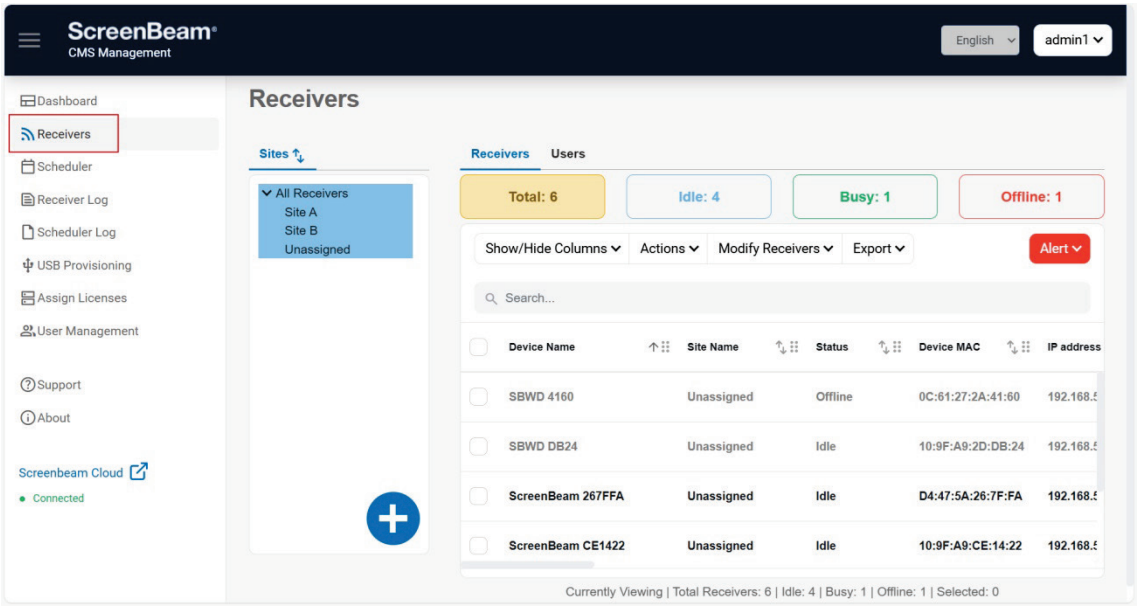
3. Click **Proceed** on the **Delete Site** message box.



4.5.4 Add Receivers to a Site

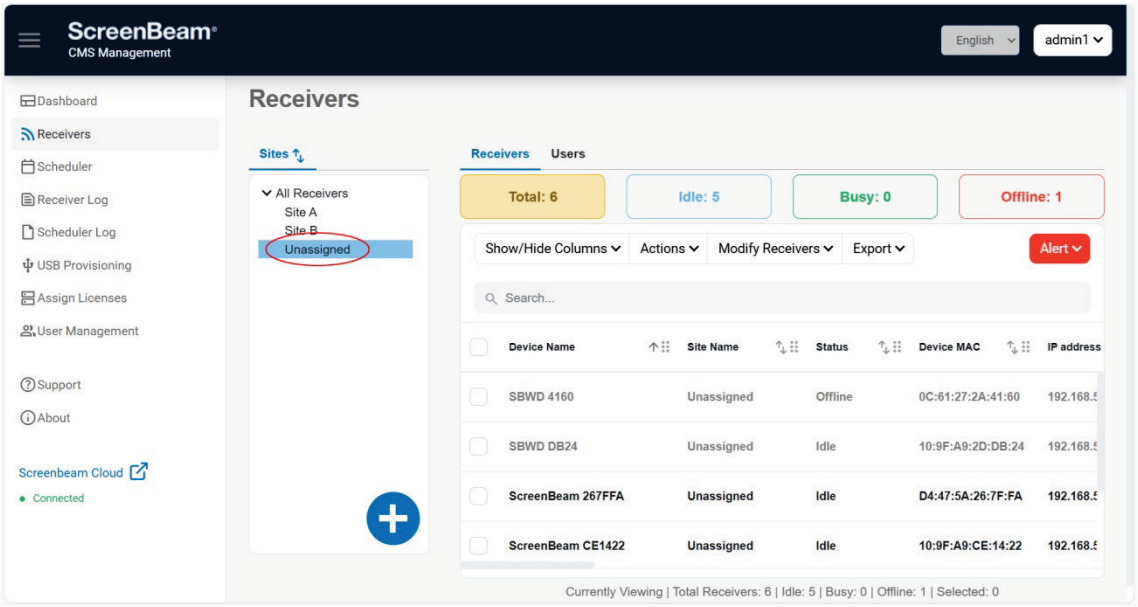
To add one or more receivers to a site, follow this procedure:

1. Go to the **Receivers** page by clicking **Receivers** on the left pane.

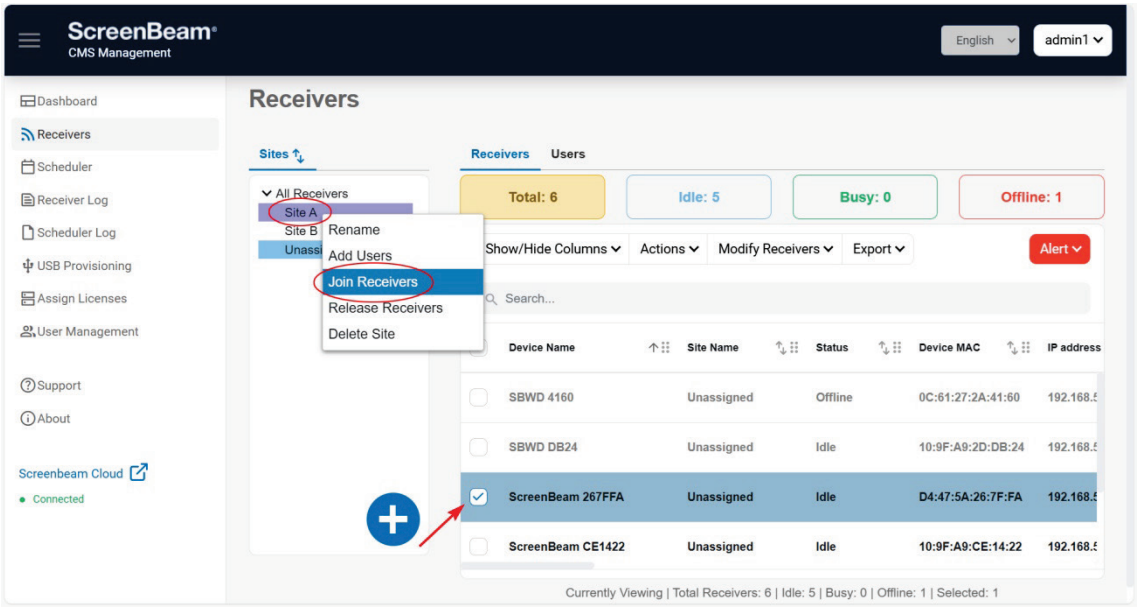


2. Click the **Receivers** tab to bring the **Receivers** pane to the front if it is not.

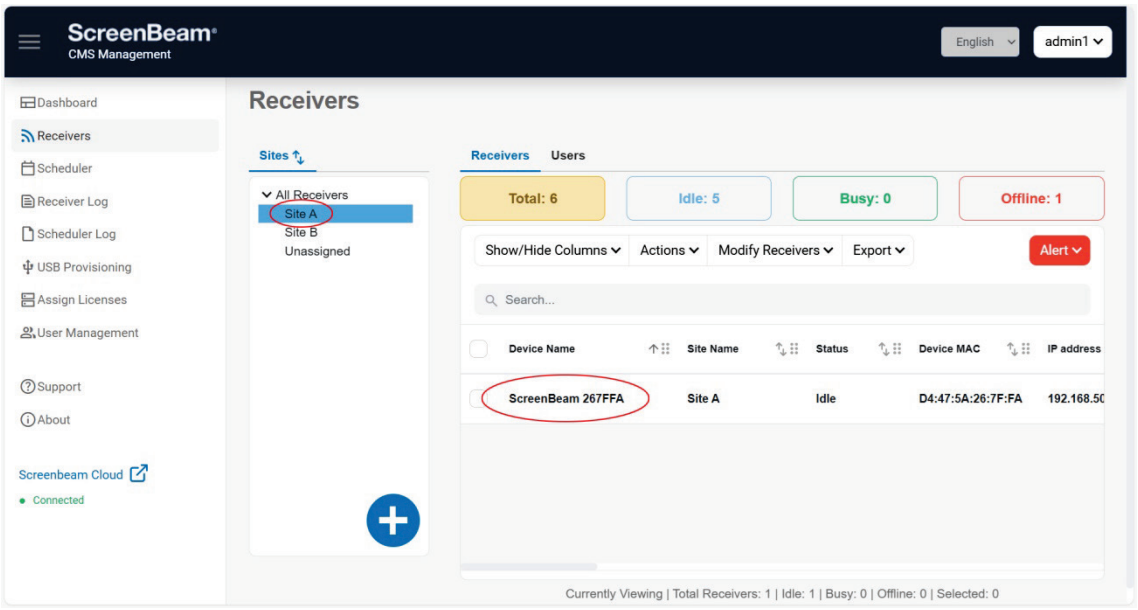
3. Click **Unassigned** on the **Sites** pane to display the receivers that are not added to any site on the **Receivers** pane.



4. Select the receiver(s) to be added on the **Receivers** pane, right-click the site where the selected receiver(s) are to be added and select **Join Receivers** from the short-cut menu.



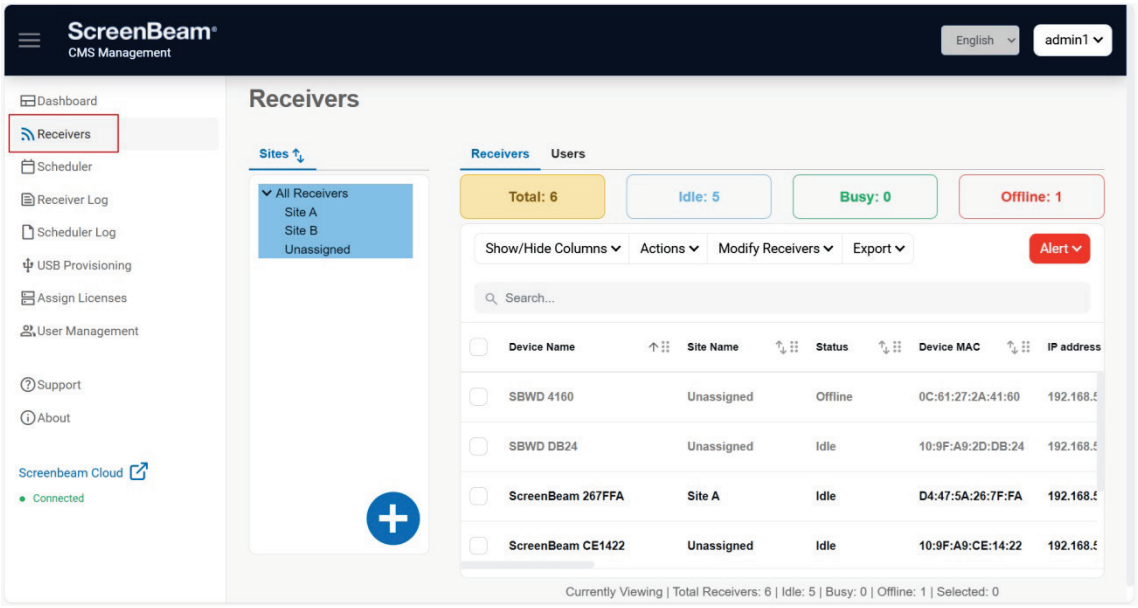
5. The selected receiver(s) are added to the desired site.



4.5.5 Release Receivers from a Site

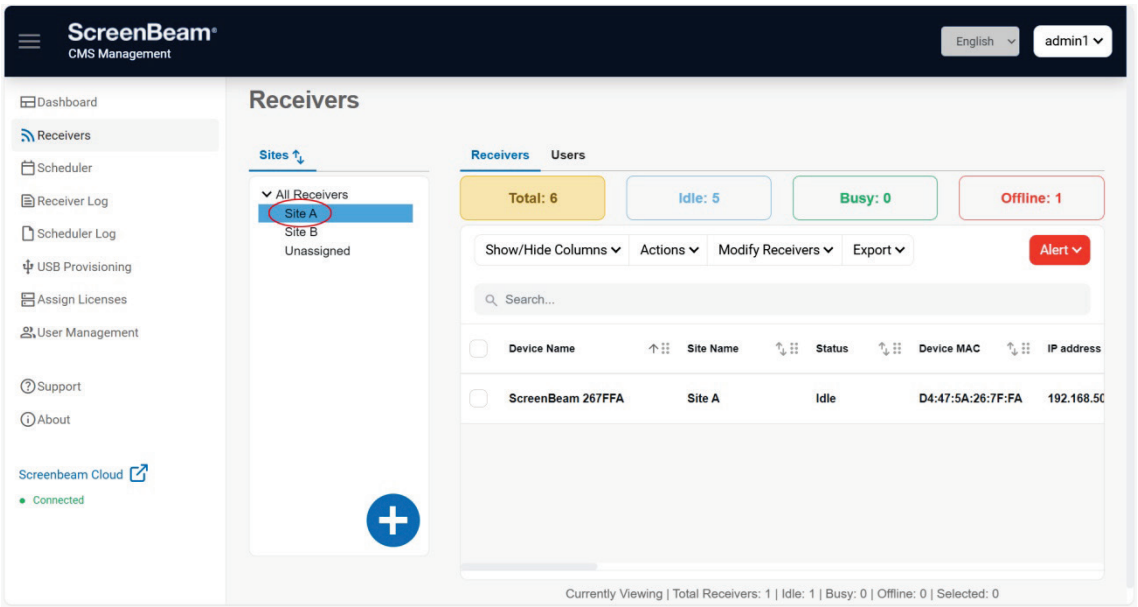
To release one or more receivers from a site, follow this procedure:

1. Go to the **Receivers** page by clicking **Receivers** on the left pane.

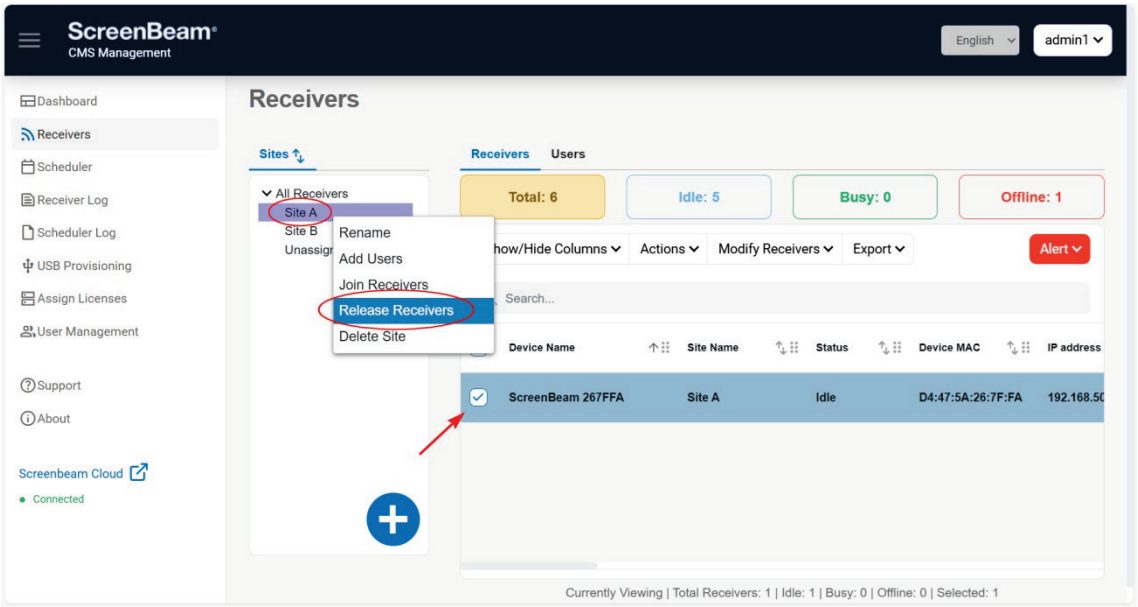


2. Click the **Receivers** tab to bring the **Receivers** pane to the front if it is not.

3. Select the site to display the receivers that are added to the site.



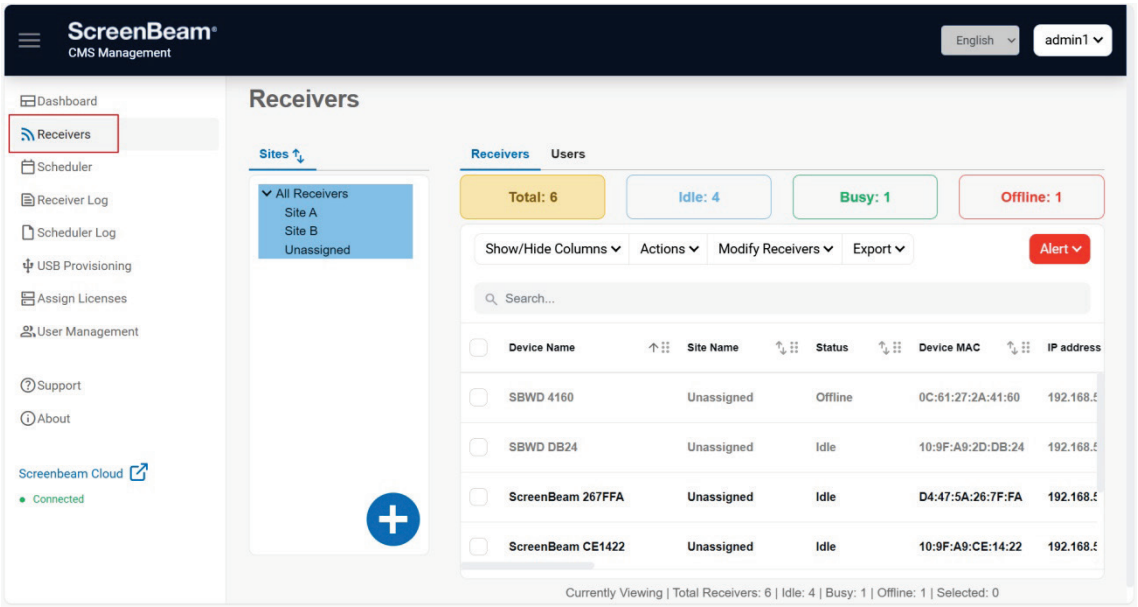
4. Select the receiver(s) that you want to release, right-click the site name in the **Site** pane and select **Release Receivers** from the shortcut menu. The selected receiver(s) will be released from the site immediately.



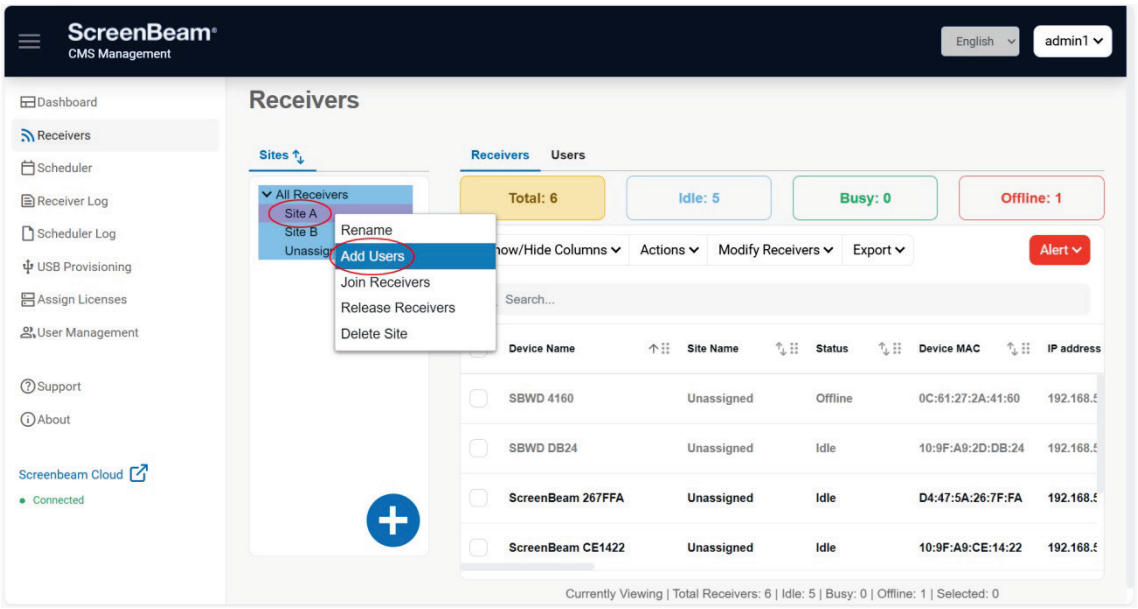
4.5.6 Add Users to a Site

To add one or more users to a site, follow this procedure:

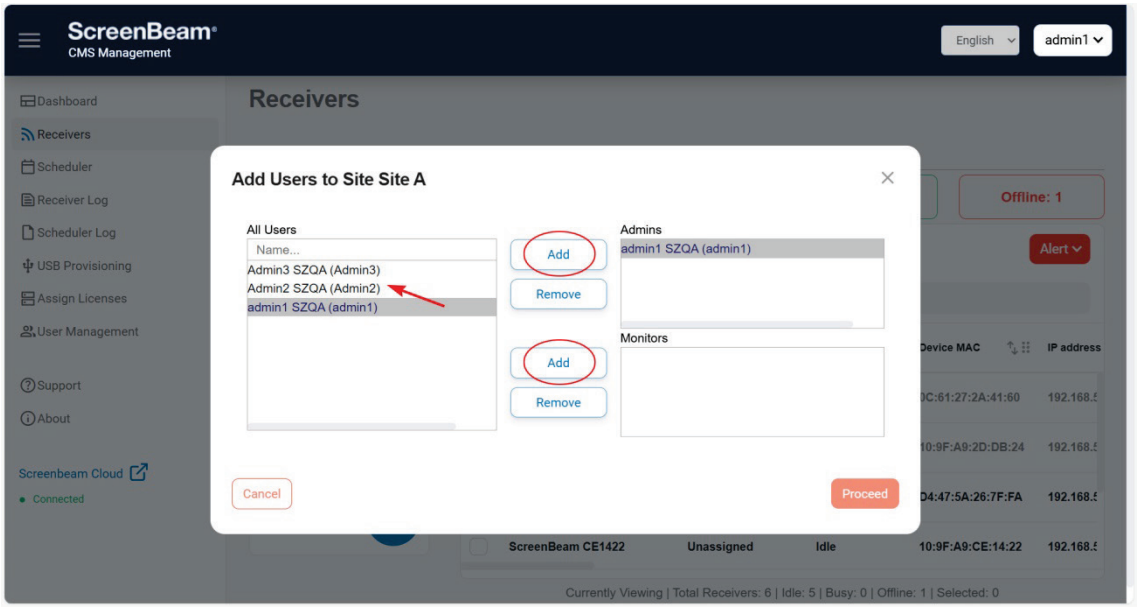
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



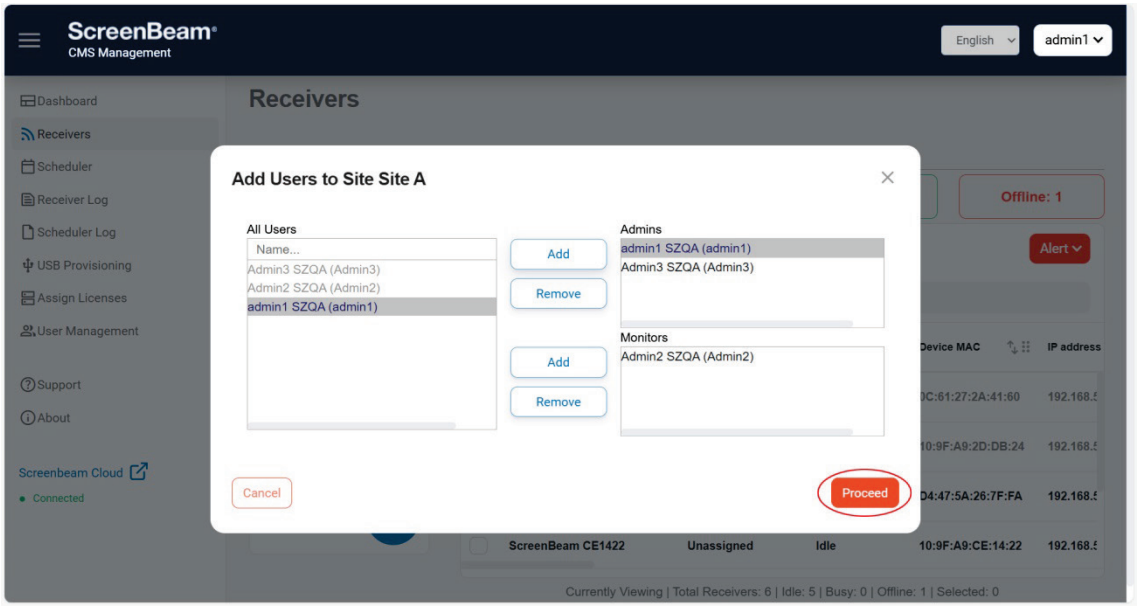
2. Right-click the site where you are going to add users and select **Add Users** from the short-cut menu.



3. The **Add Users to Site xxx** window appears. Select one or more users from the **All Users** box, and then click **Add** to add the selected users to the Admins box or the Monitors box.
   Note: The username format in the box below is First Name + Last Name + (Username).



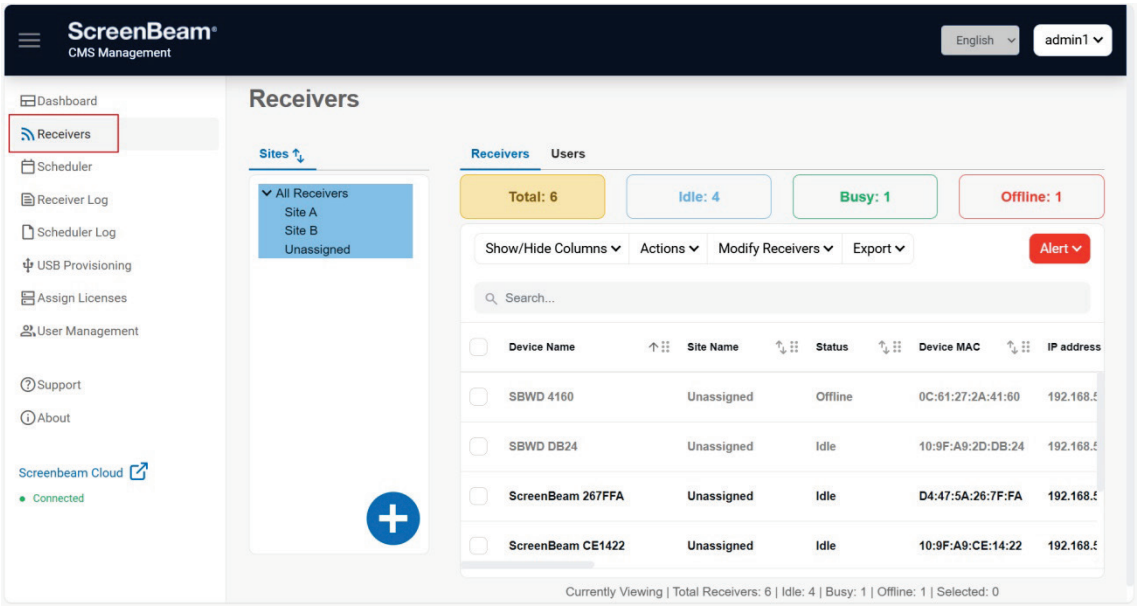
4. Click **Proceed** to confirm.
   Note: The figure below shows adding **Admin2** to **Site A** as Monitor and **Admin3** to **Site A** as Admin.



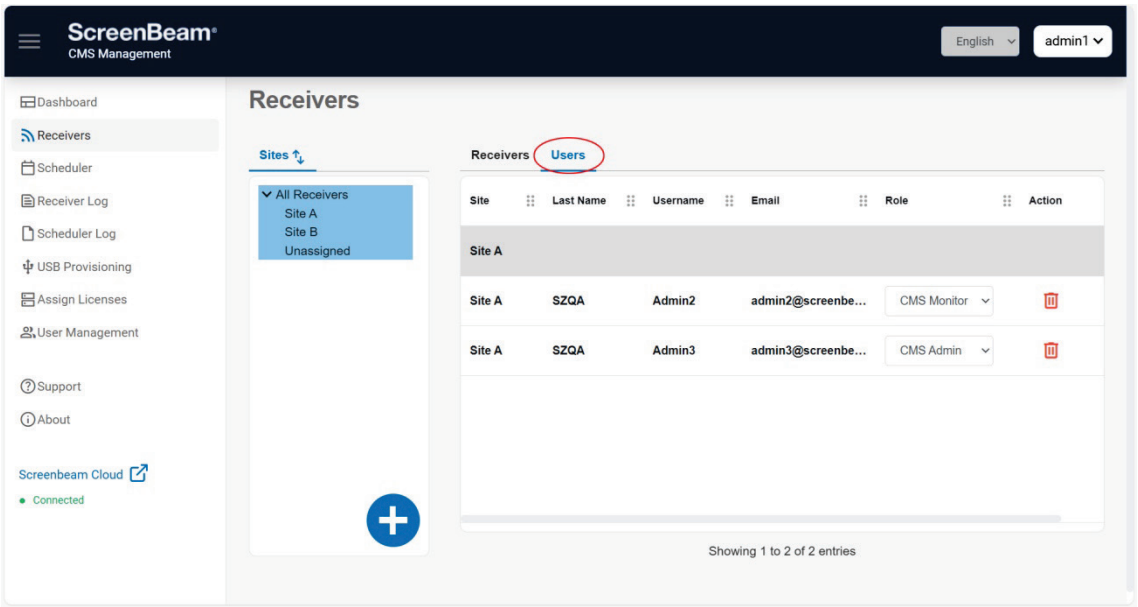
4.5.7 Release a User from a Site

To release a user from a site, follow this procedure:

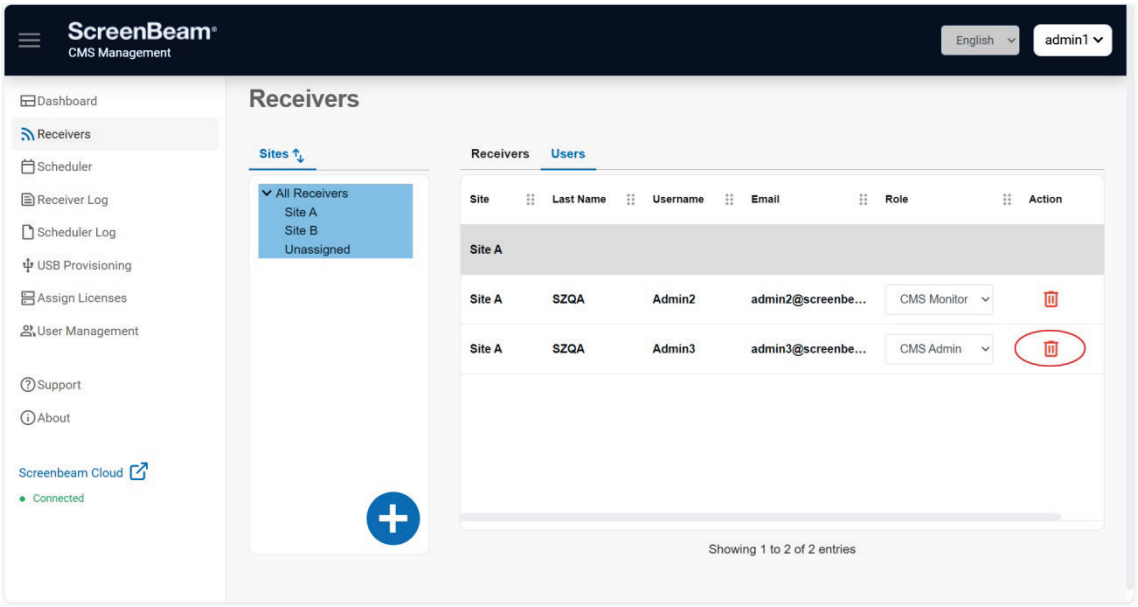
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Click the **Users** tab to display the **Users** page.



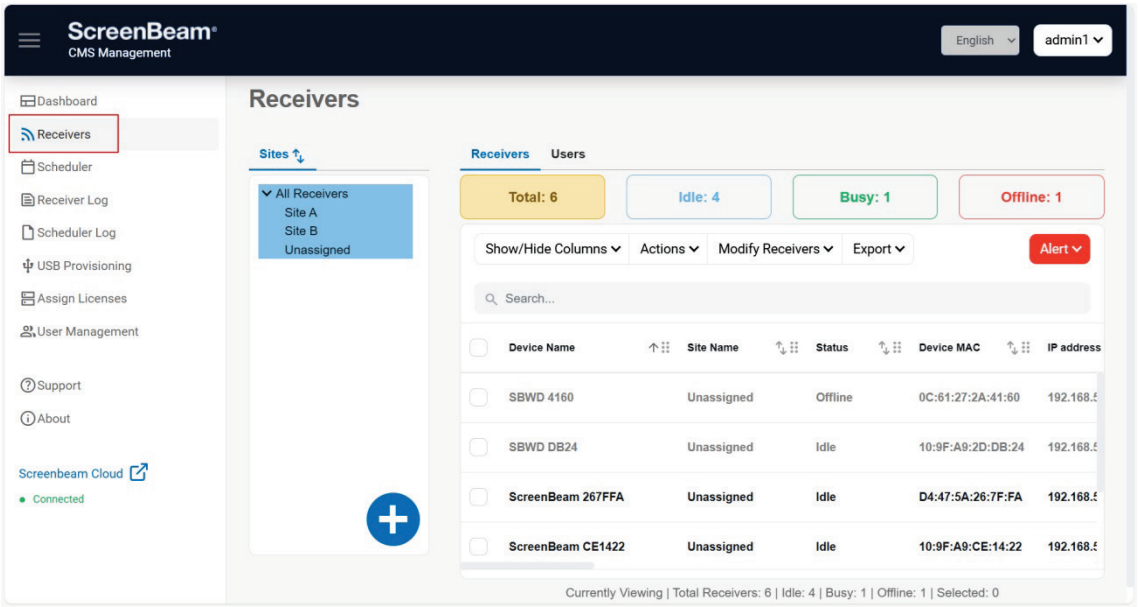
3. Click the Delete button (the red trash bin icon) in the Action column of a user entry to release the corresponding user from the site.



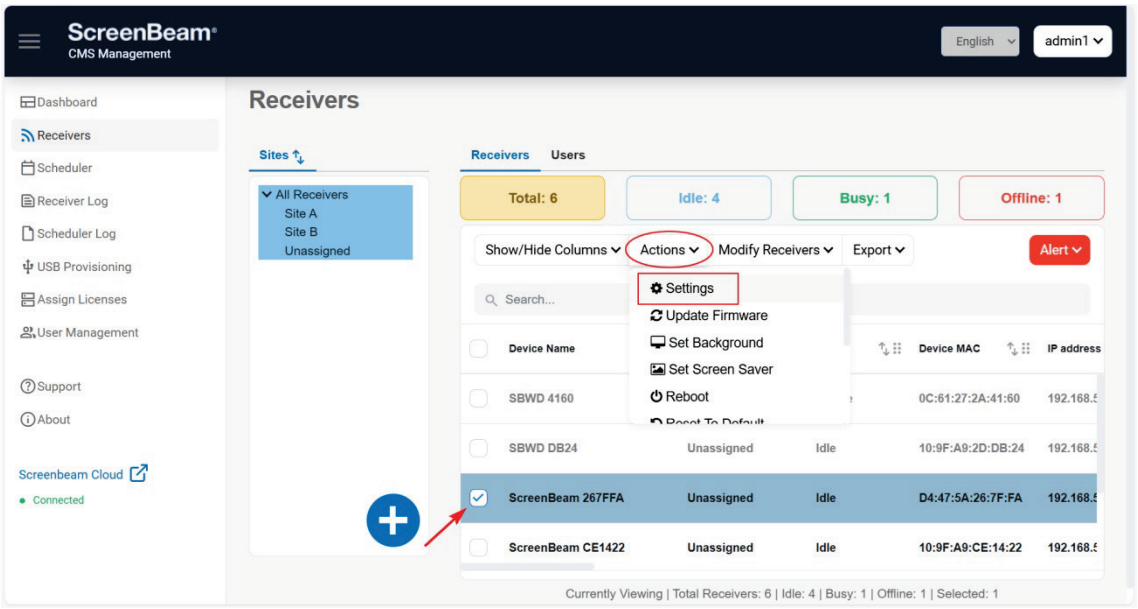
4.5.8 Configure Receiver Remotely

To configure one or more receivers, follow this procedure:

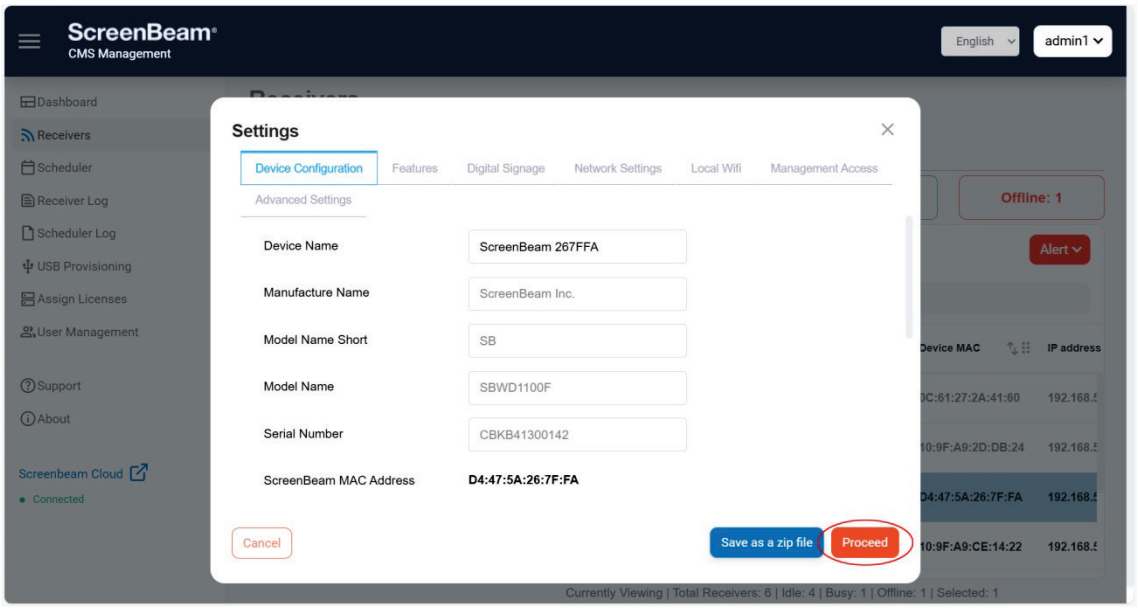
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Settings**.



3. The **Settings** or **Multiple Receiver Settings** window appears. Configure the receiver settings on the window and click **Proceed**.
   The **Save as a zip file** button is used to save all current settings of a receiver for technical support purposes.
   Note: Refer to the receiver's user manual for details about setting up a receiver.

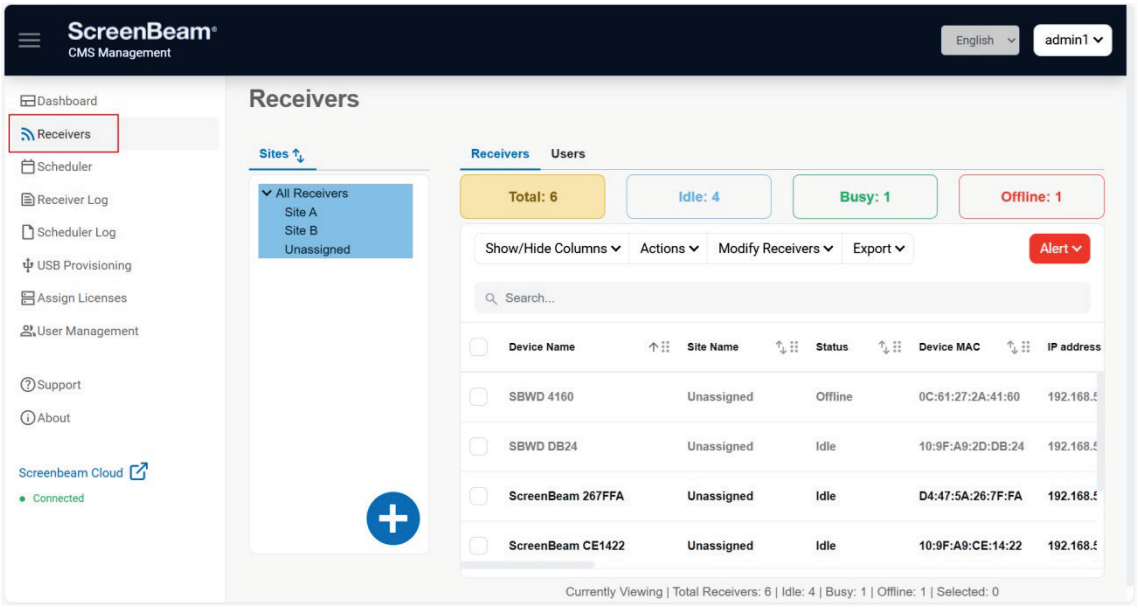


4.5.9 Save / Load Settings for Batch Configuration

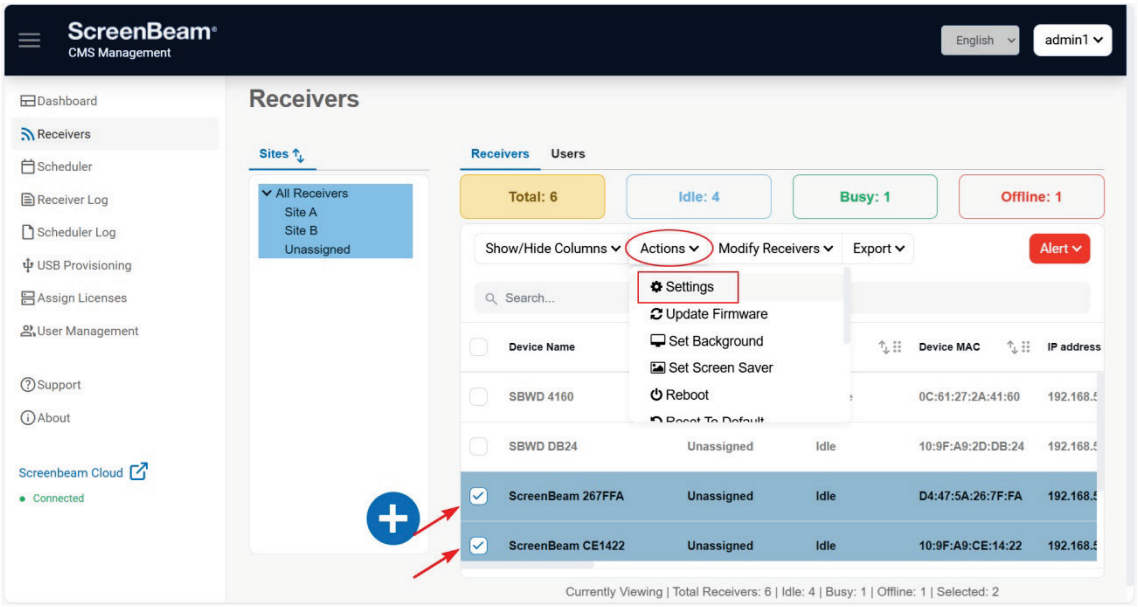
ScreenBeam CMS Enterprise allows users to save receiver batch configuration for future use.

To save settings for batch configuration, follow this procedure:

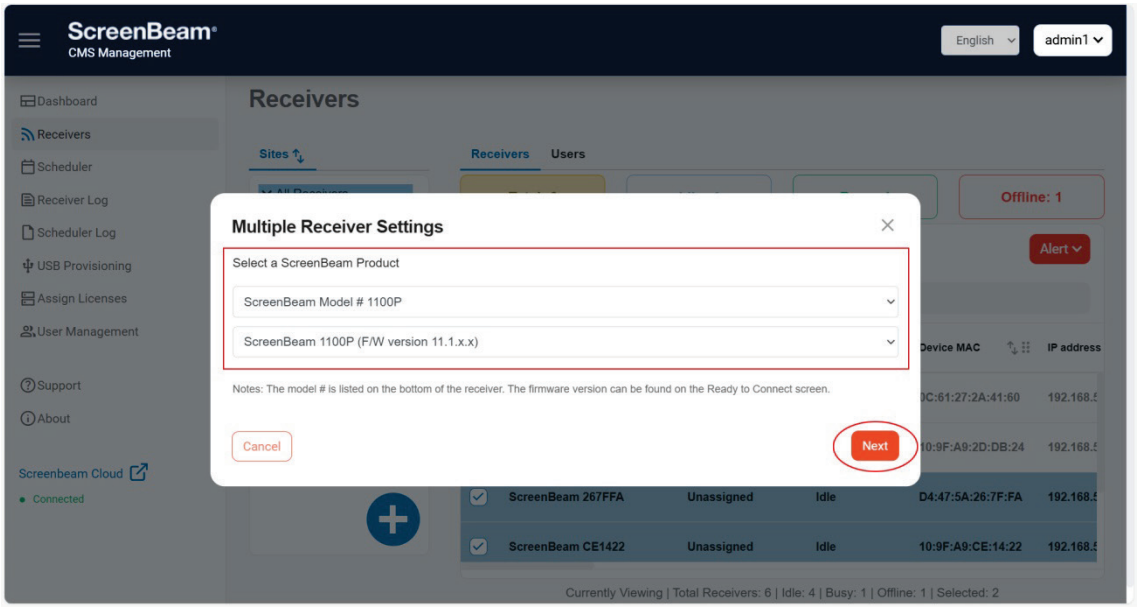
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



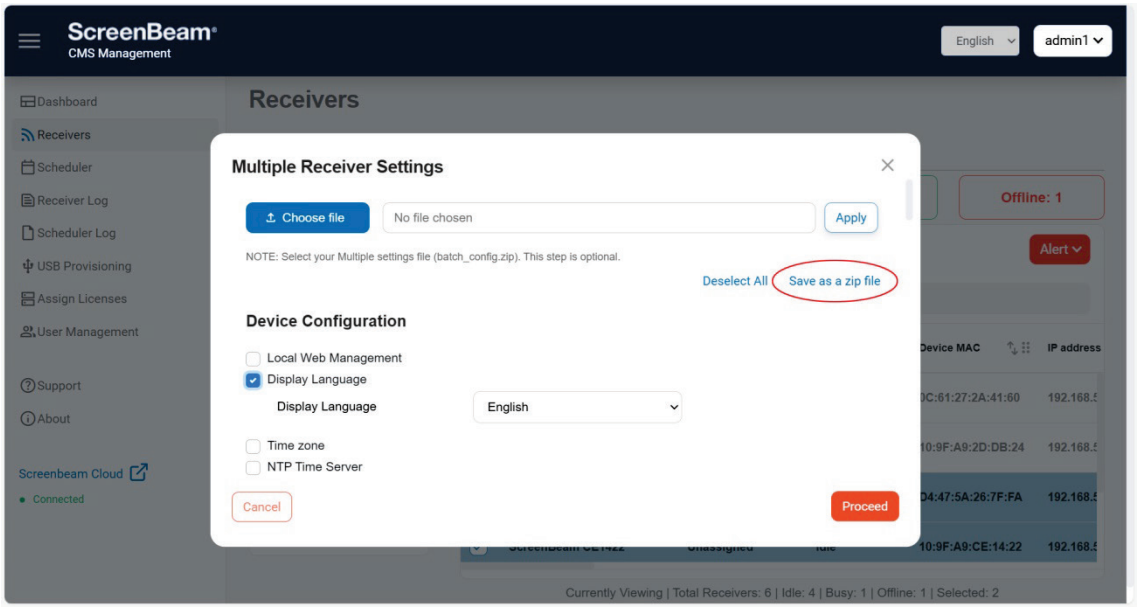
2. Select two or more receivers on the **Receivers** page, and then select **Actions** > **Settings**.



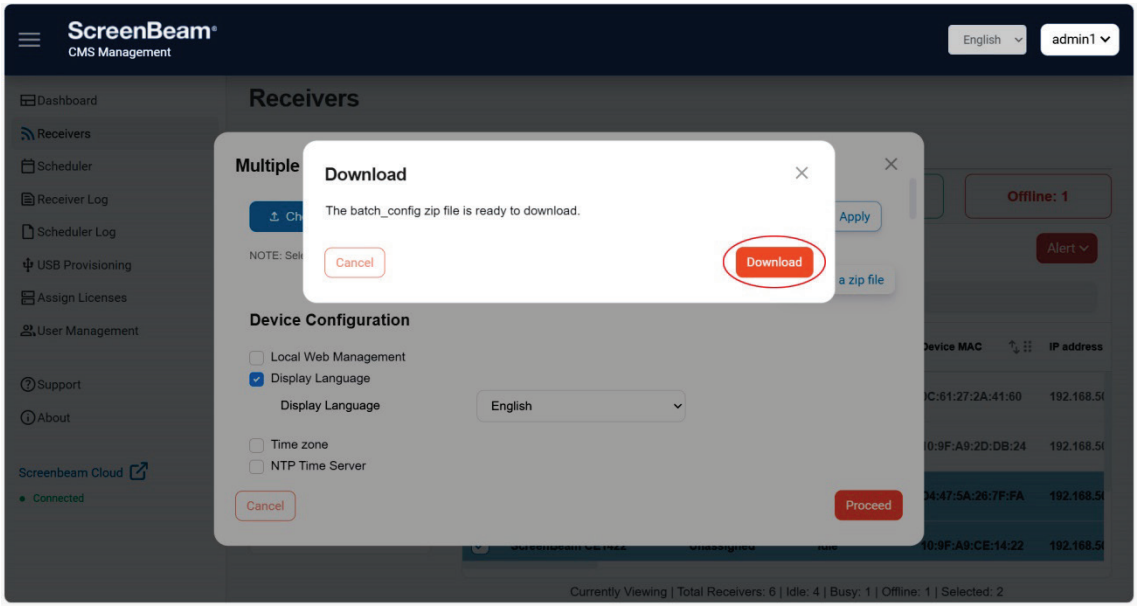
3. The **Select a ScreenBeam Product** box will appear if ScreenBeam receivers of different models are selected. Select a ScreenBeam model and its firmware version. Click **Next** to continue.



4. The **Multiple Receiver Settings** window appears. Make changes to the receiver configuration items and click the **Save as a zip file** button.

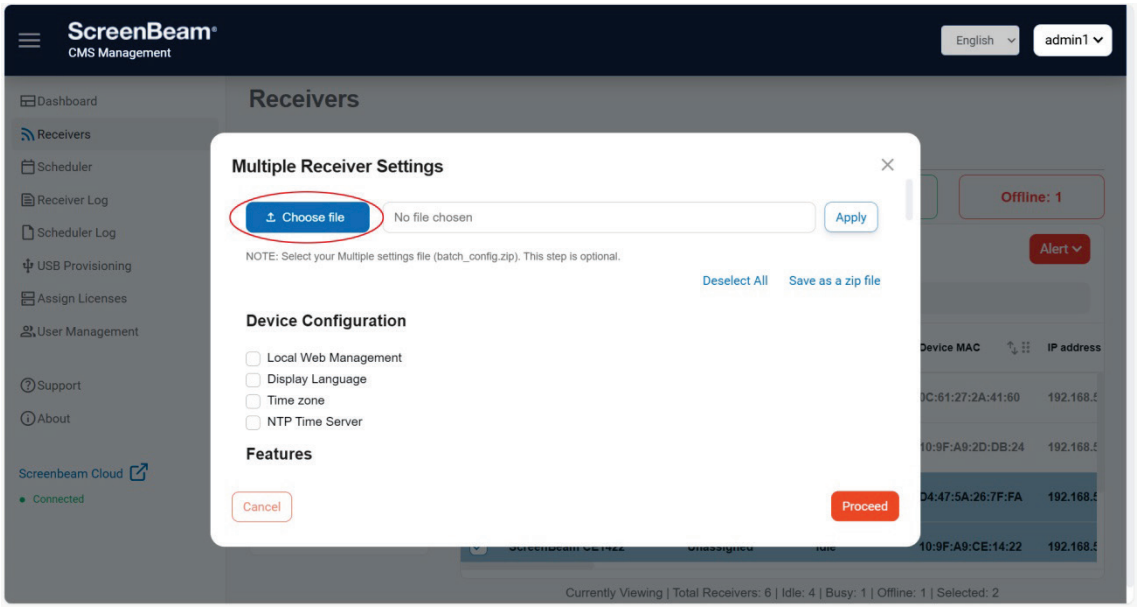


5. The **Download** message box appears. Click **Download** to save batch settings on your device. All changes on the **Multiple Receiver Settings** page will be saved in the **batch_config.zip** file.

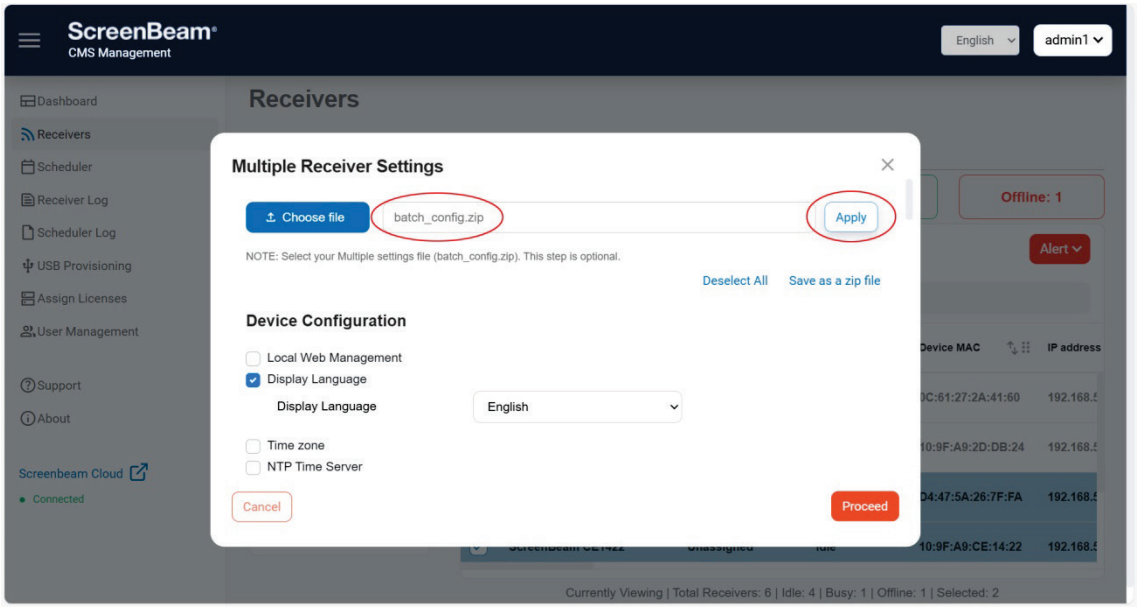


To load receiver batch settings, follow this procedure:

1. Follow steps 1-3 above to open the **Multiple Receiver Settings** window.
2. Click the **Choose file** button and choose a batch configuration file you saved previously.



3. The chosen batch configuration file will be displayed in the **Choose file** box. Click **Apply**. ScreenBeam CMS will read the batch configuration file and apply changes on the **Multiple Receiver Settings** page according to settings on the batch configuration file.

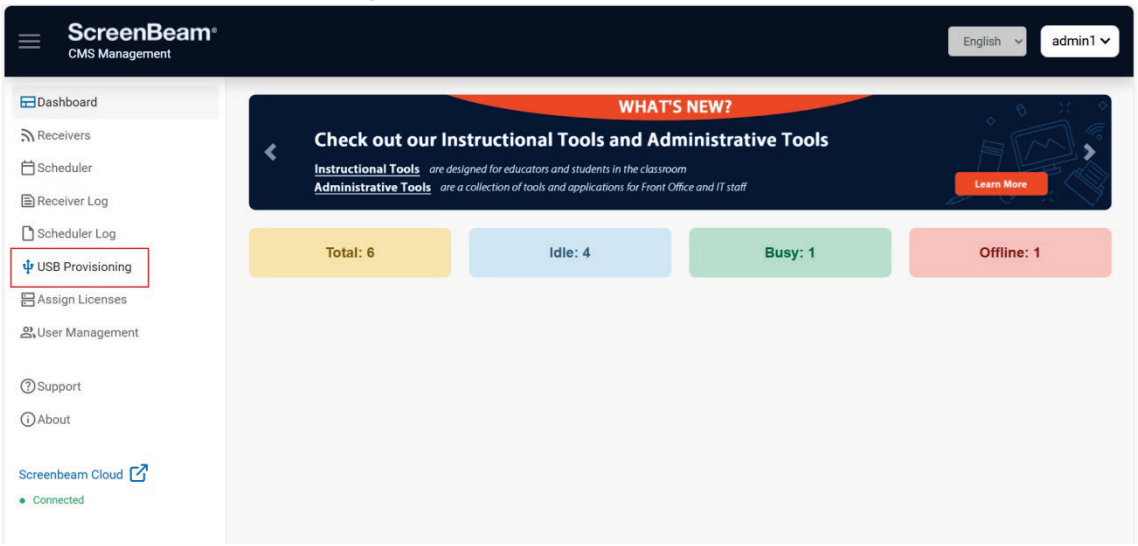


Note: This is an optional operation when you are configuring multiple receivers.

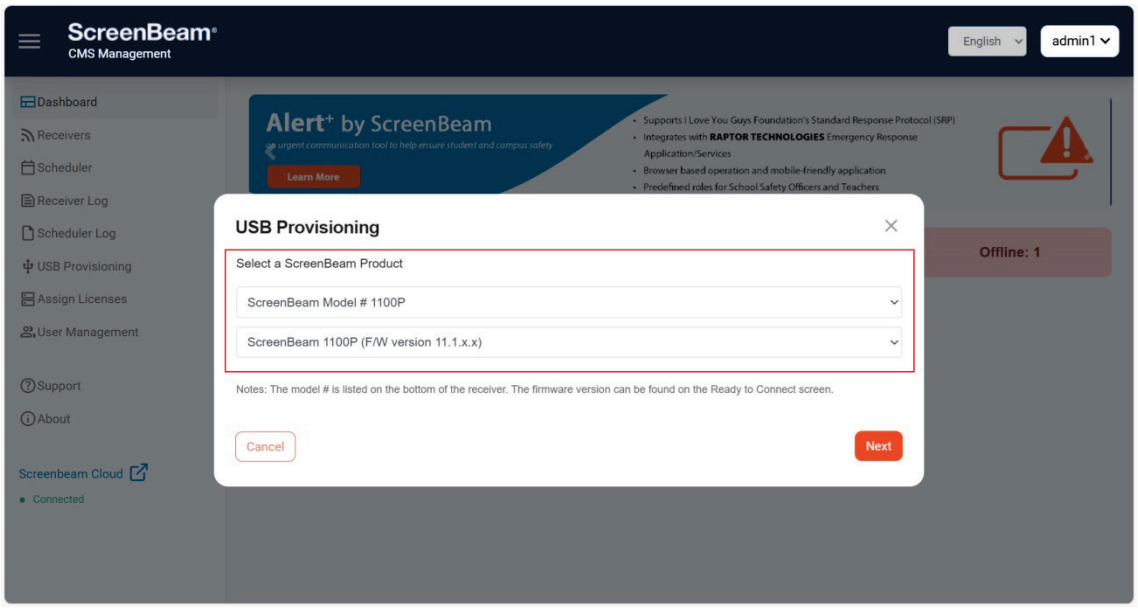
4.5.10 Configure Receiver with a USB Flash Drive

To configure ScreenBeam receiver with a USB flash drive, follow this procedure:

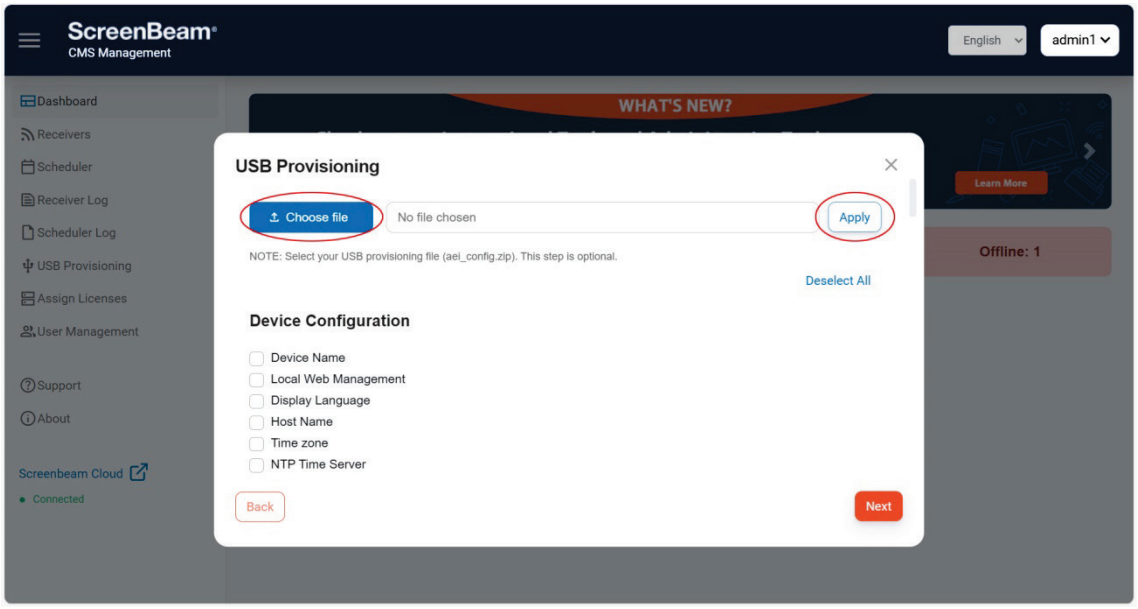
1. Select **USB Provisioning** from the left pane.



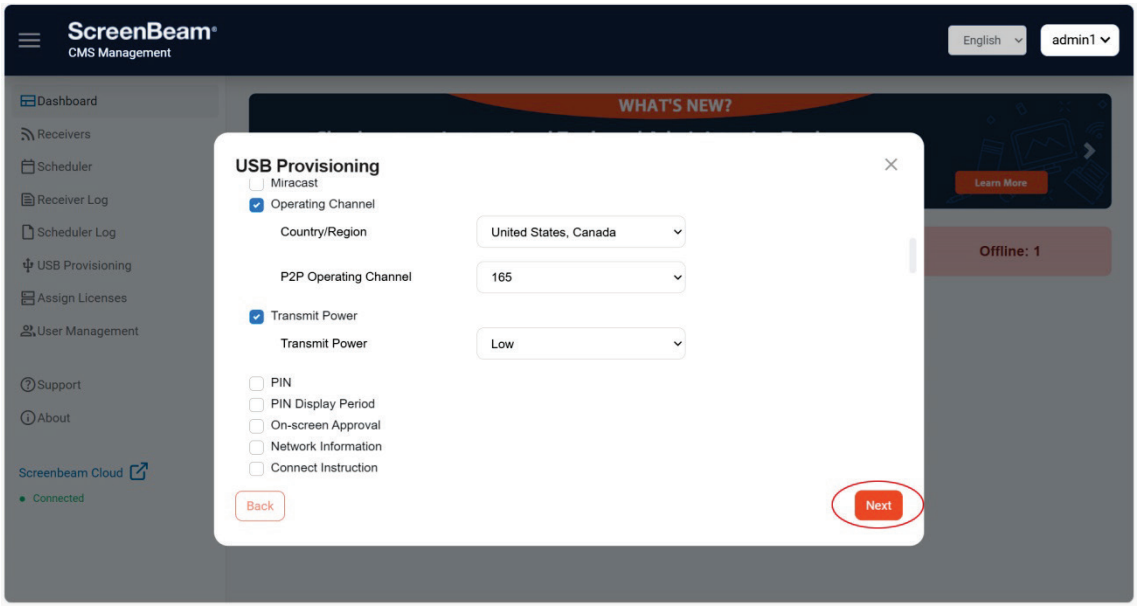
2. The **USB Provisioning** window appears. Select a ScreenBeam product and its firmware. Click **Next**.



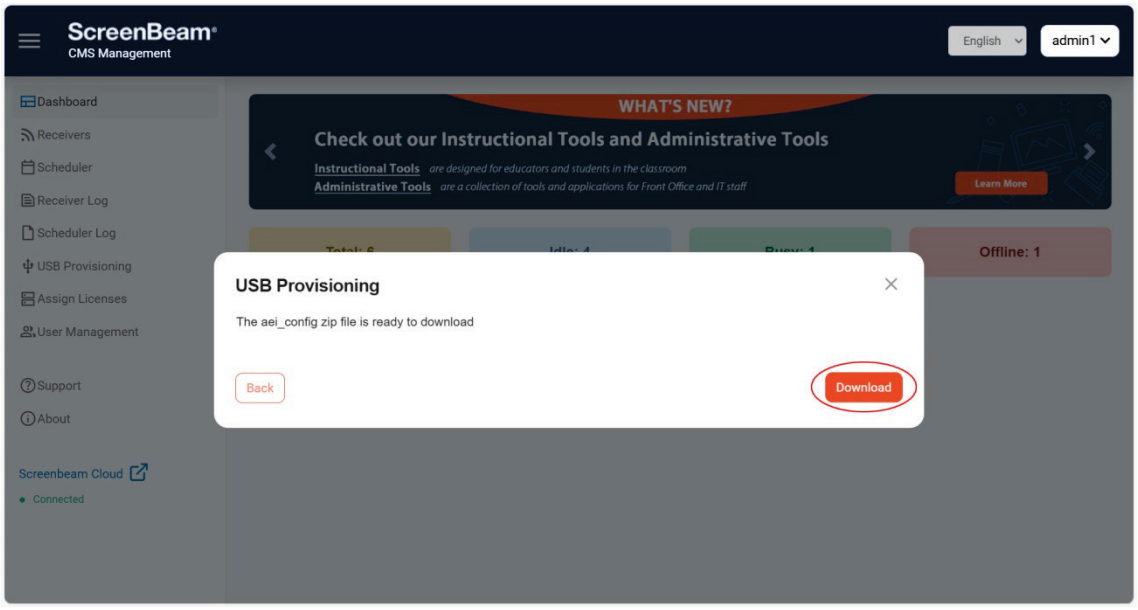
3. (Optional) CMS allow users to load a previously saved configuration file and make new configurations based on that file. Click **Choose file** to select a USB configuration file and click **Apply**.



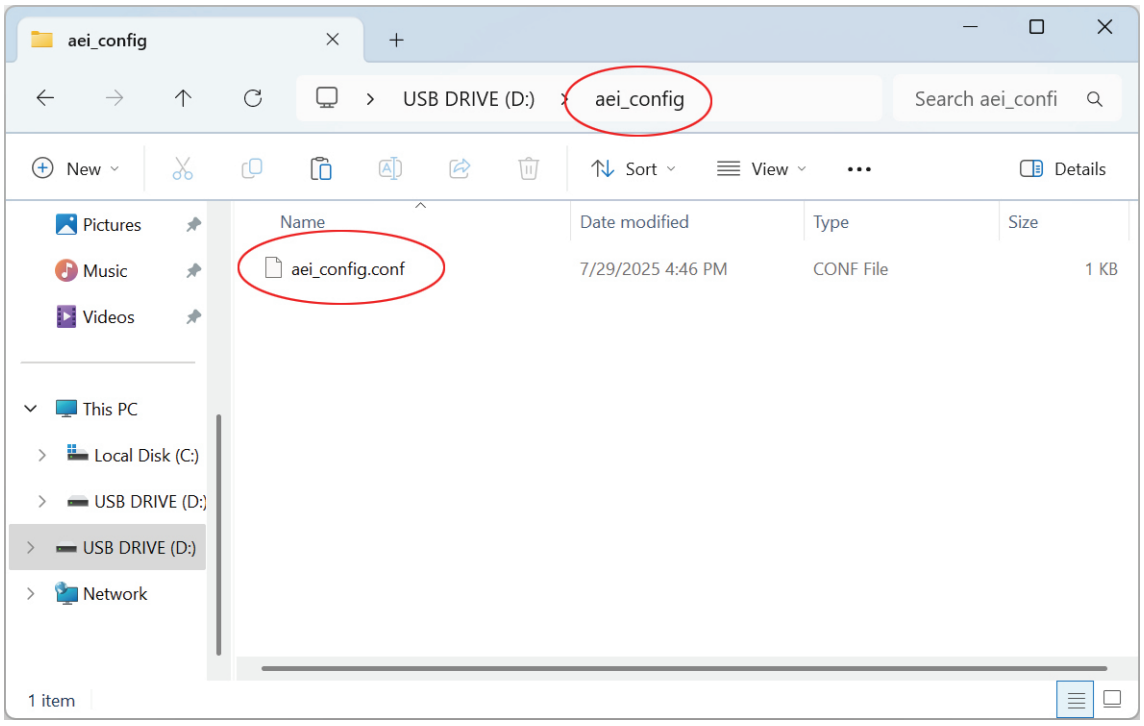
4. Select and configure the desired items on the list and then click **Next**.
   Note: Refer to the receiver's user manual for details about setting up a receiver.



5. The download page appears. Click **Download** and save the receiver configuration file (**aei_config.zip**).



6. Unzip the downloaded receiver configuration file (**aei_config.zip**) and copy the "aei_config" folder to the root directory of a FAT32 formatted USB flash drive. Ensure that the receiver configuration file (aei_config.conf) is in the **aei_config** folder, and no modifications to the name or file contents are made.



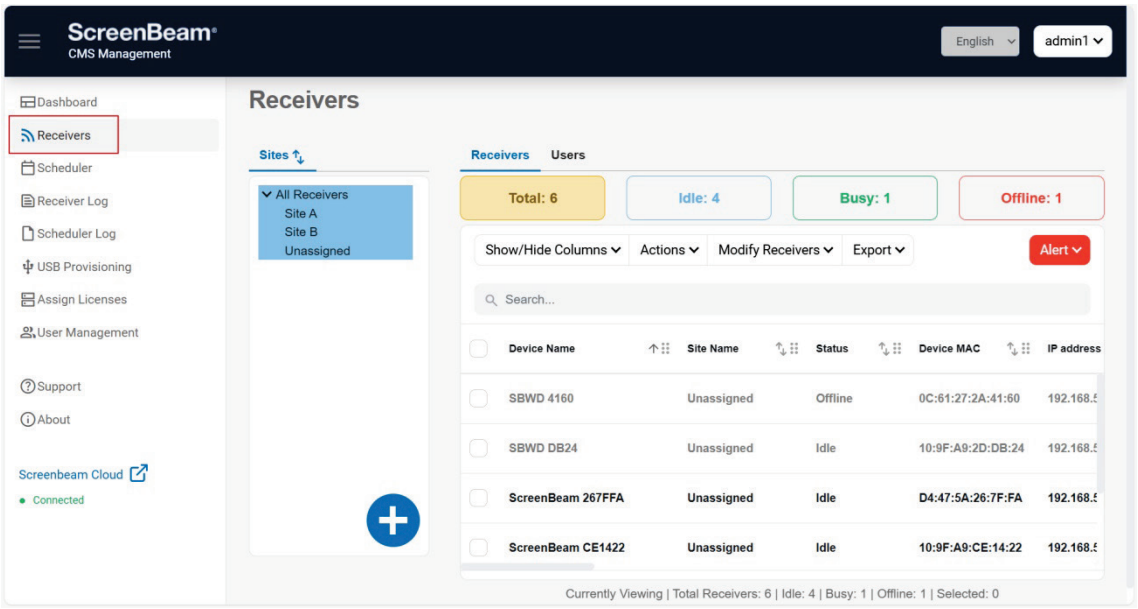
7. Power on the ScreenBeam receiver. When the idle screen appears, plug in the USB flash drive. After the receiver has rebooted, it is configured with the settings you have defined in Step 4.

4.5.11 Update Receiver Firmware

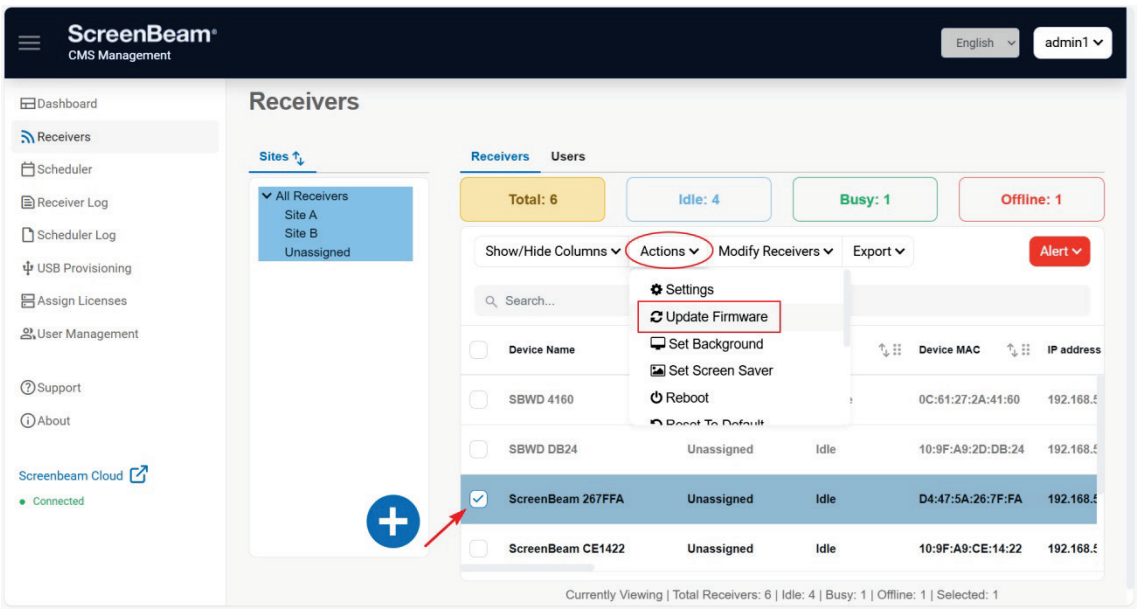
Go to https://www.screenbeam.com/support, locate your product and download the latest receiver firmware.

To update firmware for one or more receivers, follow this procedure:

1. Ensure the receiver's firmware update image resides on an HTTP server.
2. Go to the **Receivers** page by clicking **Receivers** on the left pane.

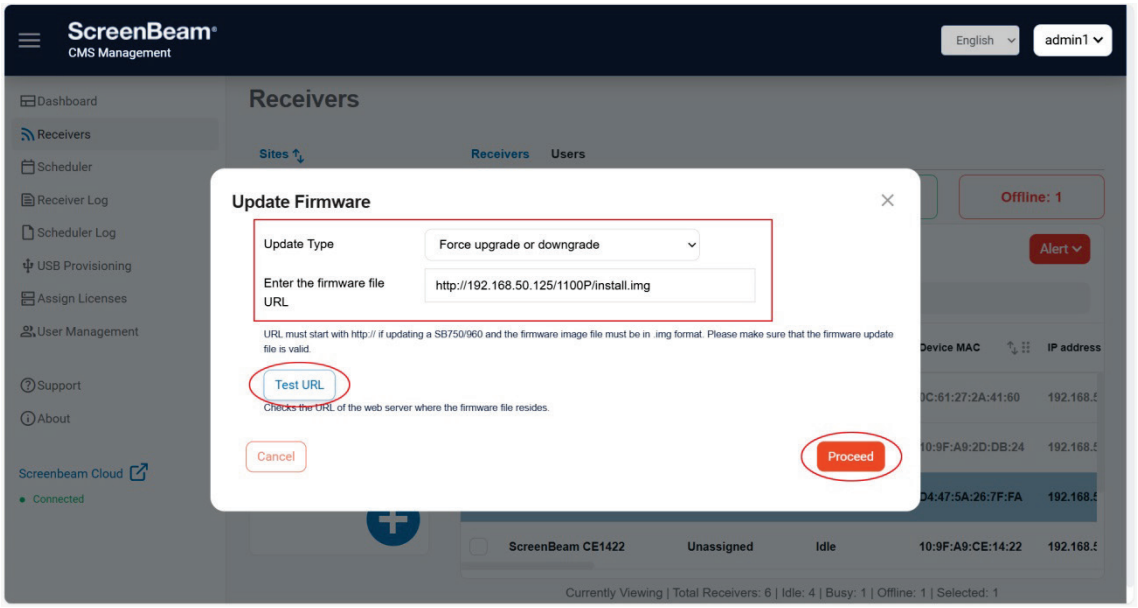


3. Select one or more receivers on the **Receivers** pane, and then select **Actions** > **Update Firmware**.



4. The **Update Firmware** window appears. Select an Update Type, enter the firmware file URL in the **Enter the firmware file URL** box, and click **Proceed**.
   - **Per receiver's setting**: The selected receivers will be upgraded to a higher version if firmware upgrade is enabled for the receiver. Otherwise, firmware update will not be executed.
   - **Force upgrade to a higher version**: The selected receivers will be upgraded to a higher version no matter if firmware upgrade is enabled for the receiver or not.
   - **Force upgrade or downgrade**: The selected receivers will be upgraded to a higher version or downgraded to a lower version no matter if firmware upgrade is enabled for the receiver or not.
   - **Special firmware update**: The receiver will be updated to a special firmware.

   Note: Click the **Test URL** button to check the validity of the URL if desired.

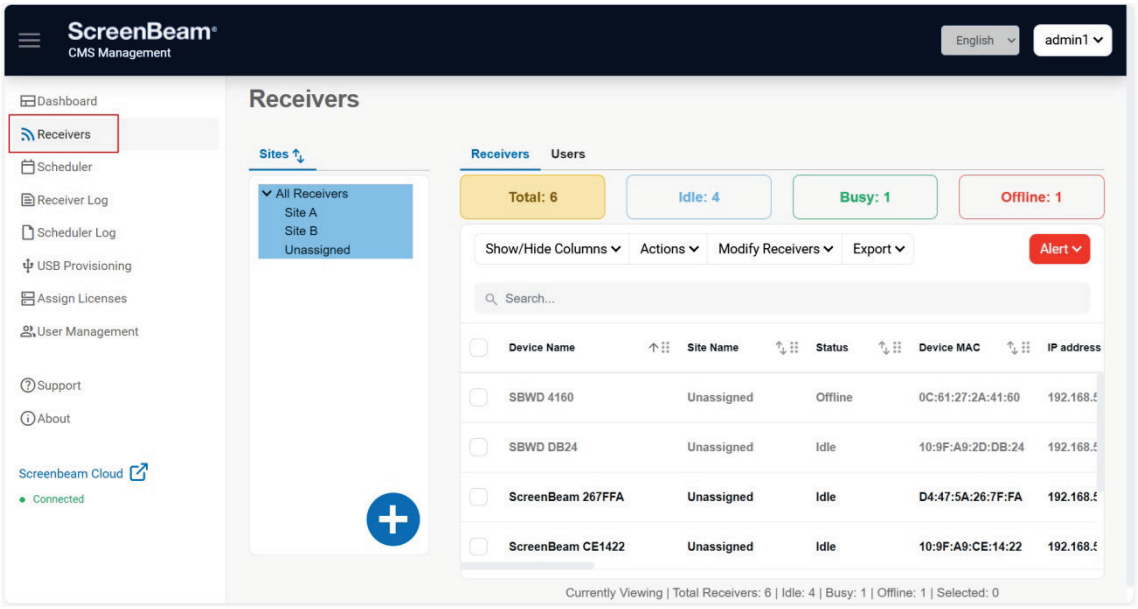


4.5.12 Connect Receiver to RADIUS Authenticated AP/LAN

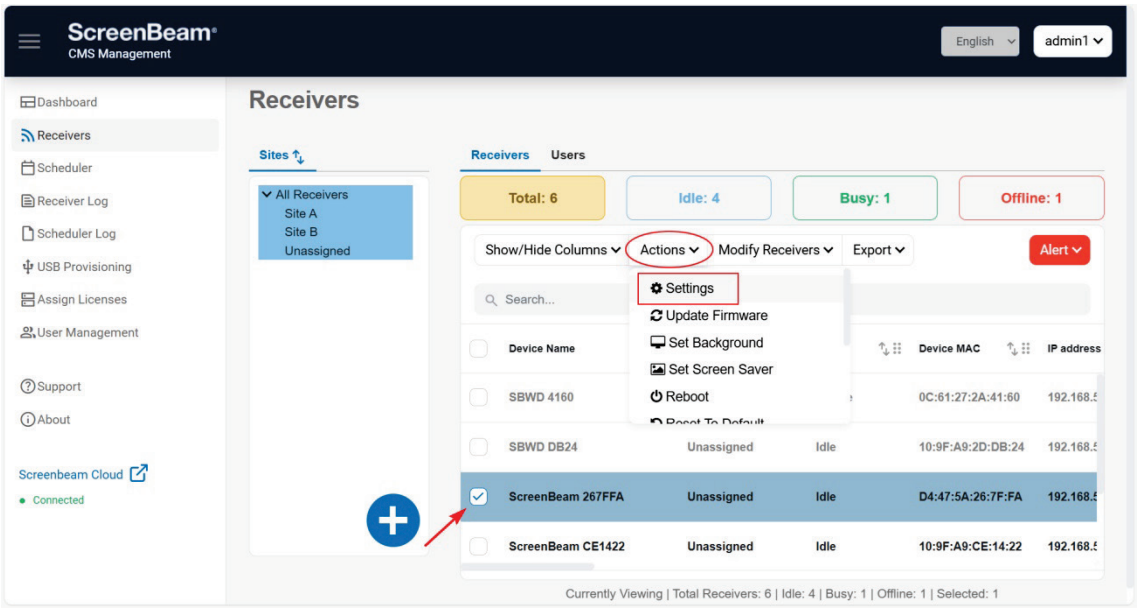
ScreenBeam receivers can connect to a RADIUS authenticated access point (AP) or local area network (LAN) using IEEE 802.1x protocol.

To connect a ScreenBeam receiver to a RADIUS authenticated access point, follow this procedure:

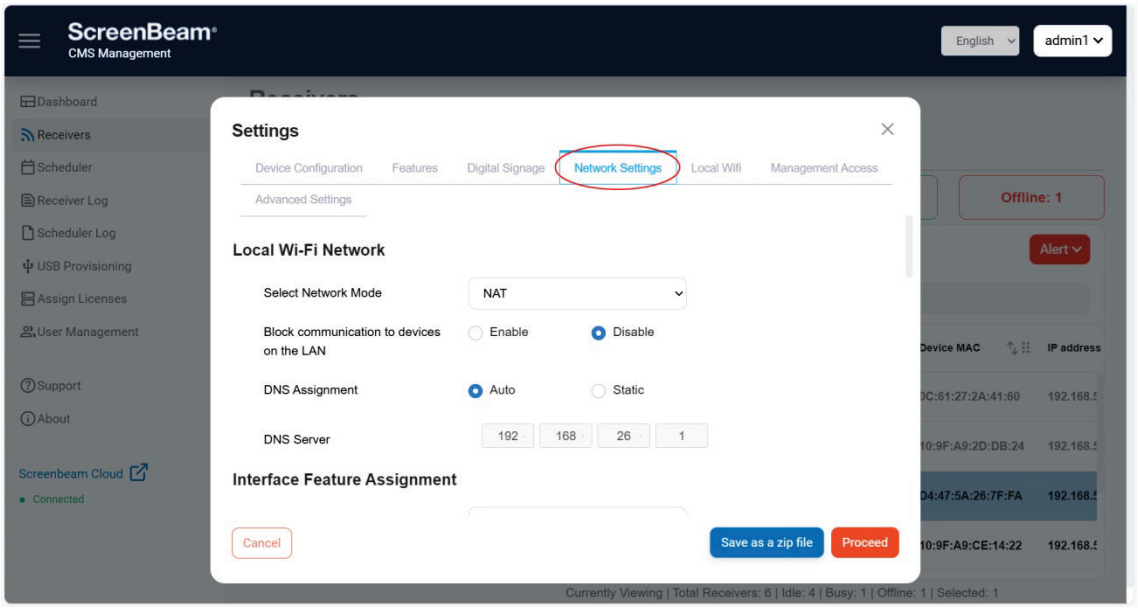
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



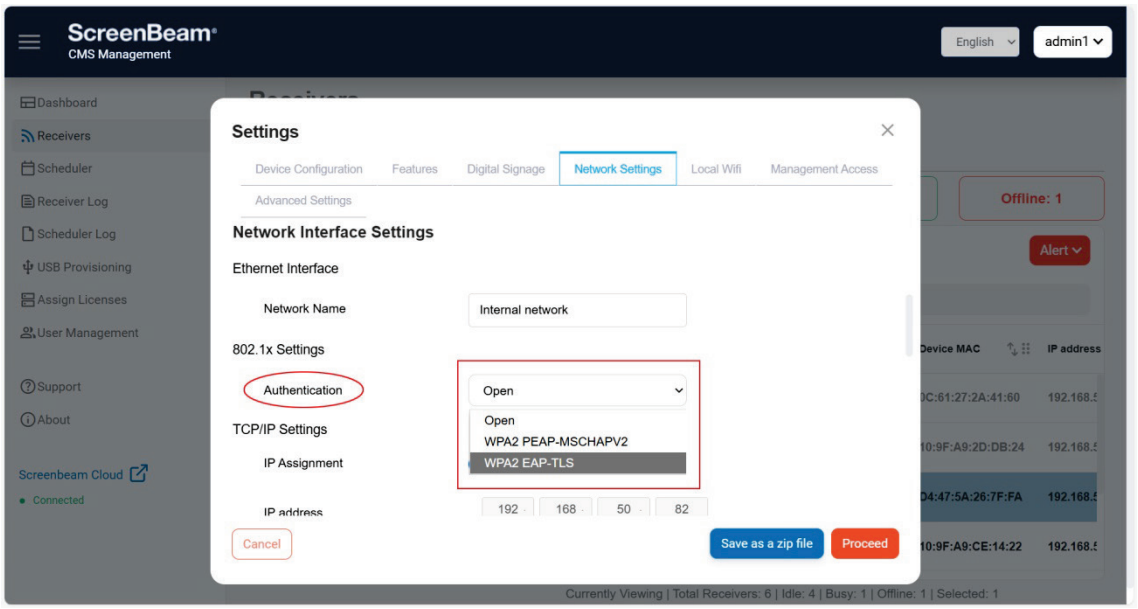
2. Select the receiver to connect to a RADIUS authenticated AP/LAN on the **Receivers** page, and then select **Actions** > **Settings**.

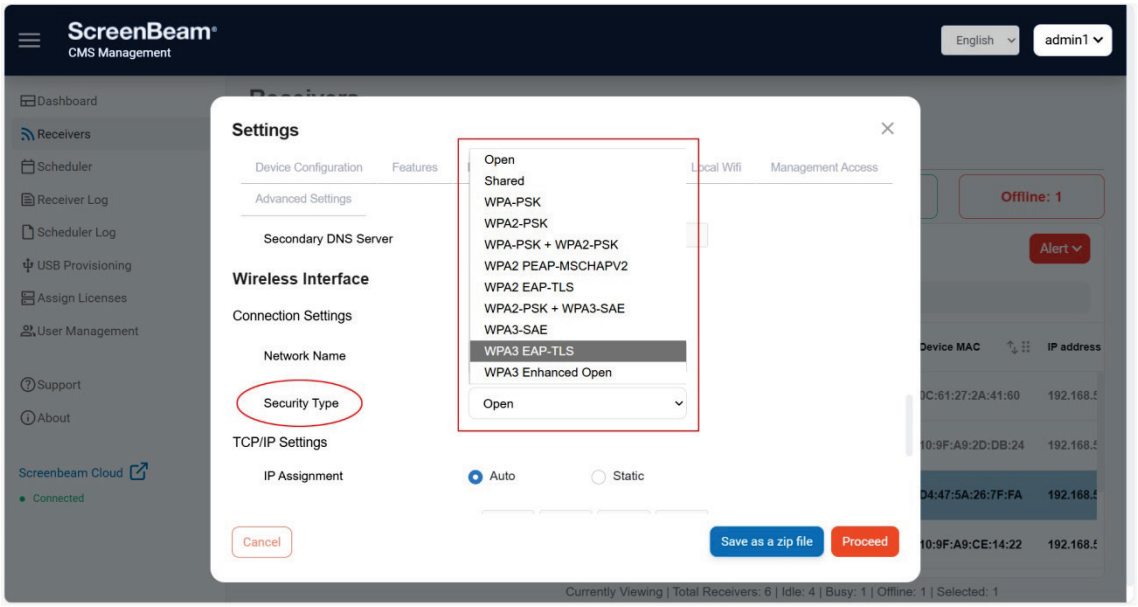


3. The **Settings** window appears. Navigate to the **Network Settings** page.



4. To connect to a RADIUS authenticated LAN, go to **Network Interface Settings** > **Ethernet Interface**, and select **WPA2 PEAP-MSCHAPV2** or **WPA2 EAP-TLS** in the **Authentication** box, enter Username and Password for authentication.
   To connect to a RADIUS authenticated AP, go to **Network Interface Settings** > **Wireless Interface**, and select **WPA2 PEAP-MSCHAPV2**, **WPA2 EAP-TLS** or **WPA3 EAP-TLS** in the **Security Type** box, enter network name of the AP, Username and Password for authentication.
   - Network Name - It is the network name of the AP.
   - User Name - It is the User Name of the RADIUS account.
   - Password - It is the password of the RADIUS account.
   - Validity Period - It displays the effective period of the certificates.

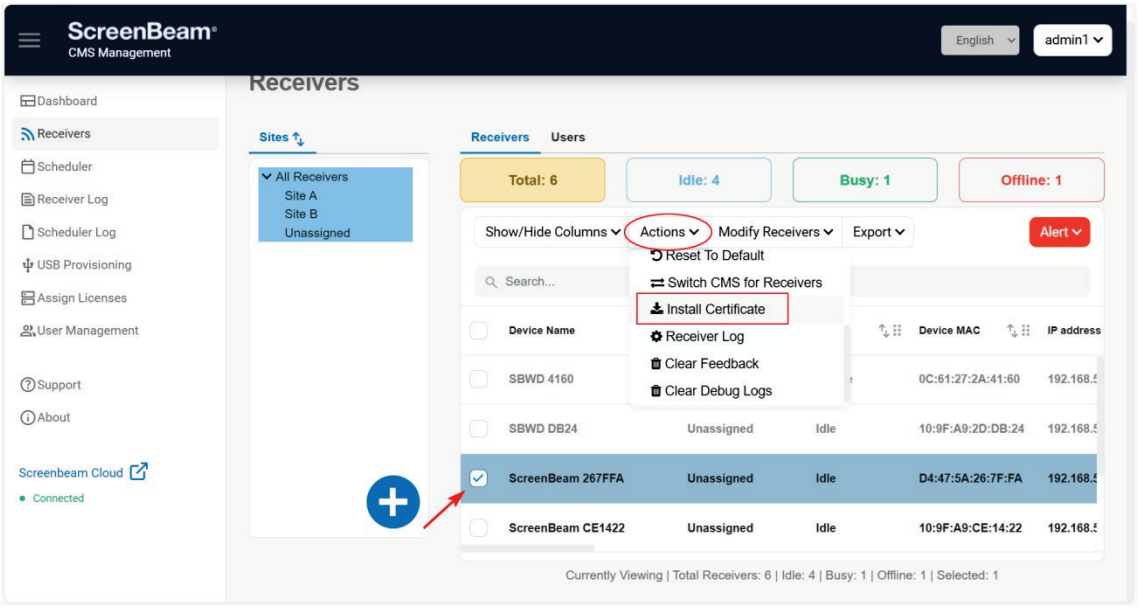




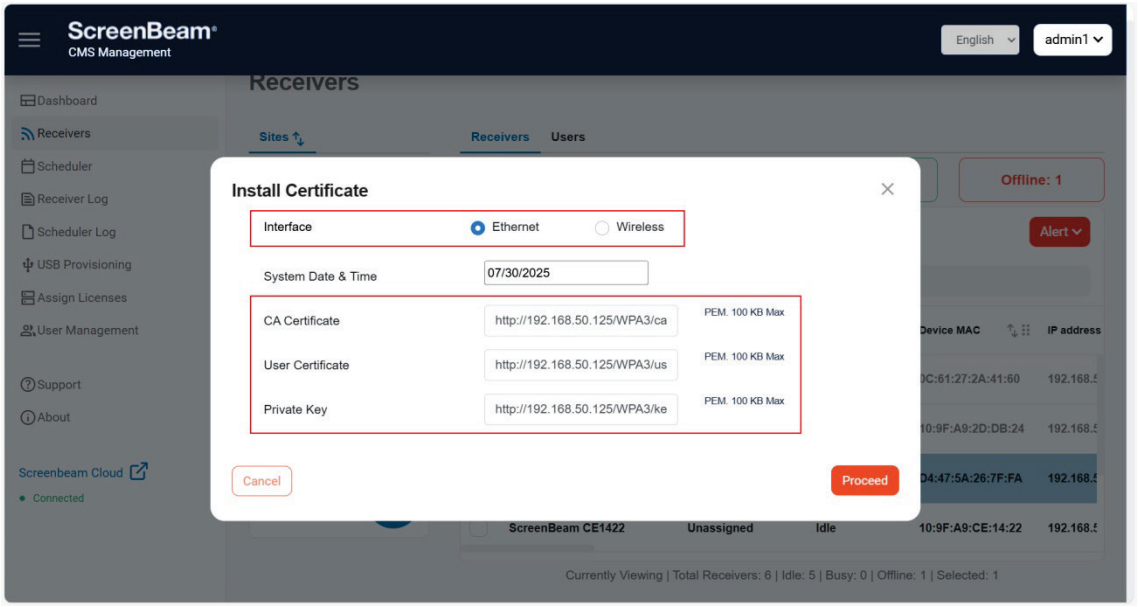
5. Click **Proceed** to confirm.

6. If **WPA2 EAP-TLS** or **WPA3 EAP-TLS** is selected, valid certificates are required for authentication. Ensure these certificates are resided on an HTTP server.
   Note: Some wireless APs may require CA certificate for authentication using the **WPA2 PEAP-MSCHAPV2** protocol.

7. Select the receiver, and then select **Actions** > **Install Certificate**.



8. The **Install Certificate** window appears. Select **Ethernet** or **Wireless** according to the kind of network the receiver connects to and enter URLs of the certificates.
   - CA Certificate - Root certificate.
   - User Certificate - User certificate.
   - Private Key - User's private key.



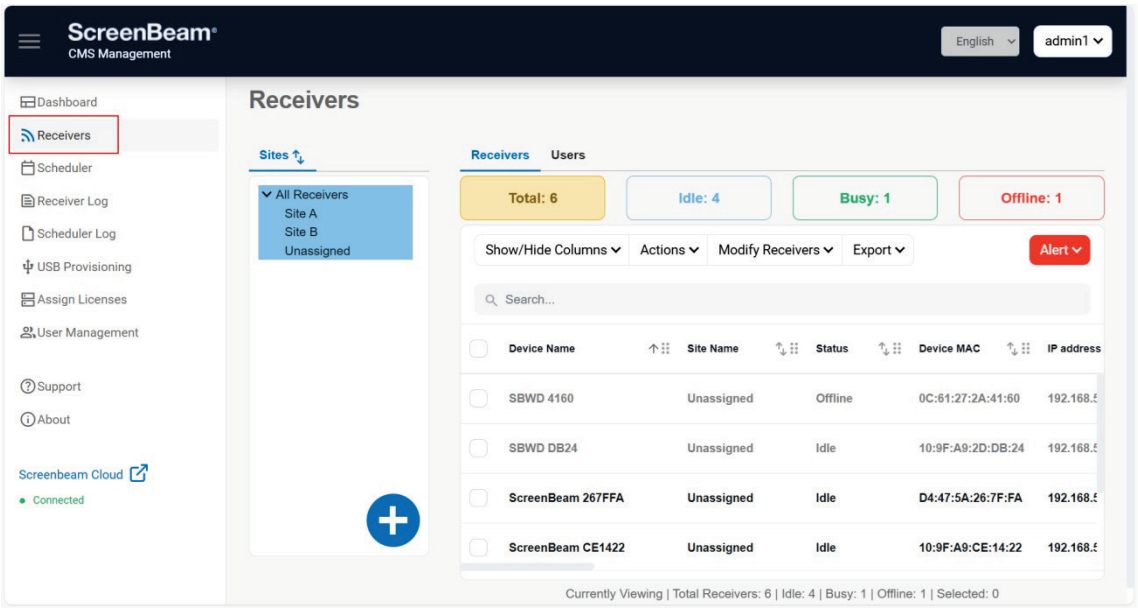
9. Click **Proceed** to confirm.

4.5.13 Switch CMS Server for Receivers

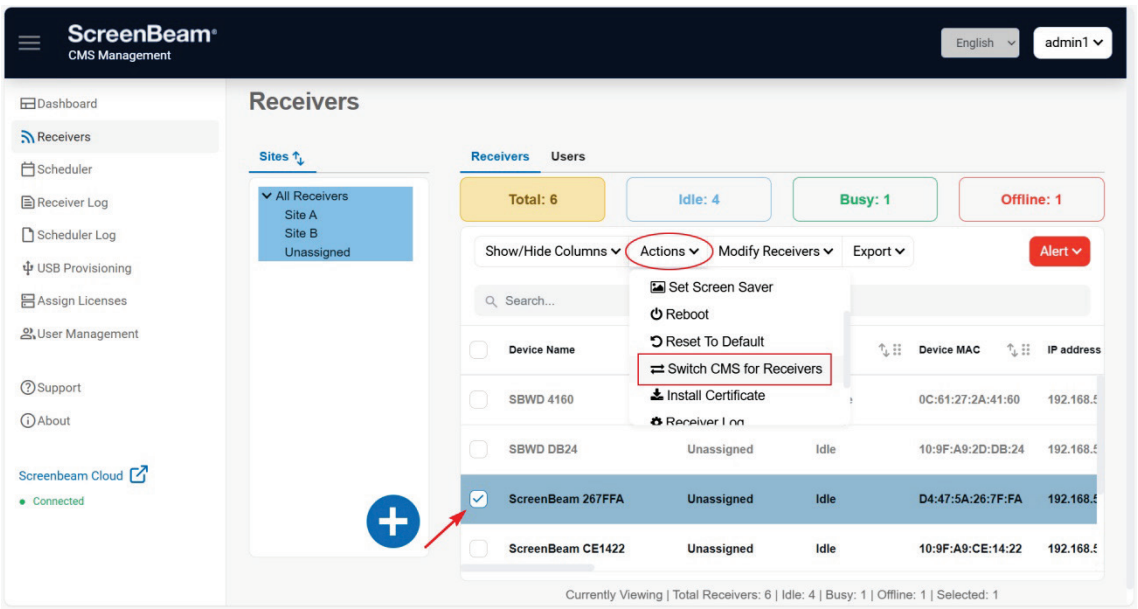
If multiple ScreenBeam Central Management System servers are deployed, some receivers on the current CMS server may be required to be switched to these additional or replacement servers. ScreenBeam CMS provides a simple server switch function, which can switch receivers to another CMS easily and quickly.

To assign one or more receivers to another server, follow this procedure:

1. Go to the **Receivers** page by clicking **Receivers** on the left pane.

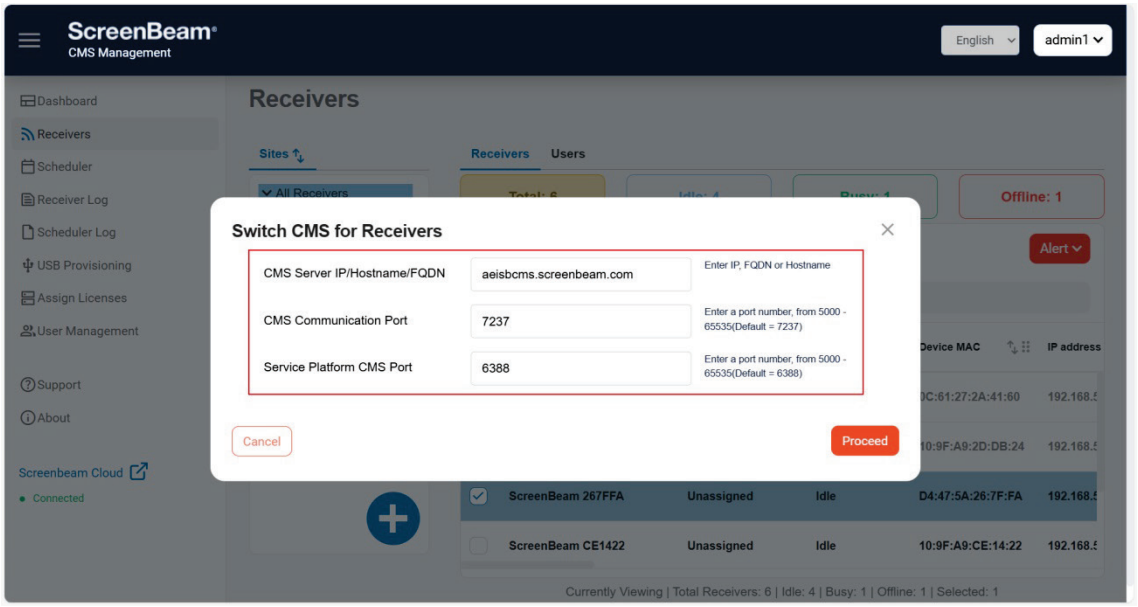


2. Select the online receivers to be switched to another CMS server on the **Receivers** page, and then select **Actions** > **Switch CMS for Receivers**.



3. The **Switch CMS for Receivers** window appears. Enter the IP address, hostname, or FQDN of the CMS server in the **CMS Server IP/Hostname/FQDN** box, and the communication port of the CMS server in the **CMS Communication Port** box and the Service Platform communication port in the **Service Platform Port** box.
   - **CMS Communication Port**: Receivers communicate with CMS via this port.
   - **Service Platform Port**: Receivers communicate with Service Platform via this port.

   Note: The Service Platform Port is used for communication between ScreenBeam receivers and ScreenBeam CMSE 4.3.10.13 or older.



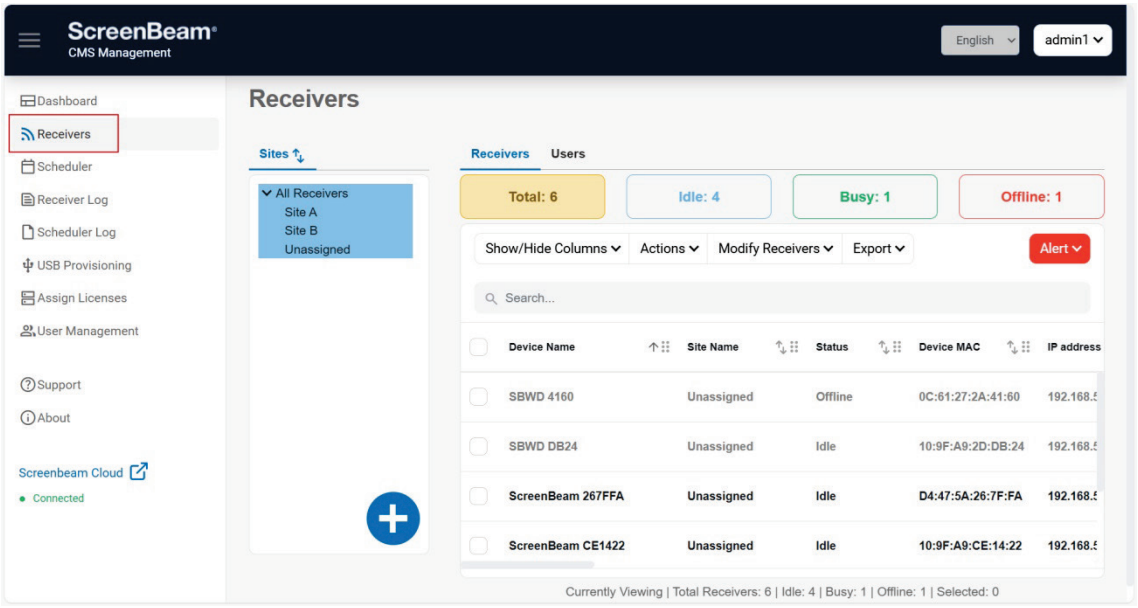
4. Click **Proceed** to confirm.

4.5.14 Update Receiver Background Image

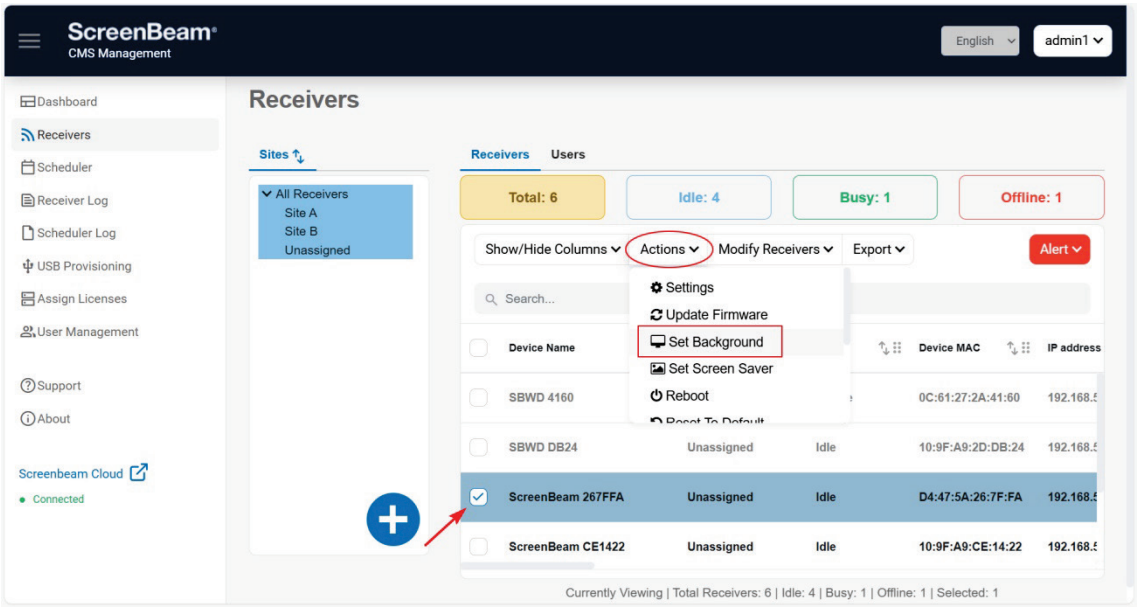
ScreenBeam receivers allow users to customize their background images on the Ready to Connect screen.

To set the background image for one or more receivers, follow this procedure:

1. Ensure the image for updating receiver's background resides on an HTTP server.
2. Go to the **Receivers** page by clicking **Receivers** on the left pane.

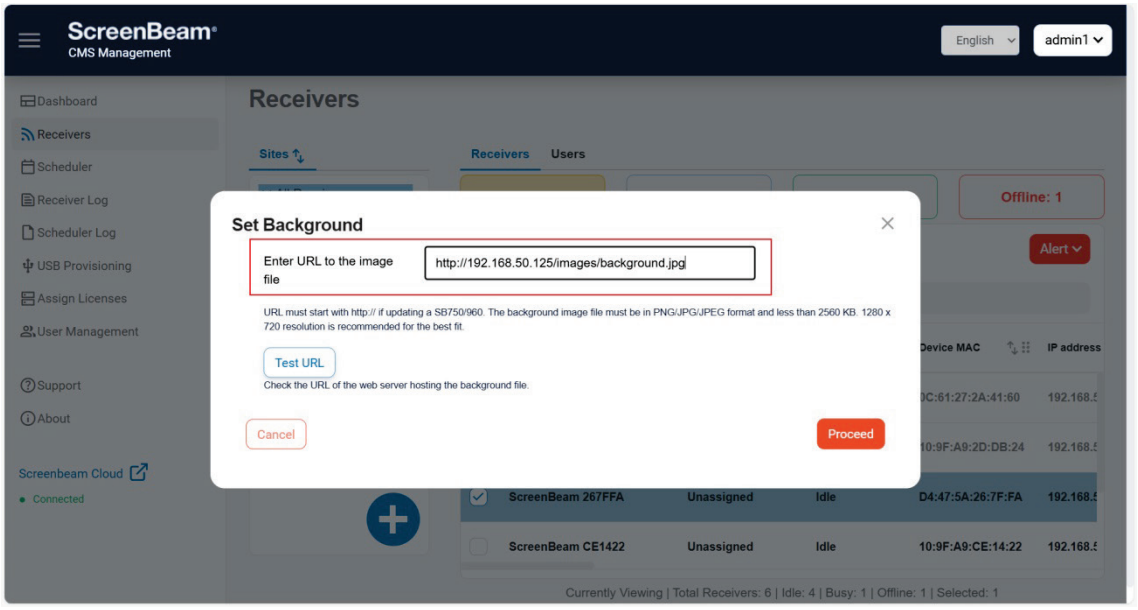


3. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Set Background**.



4. The **Set Background** window appears. Enter the image URL in the **Enter an image URL** box and click **Proceed**.
   - The image must be in .png or .jpeg/.jpg format.
   - The file size must not exceed 2.5 MB.
   - The recommended image size is 1920*1080 pixels (width x height).

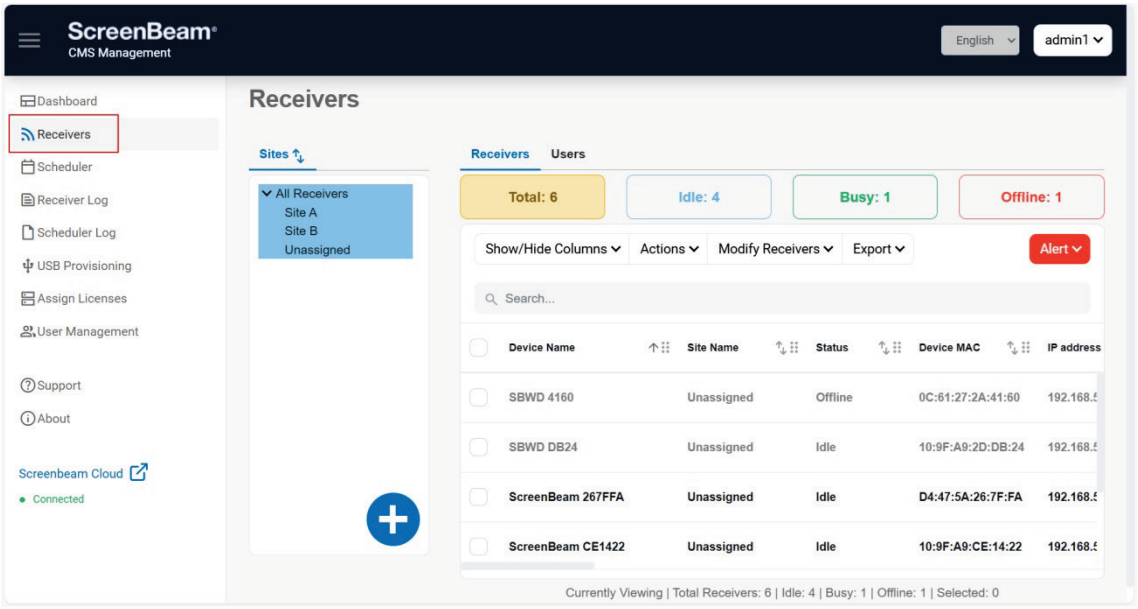
   Note: Click the **Test URL** button to check the validity of the URL if desired.



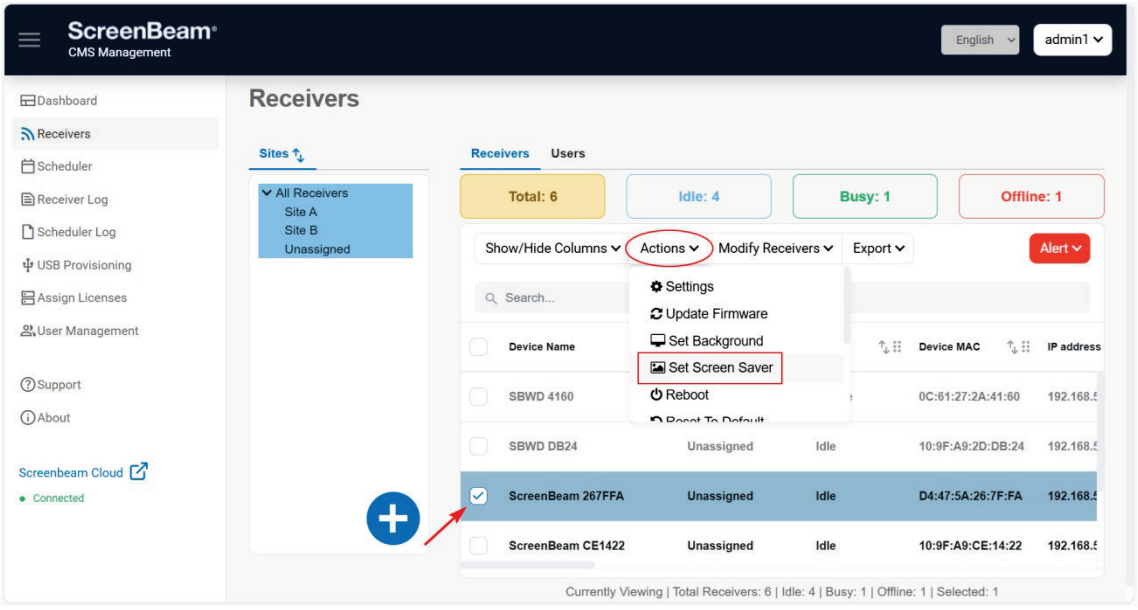
4.5.15 Update Receiver Screensaver Image

ScreenBeam receivers allow users to customize their screensaver images.
To set the screensaver image for one or more receivers, follow this procedure:

1. Ensure the image for updating receiver's screensaver resides on an HTTP server.
2. Go to the **Receivers** page by clicking **Receivers** on the left pane.

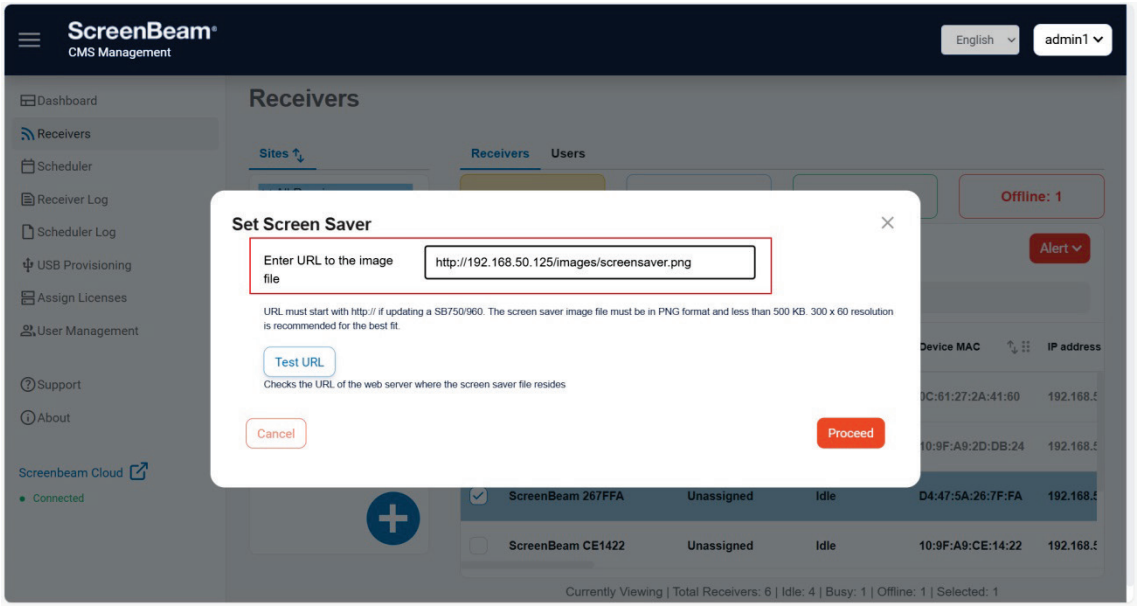


3. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Set Screen Saver**.



4. The **Set Screen Saver** window appears. Enter the image URL in the **Enter an image URL** box and click **Proceed**.
   - The image must be in .png format.
   - The file size must not exceed 200 KB.
   - The best image size is 300*60 pixels.

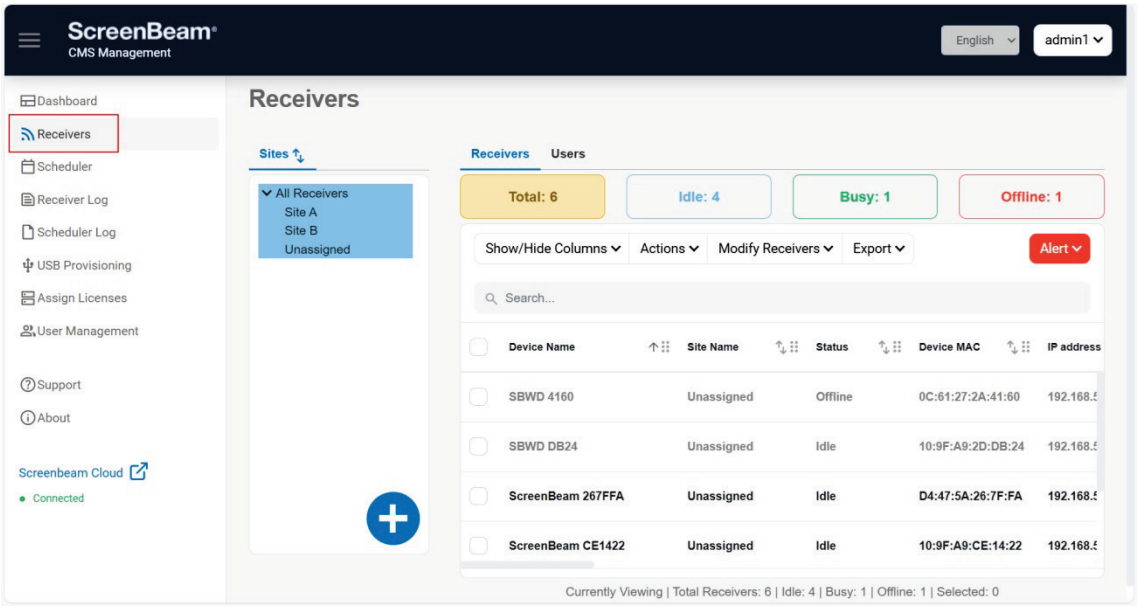
   Note: Click the **Test URL** button to check the validity of the URL if desired.



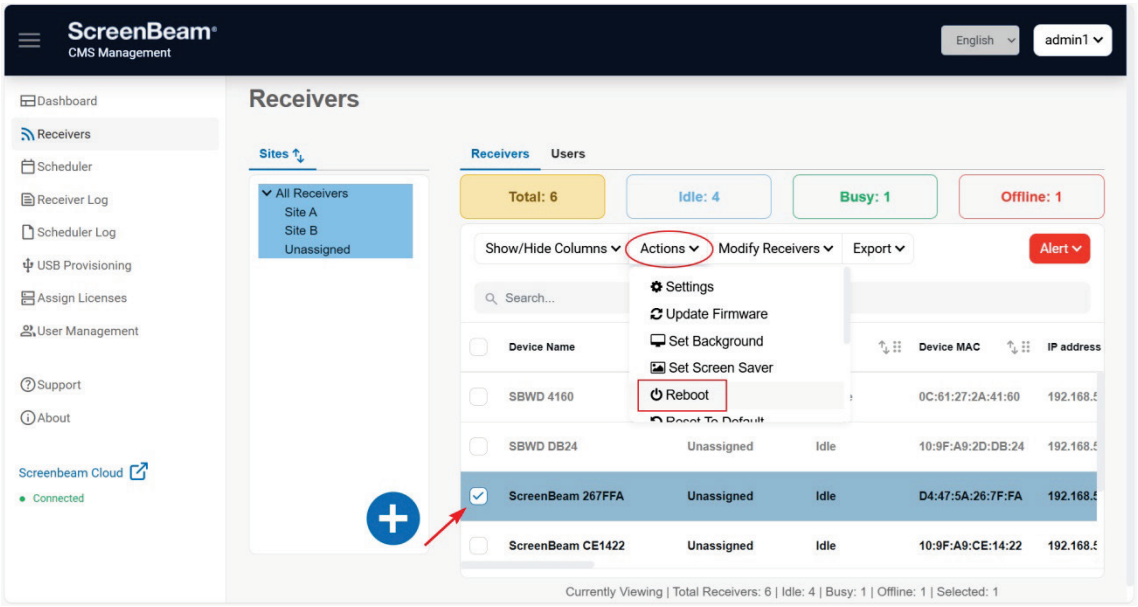
4.5.16 Reboot Receivers

ScreenBeam CMS allows users to reboot ScreenBeam receivers remotely.
To reboot one or more ScreenBeam receivers remotely, follow this procedure:

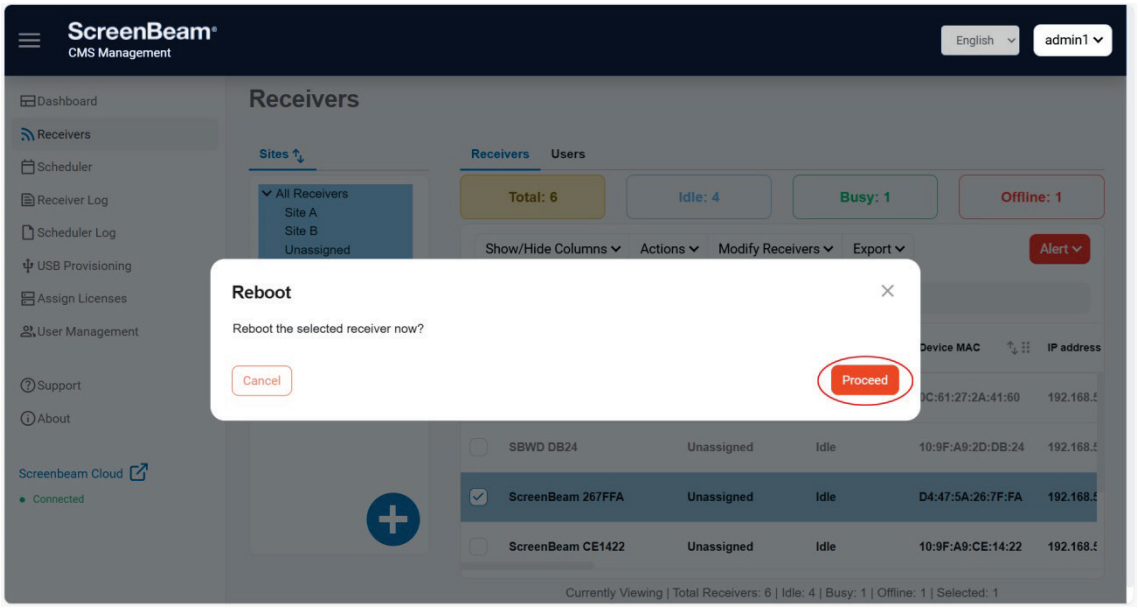
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Reboot**.



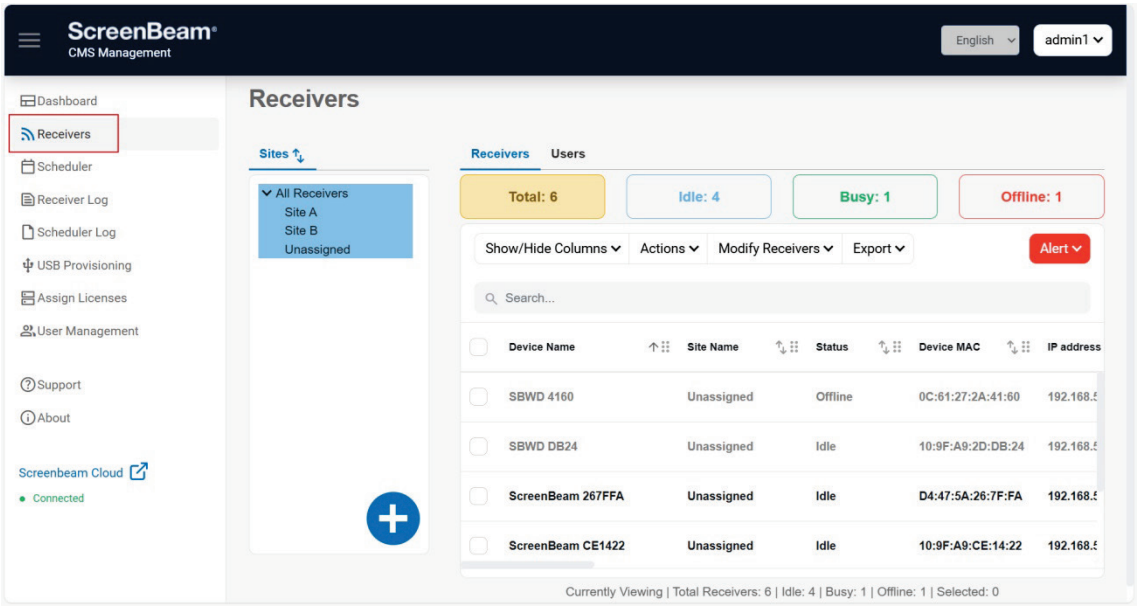
3. The **Reboot** message box appears. Click **Proceed**.



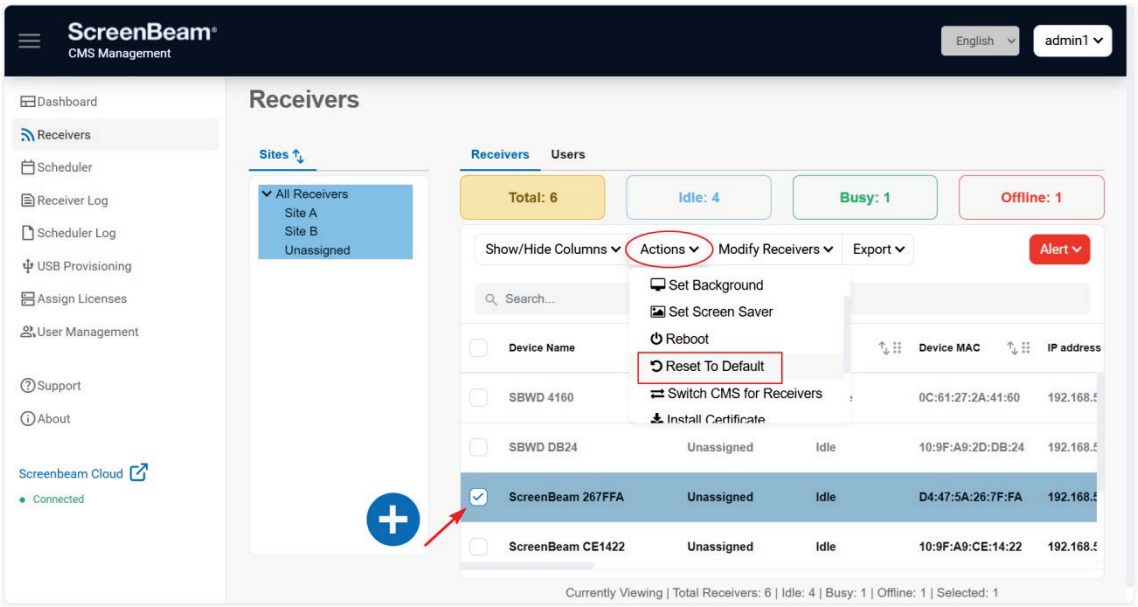
4.5.17 Reset Receivers

ScreenBeam CMS allows users to reset ScreenBeam receivers remotely.
To reset one or more ScreenBeam receivers remotely, follow this procedure:

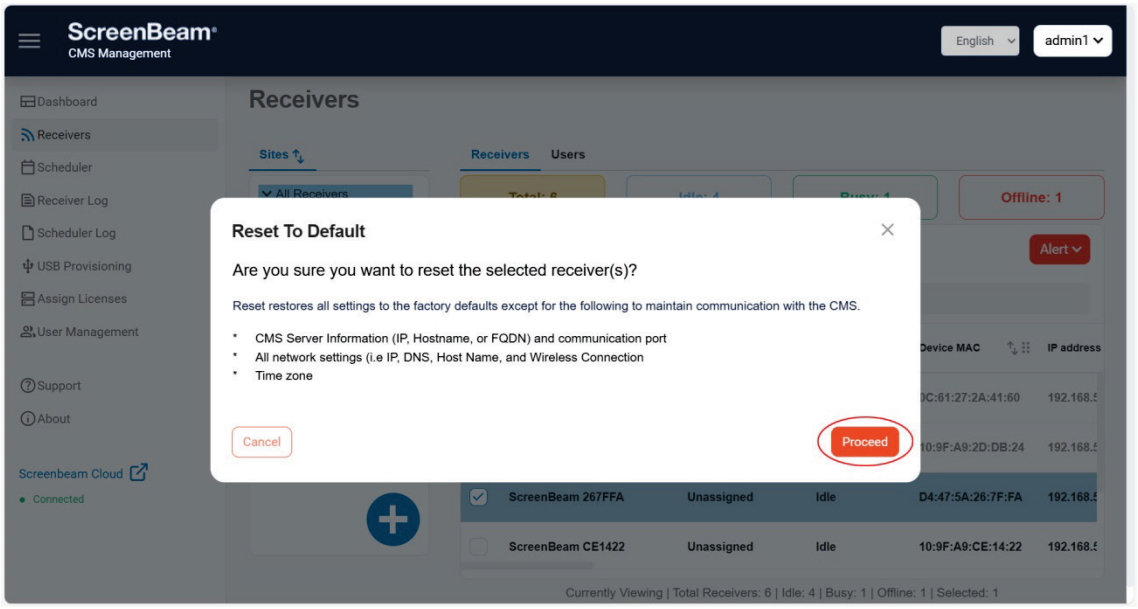
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Reset To Default**.



3. The **Reset To Default** message box appears. Click **Proceed**.



Note: To maintain communications with CMS, the following settings will not be reset to default:

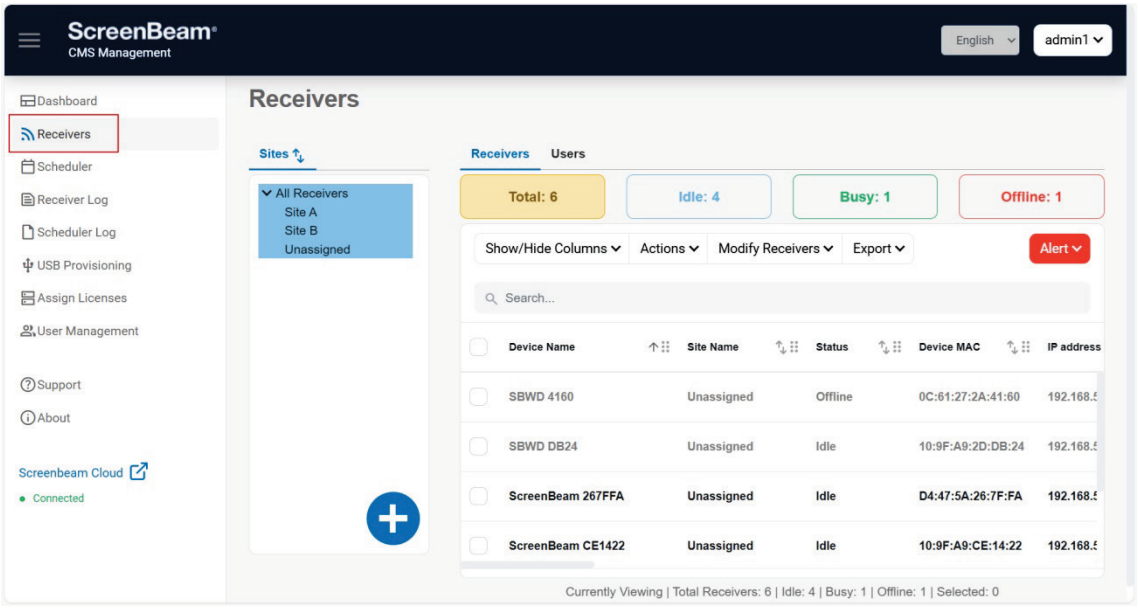
- CMS Server Information (IP, Hostname, or FQDN) and communication ports
- All network settings (i.e. IP, DNS, Host Name, Wireless Connection settings, and Ethernet connection settings)
- Time zone

4.5.18 Delete Offline Receivers

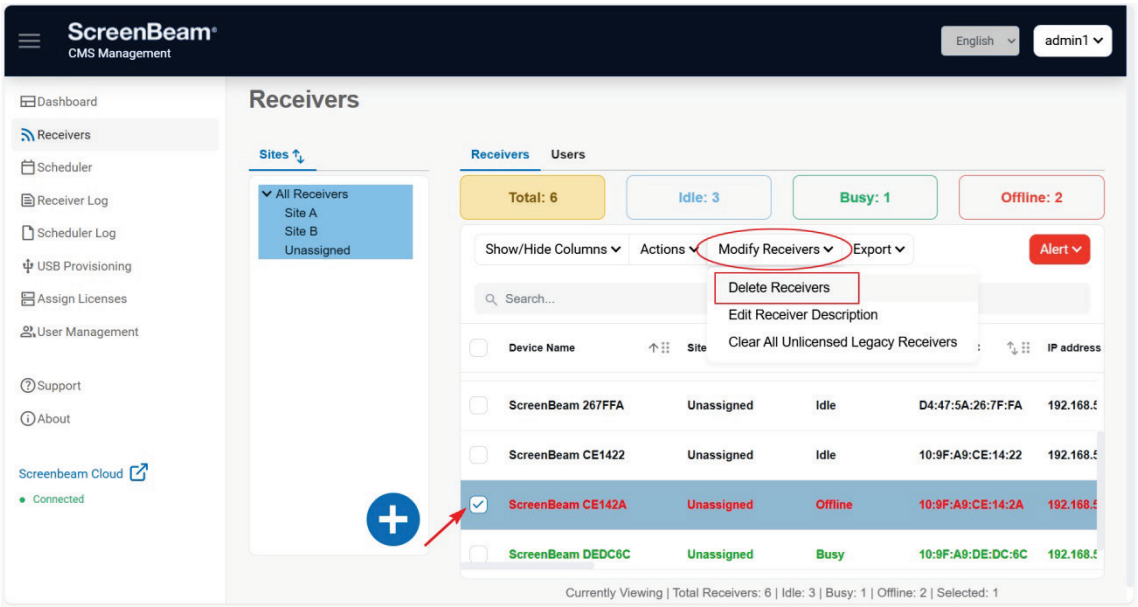
Disconnecting a ScreenBeam receiver from your network will cause it to appear as “offline” on CMS. In the case where such a receiver will no longer be used you can remove it from the Receiver list.

To delete one or more offline receivers, follow this procedure:

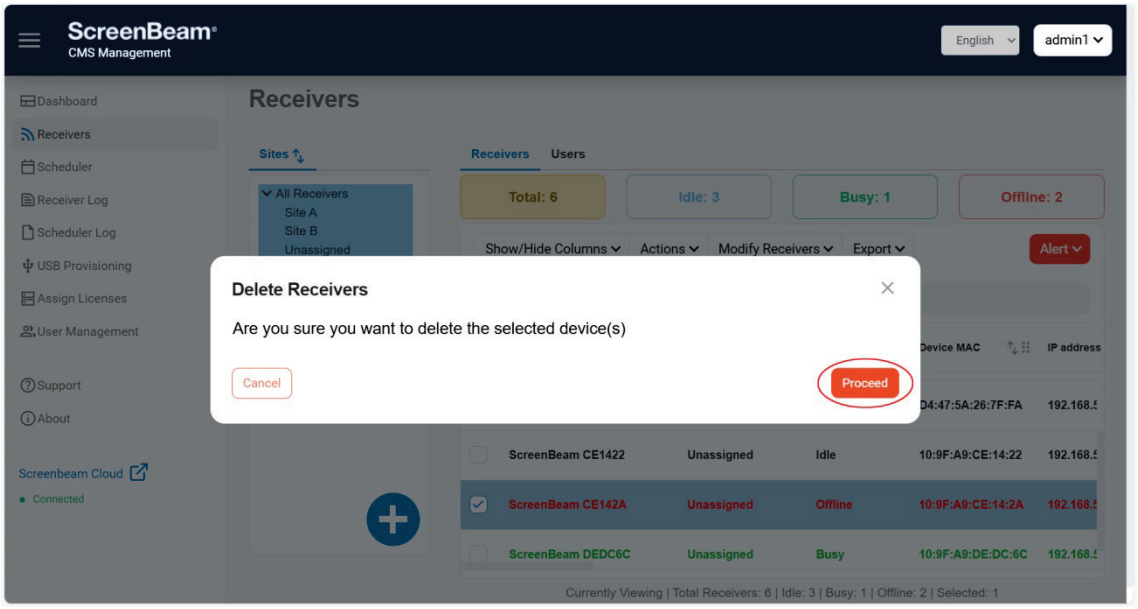
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Select one or more offline receivers on the **Receivers** page, and then select **Modify Receivers** > **Delete Receiver**.



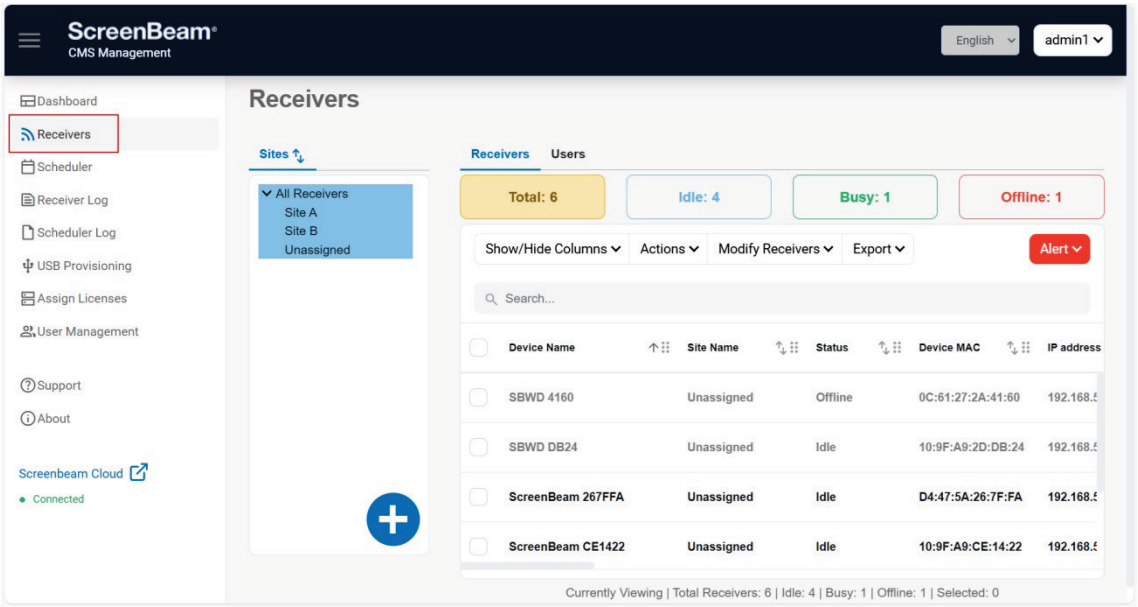
3. The **Delete Receivers** message box appears. Click **Proceed**.



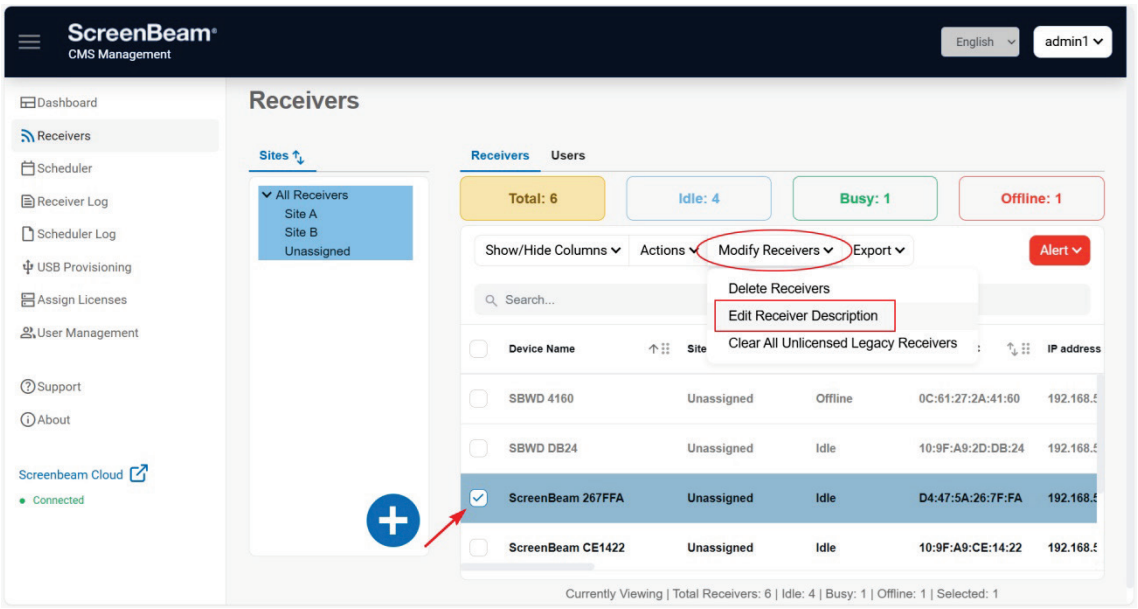
4.5.19 Edit Receiver Descriptions

To edit descriptions for one or more receivers, follow this procedure:

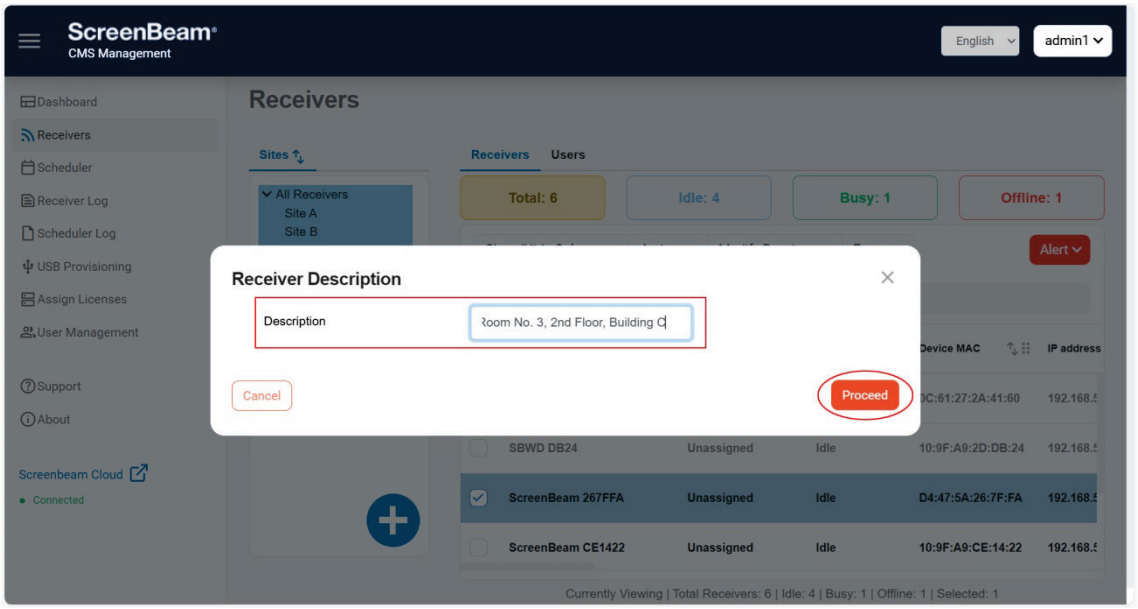
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



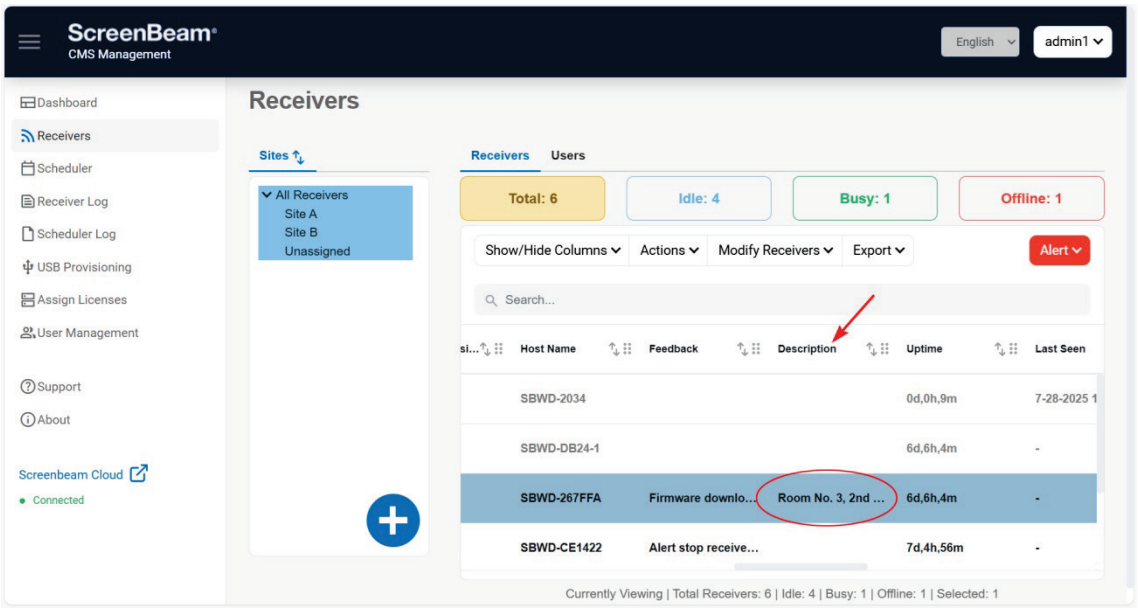
2. Select one or more receivers on the **Receivers** page, and then select **Modify Receivers** > **Edit Receiver Description**.



3. The **Receiver Description** window appears. Type your receiver descriptions in the **Description** box and click **Proceed**.
   Note: New descriptions will overwrite old ones.



4. The receiver descriptions are displayed in the **Description** column.

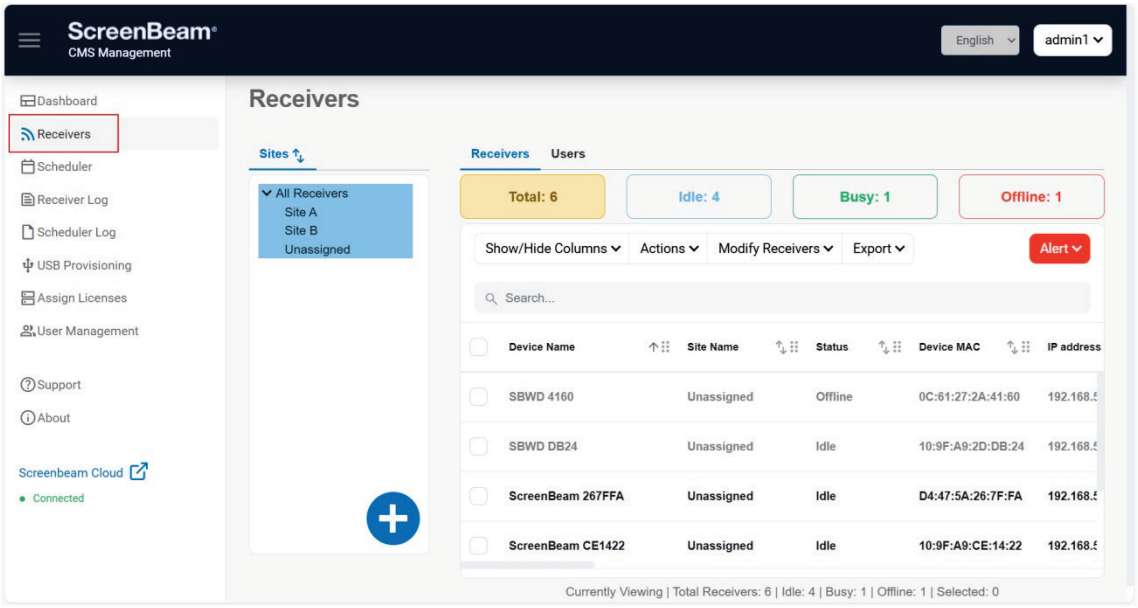


Note: Select **Show/Hide Columns** > **Description** to show the **Description** column if you can't find it, as the **Description** column is hidden by default.

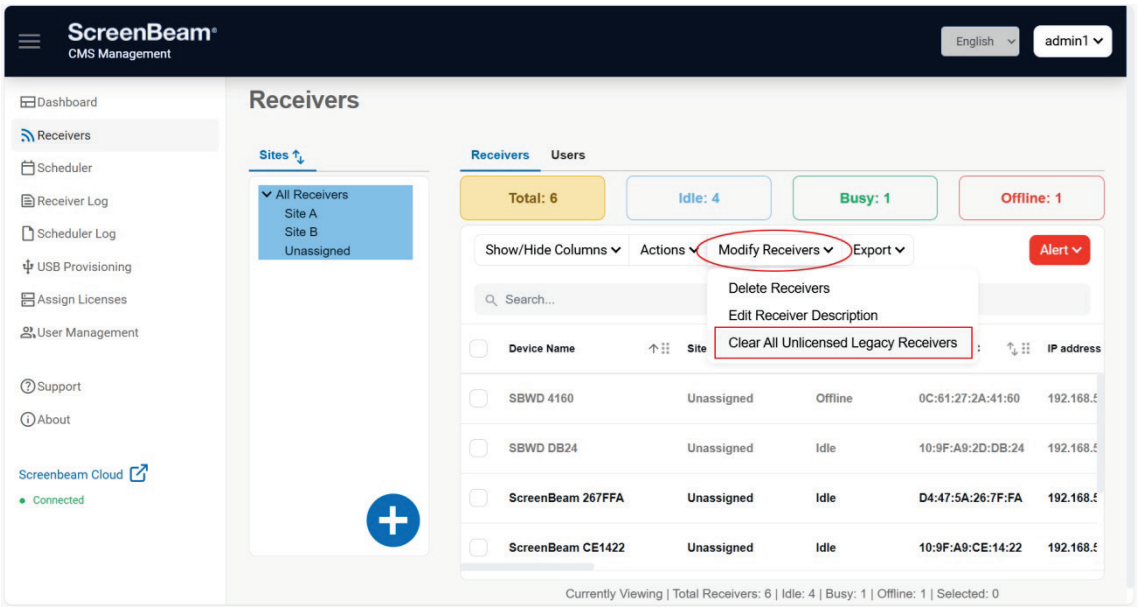
4.5.20 Clear All Unlicensed Legacy Receivers

The legacy receivers, such as ScreenBeam 960 and ScreenBeam 750, are not supported by ScreenBeam CMS V4 natively. They can't be managed if they are not licensed. As a result, you may want to switch them to a manageable platform, such ScreenBeam CMS V2. To switch the unlicensed legacy receivers to another CMS, follow this procedure:

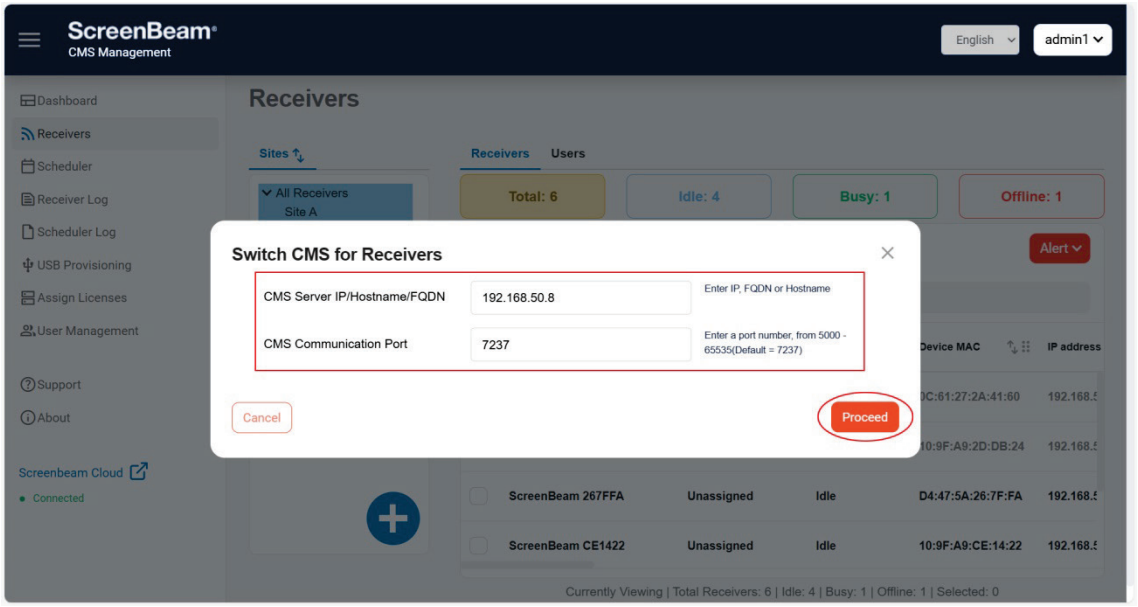
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



2. Select **Modify Receivers** > **Clear All Unlicensed Legacy Receivers**.



3. The **Switch CMS for Receivers** window appears. Type the IP address, hostname, or FQDN of the CMS server in the **CMS Server IP/Hostname/FQDN** box, and the communication port of the CMS server in the **CMS Communication Port** box. Click **Proceed**.

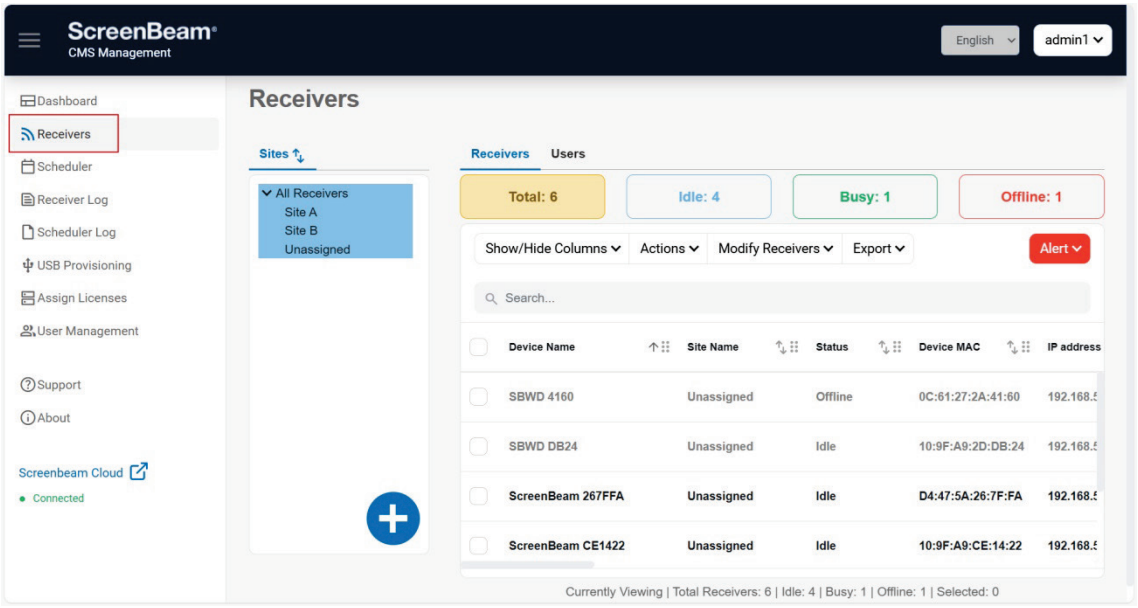


4.5.21 Clear Feedback

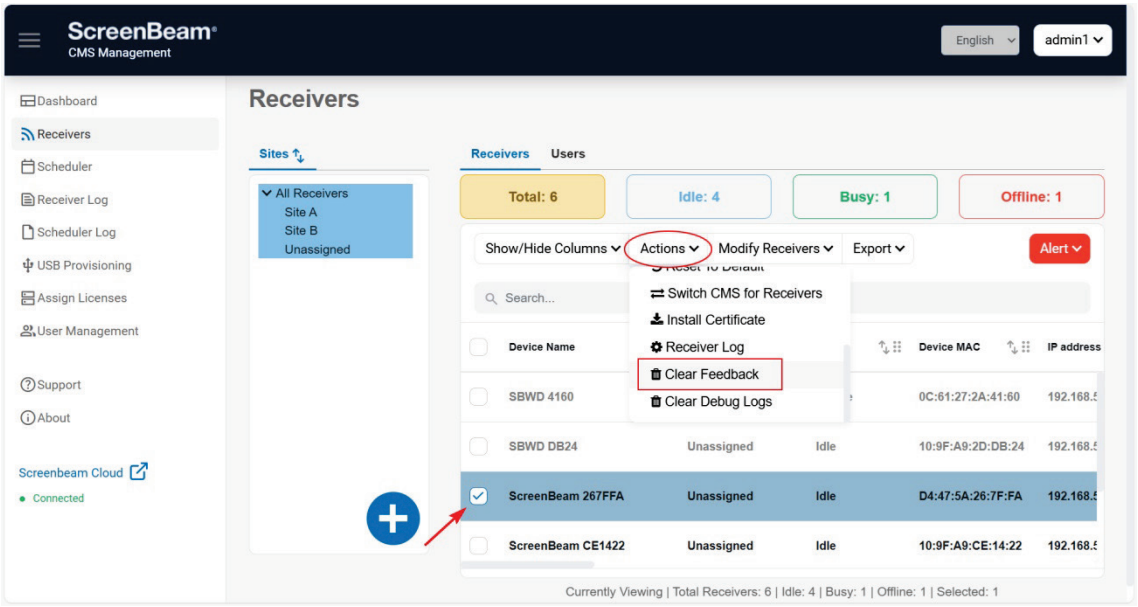
ScreenBeam CMS provides feedback for all operations so that users know the results of the operations they execute. CMS allows users to clear the feedback.

To clear feedback for one or more receivers, follow this procedure:

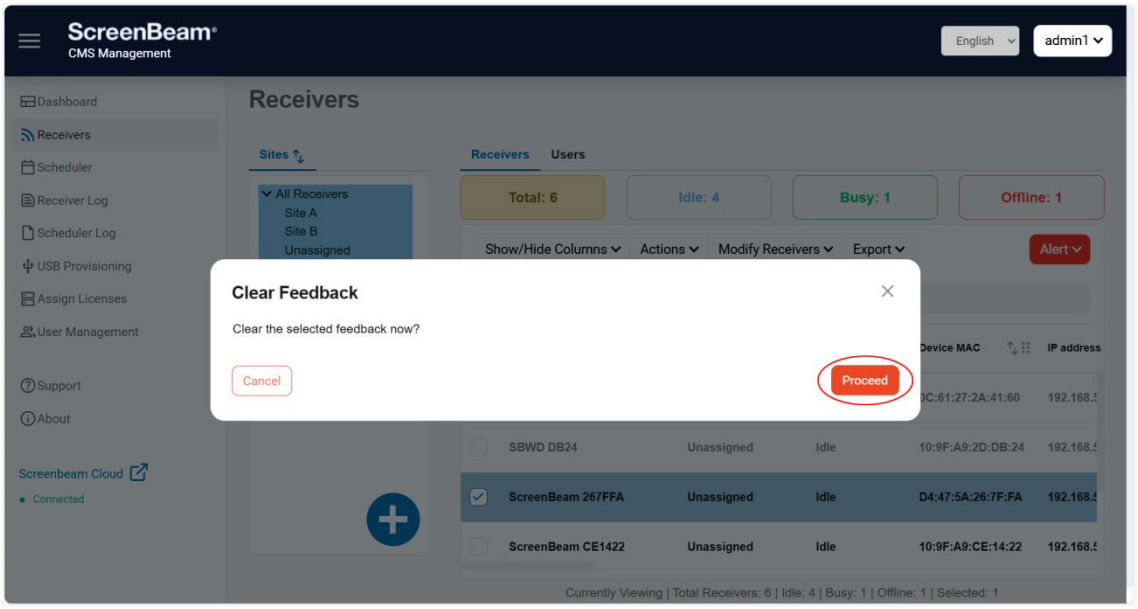
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



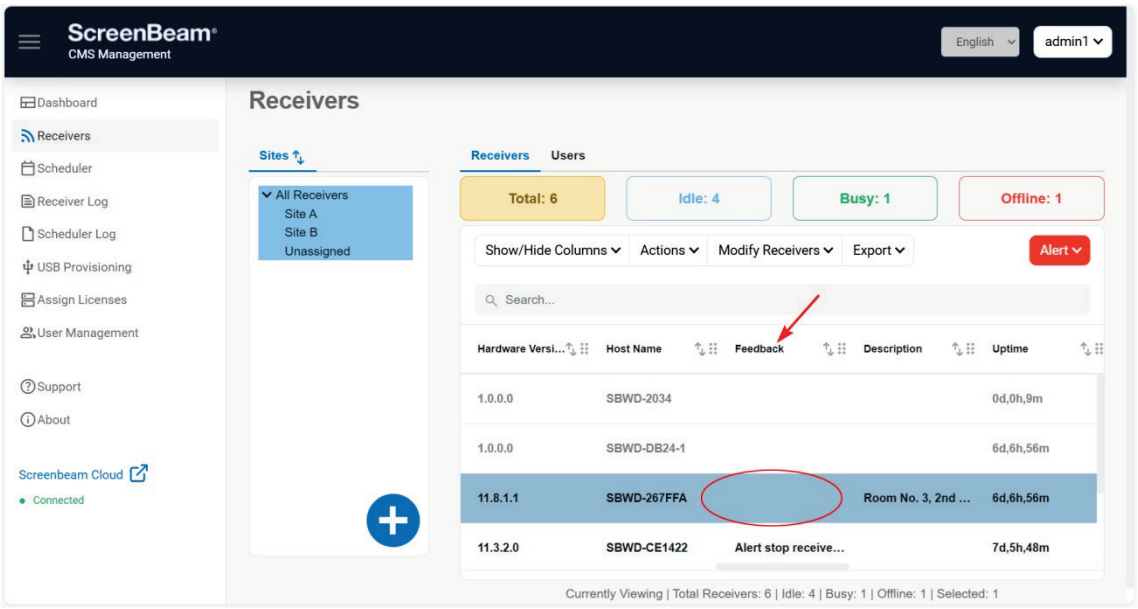
2. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Clear Feedback**.



3. The **Clear Feedback** window appears. Click **Proceed**.



4. The feedback for the selected receivers will be cleared.

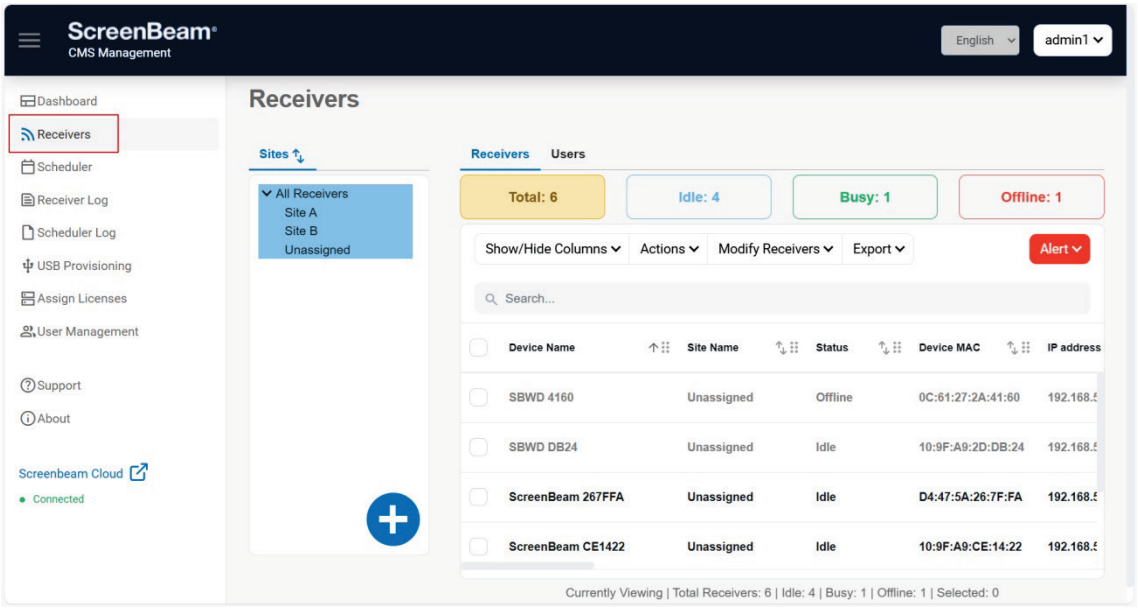


4.5.22 Clear Debug Logs

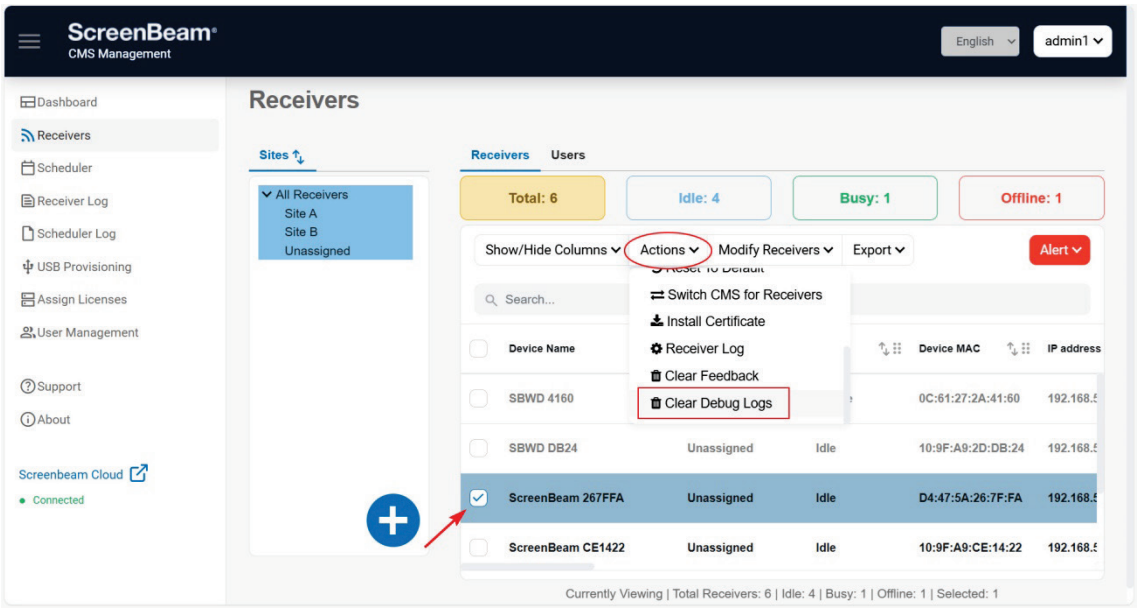
ScreenBeam receivers can save TTY logs in their memories for debugging purpose if the Store Log to System feature (under Advanced Settings) is enabled.
ScreenBeam CMS allows users to clear these debug logs.

To clear debug logs for one or more receivers, follow this procedure:

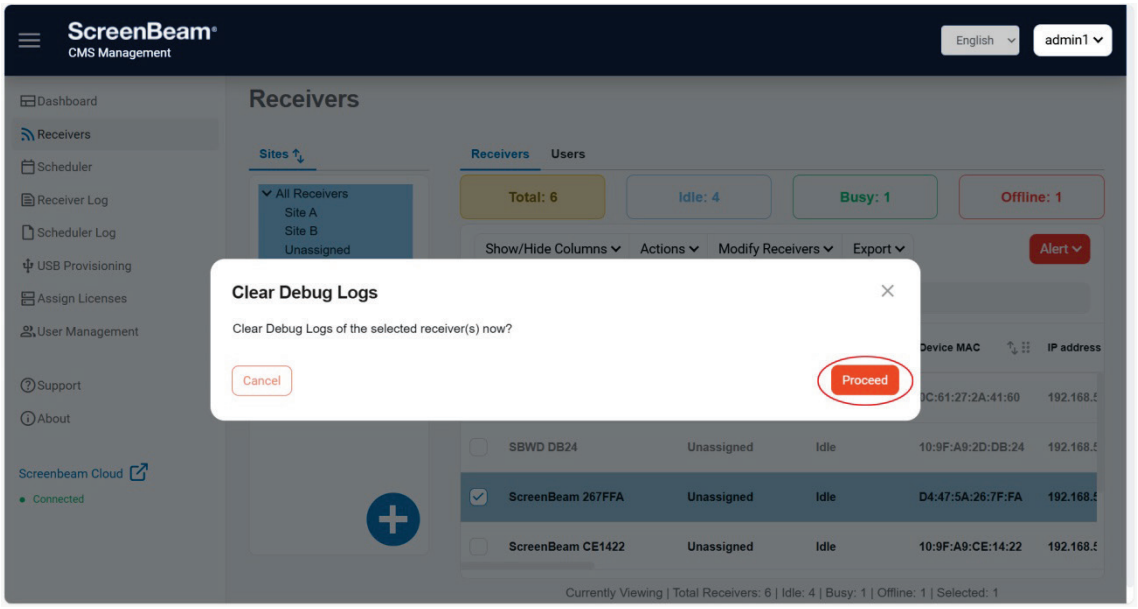
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



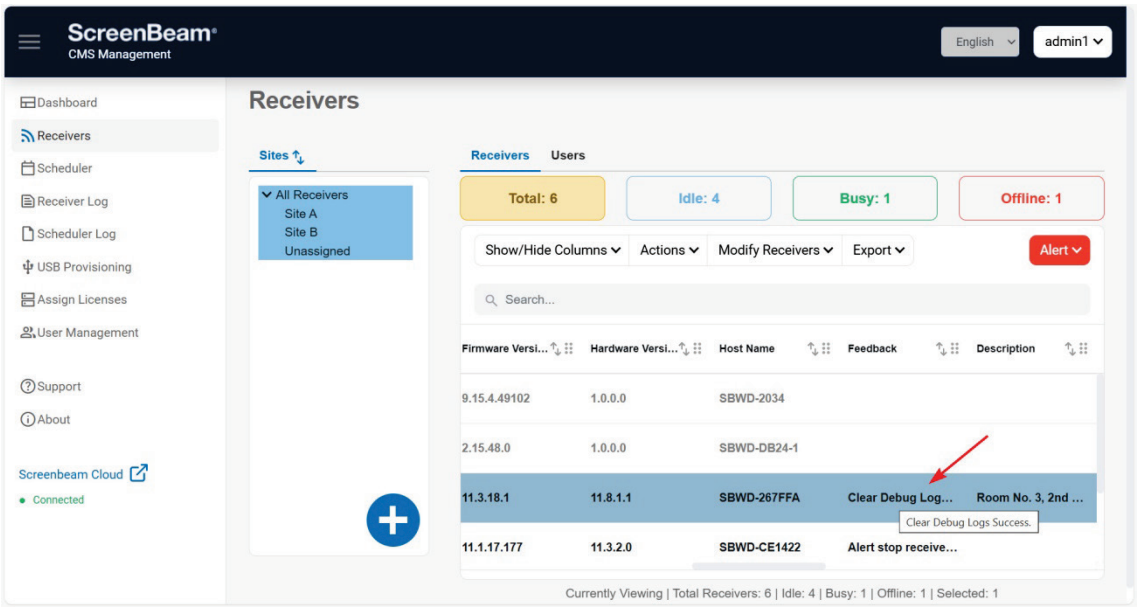
2. Select one or more receivers on the **Receivers** page, and then select **Actions** > **Clear Debug Logs**.



3. The **Clear Debug Logs** window appears. Click **Proceed**.



4. Debug logs on the selected receivers will be cleared.

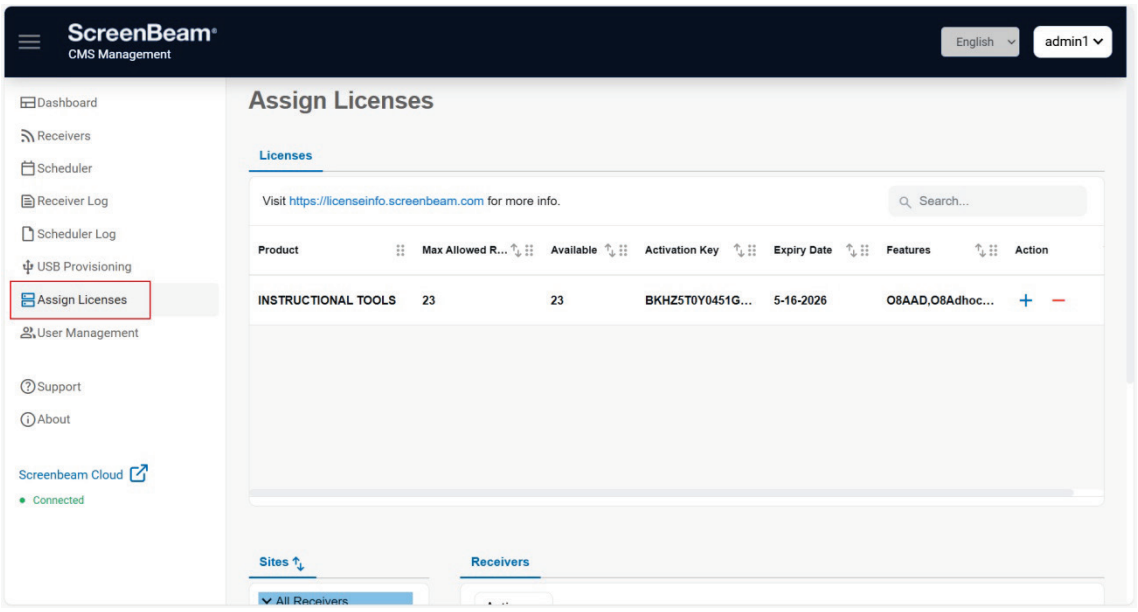


4.5.23 Assign Licenses to Receivers

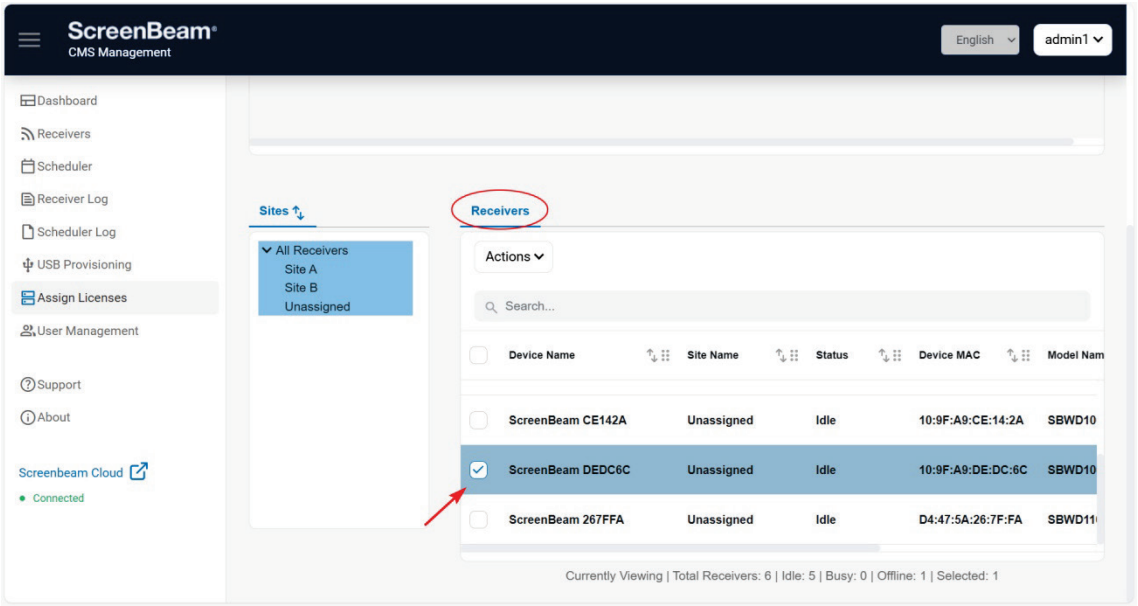
The license for managing legacy ScreenBeam 960/750 receivers will be assigned to the receivers automatically when the receivers connect to the ScreenBeam CMS. For other licenses, you need to assign them to the receivers manually.

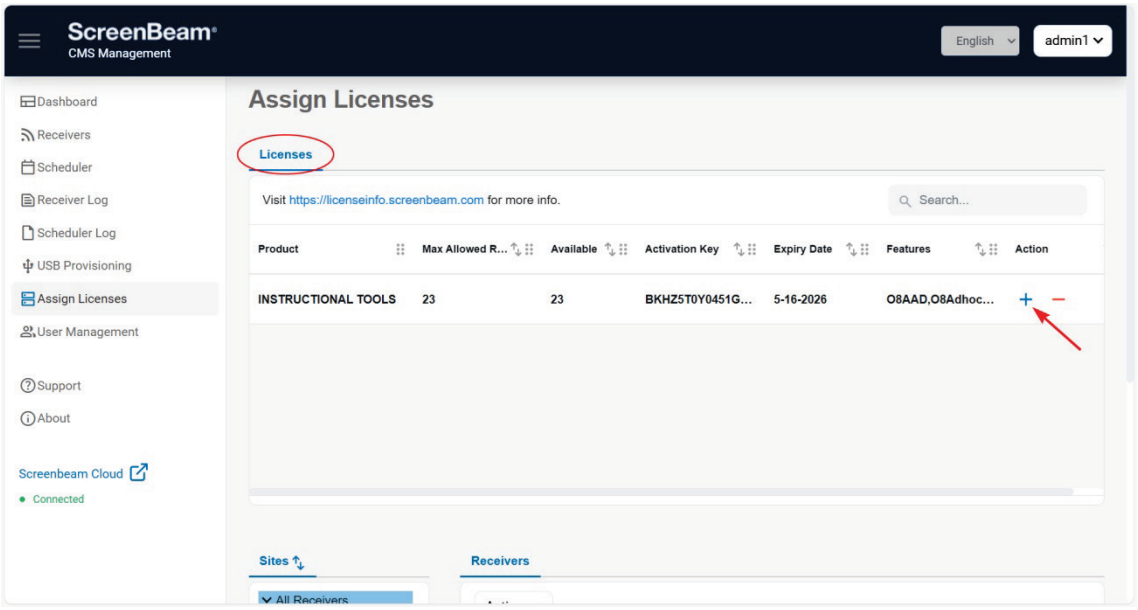
To assign a license to one or more receivers, follow this procedure:

1. Ensure that the license is activated on ScreenBeam Cloud and the CMS is connected to ScreenBeam Cloud.
2. Go to the **Assign Licenses** page by clicking **Assign Licenses** on the left pane.

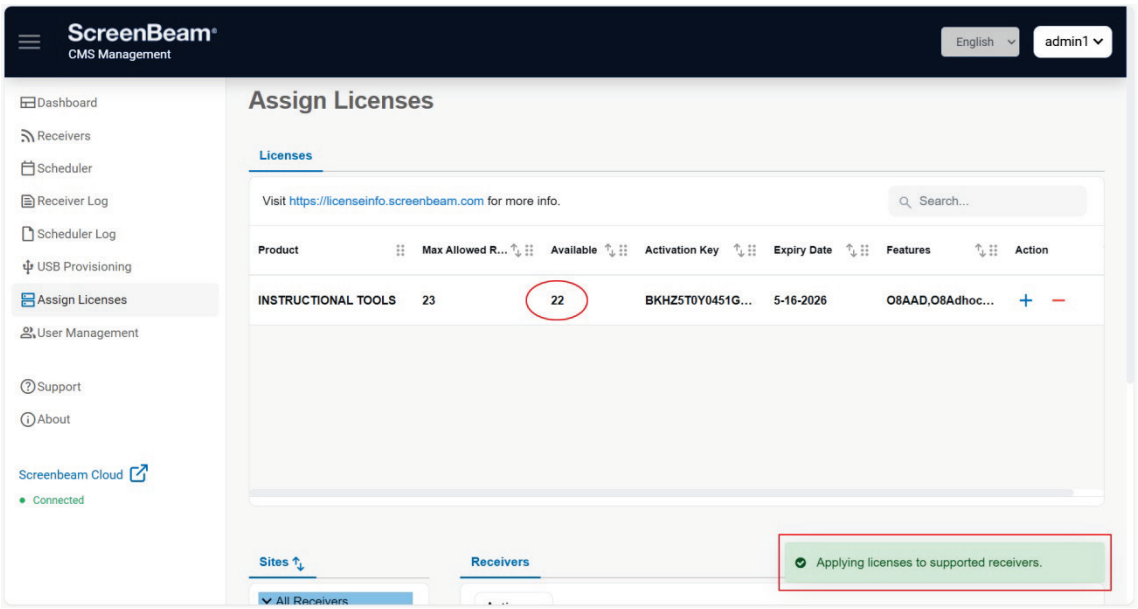


3. Select one or more receivers in the **Receivers** pane and then go to the **Licenses** pane and click the “+” sign in the **Action** column of the desired license.



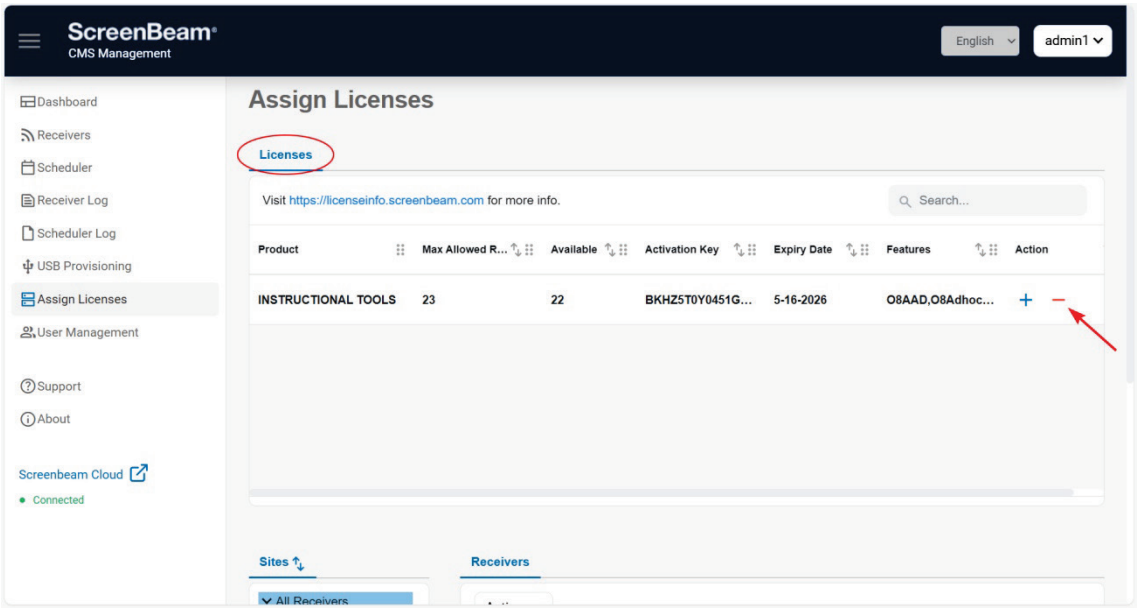


4. The license will be assigned to the selected receiver(s), and the number of available license seats will be deducted by the number of selected receivers.

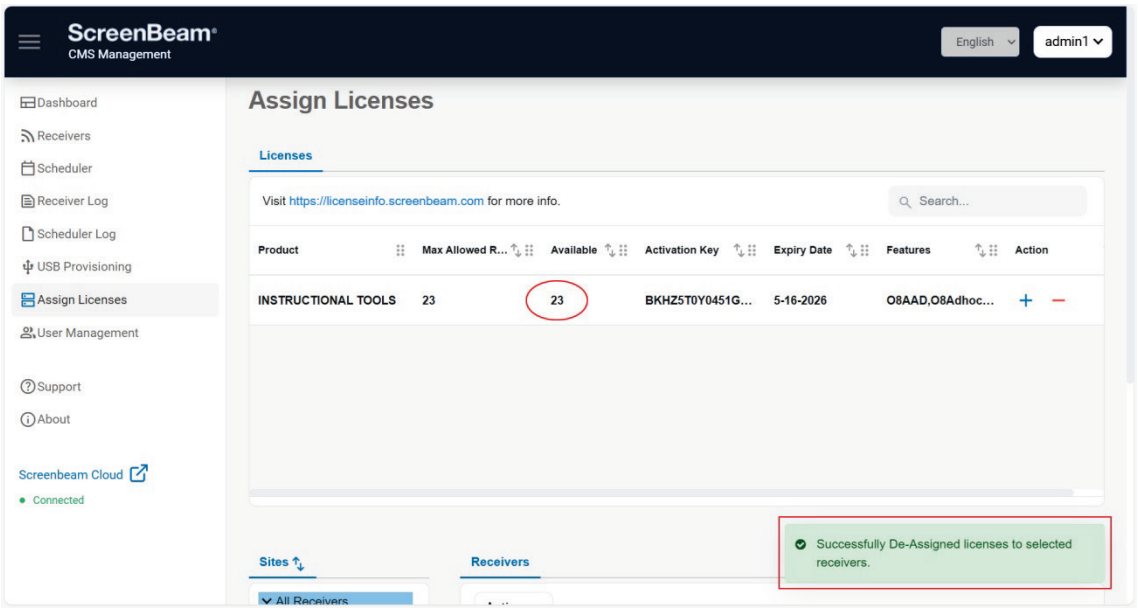


To de-assign license from one or more receivers, follow this procedure:

1. Select one or more receivers in the **Receivers** pane and then go to the **Licenses** pane and click the "-" sign in the **Action** column of the desired license.



2. The license will be de-assigned from the selected receiver(s). And the number of available license seats will be added by the number of selected receivers.

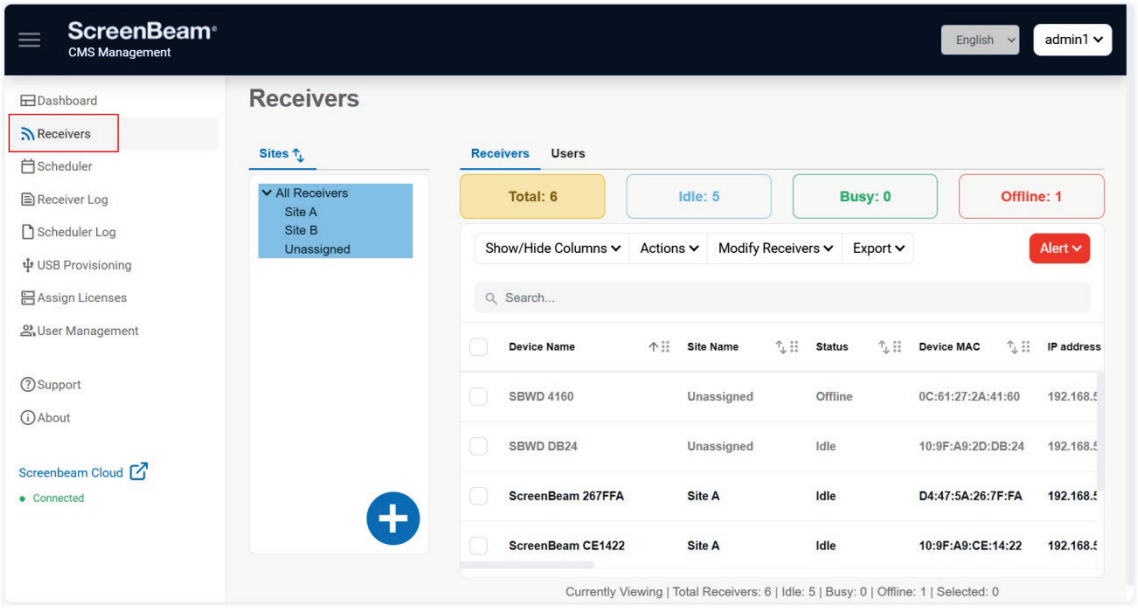


4.5.24 Push an Alert to Receivers

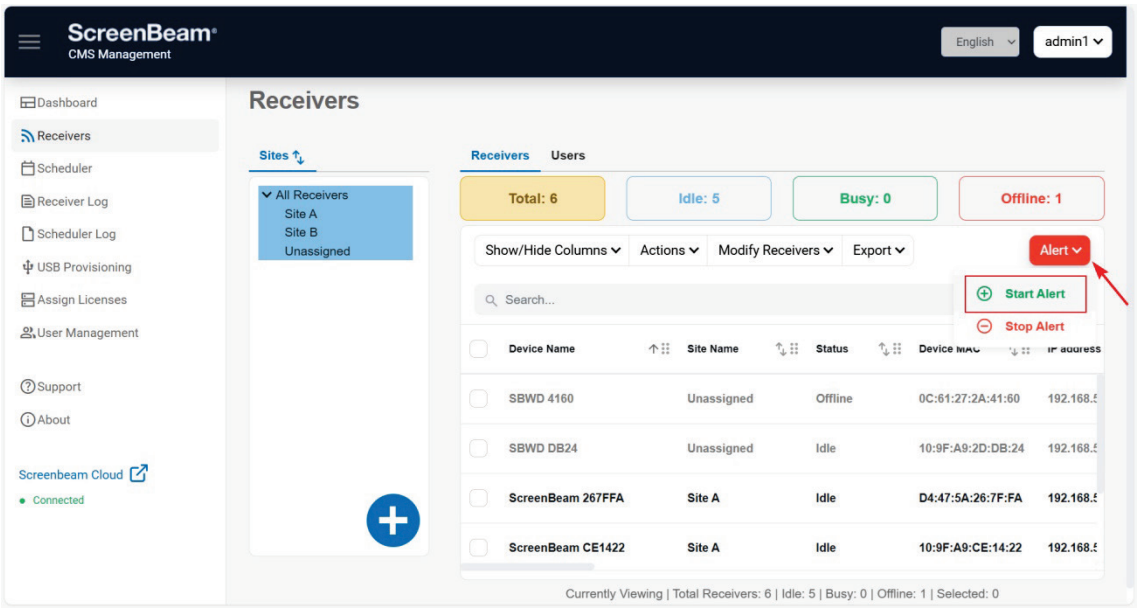
ScreenBeam CMS can push an alert message to ScreenBeam receivers and display it on the connected display device.

To push an alert message to ScreenBeam receivers, follow this procedure:

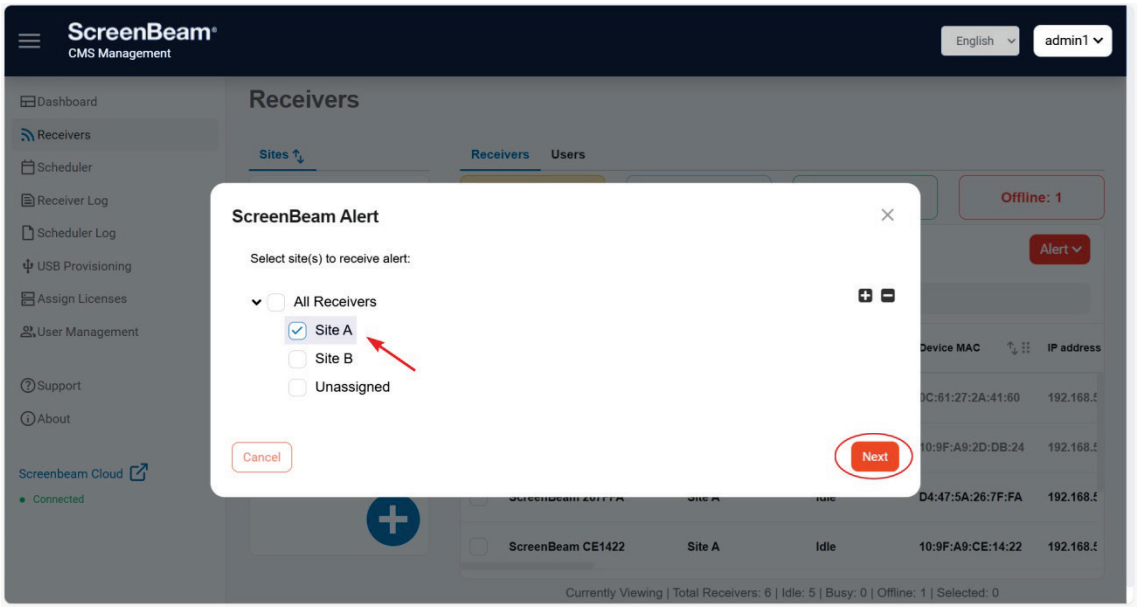
1. Go to the **Receivers** page by clicking **Receivers** on the left pane.



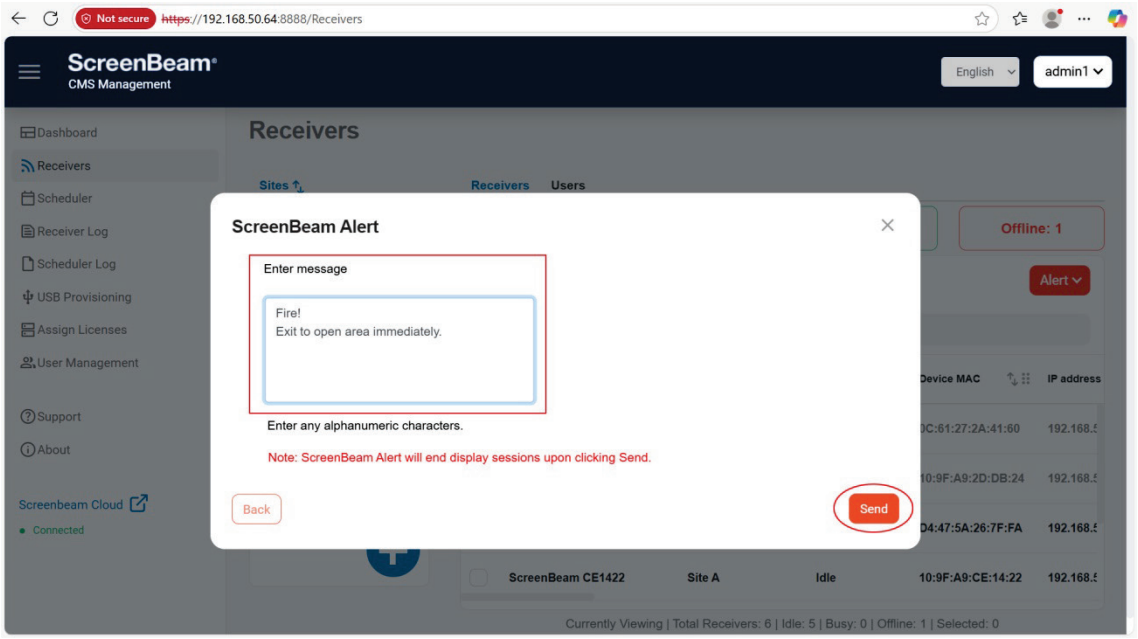
2. Select **Alert** -> **Start Alert** to open the **ScreenBeam Alert** dialog box.



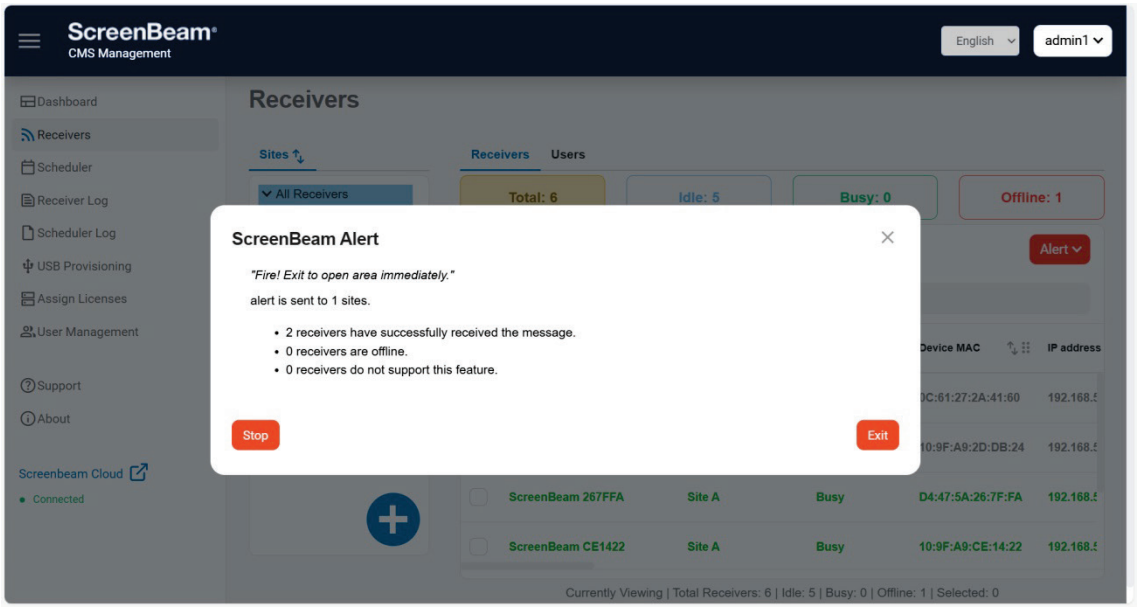
3. On the **ScreenBeam Alert** dialog box, select the site(s) where the receivers you want to push the alert. And click **Next**.



4. Type your alert message in the **Enter message** box. Click **Send**.
   Note: Pushing an alert to ScreenBeam receivers will interrupt all current display sessions.

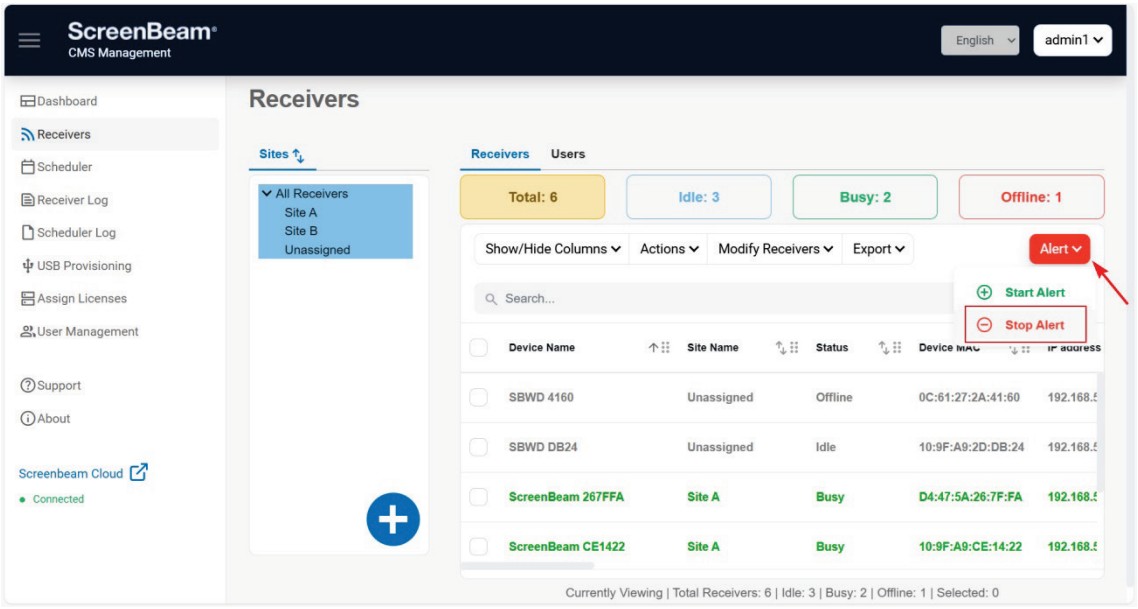


5. The alert message will be pushed to the receivers in the selected site(s). It is shown on the displays that are connected to the receivers.

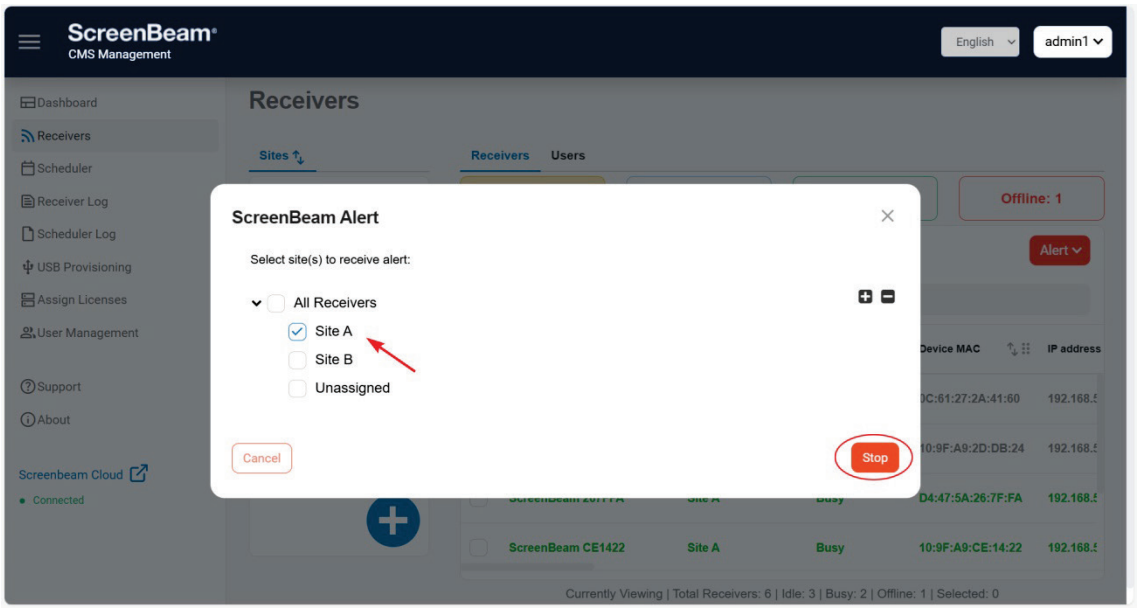


To stop an alert, follow this procedure:

1. Go to the **Receivers** page by clicking **Receivers** on the left pane.
2. Select **Alert** -> **Stop Alert** to open the **ScreenBeam Alert** dialog box.



3. On the **ScreenBeam Alert** dialog box, select the site(s) where the alert you want to stop, and click **Stop**.



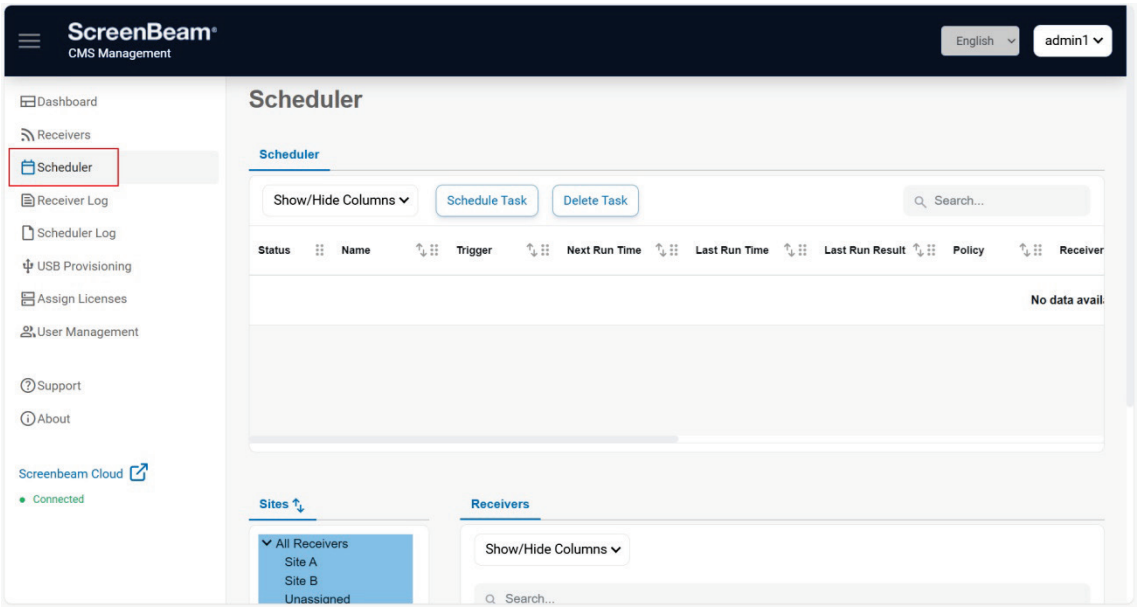
4.6 Managing Scheduled Tasks

The scheduler helps administrators automate receiver management, allowing activities such as staggering large firmware updates during off-work hours.

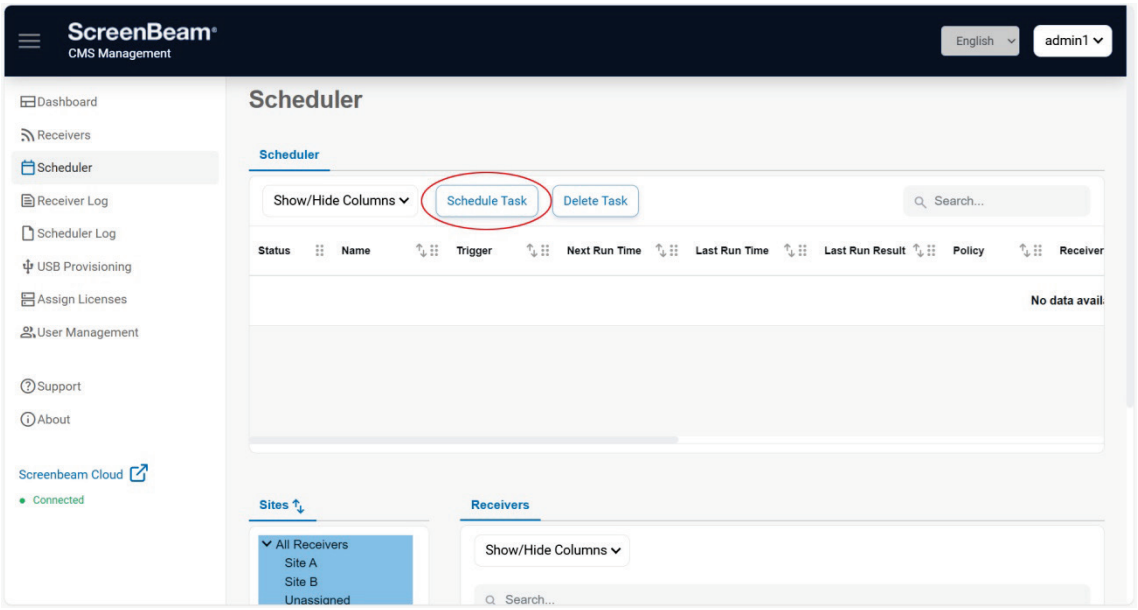
4.6.1 Schedule a Task

To schedule a task, follow this procedure:

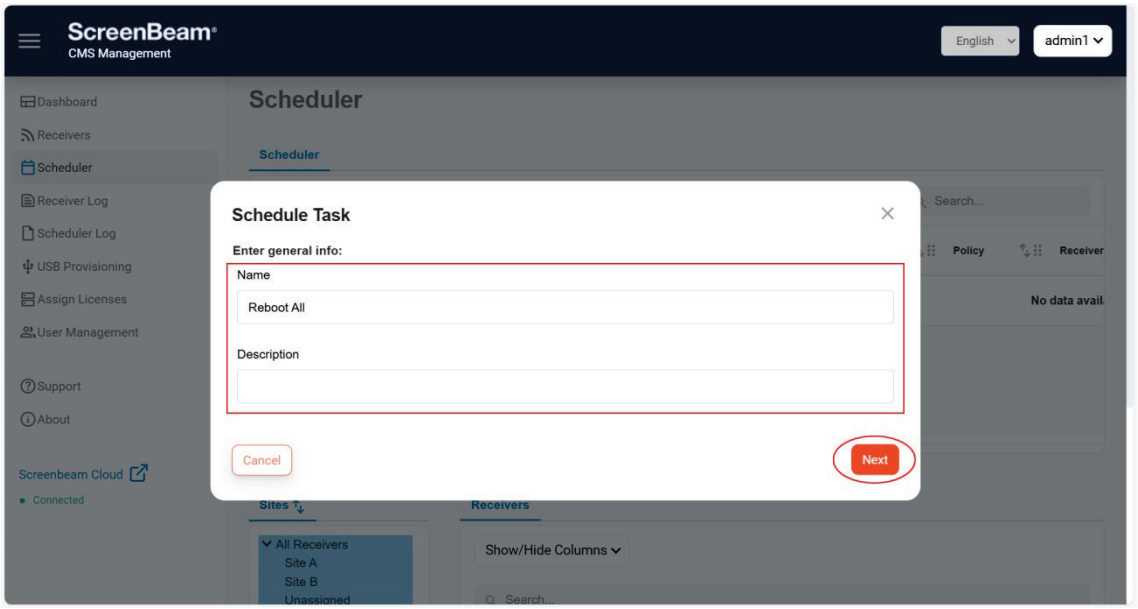
1. Go to the **Scheduler** page by clicking **Scheduler** on the left pane.



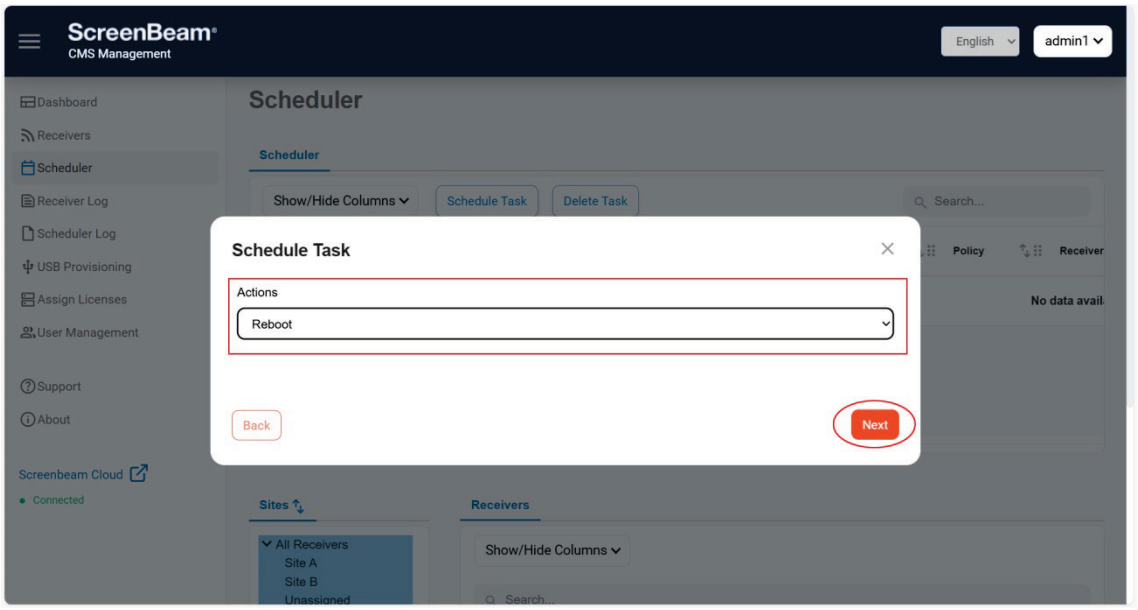
2. Click the **Schedule Task** button on the **Scheduler** pane.



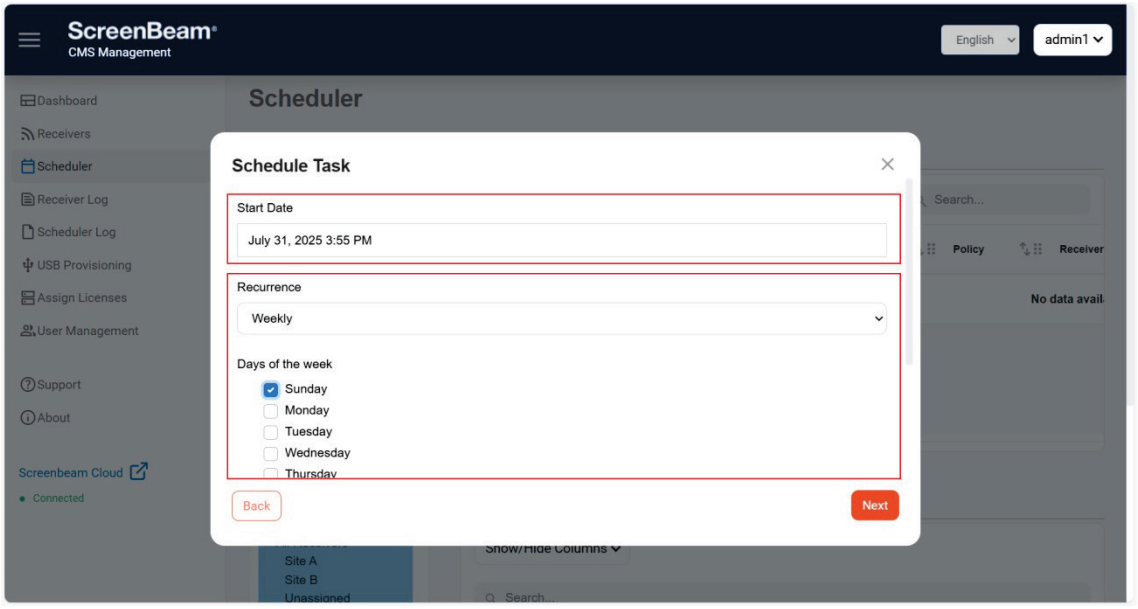
3. The **Schedule Task** window appears. On the **General info** page, give your task a name in the **Name** box, and describe your task in the **Description** box. Click **Next** to continue.



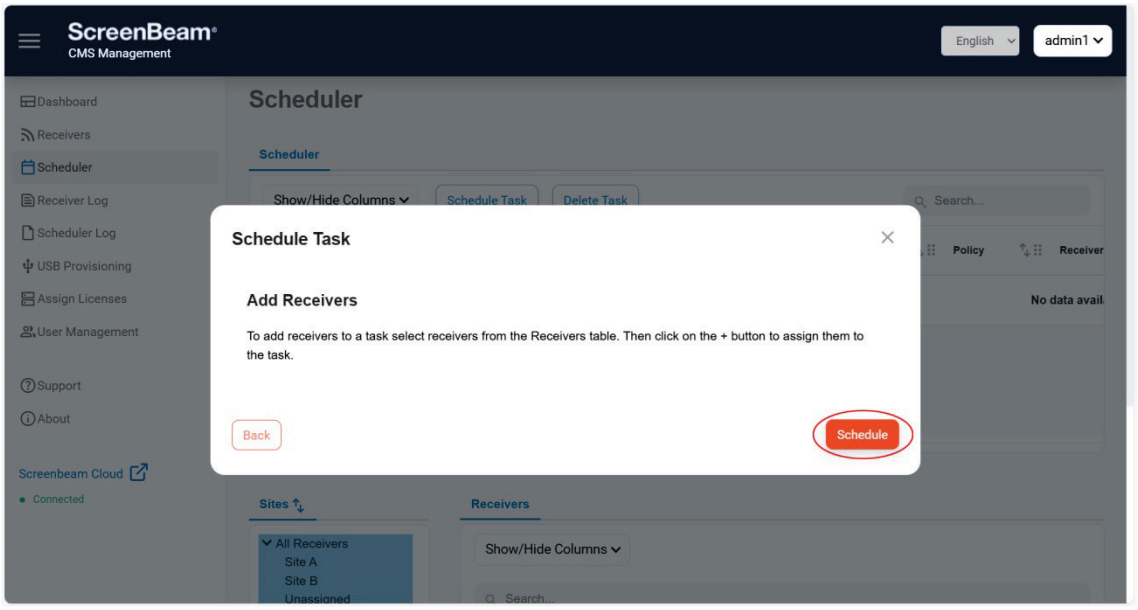
4. On the **Actions** page, select an action. Click **Next** to continue.



5. On the **Trigger** page, define a start date and select a recurrence.
   - Start Date: It is the date and time when the task is executed.
   - Recurrence:
     - Once - the task will be executed once on the defined start date.
     - Minutes - execution of the task will be repeated every xx minutes (xx refers to the number of minutes you define). (used only for testing)
     - Daily - execution of the task will be repeated every xx days (xx refers to the number of days you define).
     - Weekly - execution of the task will be repeated on the defined day(s) of the week.
     - Monthly - execution of the task will be repeated on the defined date of month.
   - End Date: This is the date and time when execution of the task is stopped. Check the End Date box and then select an end date in the End Date box.



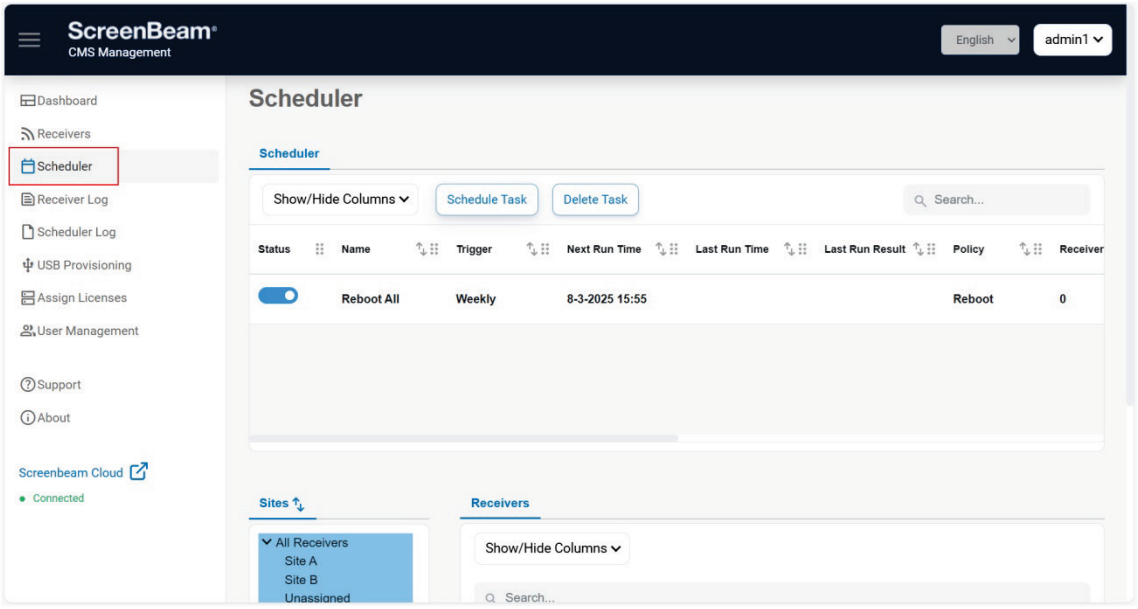
6. On the **Add Receivers** page, read the instructions on how to add receivers to a task. Click **Proceed**.



4.6.2 Add Receiver to Task

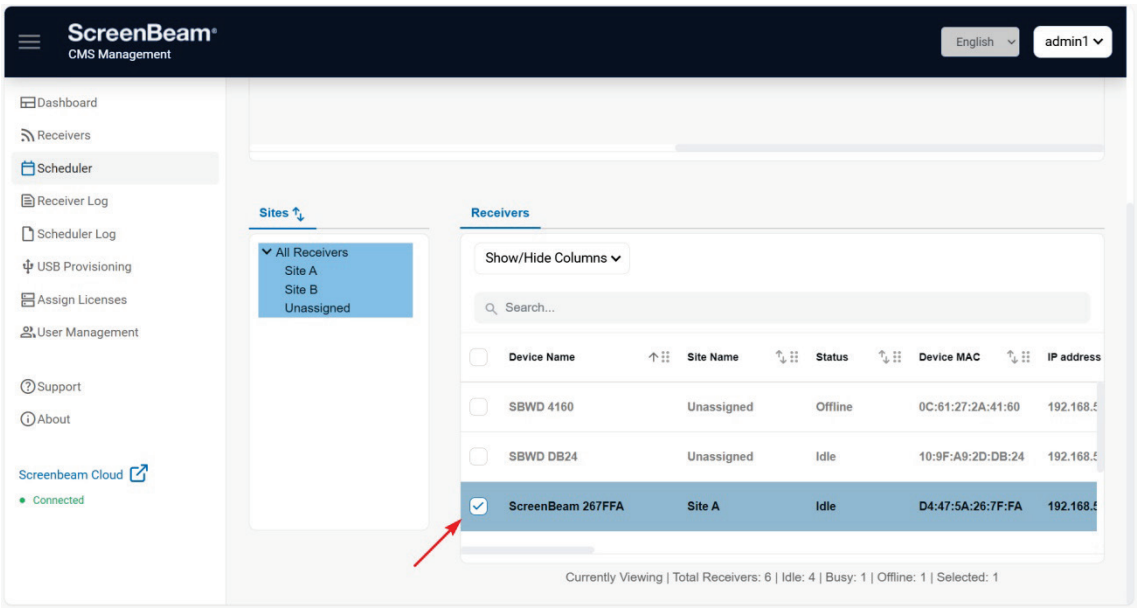
To add receivers to a task, follow this procedure:

1. Go to the **Scheduler** page by clicking **Scheduler** on the left pane.

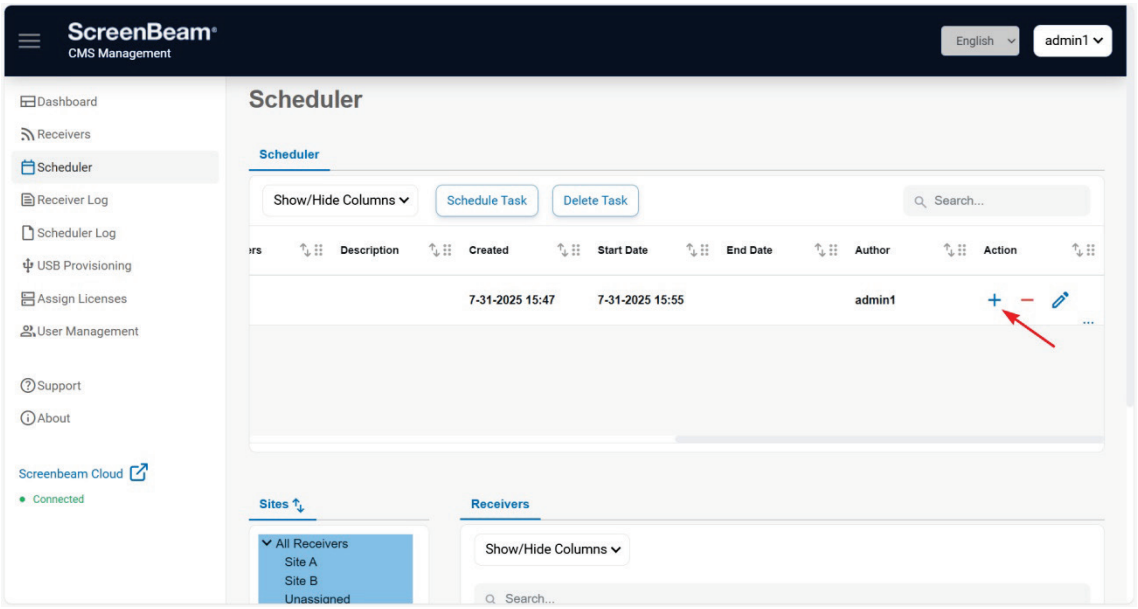


2. Ensure no task is selected.

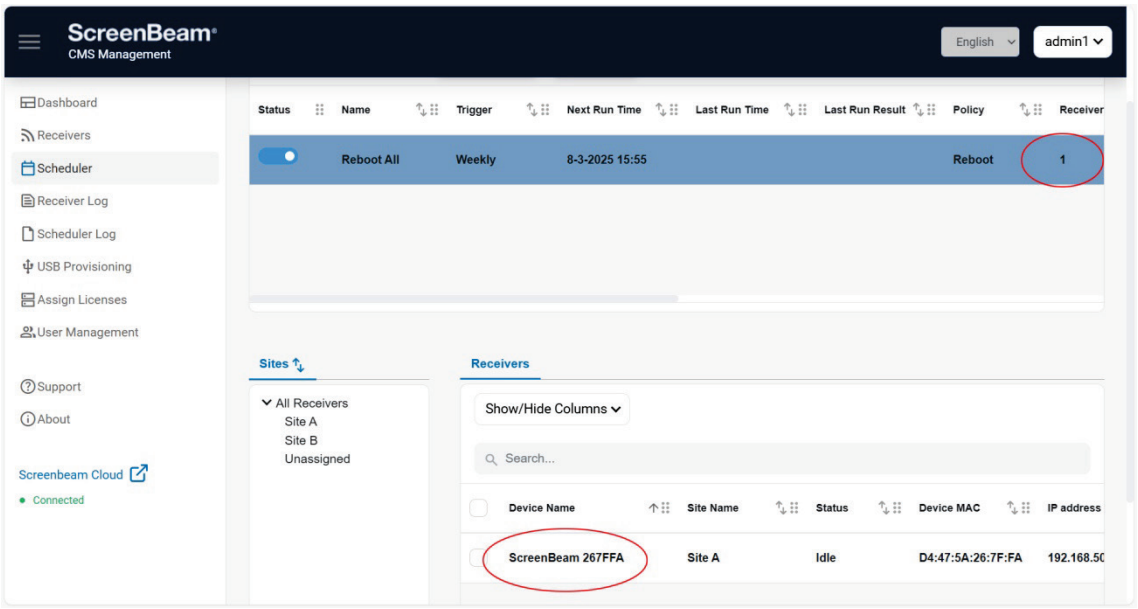
3. On the **Receivers** pane, select the receiver(s) that you want to add to a task.



4. On the **Scheduler** pane, click the “+” sign in the **Action** column of the intended task.



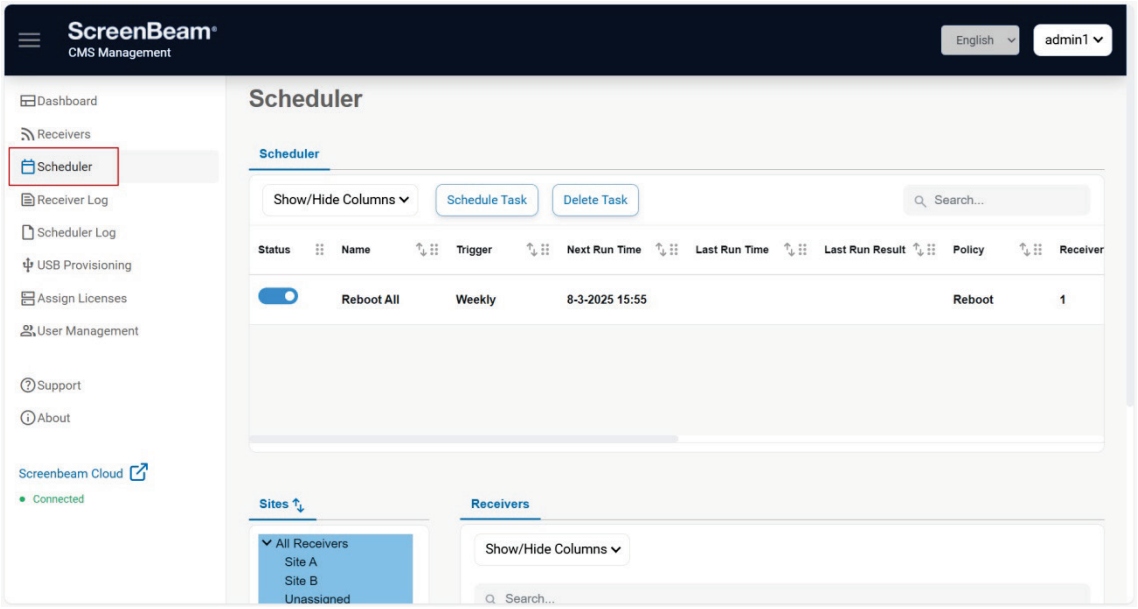
5. The selected receivers are added to the intended task.



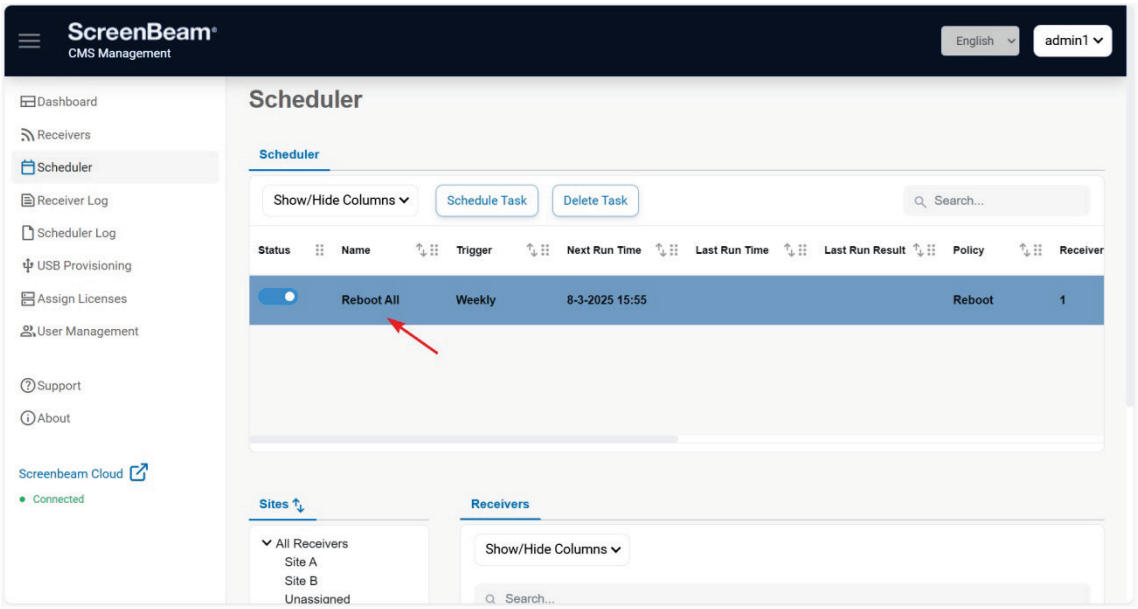
4.6.3 Remove Receivers from a Task

To remove receivers from a task, follow this procedure:

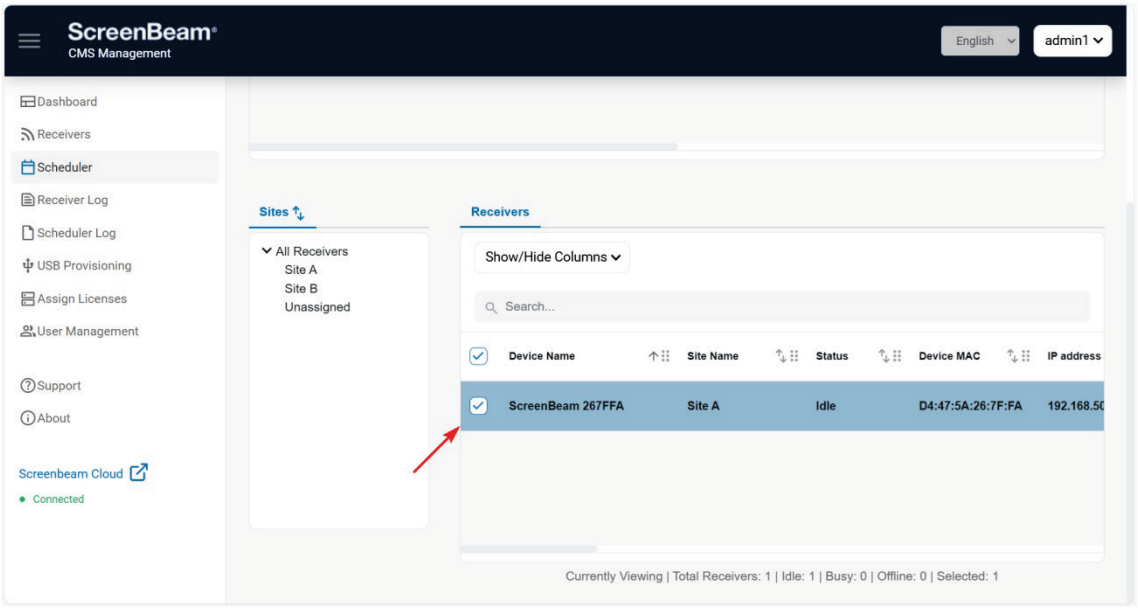
1. Go to the **Scheduler** page by clicking **Scheduler** on the left pane.



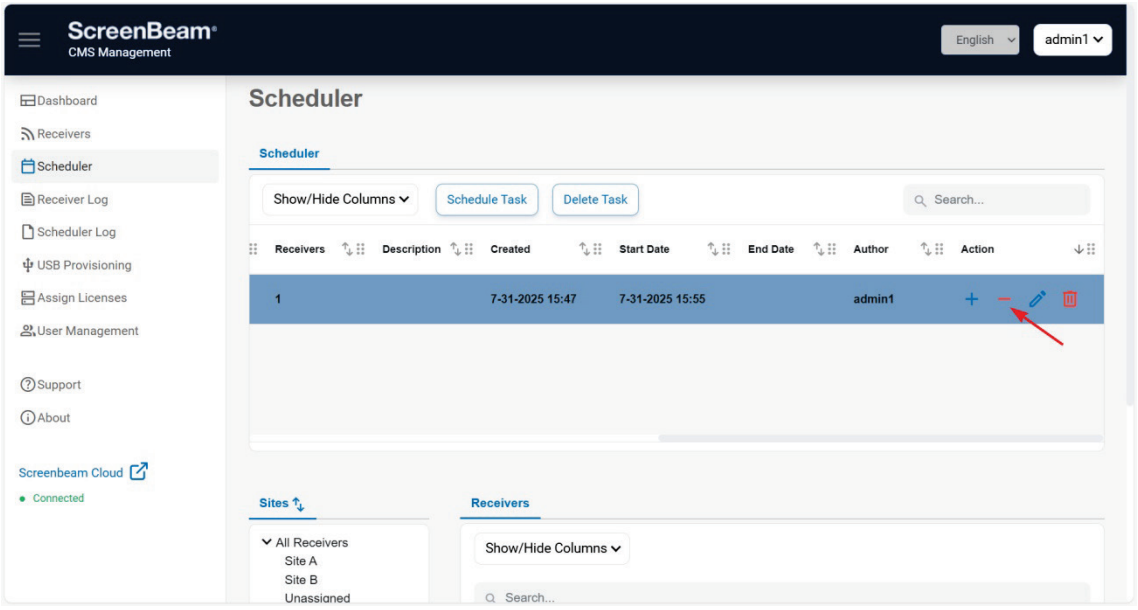
2. Select the task where receivers are to be removed. This step is optional if you know which receivers are assigned to the task.



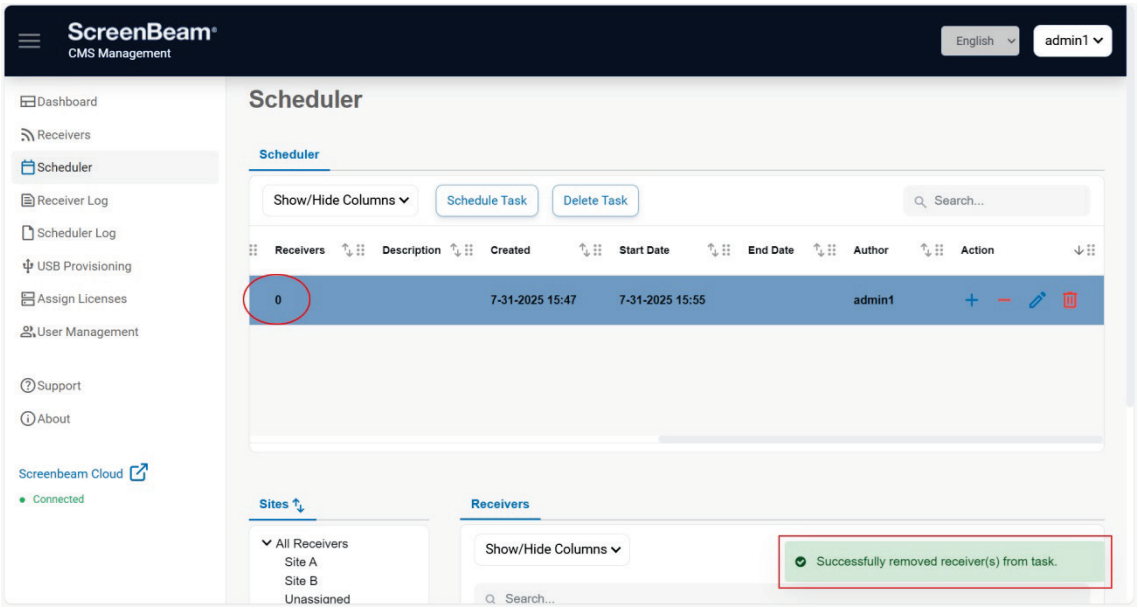
3. On the **Receivers** pane, select the receiver(s) to be removed from the task.



4. On the **Scheduler** pane, click the "-" sign in the **Action** column of the intended task.



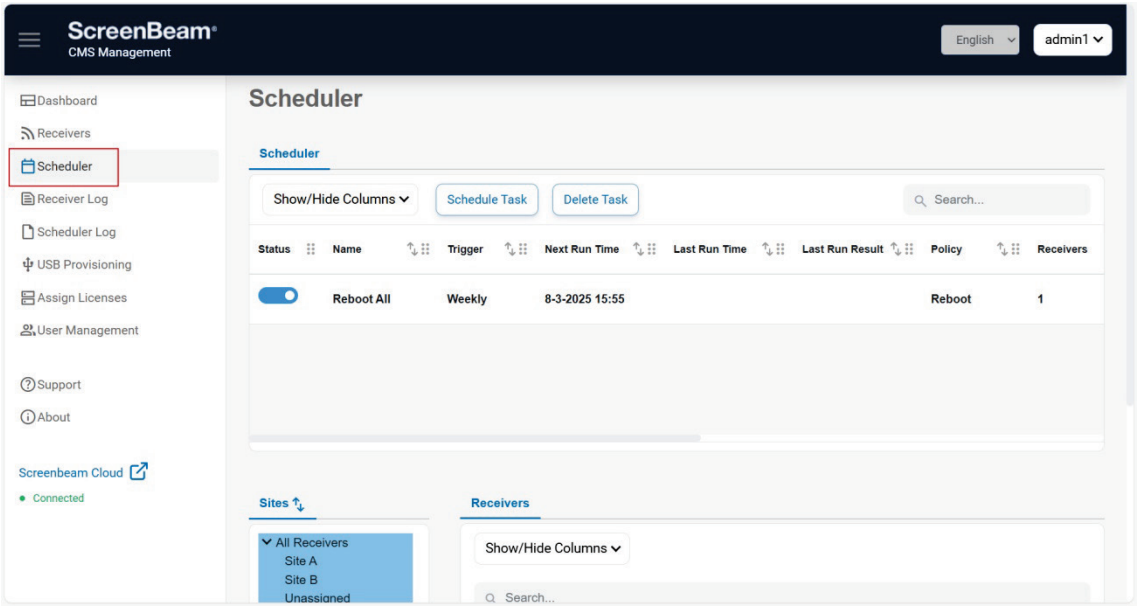
5. The selected receivers are removed from the task.



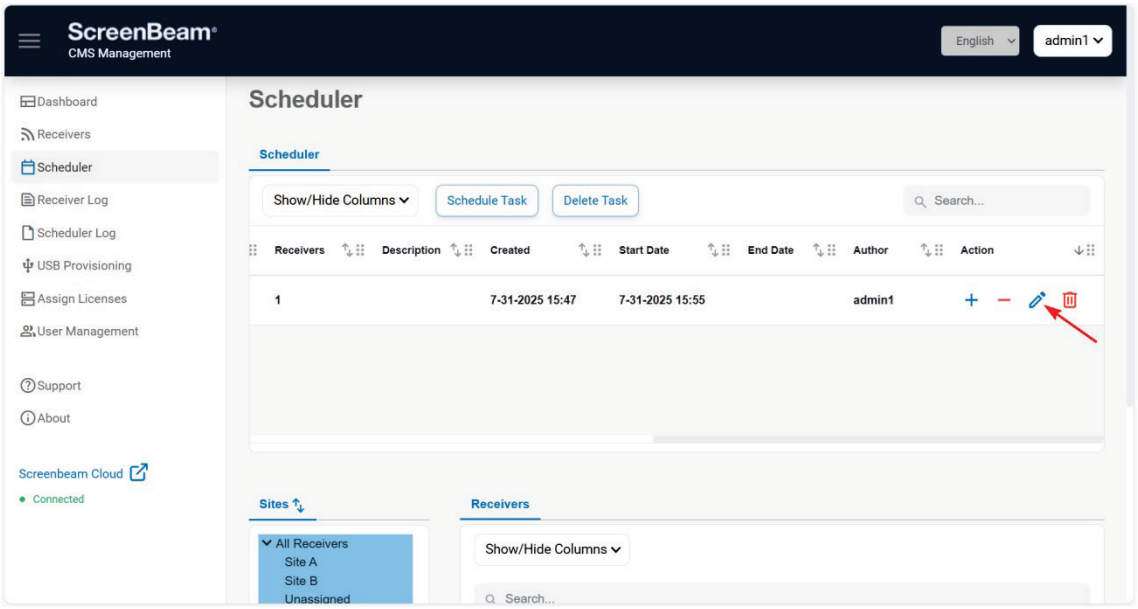
4.6.4 Edit a Task

To edit a task, follow this procedure:

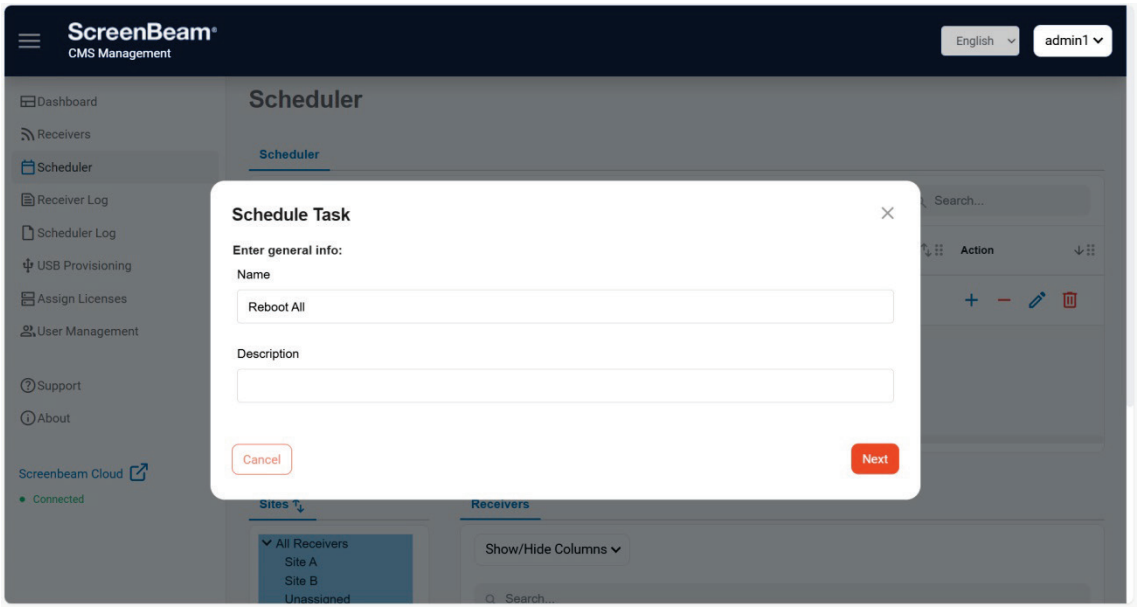
1. Go to the **Scheduler** page by clicking **Scheduler** on the left pane.



2. On the **Scheduler** pane, click the pen icon in the **Action** column of the intended task to edit the task.



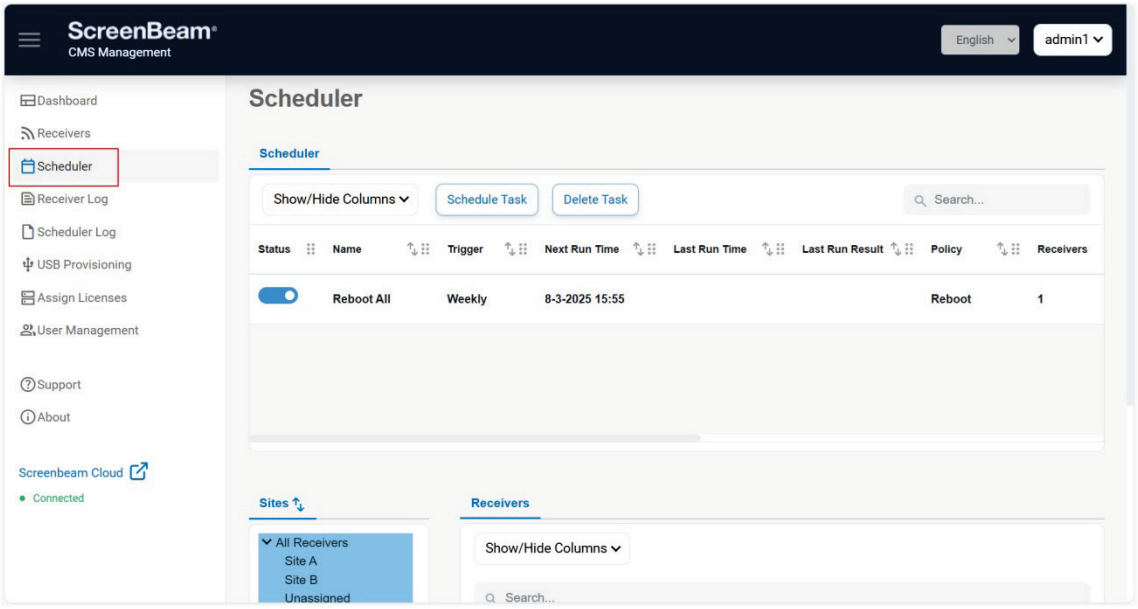
3. Follow the procedure described in Section 4.6.1 **Schedule a Task** to edit the task.



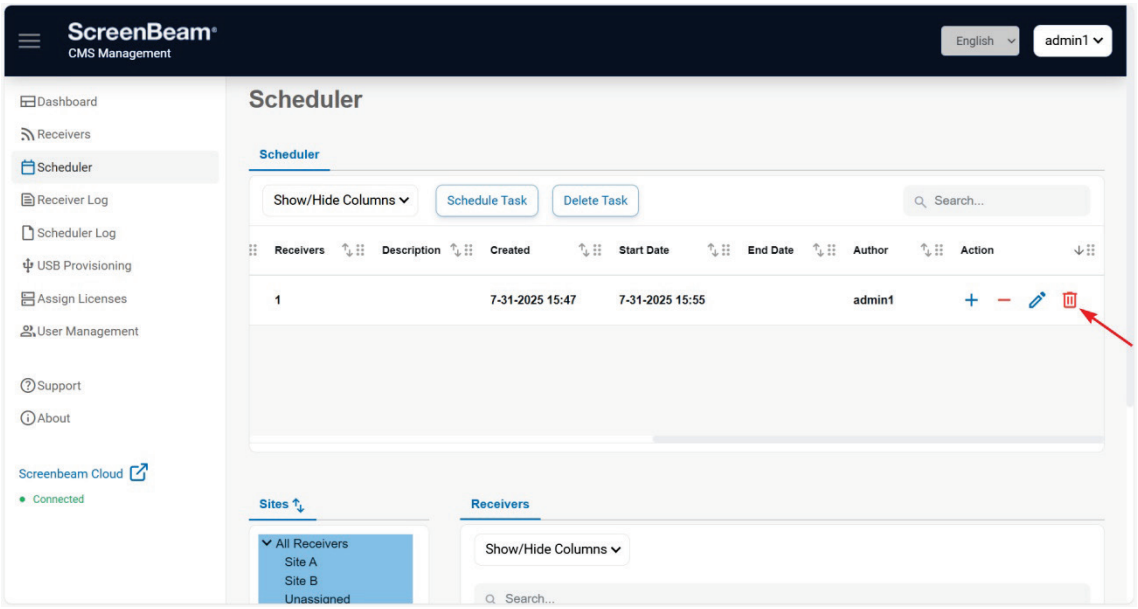
4.6.5 Delete a Task

To delete a task, follow this procedure:

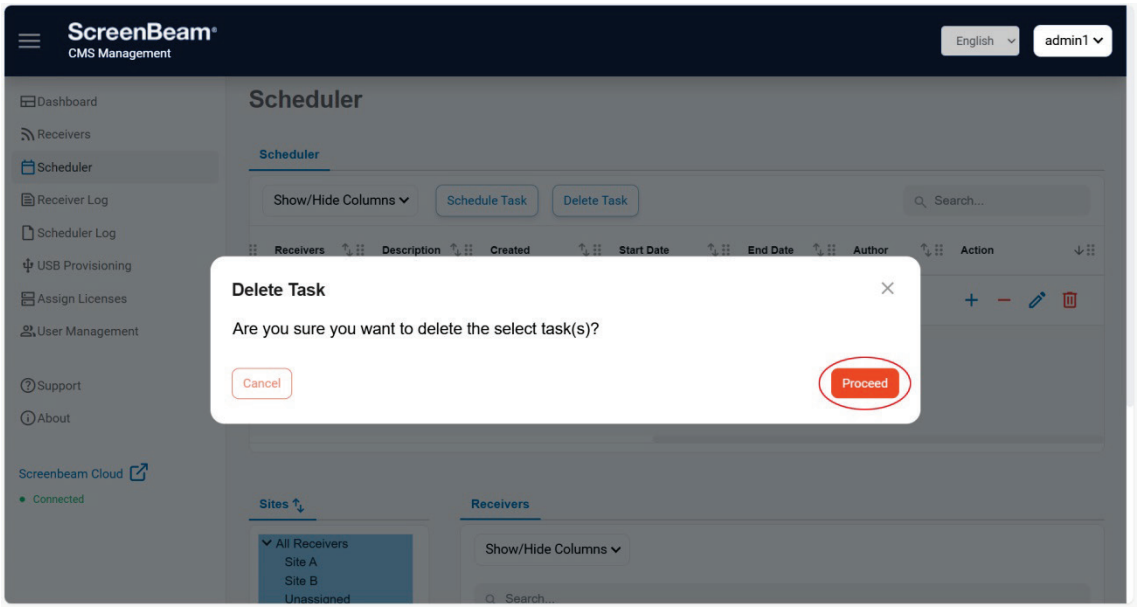
1. Go to the **Scheduler** page by clicking **Scheduler** on the left pane.



2. On the **Scheduler** pane, click the trash bin icon in the **Action** column of the intended task to delete the task.



3. The **Delete Task** message box appears. Click **Proceed**.



4.7 Managing Logs

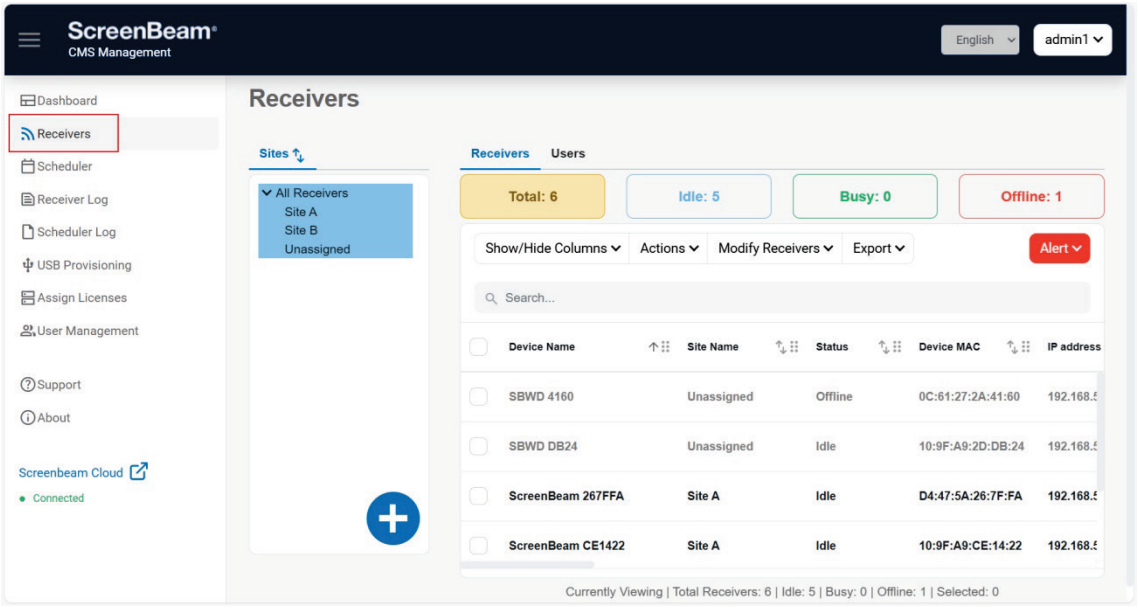
Receiver logs and scheduler logs capture basic events of ScreenBeam receivers to be able to track down problems efficiently. Logs are available to CMS system administrators only.

4.7.1 Upload Receiver Log

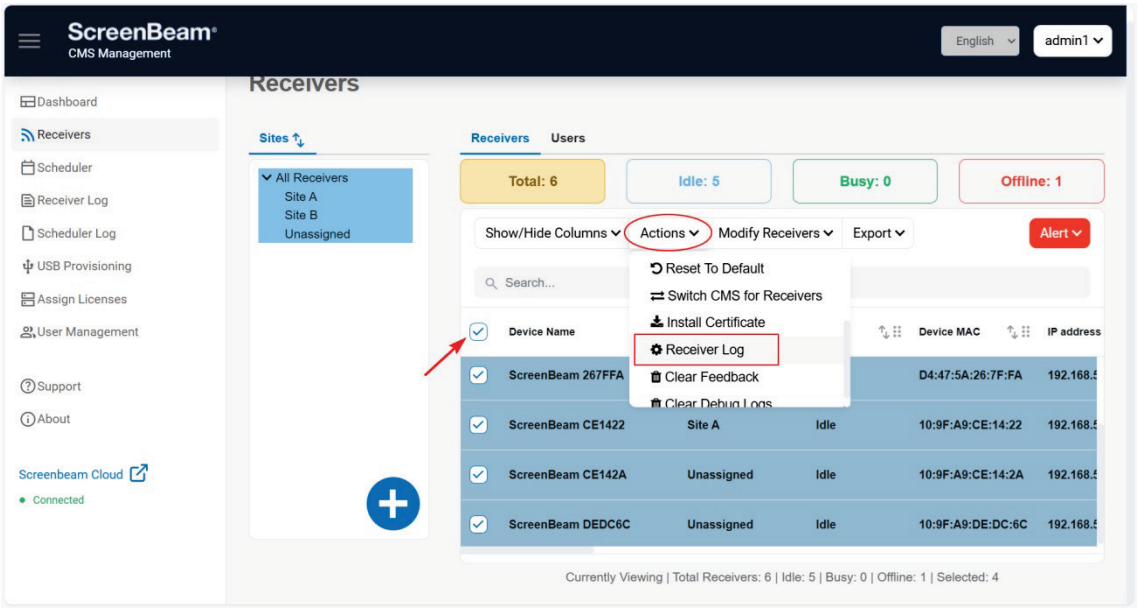
ScreenBeam receivers will log events automatically, with new event logs replacing the oldest event logs when the log cache is full. Event logs will not, however, be uploaded to CMS by default. The logs can be uploaded to the CMS server manually using the Receiver Log function or automatically using Scheduler.

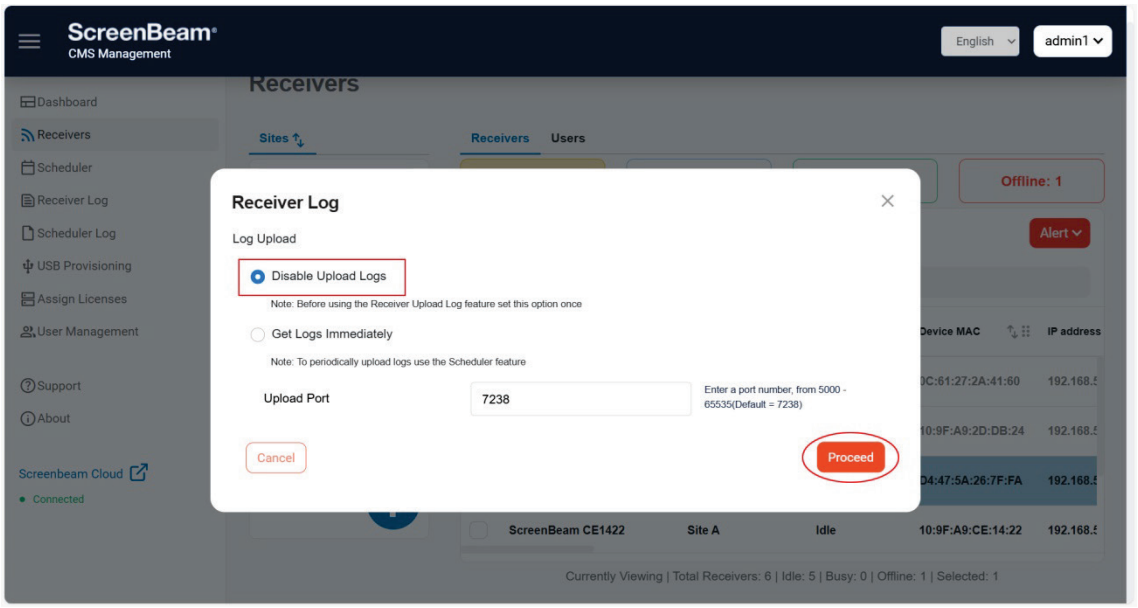
To upload receiver logs, follow this procedure:

1. Go to the **Receivers** page by clicking **Receivers** on the left pane.

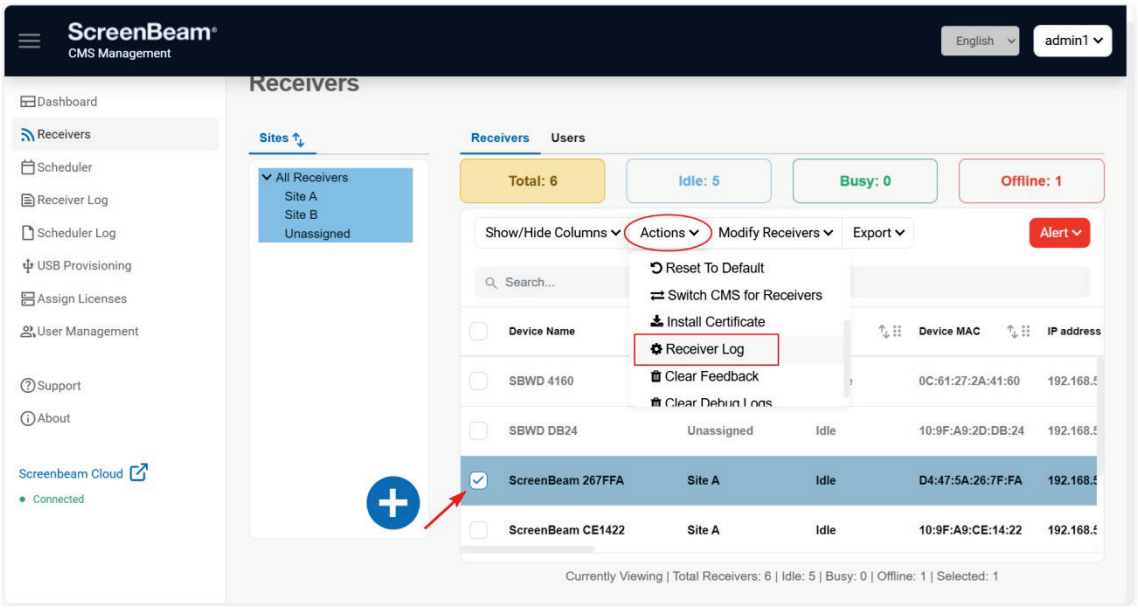


2. (Optional) Select all receivers, go to **Actions** > **Receiver Log**, and select **Disable Upload Logs**. Click **Proceed**.
   Note: This step is only required to be done once.

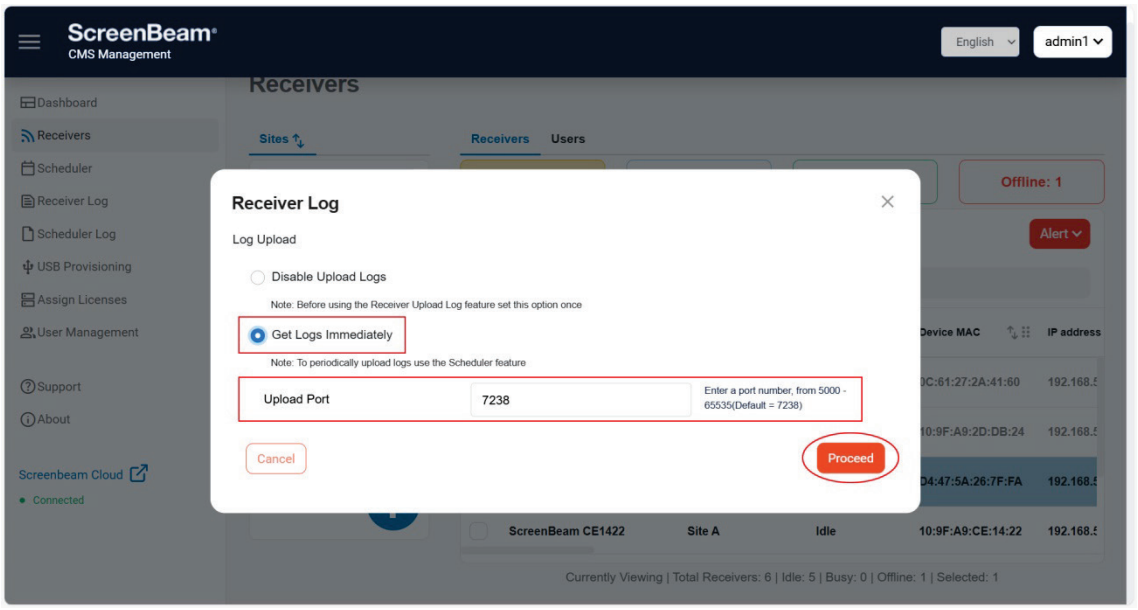




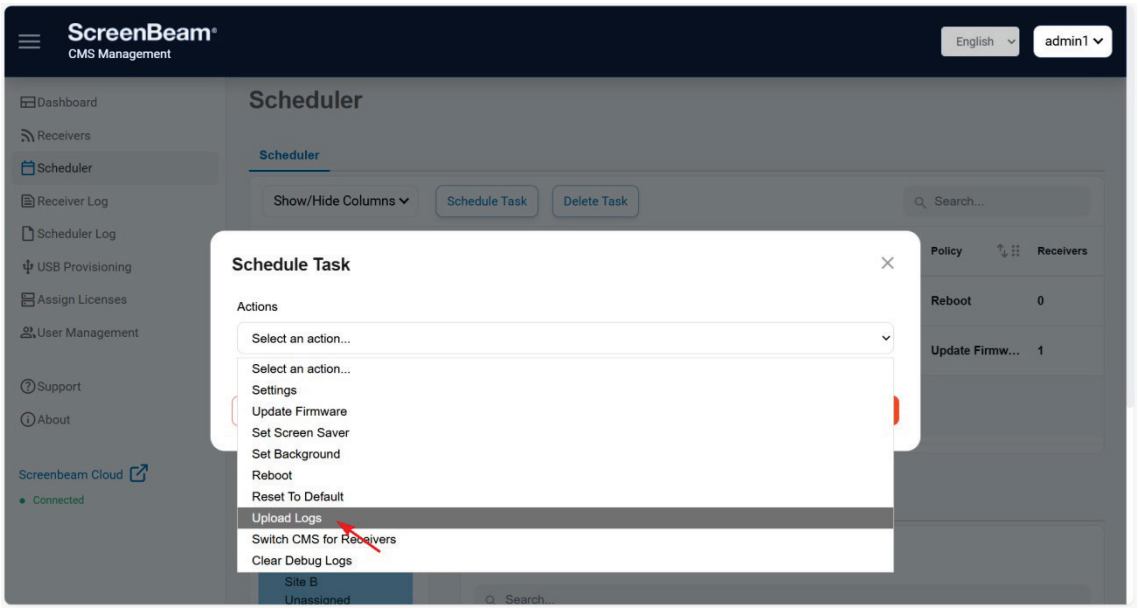
3. Select the receiver(s) for log upload to CMS on the **Receivers** page, and then open **Receiver Log** window through **Actions** > **Receiver Log**.



4. The **Receiver Log** window will then appear. On the **Receiver Log** window, select **Get Logs immediately** and specify the log **Upload Port**. Click **Proceed**.



Alternatively, logs can be uploaded automatically using the **Scheduler**. Create a new task and select **Upload Logs** in the **Actions** page.



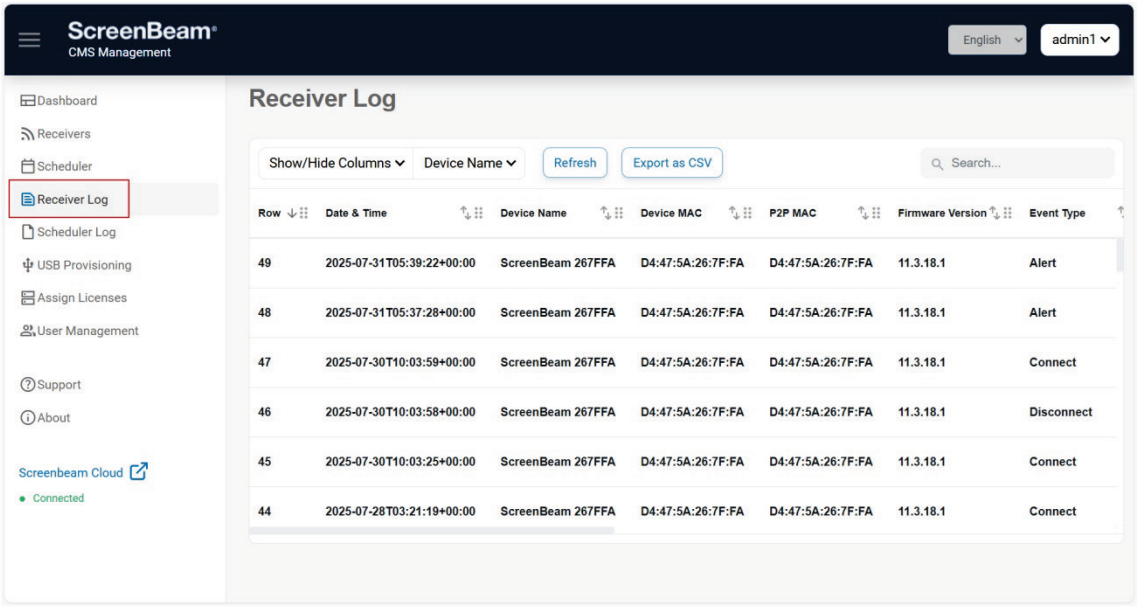
As the receiver log upload can sometimes take a few hours, it is recommended to schedule the receiver uploads during non-business hours. Once a log uploading task is scheduled and started, it is not able to request receiver log immediately until the task has completed.

4.7.2 View Receiver Logs

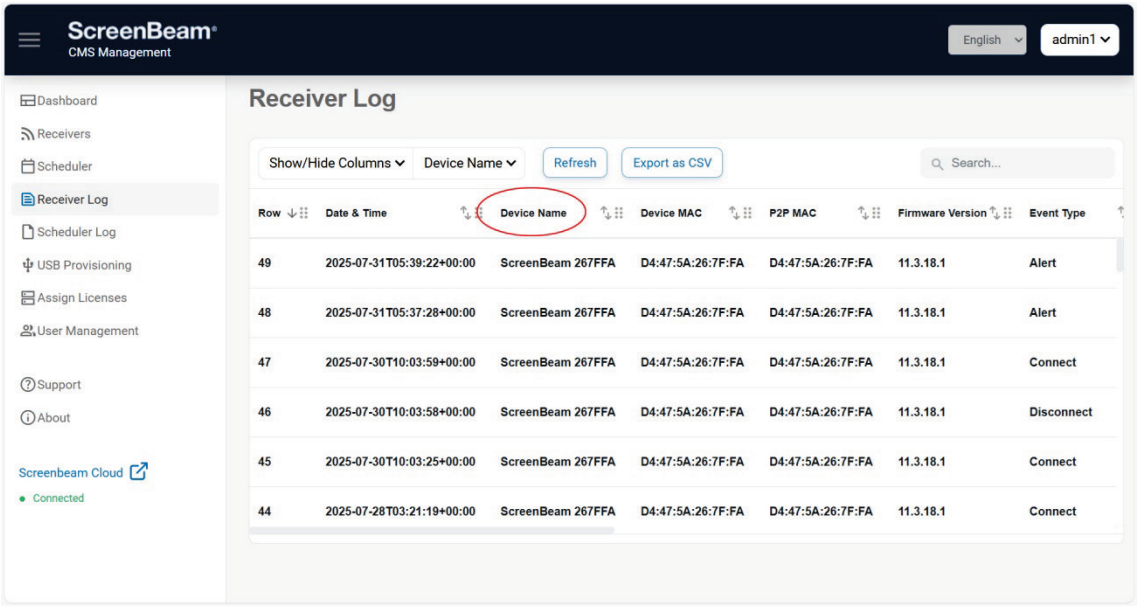
To view receiver logs, follow this procedure:

1. Log in as a CMS system administrator (CMS SysAdmin).

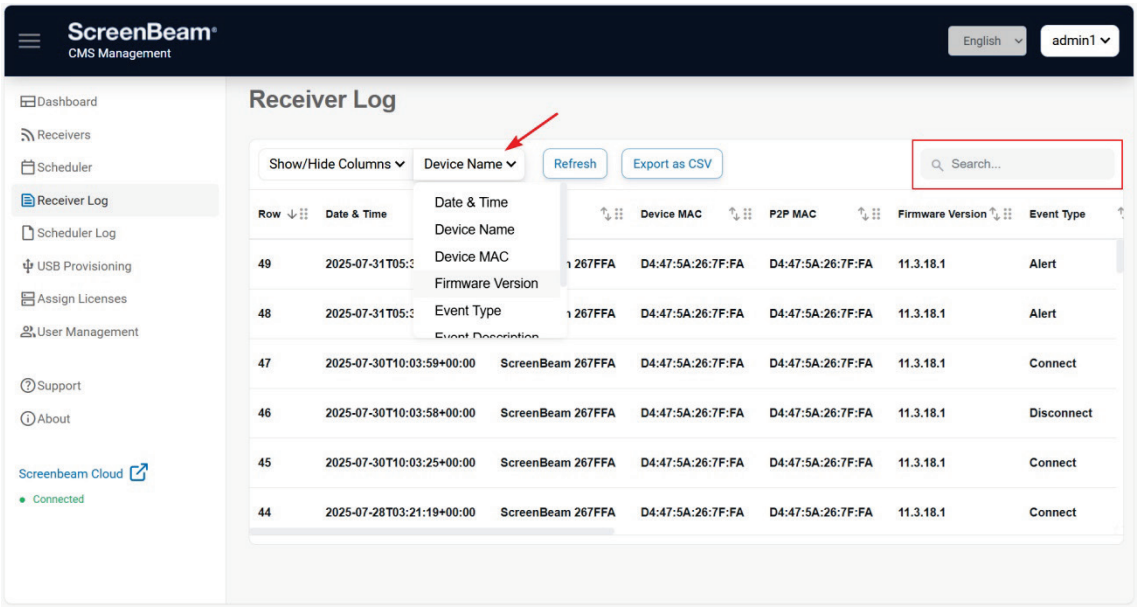
2. Go to the **Receiver Log** page by clicking **Receiver Log** on the left pane.



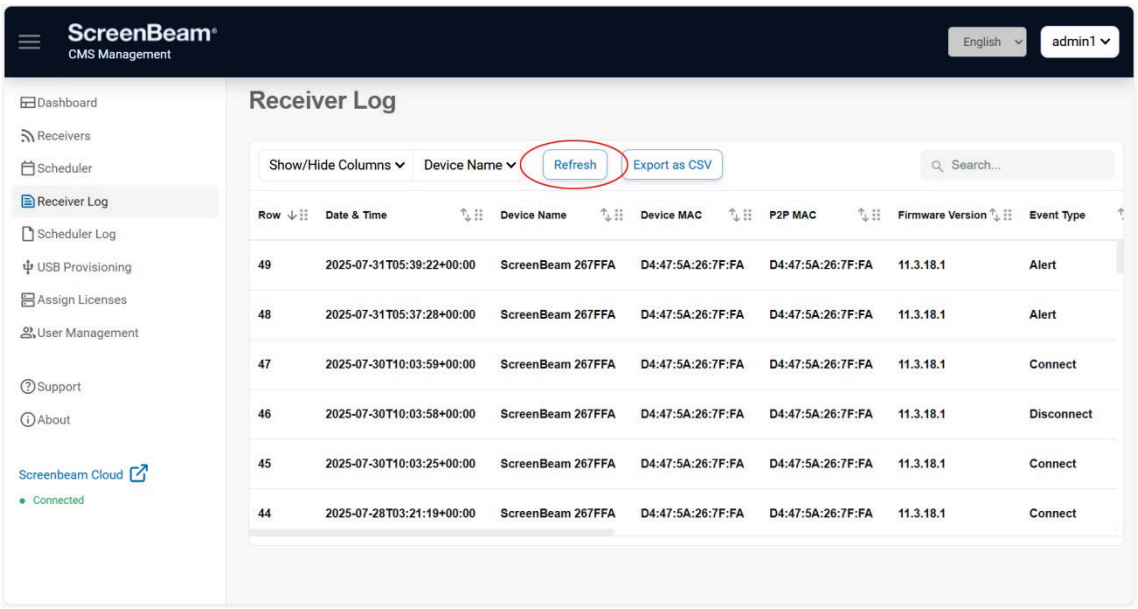
3. Click a column name to sort events by the respective type.



4. Select a filter type from the filter menu and select a time period or type your key word in the Search box to search.
   - Date & Time - defines a time period to search.
   - Receiver Name - CMS will search for the receiver name only.
   - Receiver MAC - CMS will search for the receiver MAC only.
   - Firmware Version - CMS will search for the receiver's firmware version only.
   - Event Type - CMS will search for the event type only.
   - Event Description - CMS will search for the event description only.
   - Source Name - CMS will search for the source name only.
   - Source MAC - CMS will search for the source MAC only.



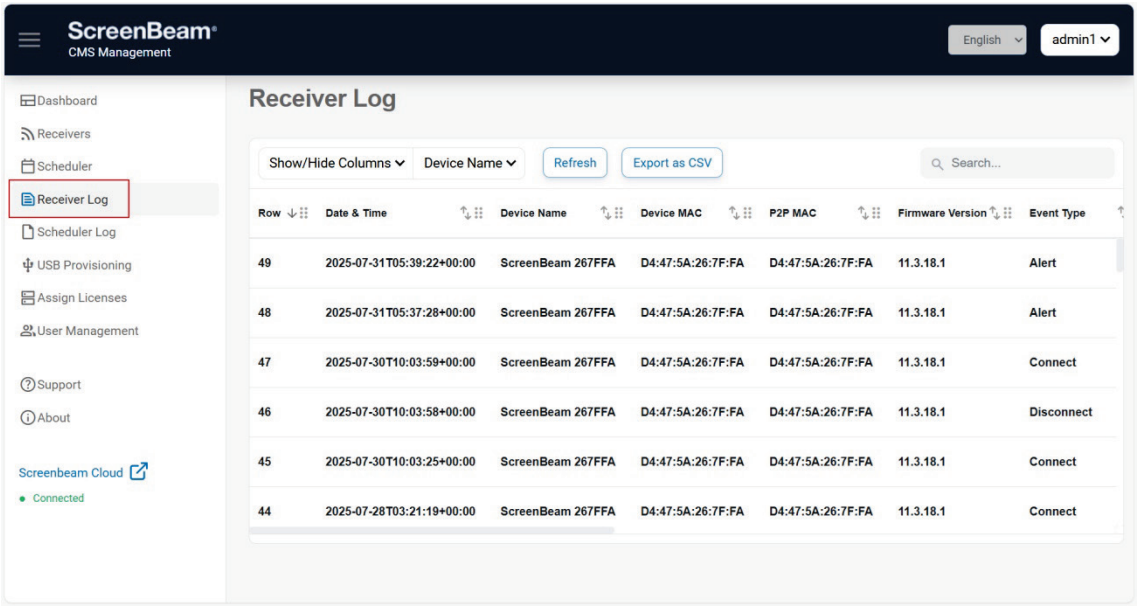
5. To check if there are new logged events that are not displayed in the **Receiver Log** page, click the **Refresh** button.



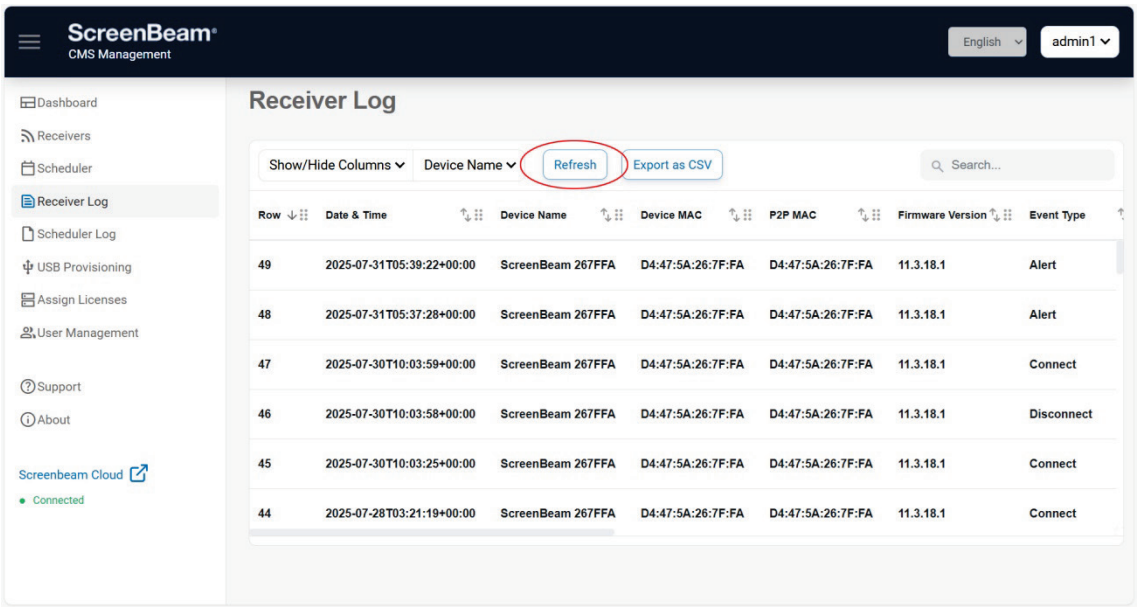
4.7.3 Export Receiver Logs

To export receiver logs, follow this procedure:

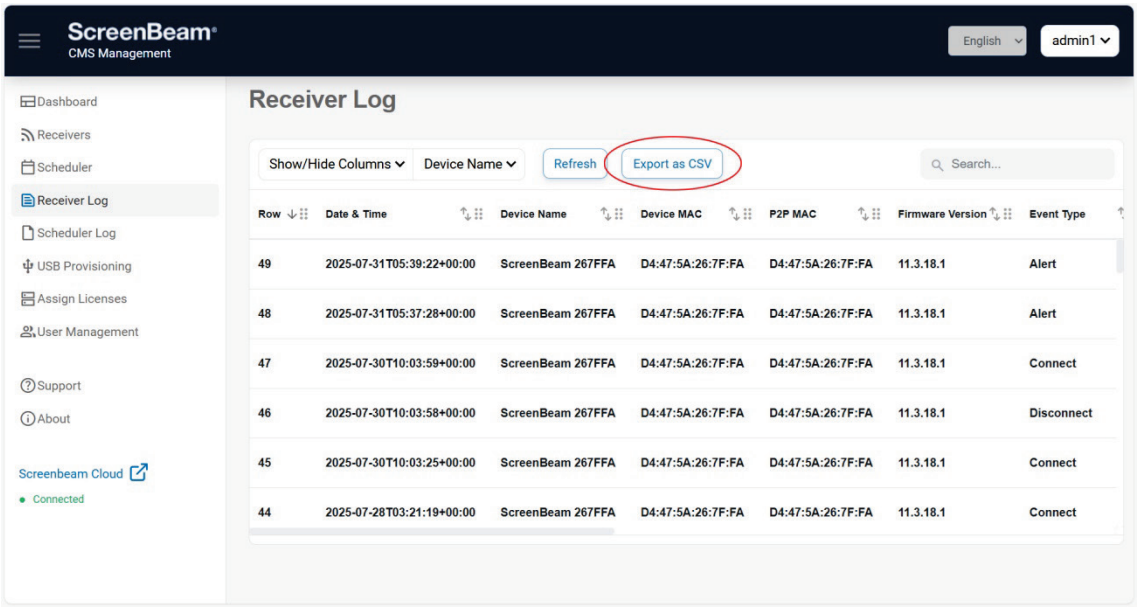
1. Log in as a CMS system administrator (CMS SysAdmin).
2. Go to the **Receiver Log** page by clicking **Receiver Log** on the left pane.



3. Click the **Refresh** button to check if there are new logged events that are not displayed in the **Receiver Log** page.



4. Click the **Export as CSV** button. Receiver logs will be exported in CSV format.



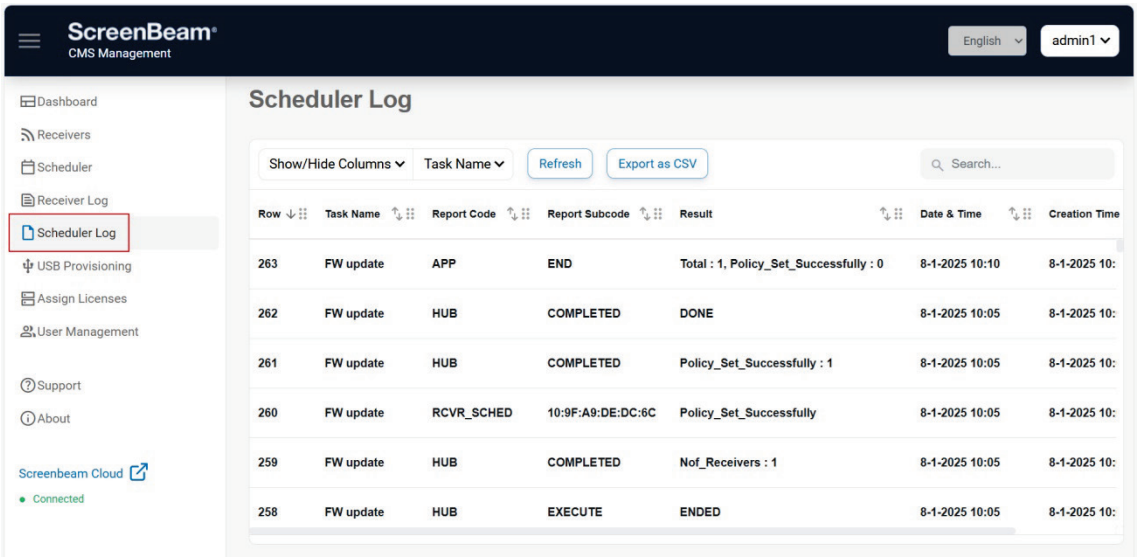
4.7.4 View Scheduler Log

ScreenBeam CMS records scheduler logs automatically and displays them in the **Scheduler Log** page.

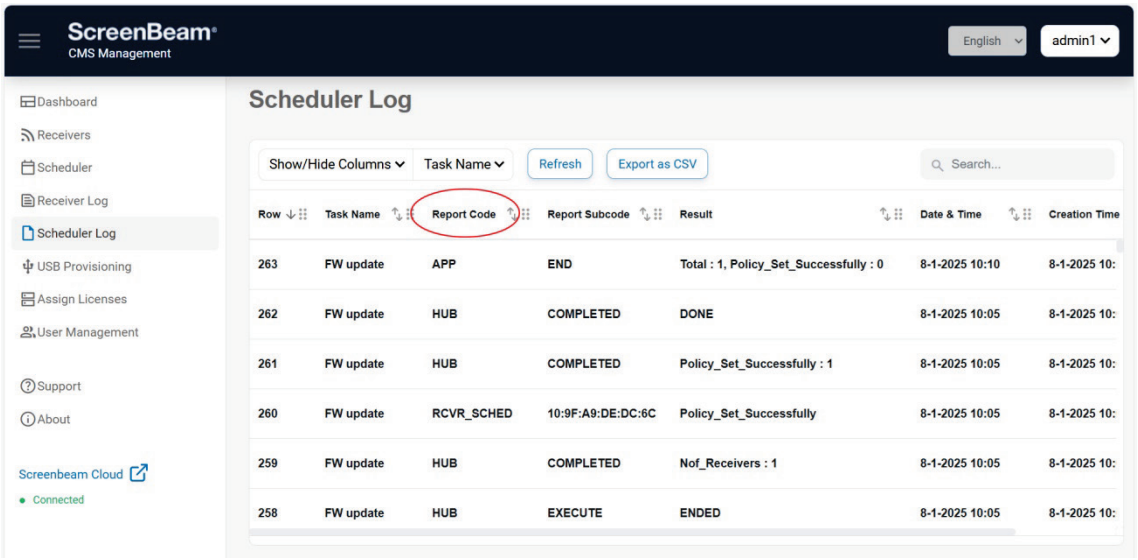
To view scheduler logs, follow this procedure:

1. Log in as a CMS system administrator (CMS SysAdmin).

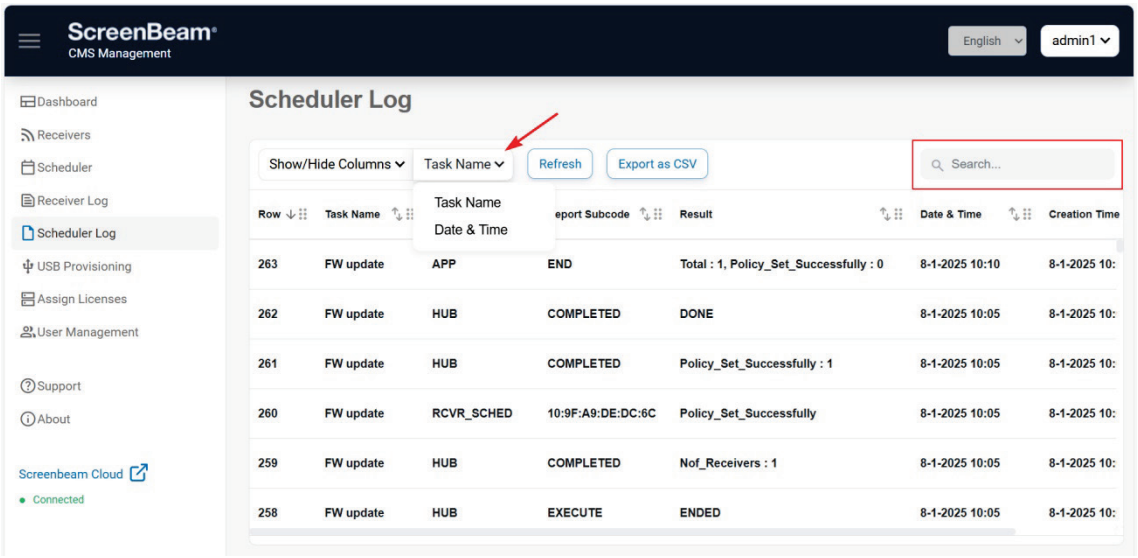
2. Go to the **Scheduler Log** page by clicking **Scheduler Log** on the left pane.



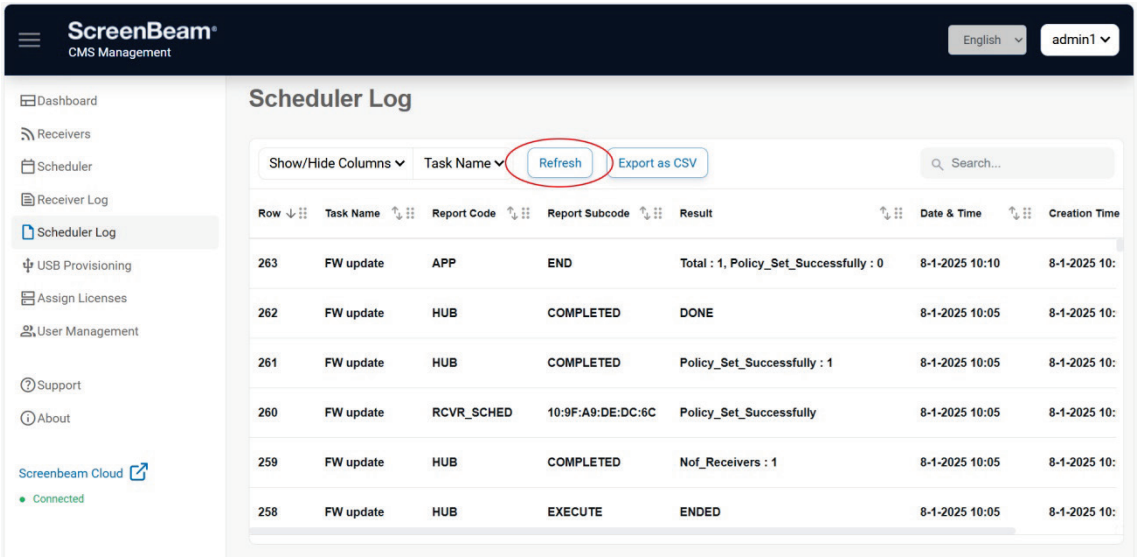
3. Click a column name to sort events by the respective type.



4. Select a filter type from the filter menu and select a time period or type your key word in the Search box to search.
   - Task Name - CMS will search for the task name only.
   - Date & Time - Searches within a specified time period.



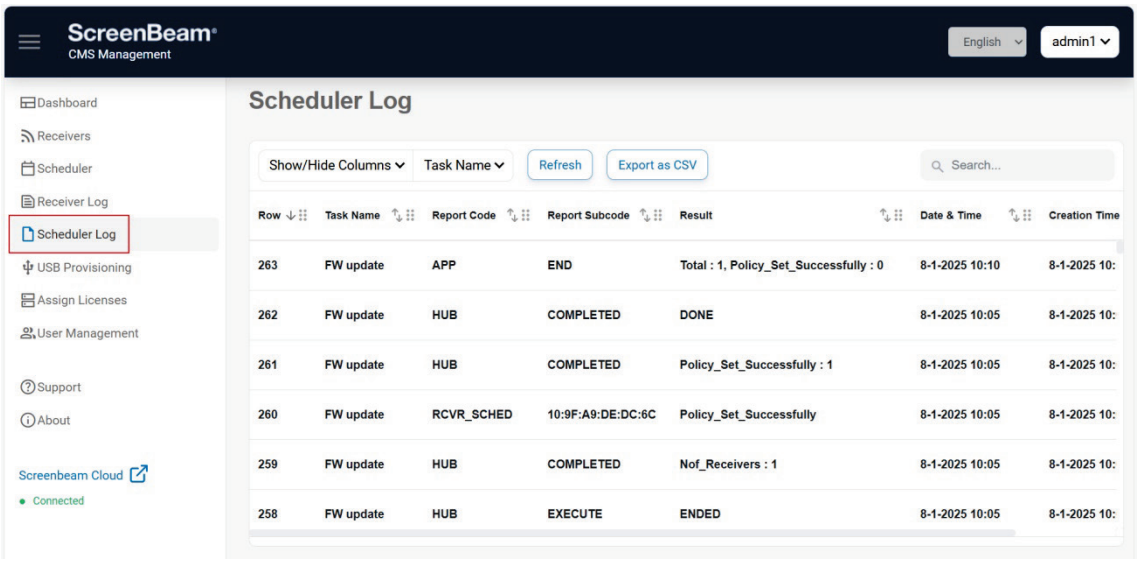
5. To check if there are new logged events that are not displayed in the **Scheduler Log** page, click the **Refresh** button.



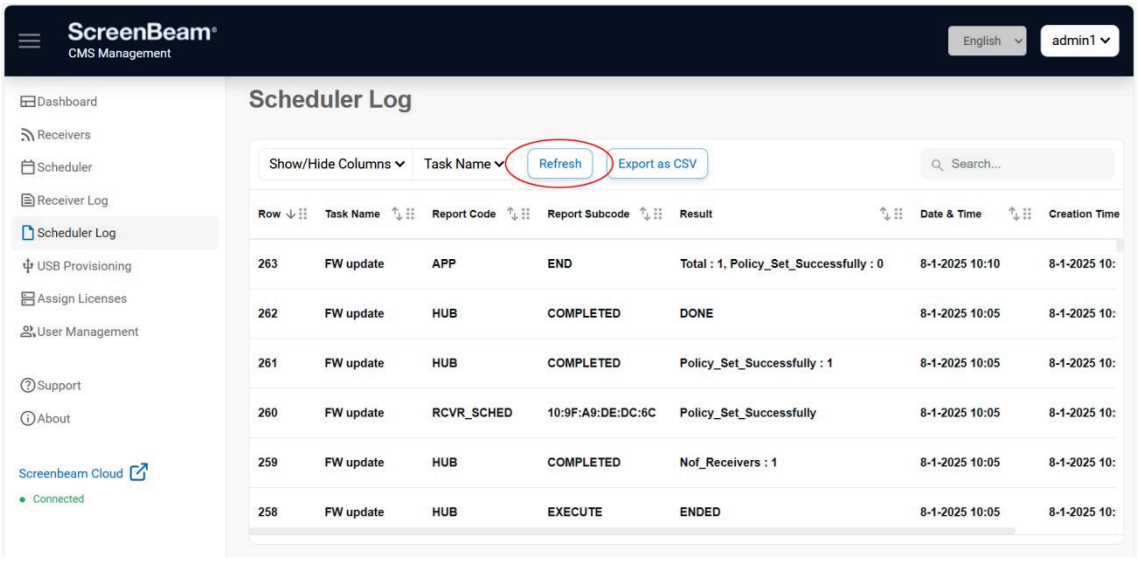
4.7.5 Export Scheduler Log

To export scheduler logs, follow this procedure:

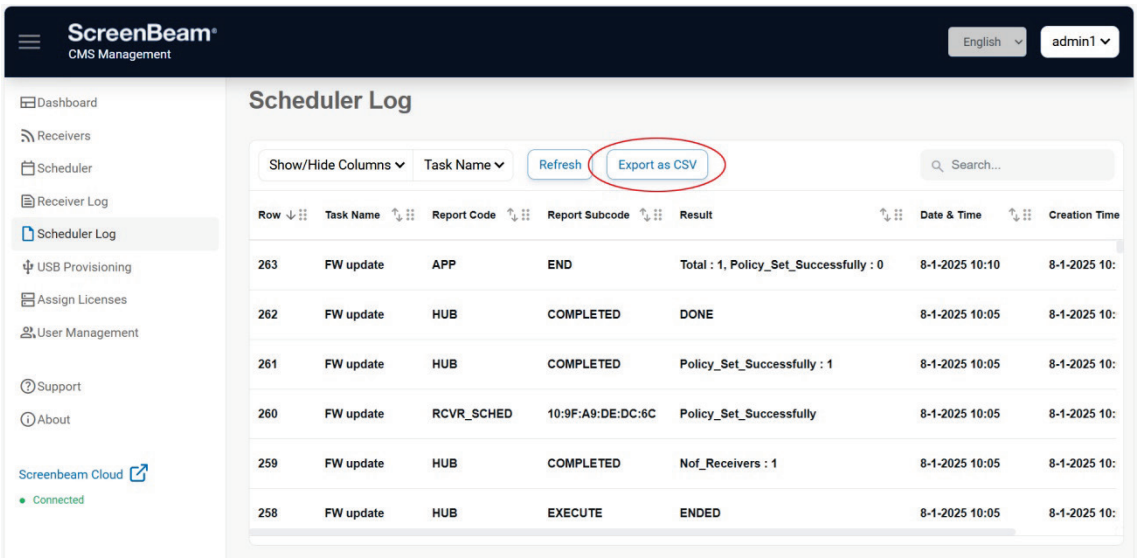
1. Log in as a CMS system administrator (CMS SysAdmin).
2. Go to the **Scheduler Log** page by clicking **Scheduler Log** on the left pane.



3. Click the **Refresh** button to check if there are new logged events that are not displayed in the **Scheduler Log** page.



4. Click the **Export as CSV** button to export scheduler logs.



Appendix I Using Azure AD for User Management

ScreenBeam CMS V4 supports Microsoft Azure Active Directory for user management.

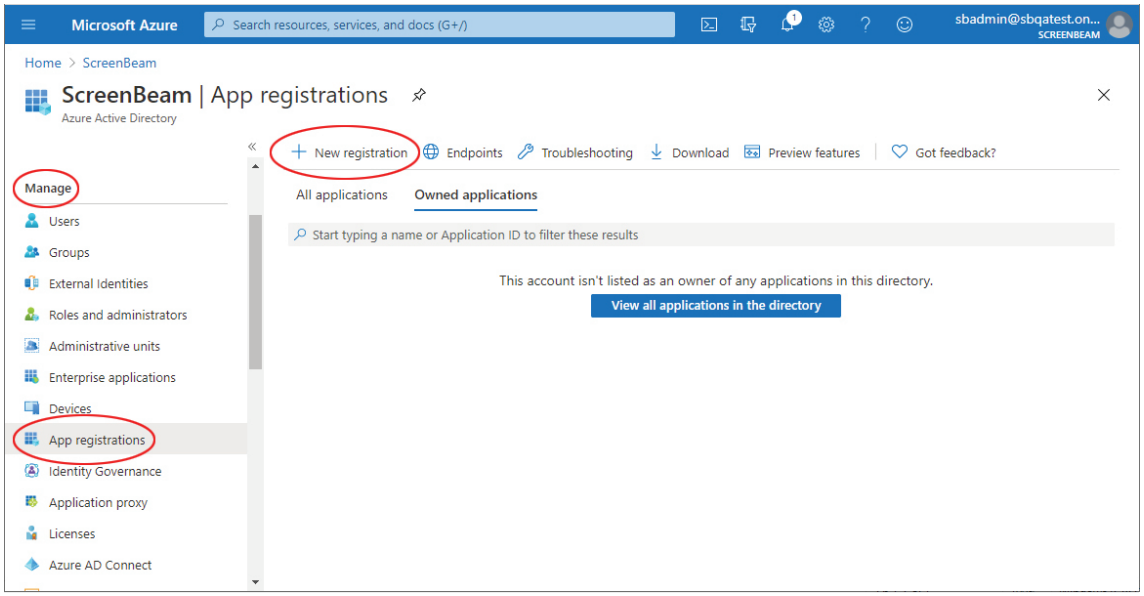
Prerequisite

- An Azure Active Directory (AAD) user account with at least "**Application Administrator**" role.
- A Security group (its Group Type is set to Security) is created, and all users with access to CMS V4 are added to this group. CMS will read users from this group and list them as CMS users. (Learn more about creating a group and adding member to a group on AAD)
- Decide AAD application authentication type. (Learn more about application identity on AAD)
  - Using application secret
  - Using a certificate (not supported currently)
- Decide permission type granting to CMS:
  To access user data from AAD, CMS needs an appropriate set of permissions from AAD. There are two (2) ways to grant permissions to CMS: delegated permissions and application permissions (Learn more):
  - **Delegated permissions**: CMS needs a signed-in user to request data from AAD. Required following AAD permissions:
    - *GroupMember.Read.All*: read list of users from given group. Learn more.
    - *User.ReadBasic.All*: read basic data from each user on the list. Learn more.
  - **Application permissions (Daemon)**: CMS can request permitted data without a signed-in user.
    - *GroupMember.Read.All*: read list of users from given group. Learn more.
    - *User.Read.All*: read basic data from each user on the list. Learn more.

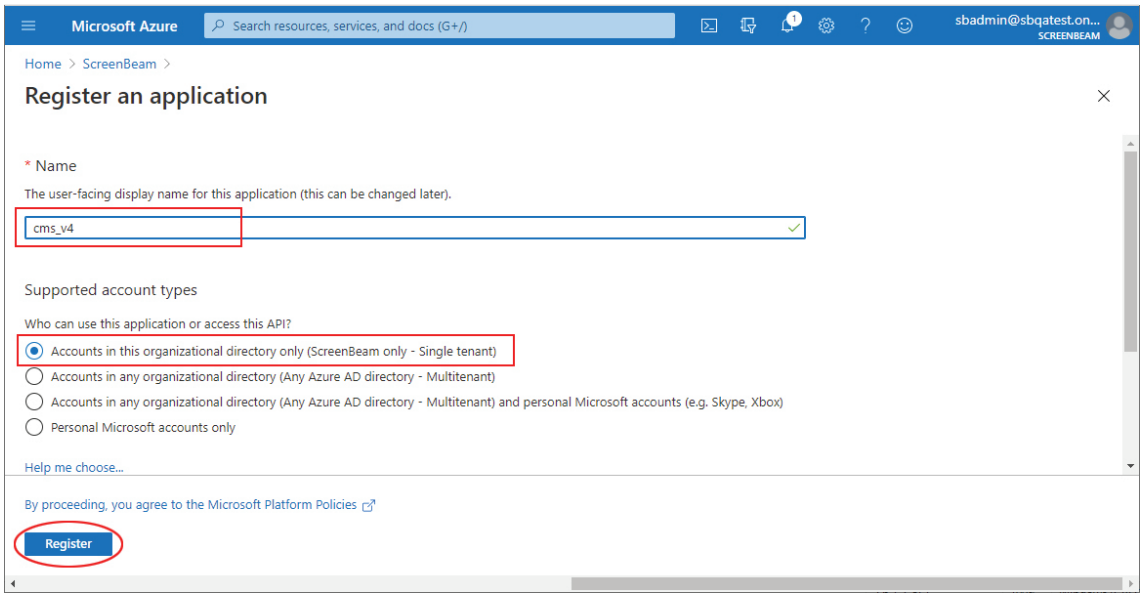
  Note: Regardless of which setup, CMS only reads data from the AAD group you have provided when installing CMS.

Setting up Azure AD and ScreenBeam CMS

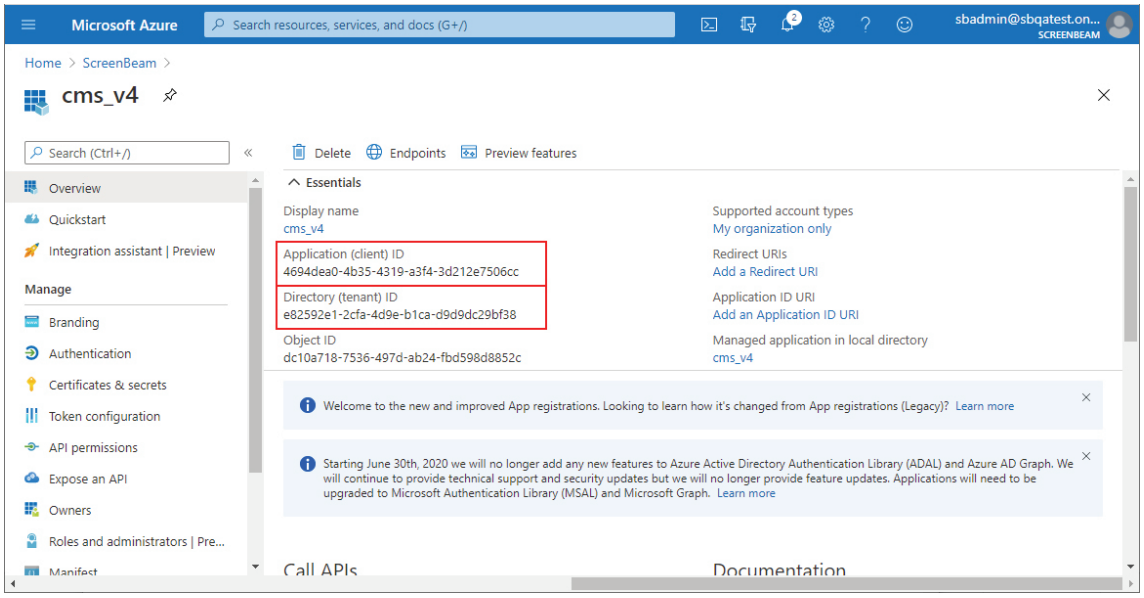
1. Register CMS to your AAD. To do this, follow the procedure below:
   a. Sign into the Azure portal (portal.azure.com) using either a work or school account.
   b. Search for and select **Azure Active Directory**.
   c. Select the Azure AD tenant that you want.
   d. Select **App registrations** under **Manage** in the left menu, and then select the **New registration** button in the right pane.



   e. The **Register an application** window appears. Enter a meaningful application name to display to users, and specify who can use the application, choosing the "**Accounts in this organizational directory only**" option. Click **Register** to continue**.**

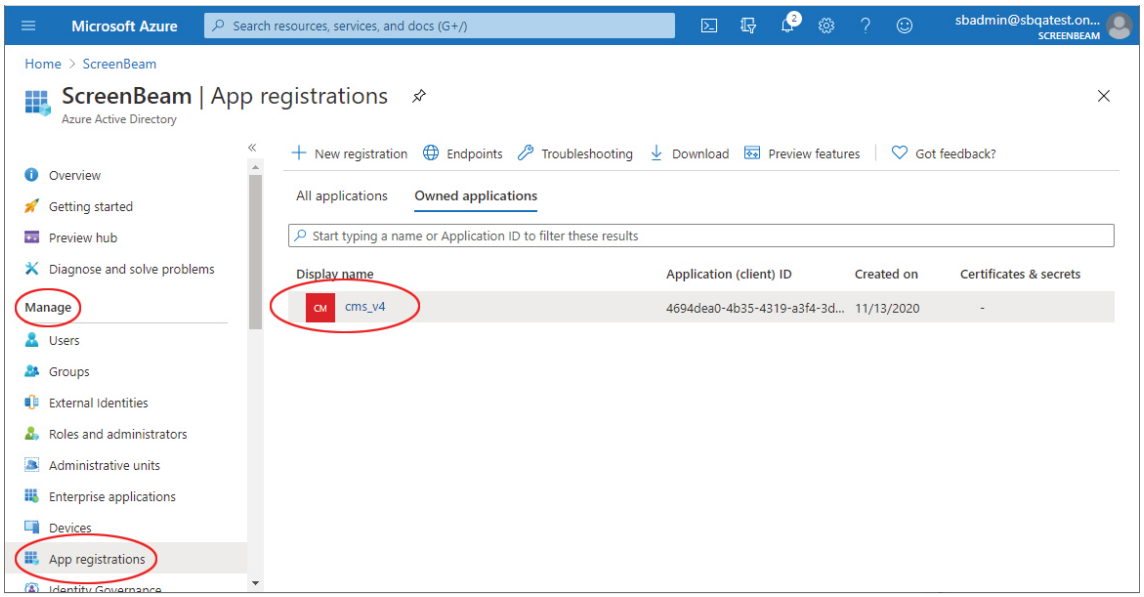


f. Upon successfully processing the request, a detailed page for the newly created app is shown. Note down the **Application (client) ID** and **Directory (tenant) ID**, which will be used for CMS installation.

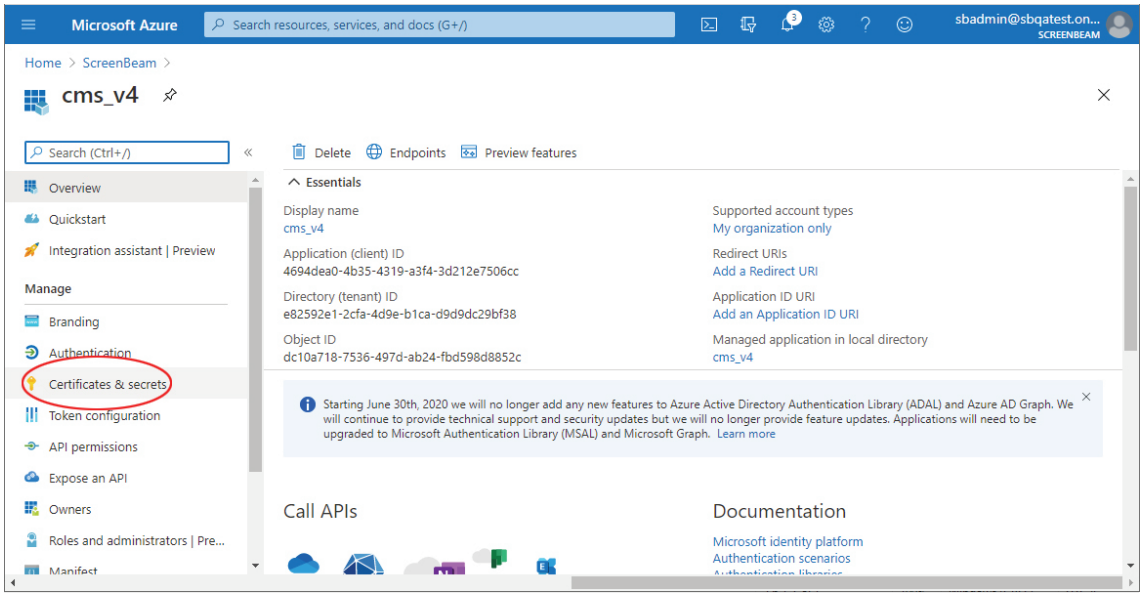


Note: For more information about registering an application, visit https://docs.microsoft.com/en-us/azure/active-directory/develop/quickstart-register-app#register-a-new-application-using-the-azure-portal

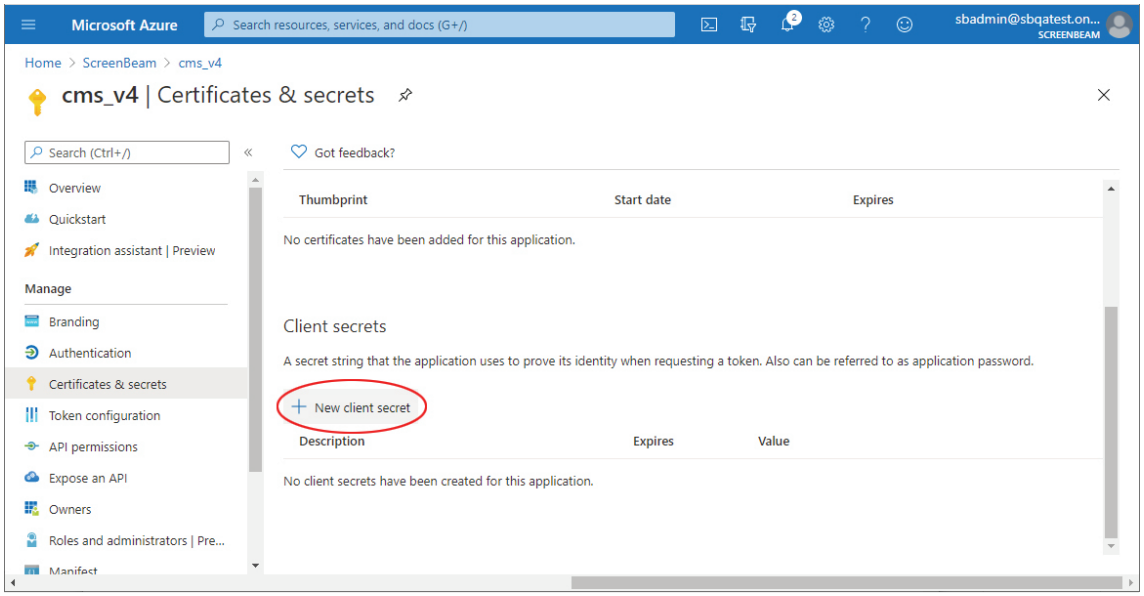
2. Choose how Azure AD authenticates CMS. To do this, follow the procedure below:
   - Using application secret:
     a. Sign into the Azure portal (portal.azure.com) using either a work or school account.
     b. Search for and select **Azure Active Directory**.
     c. Select the Azure AD tenant that you want.
     d. Select **App registrations** under **Manage** in the left menu, and then select the application you created in Step 1 in the right pane.



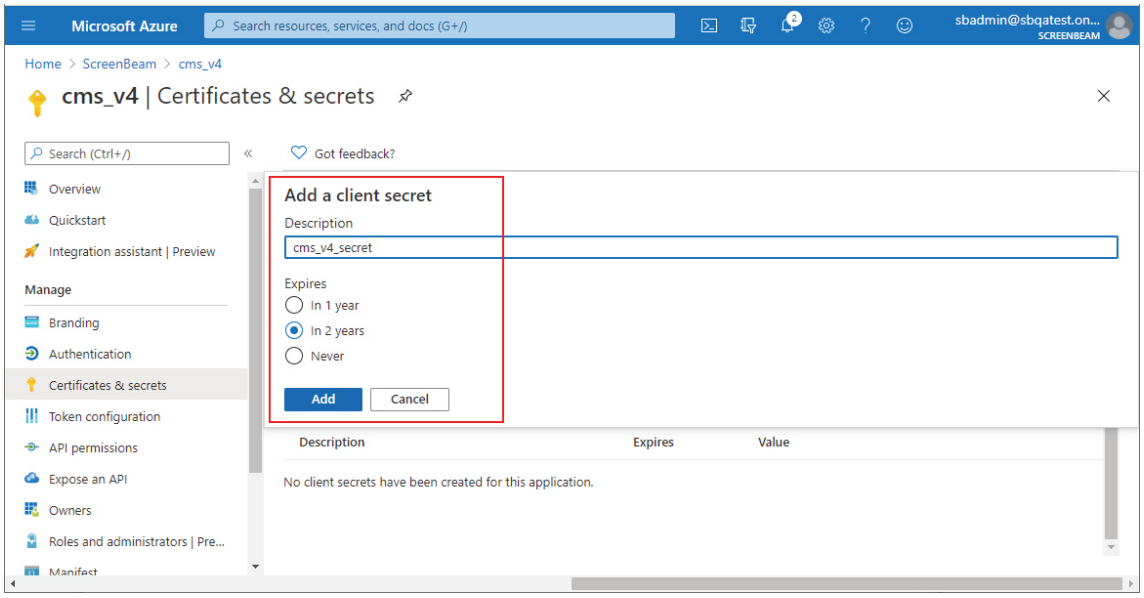
e. The application's setup page appears. Select **Certificates & secrets** in the left menu.



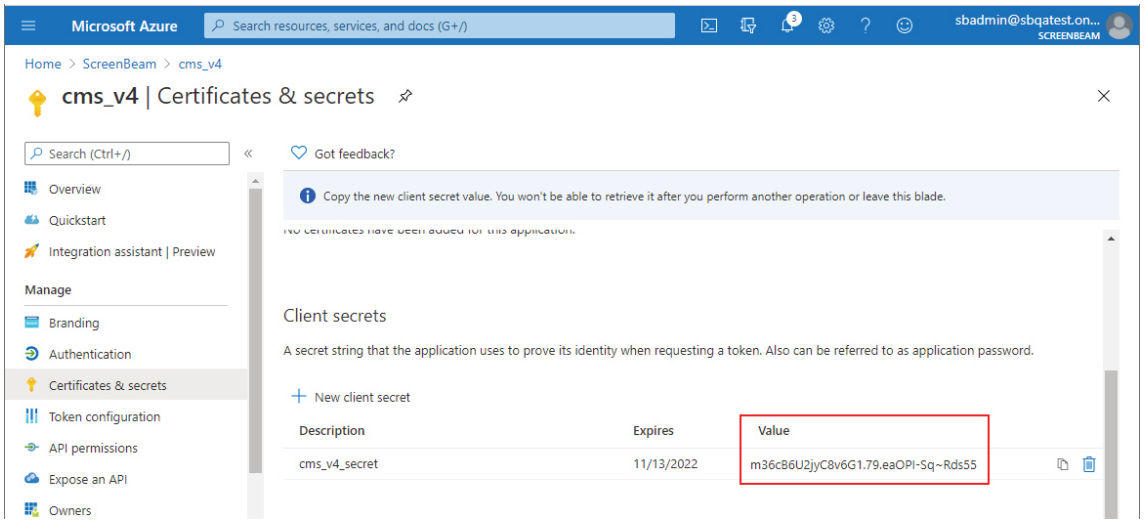
f. The **Certificates & secrets** page appears. Under **Client secrets**, select the **New client secret** button.



g. The **Add a client secret** page appears. Provide a description of the secret, specify a duration and then click **Add**.

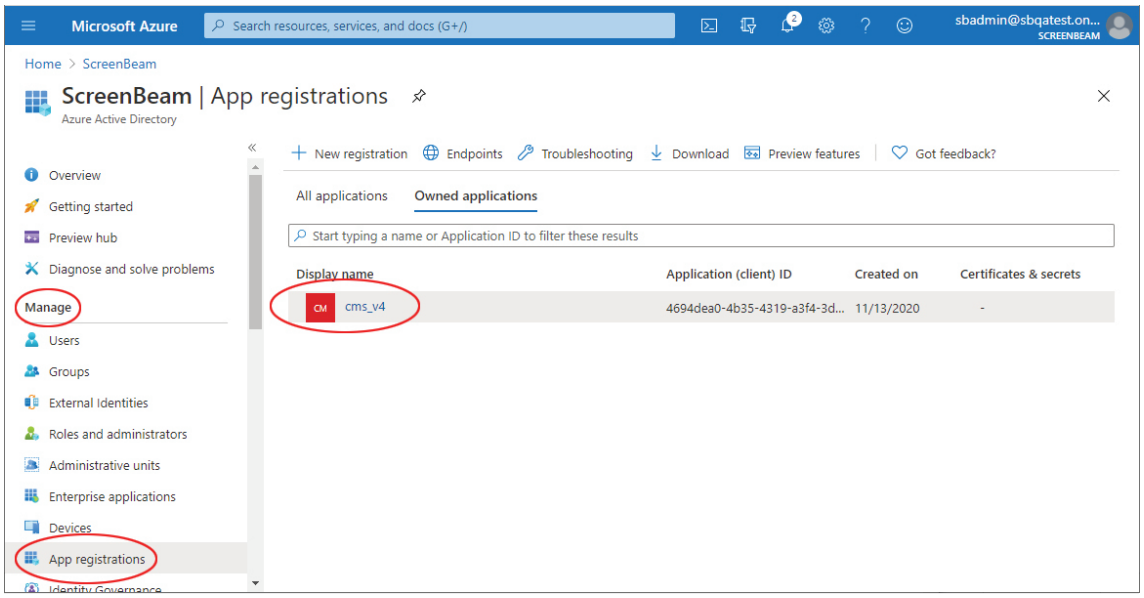


h. Copy the value of the client secret and save it for CMS installation. This value will be partially hidden after it has been added for a short period of time.

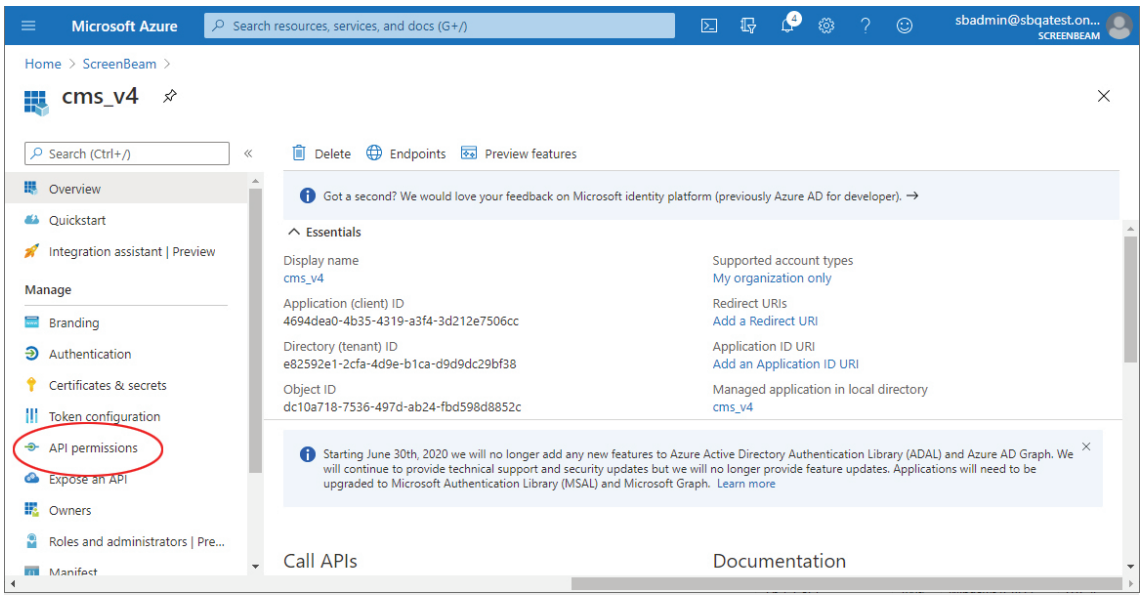


- Using a certificate (not supported currently):

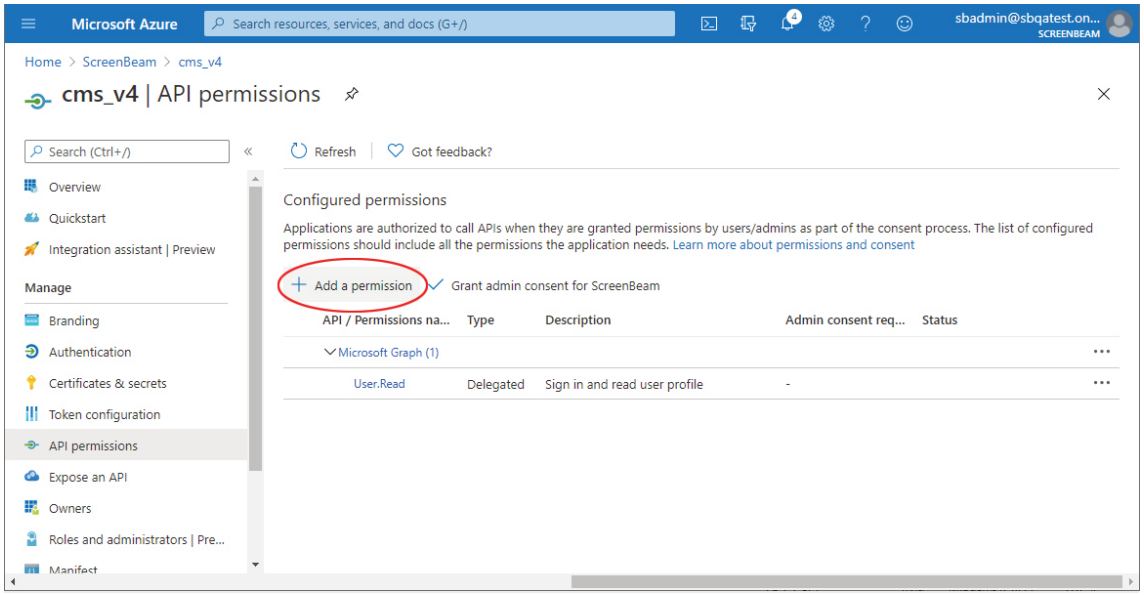
3. Grant CMS permission(s) to access your AAD data. You can choose either Delegated permissions or Application permissions. To do this, follow the procedure below:
   - Delegated permissions:
     a. Sign into the Azure portal (portal.azure.com) using either a work or school account.
     b. Search for and select **Azure Active Directory**.
     c. Select the Azure AD tenant that you want.
     d. Select **App registrations** under **Manage** in the left menu, and then select the application you created in Step 1 in the right pane.



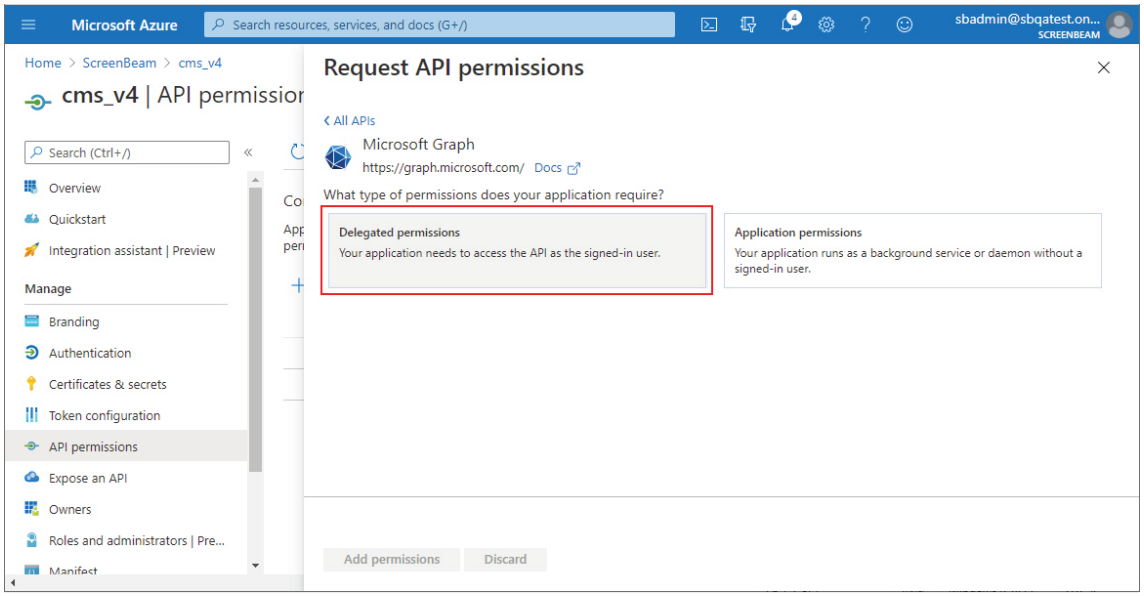
     e. The application's setup page appears. Select **API permissions** in the left menu.



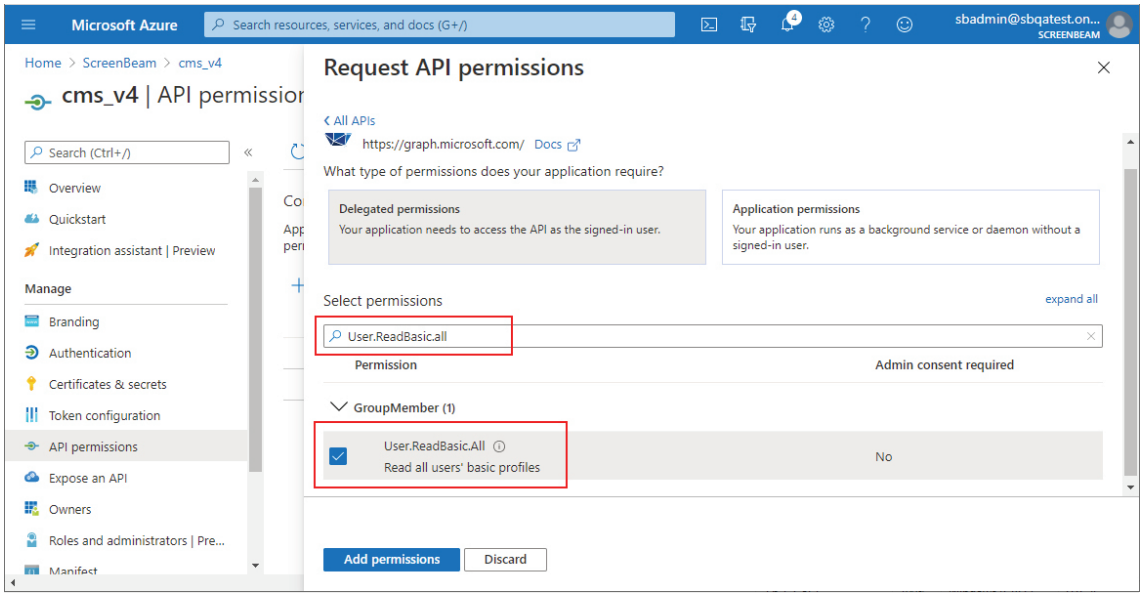
f. The **API permissions** page appears. Click the **Add a permission** button.



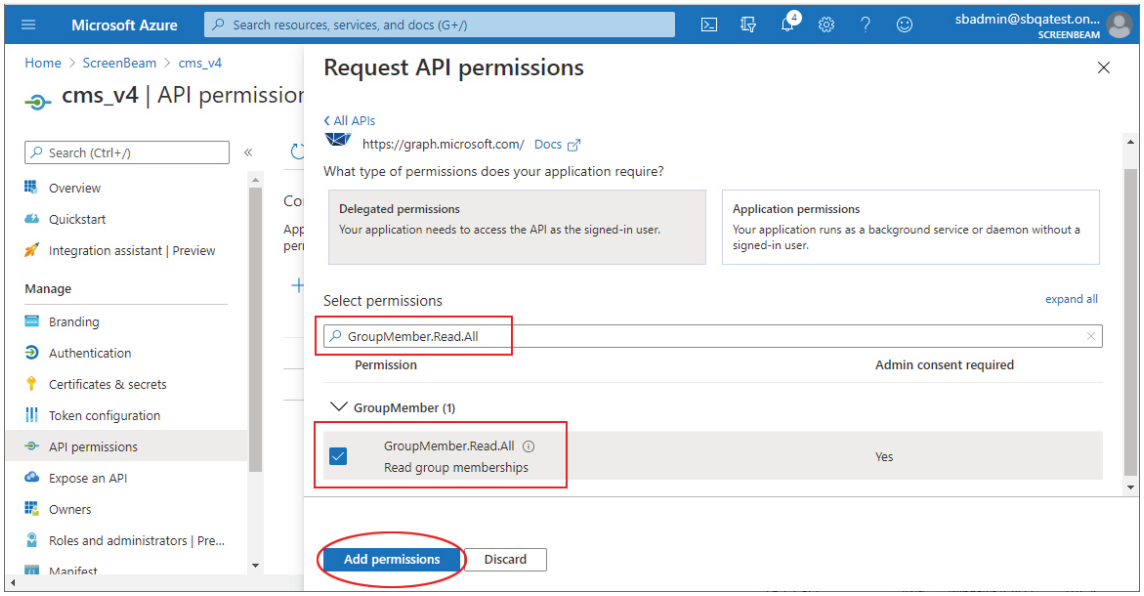
g. The **Request API permissions** page appears. Select **Microsoft Graph** then **Delegated permissions**.



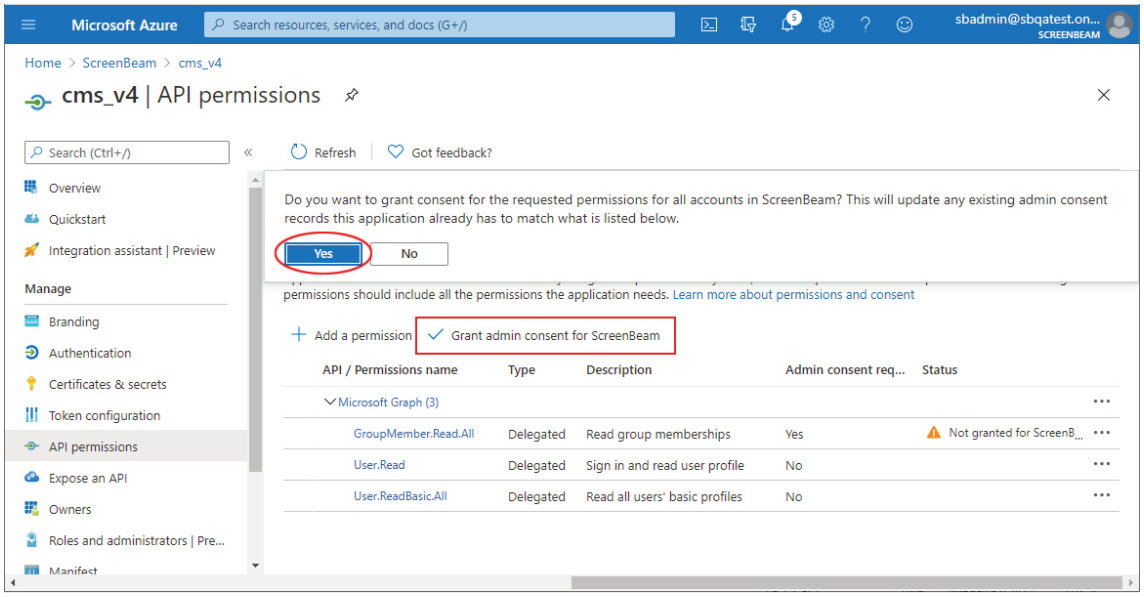
h. Type “User.ReadBasic.All” in the search box and the search will start automatically. Check the box next to “**User.ReadBasic.All**”.



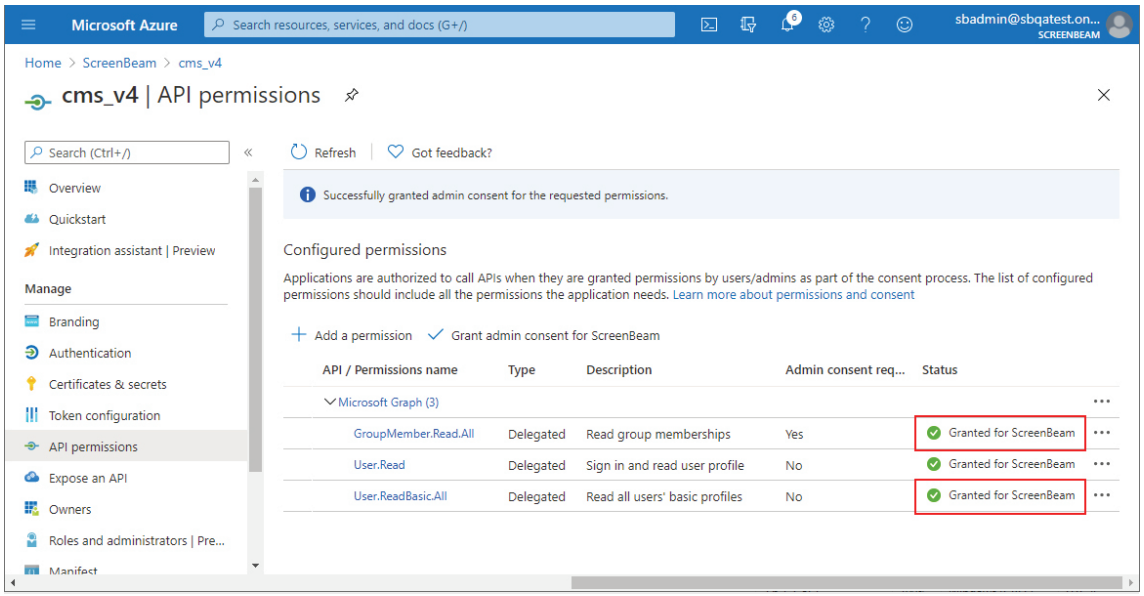
i. Type “GroupMember.Read.All” in the search box and the search will start automatically. Check the box next to “**GroupMember.Read.All**” and then press the **Add permissions** button.



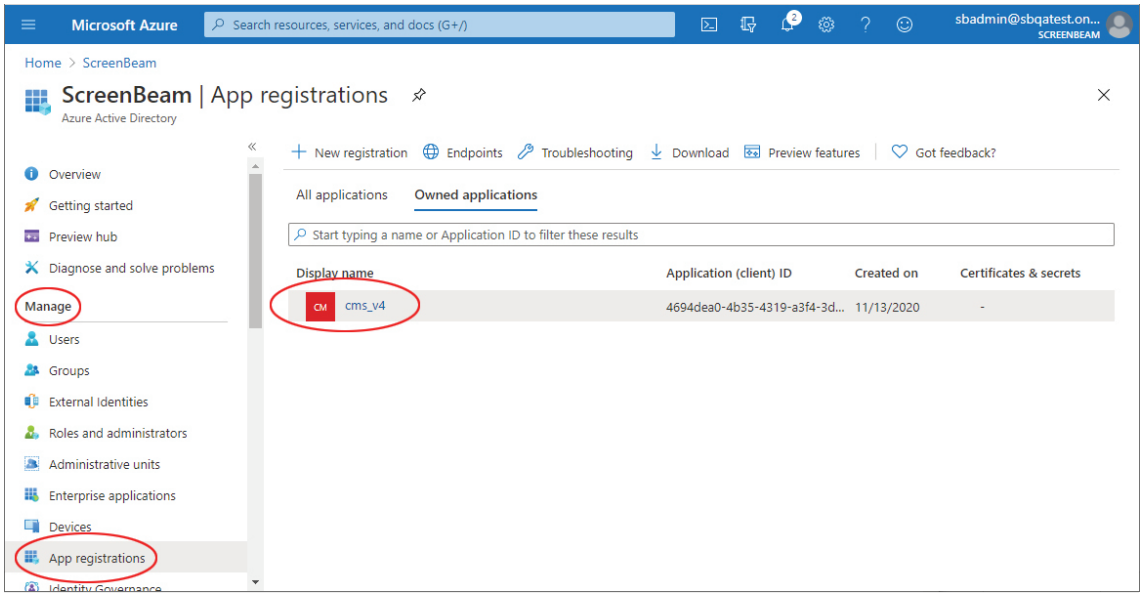
j. Click **Grant admin consent for <directory name>** and select **Yes**.



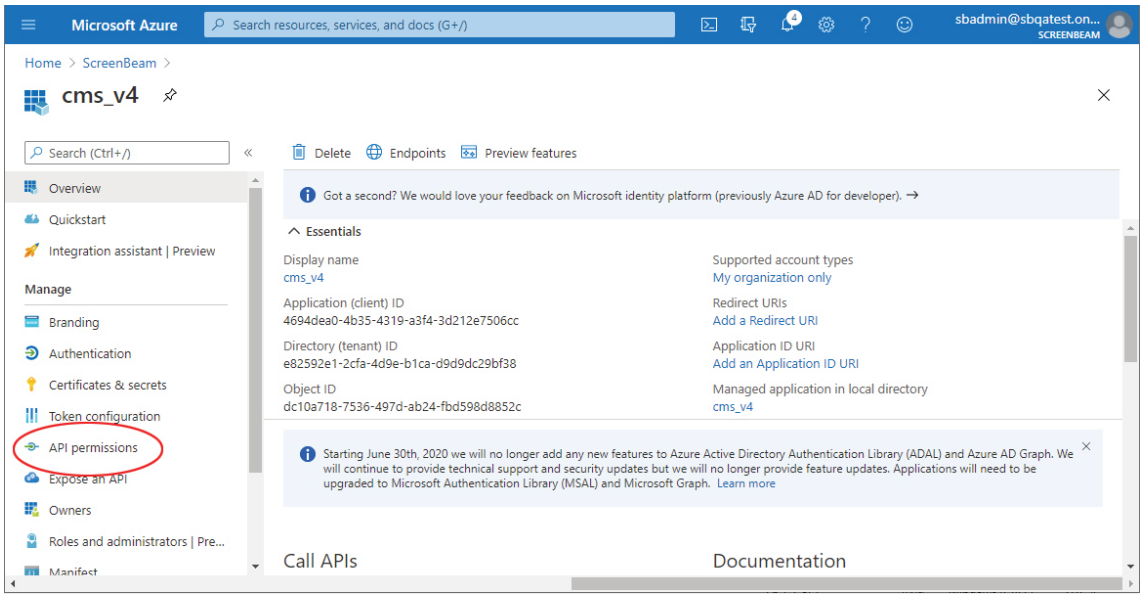
k. Admin consent should be granted to each permission.



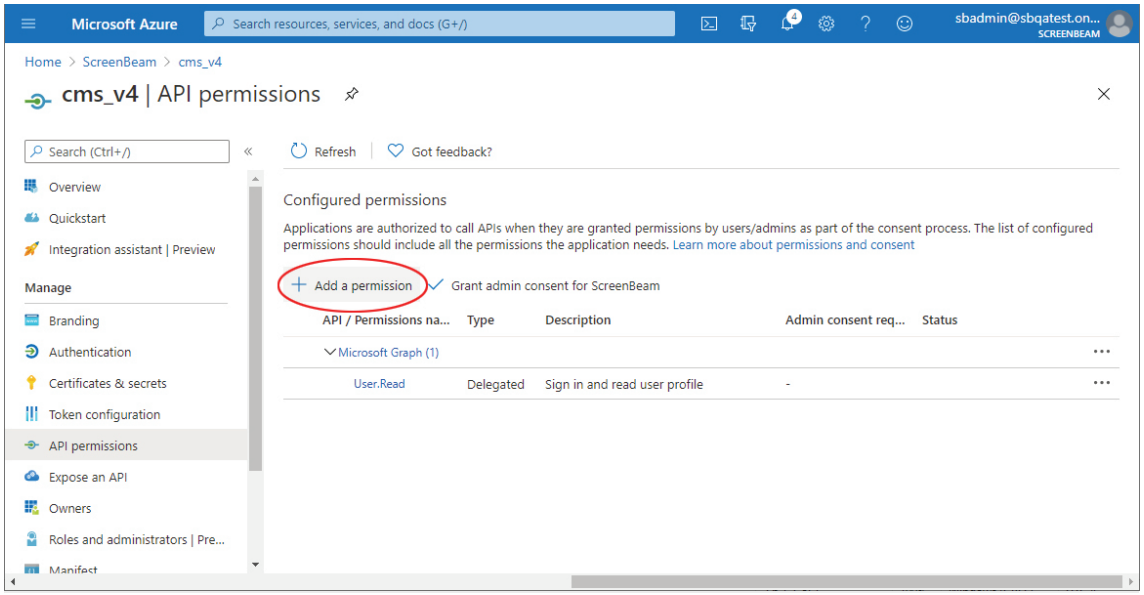
- Application permissions:
    a. Sign into the Azure portal as a **Global Administrator**.
    b. Search for and select **Azure Active Directory**.
    c. Select the Azure AD tenant that you want.
    d. Select **App registrations** under **Manage** in the left menu, and then select the application you created in Step 1 in the right pane.



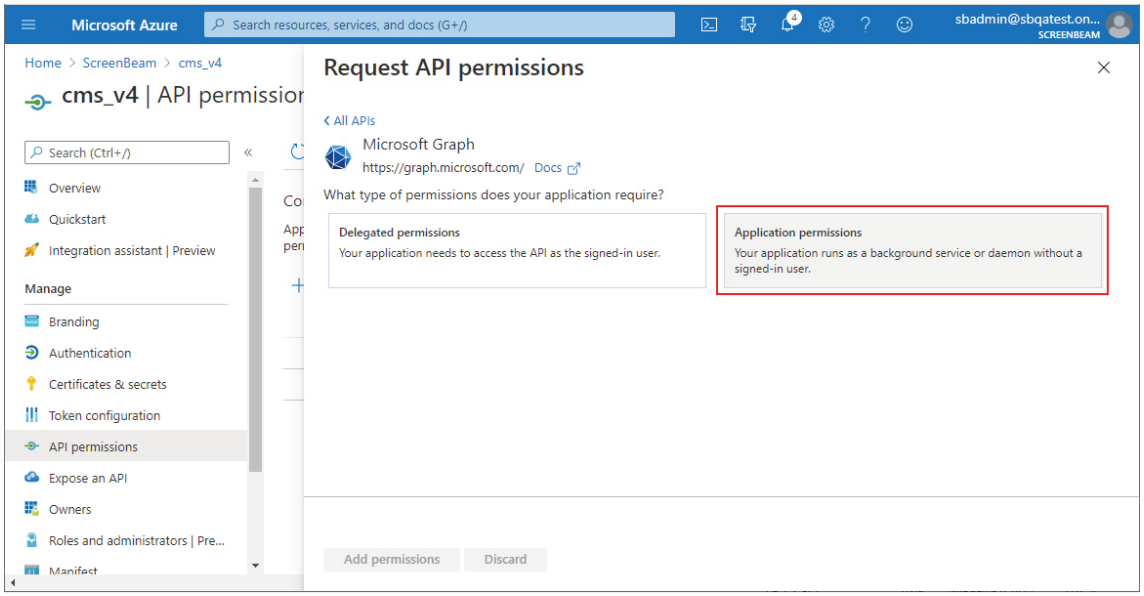
    e. The application's setup page appears. Select **API permissions** in the left menu.



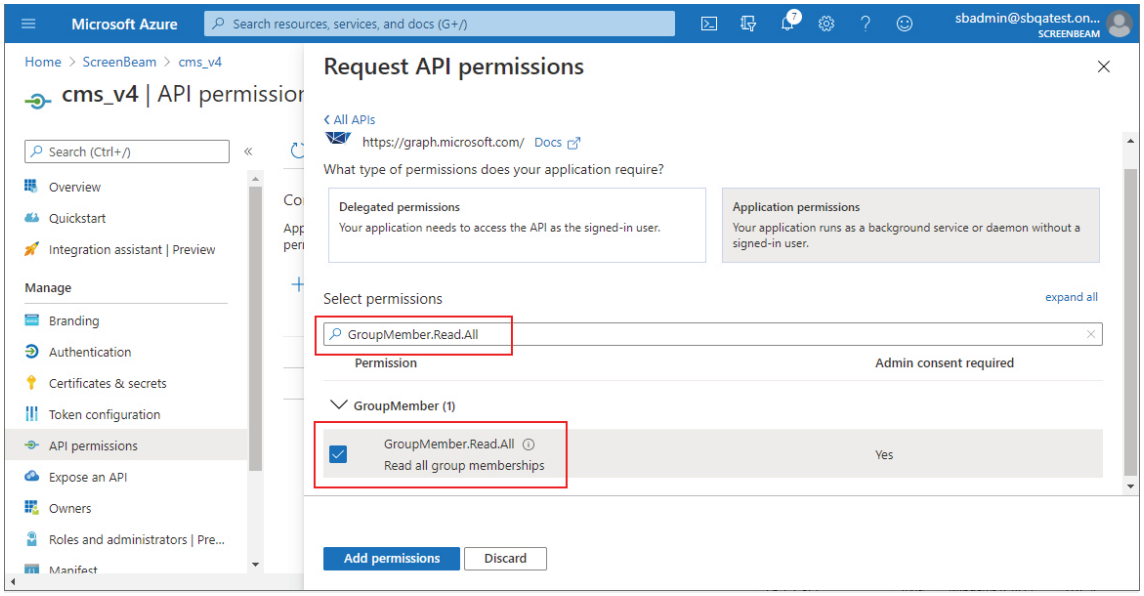
f. The **API permissions** page appears. Click the **Add a permission** button.



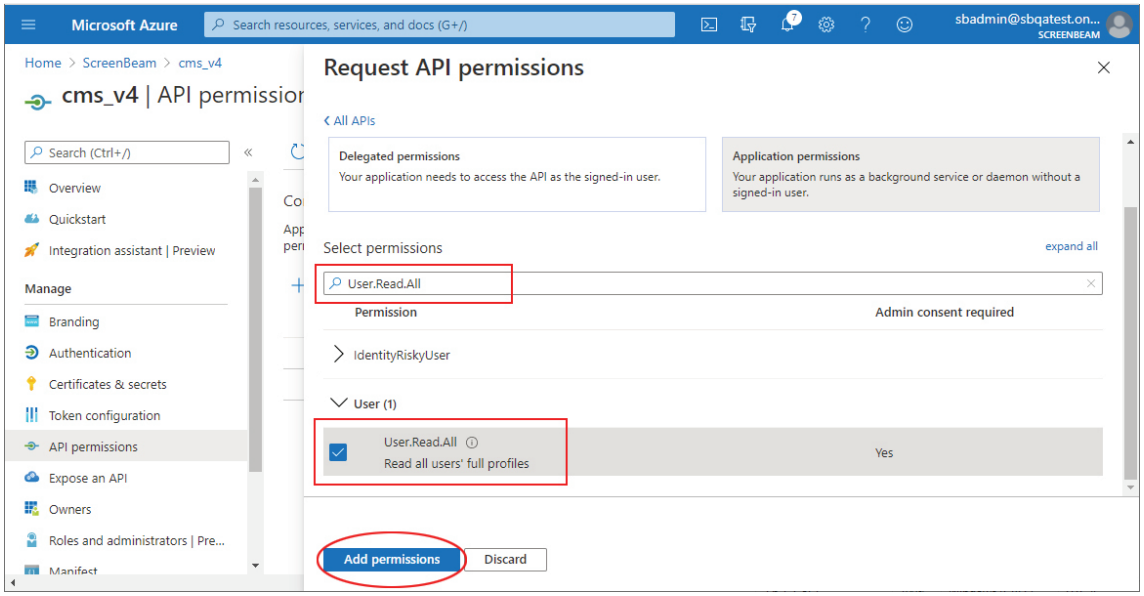
g. The **Request API permissions** page appears. Select **Microsoft Graph** then **Application permissions**.



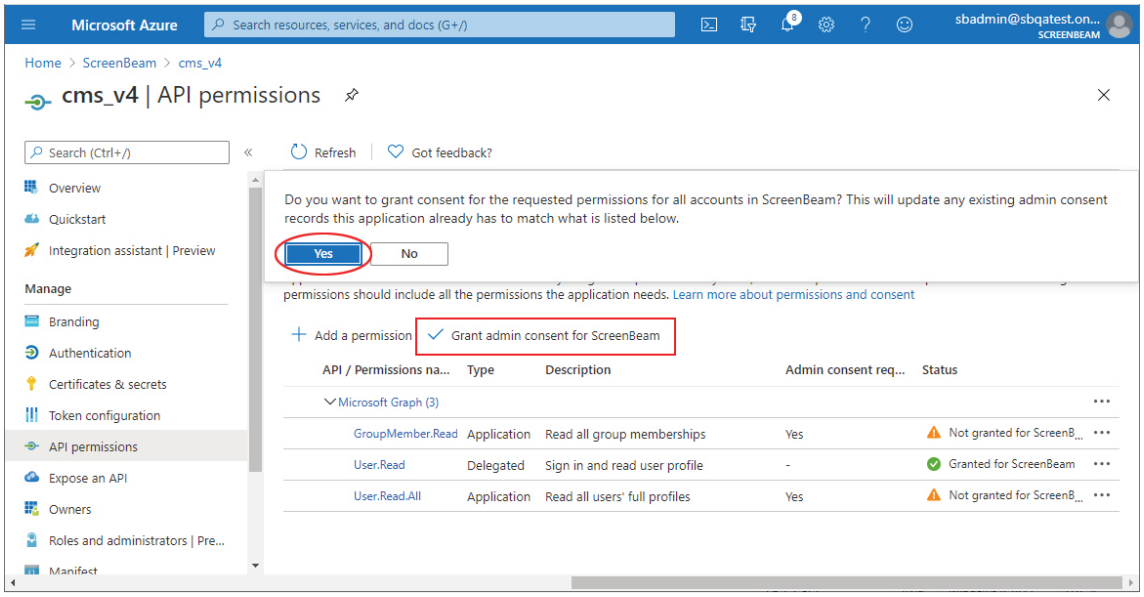
h. Type “GroupMember.Read.All” in the search box and the search will start automatically. Check the box next to “**GroupMember.Read.All**”.



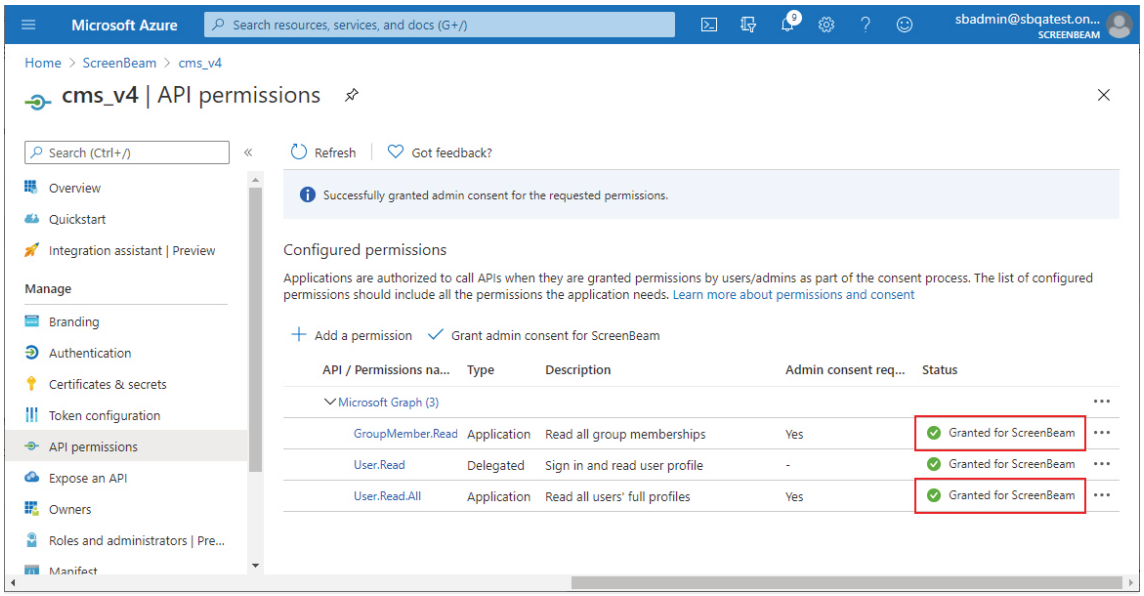
i. Type “User.Read.All” in the search box, and then check the box next to “**User.Read.All**”. Click the **Add permissions** button to add the two selected permissions.



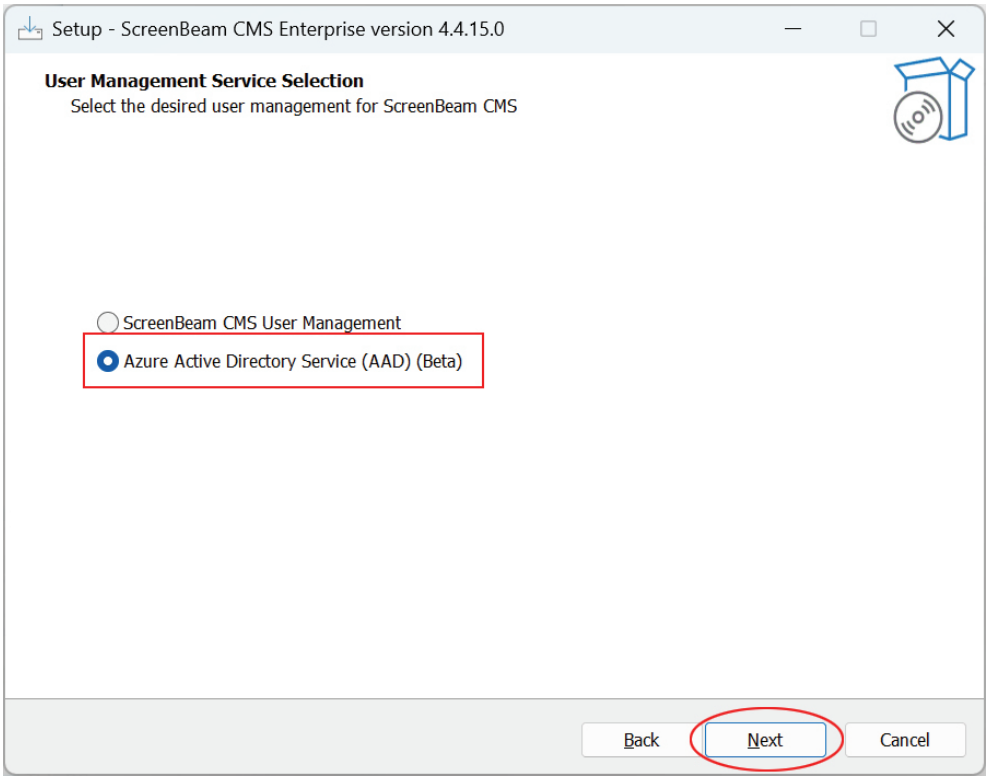
j. Click **Grant admin consent for <directory name>** and select **Yes**.



k. Admin consent should be granted to each permission.

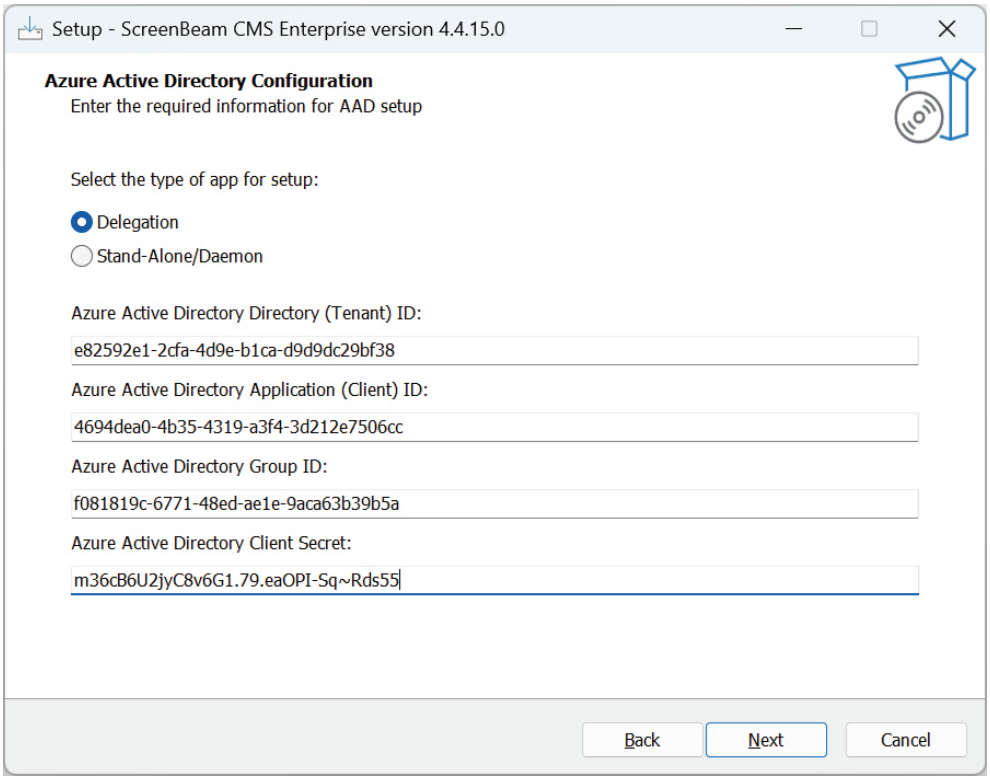


4. Install ScreenBeam CMS.
   a. Start ScreenBeam CMS installation and choose **Azure Active Directory Service (AAD) (Beta)** when the **User Management Service Selection** page appears, and click **Next** to continue.

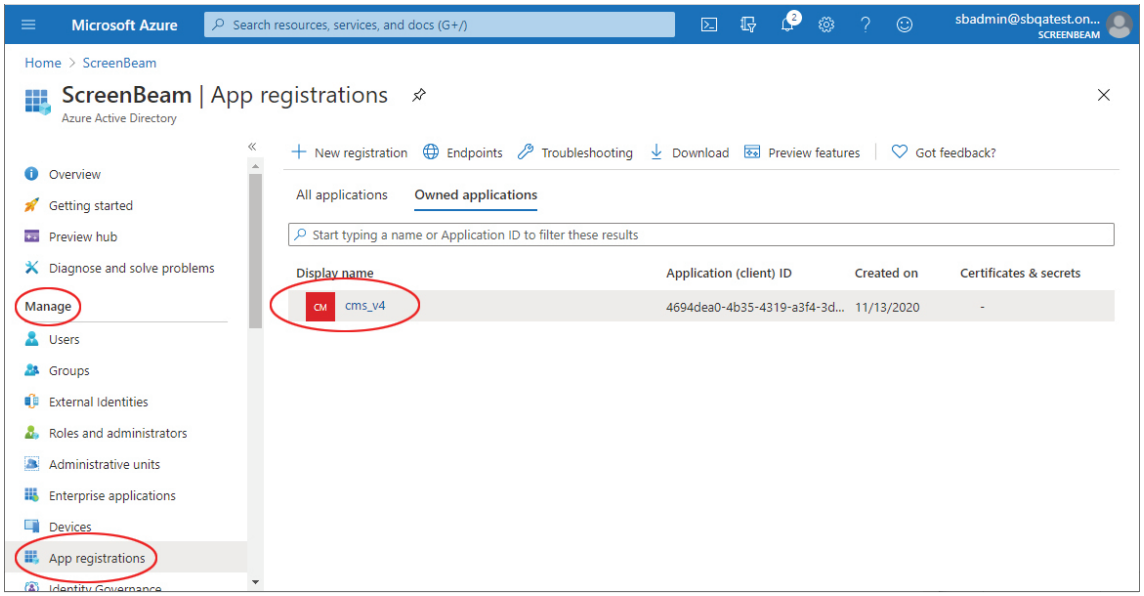


b. Specify the following parameters on the **Azure Active Directory Configuration** page that appears.

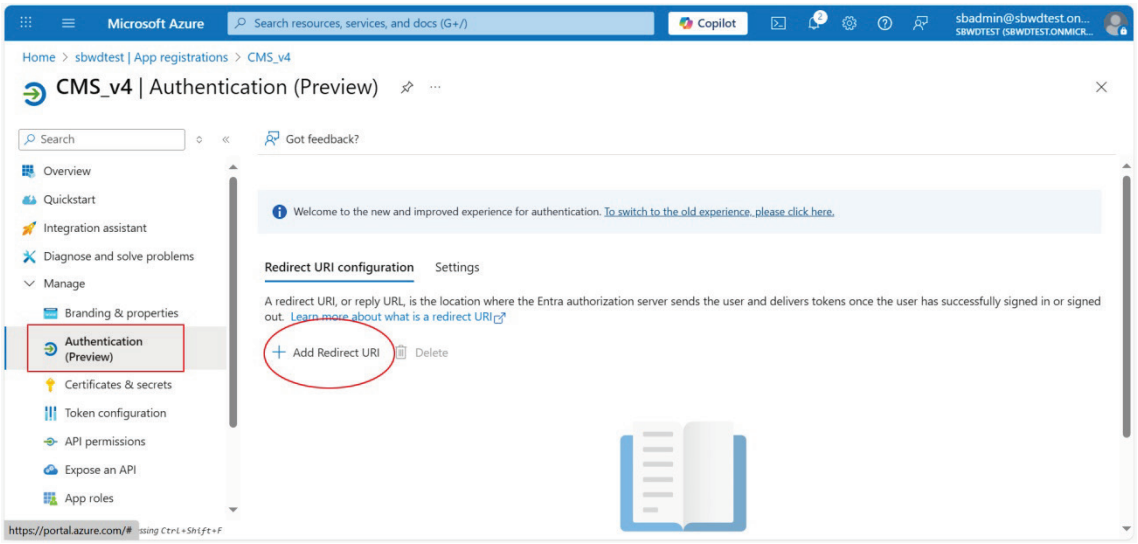
- Choose a permission type grant to CMS.
  Select the option matching your selection in Step 3.
  - Delegated permissions (Delegation)
  - Application permissions (Stand-Alone/Daemon)
- Fill in **Tenant ID, Application Client ID** from App Registration in Step 1, **Group ID** from a preset security group, and the Client secret value created in step 2.



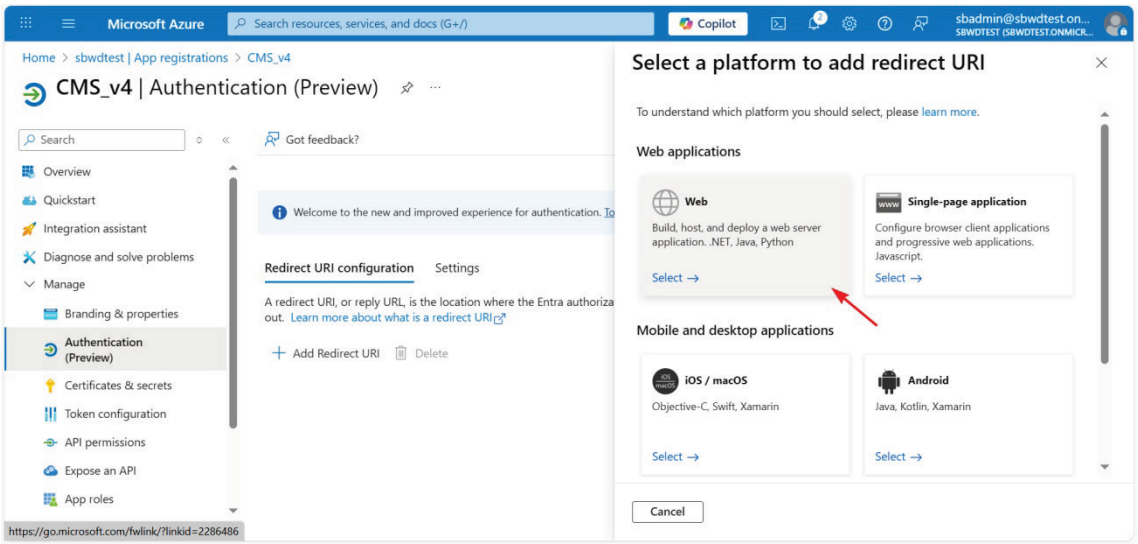
5. Link installed CMS instance to Azure AD.
   Before using the Azure AD users to manage CMS, we need to link the CMS instance to the application registered on Azure in Step 1.
   Note: The base URL of the installed CMS instance must be made available.
   a. Sign into Azure portal using the same Azure account used in Step 1. (An admin account with higher privilege can also be used.)
   b. Set your portal session to the Azure AD tenant that you want.
   c. Search for and select **Azure Active Directory**.
   d. Select **App registrations** under **Manage** in the left menu and select the application you created in Step 1 from the list.



   e. Select **Authentication** under **Manage** in the left menu, and then select the **Add Redirect URI** button under **Redirect URI configurations**.

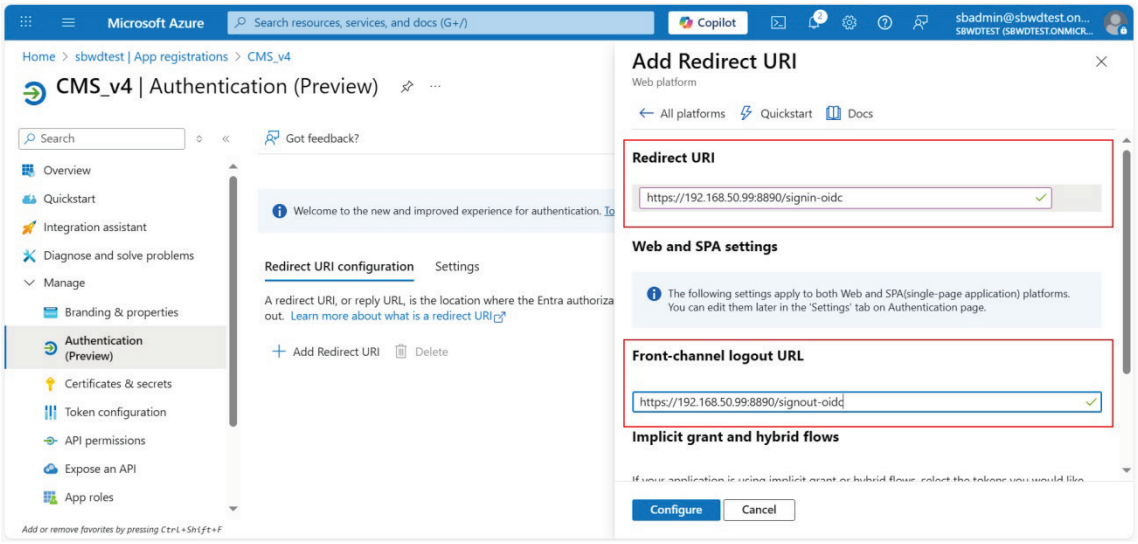


f. The **Select a platform to add redirect URI** window appears. Select **Web** from the **Web applications** section.

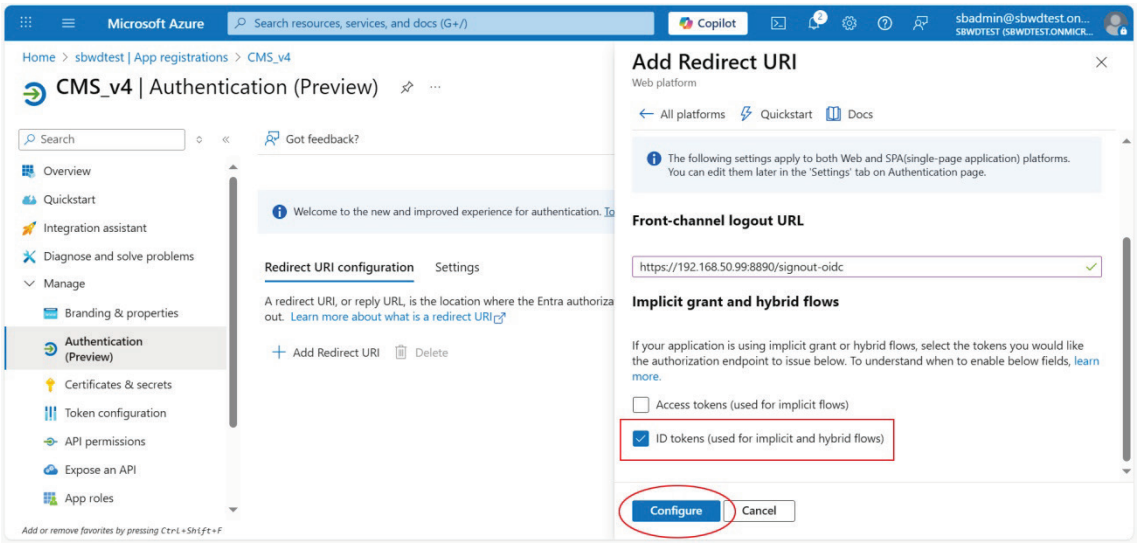


g. The **Add Redirect URI** window appears.

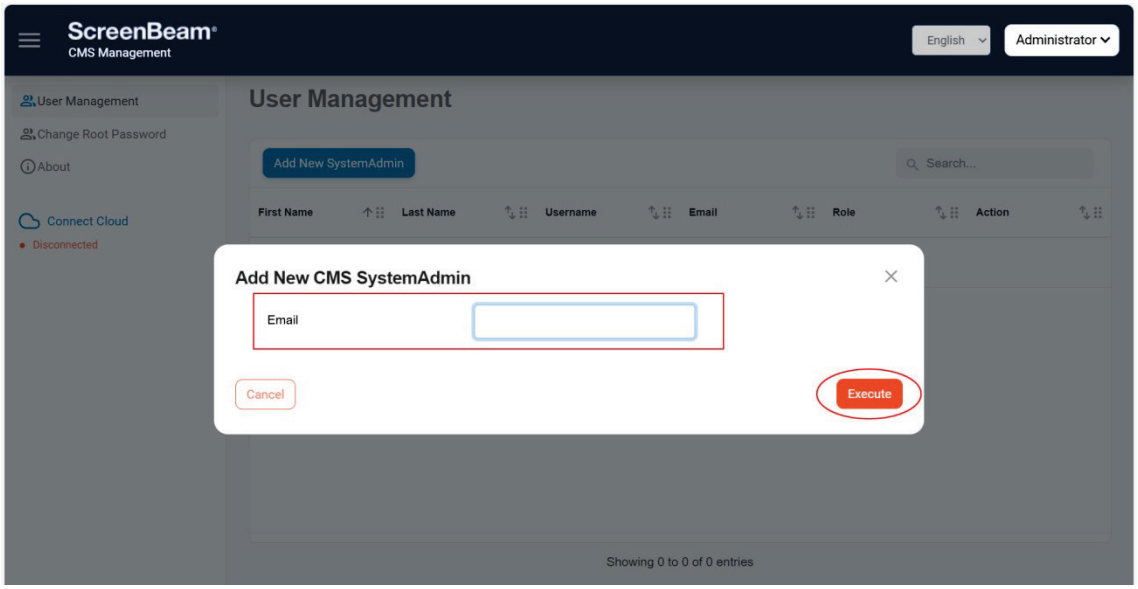
- Fill in **Redirect URI** by combining *https:// + CMS server IP + Identity Server port number (default: 8890)* + /signin-oidc.
  For example, if you access CMS from your browser using https://1.1.1.1:xxxx, the Redirect URL will be *https://1.1.1.1:8890/signin-oidc*.
- Fill in **Front-channel logout URL** by combining *https:// + CMS server IP + Identity Server port number (default: 8890)* + /signout-oidc.
  For example, if you access CMS from your browser using https://1.1.1.1:xxxx, the Logout URL will be *https://1.1.1.1:8890/signout-oidc*.



h. Under the **Implicit grant and hybrid flows** section, check **ID tokens (used for implicit and hybrid flows)**, and then click **Configure**. The installed CMS instance will be linked to the registered application on Azure AD.

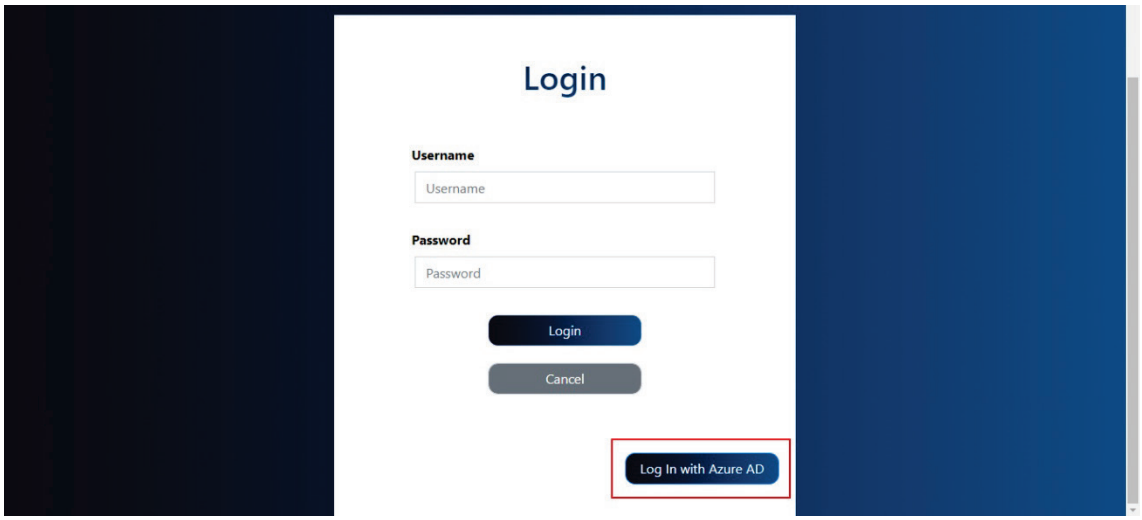


6. Set up CMS System Admin.
   - When the **Delegated permissions** setup is selected:
     Since CMS does not have permission to access AAD data, at least one of the users must be assigned CMS System Admin role before CMS can enable System Admin functionalities to any users. Follow below steps to add a System Admin user to CMS:
     a. Log into CMS using the root account “Administrator”.
     b. Select **User Management** in the left menu, and then select the **Add new SystemAdmin** button.
     c. Enter your work or school email, then click **Execute** to add the user.

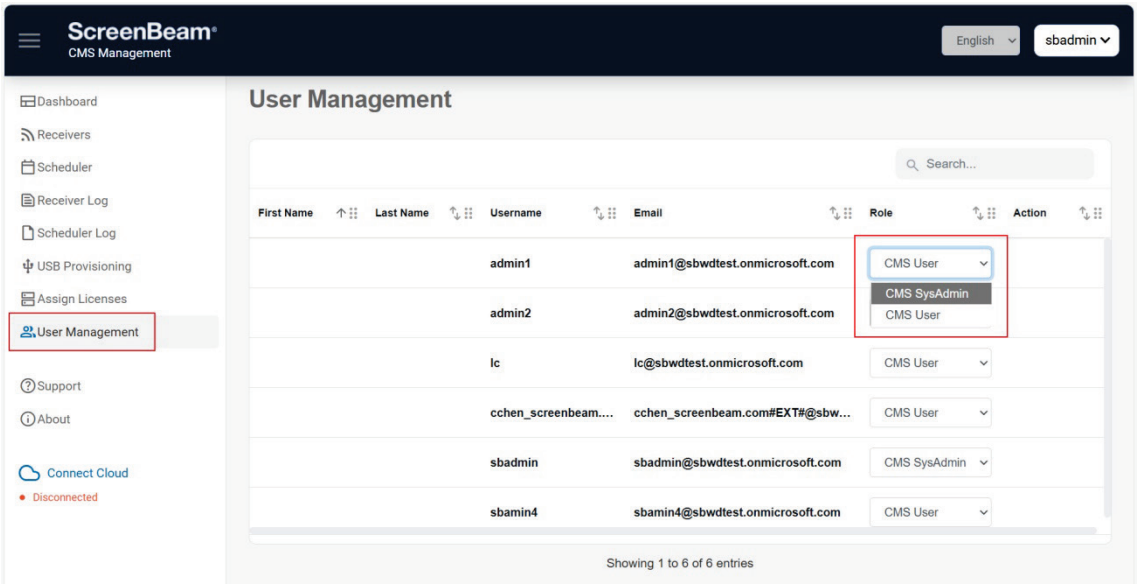


   d. A SystemAdmin user will be added to CMS and the username will show on the list.

e. Click **Log In with Azure AD**, and log into CMS with your work or school email that is added to CMS as a SystemAdmin user。

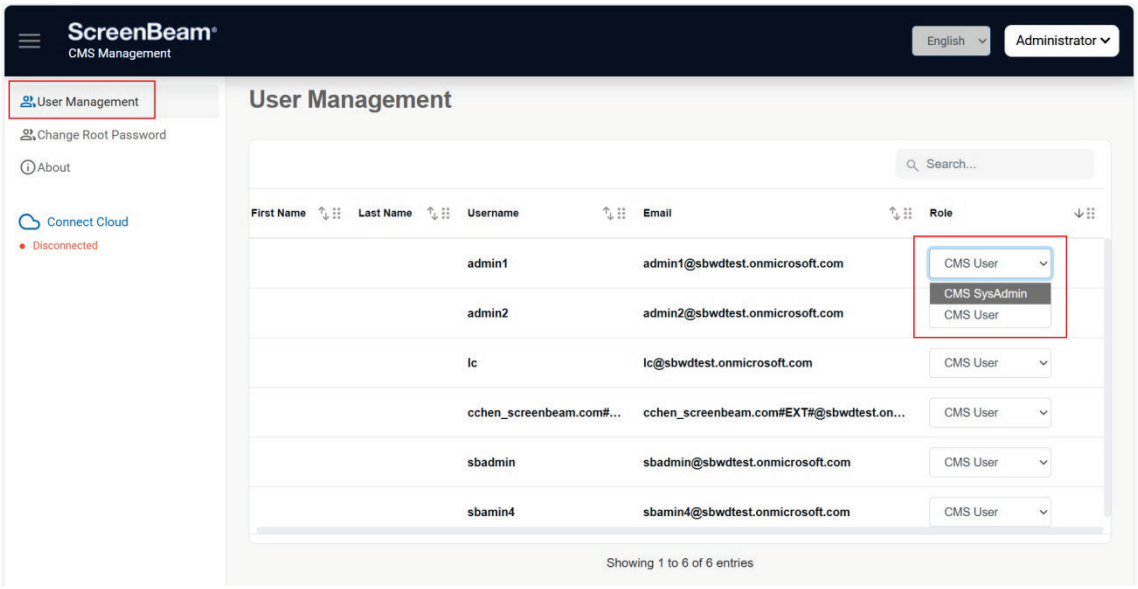


f. Go to the **User Management** page, where the users that are assigned to the AAD security group will be shown. Now you can manage your CMS users' roles.



Note: The **User Management** page will display only the users assigned to the security group that is specified during CMS installation.

- When the **Application permissions** setup is selected:
  a. Log into CMS using the root account “Administrator”
  b. Select **User Management** and a list of users within assigned AAD group will be shown.
  c. Each user’s role can be updated within the list.



Note: The **User Management** page will display only the users assigned to the security group that is specified during CMS installation.

7. (Optional) Restrict CMS access to a set of users in your organization.

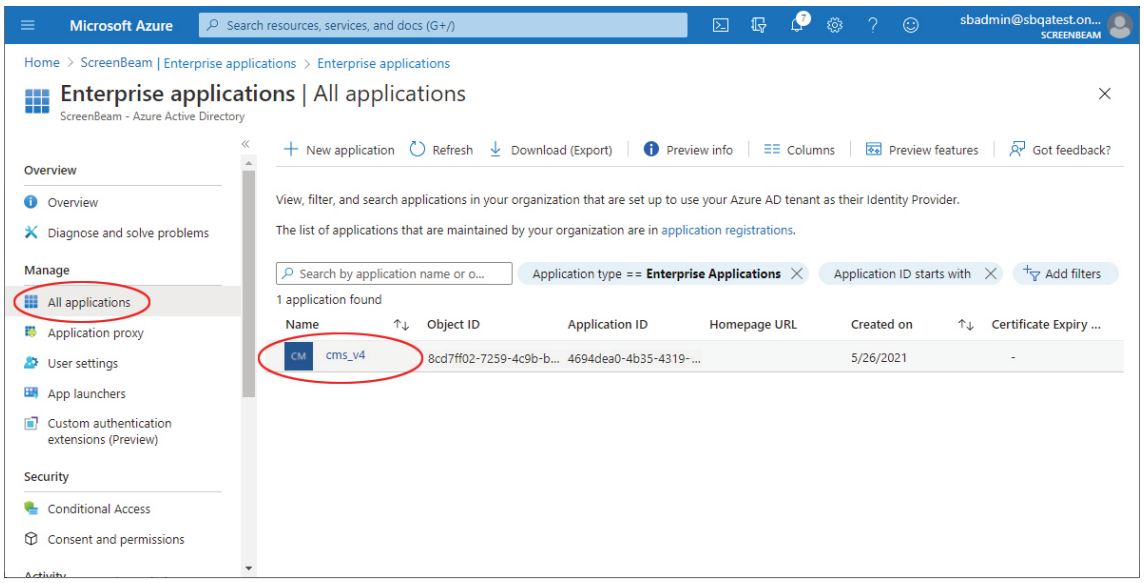
By default, any users within the organization can sign in and access CMS once the app has been set up and granted permissions. In some cases, the admin might want to restrict CMS access to a set of users. To do this, follow the procedure below:

A. Enable sign-in restriction.

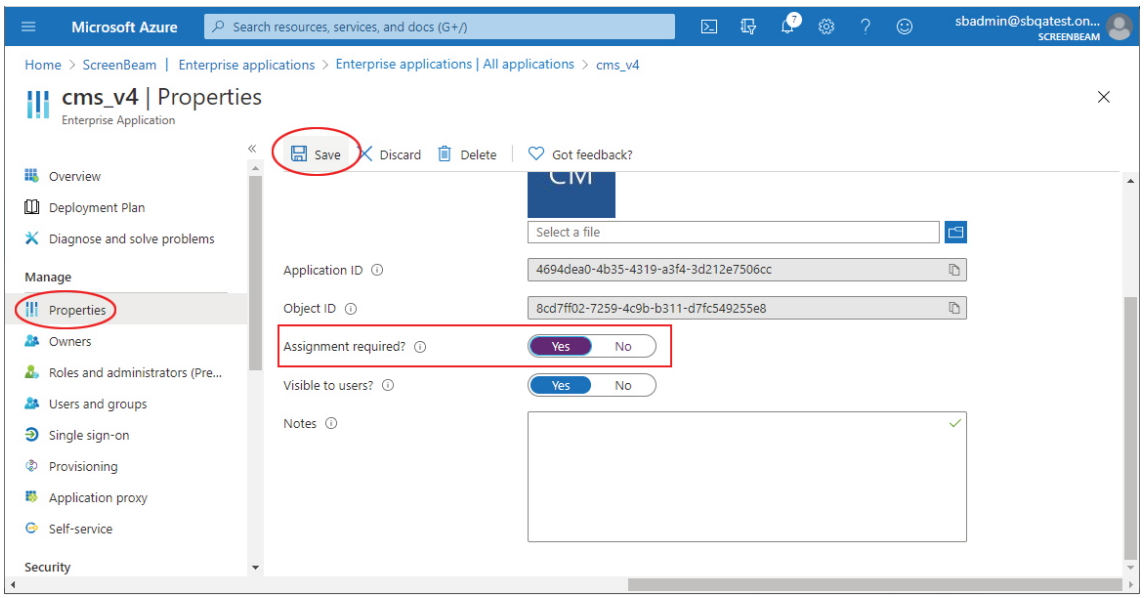
a. Sign into the Azure portal as a *Global Administrator.*

b. Select **Azure Active Directory** then **Enterprise applications**.

c. Select **All applications** on the left menu, and then select the CMS application registered in Step 1.



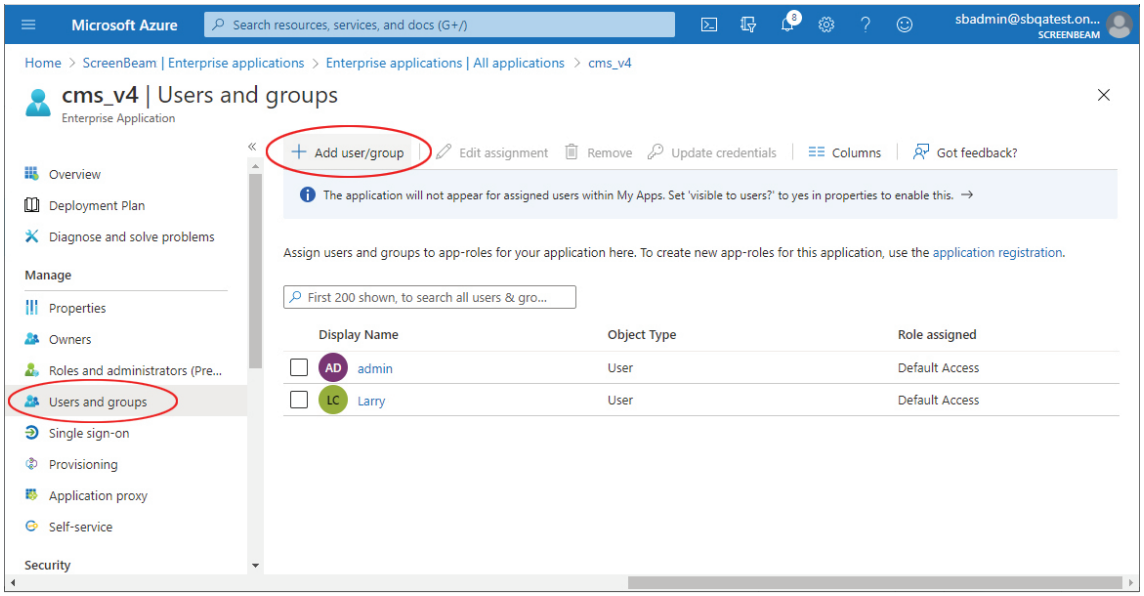
d. Select **Properties** under **Manage** in the left menu, locate **Assignment required?** and switch its setting to **Yes**. This will prevent unassigned users from logging into CMS. Click **Save** to save your configuration change. Learn more



B. Assign users to CMS.

a. Follow steps a to c from 7A.

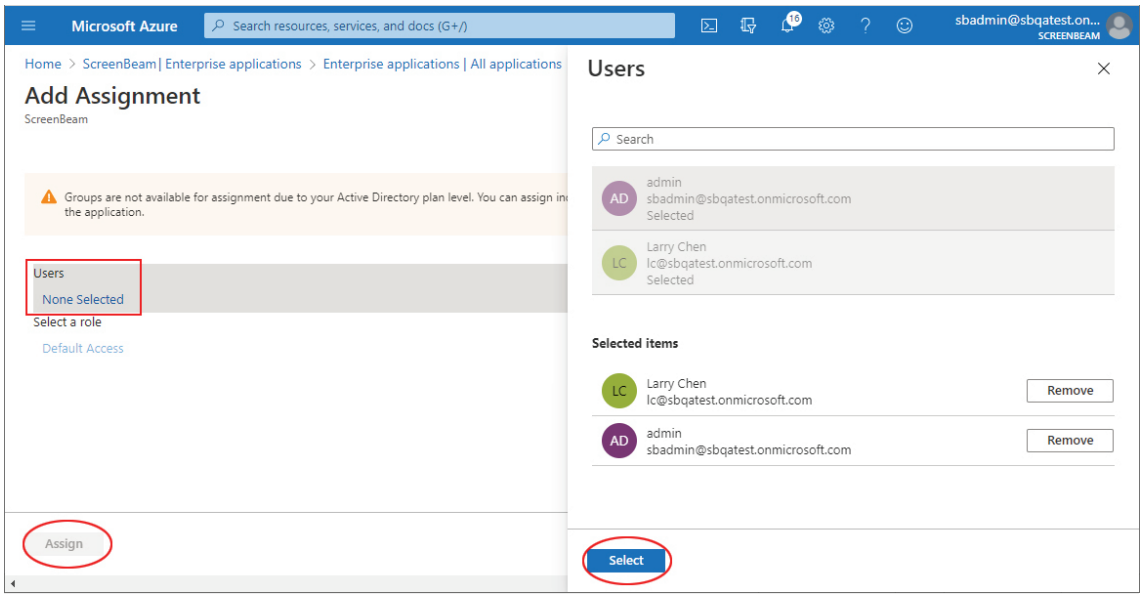
b. Select **Users and groups** on the left navigation menu, and then click the **Add user/group** button on the right pane.



c. Select the **Users** selector on the **Add Assignment** pane that appears, and then select users and/or groups in the Users panel that appears. You can search users or groups by name in the Search box. Multiple users and groups can be selected, and your selections will appear under **Selected items**.

Note: The group assignment is only available with Azure AD premium subscription. Learn more.

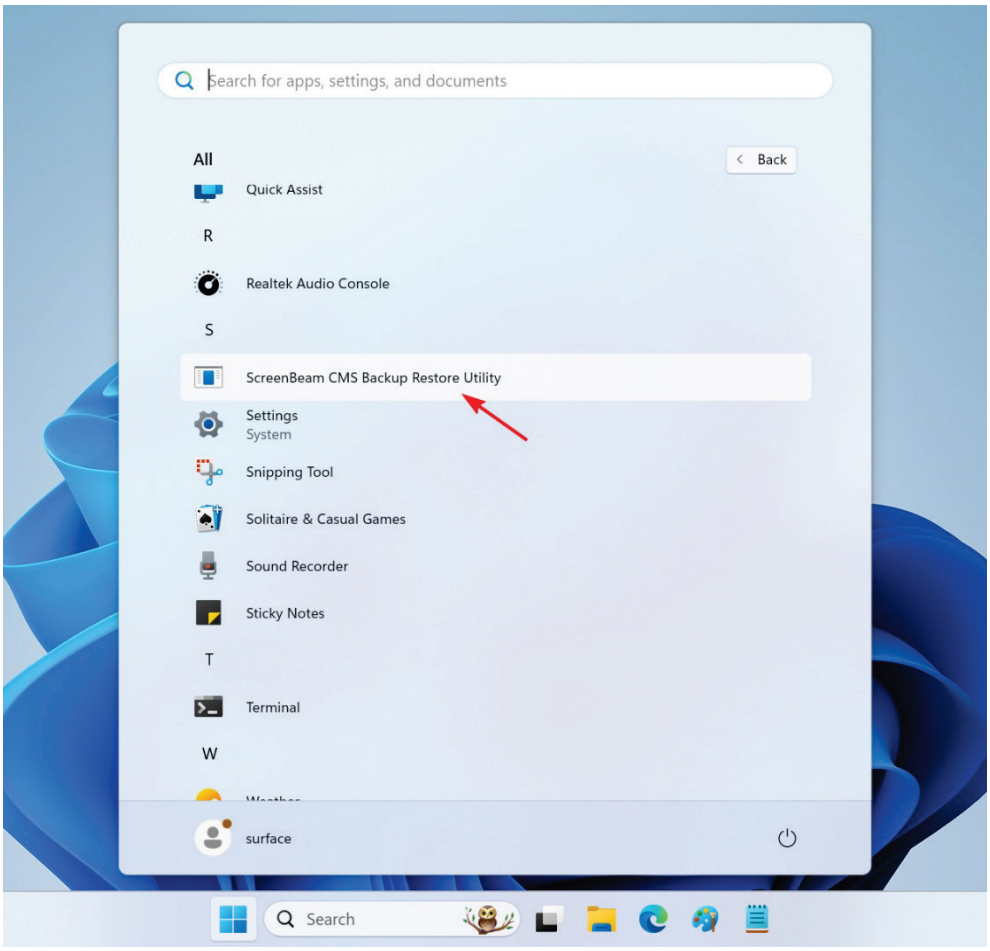
d. Once you are done selecting the users and groups, press the **Select** button. Then click **Assign** to add the selected users and groups.



Appendix II Backing up and Restoring ScreenBeam CMS

ScreenBeam CMS V4 supports data backup and restoration. Currently, only local data can be backed up and restored. AAD or external databases can't be backed up or restored.

ScreenBeam CMS Backup Restore Utility is included in the ScreenBeam CMS installation. After the installation, a shortcut to this Utility is created in the ScreenBeam folder on the Start menu.



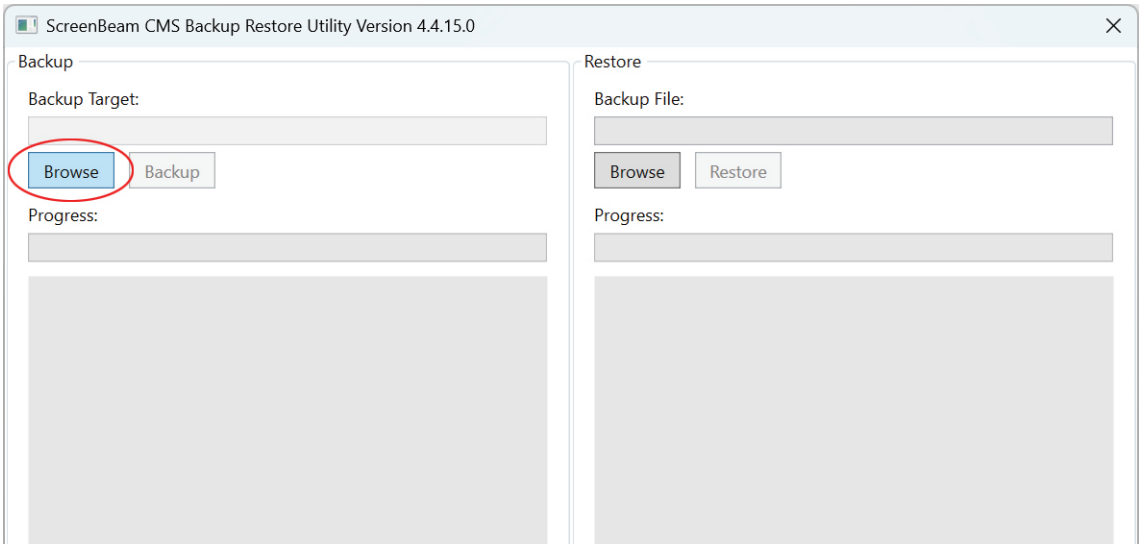
Users can also find the utility in the default installation directory: C (*or the system disk*):\Program Files\ScreenBeam\cms\backupRestoreUtil\cms-v4-backup-utility.exe. By default, it is installed in the **Program Files** folder. If you have changed the installation directory, go to the one you have defined, that is *your installation directory* \ScreenBeam\cms\backupRestoreUtil\cms-v4-backup-utility.exe.

Backing up ScreenBeam CMS

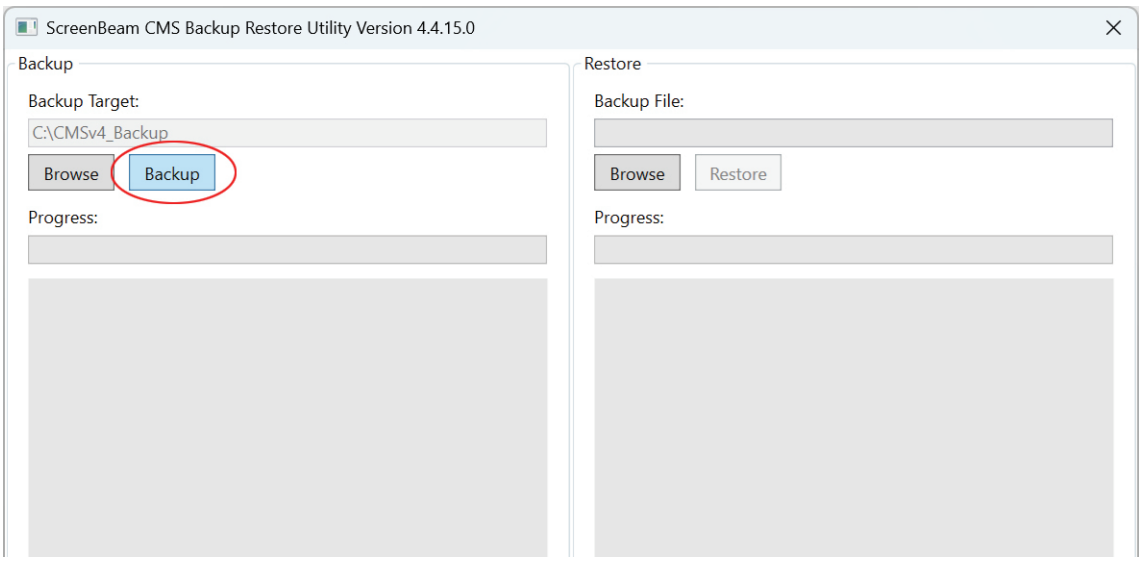
Follow the procedure below to back up ScreenBeam CMS:

1. Start ScreenBeam CMS Backup Restore Utility.

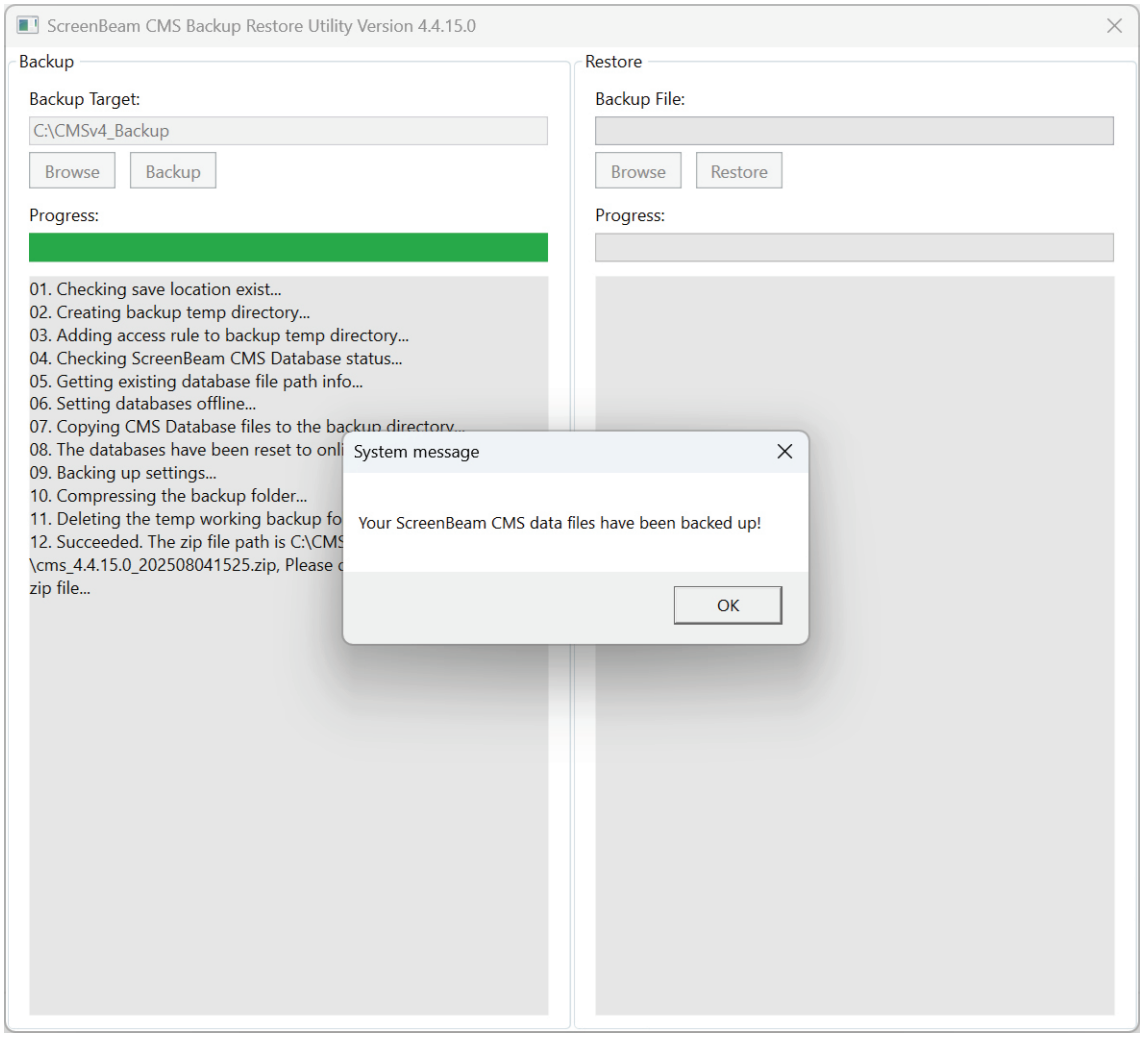
2. Click the **Browse** button and then choose a directory to save the CMS backup file. The chosen path will be displayed on the **Backup Target** box.



3. Click the **Backup** button, and a message box will appear. Click **Yes** to start the backup process.



4. The backup process will be completed in several minutes.
   Note: Don’t close the backup restore utility before the backup process is completed.



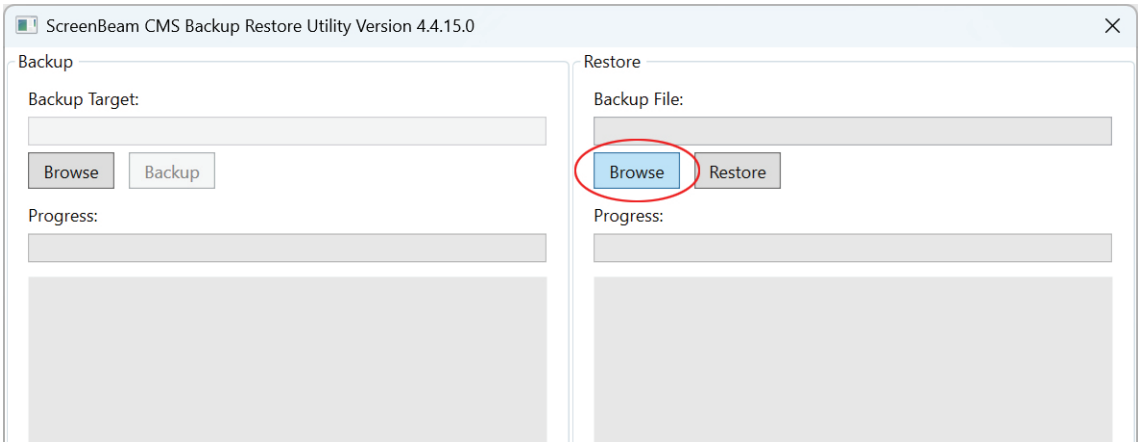
Click **OK** and close the utility. Now, the CMS is backed up.

Restoring ScreenBeam CMS

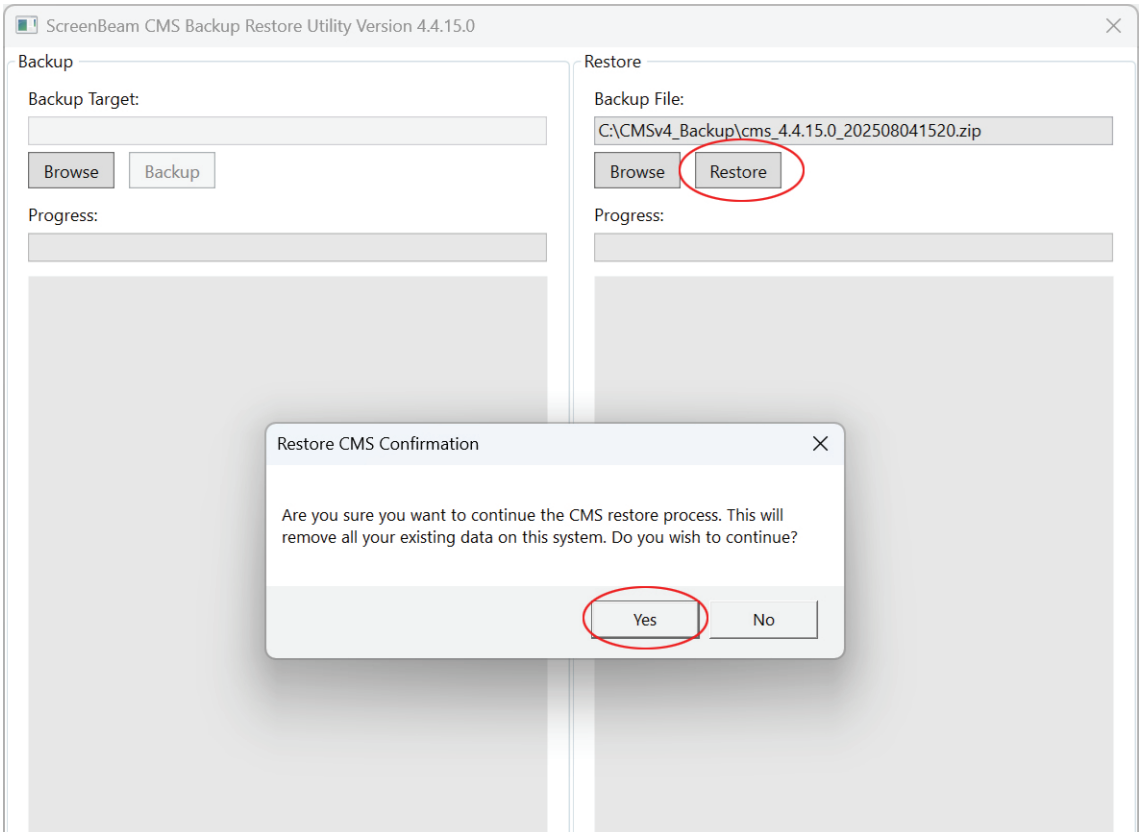
Follow the procedure below to restore your ScreenBeam CMS to a previous backup:

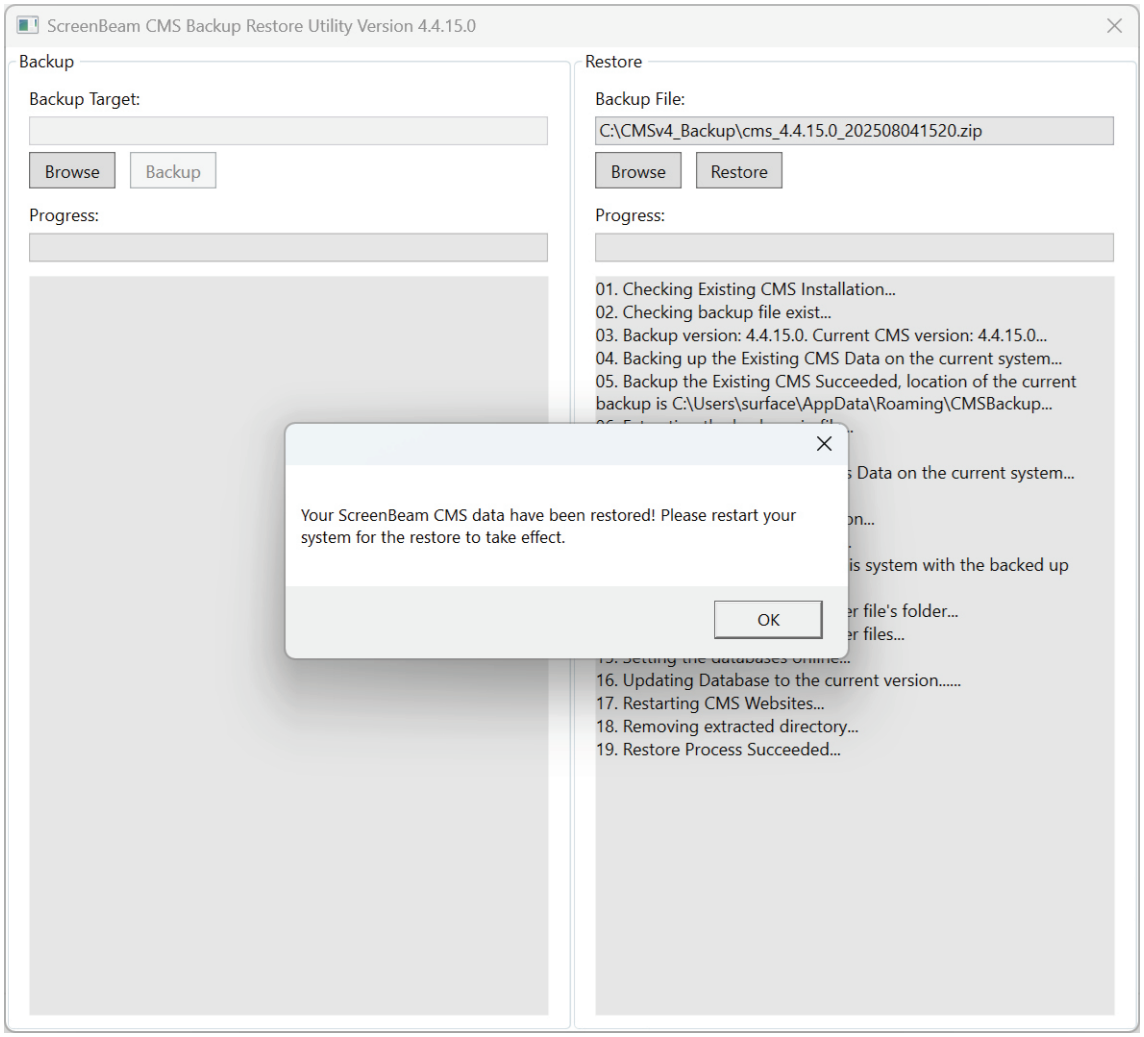
1. Start ScreenBeam CMS Backup Restore Utility.

2. Click the **Browse** button and then choose a CMS backup file. The chosen path will be displayed on the Backup File box.



3. Click the **Restore** button, and a message box will appear. Click **Yes** to start the restoration process.



Note: All current data on the system will be replaced. A backup of the current CMS is created and saved in this directory: *your installation directory* \ScreenBeam\cms\backupRestoreUtil\CMSBackup.

4. The restoration process will be completed in several minutes. Restored data will take effect after the system is restarted.
   Note: Don't close the backup restore utility before the restoration process is completed.