

Bluebeam Studio Enterprise 3.2 Installation & Configuration Guide

Revised August 2023

Bluebeam, Revu, and Bluebeam Studio are trademarks or registered trademarks of Bluebeam, Inc.

Amazon Web Services, AWS, Amazon Elastic Compute Cloud, EC2, CloudTrail, Amazon Simple Storage Service, and Amazon S3 are trademarks of Amazon.com, Inc.

Microsoft and Windows are either registered trademarks or trademarks of Microsoft Corporation in the United States and/or other countries.

Apple and iOS are trademarks of Apple Inc., registered in the U.S. and other countries.

DigiCert is a trademark of DigiCert, Inc. and is protected under the laws of the United States and other countries.

© 2023 Bluebeam, Inc. All Rights Reserved.

Patents Pending in the U.S. and/or other countries.

All other trademarks or registered trademarks are the property of their respective owners.

TABLE OF CONTENTS

Introduction	1
System Architecture Overview	2
System & Hardware Requirements	2
System Requirements	2
Supported Operating Systems	2
Microsoft SQL Server	3
Microsoft Internet Information Services (IIS)	3
Application Server and SQL Server Required Microsoft IIS Server Roles and Features	4
Microsoft Message Queuing (MSMQ).....	5
SMTP Email Server	6
Firewall.....	6
Certificate Requirements	6
Hardware Requirements	6
Processor.....	6
RAM	7
Disk Space	7
Network	7
Installing and Configuring Microsoft SQL Server	8
Basic Microsoft SQL Server Configuration.....	8
Installing a New SQL Server Instance	8
Configuring an Existing SQL Server Instance.....	10
Configuring SQL Server Accessibility	12
Windows Firewall Configuration	13
Certificate Installation and Deployment	13
Using Self-Signed, Domain, and Wildcard Certificates.....	13
Certificate Deployment through Group Policy	14
Using Trusted Root Certificates	14
Bluebeam Studio Enterprise Installation and Configuration	14
Pre-installation checklist	14
Requirements and Configurations	14
Server Accounts	15
SQL Authentication vs. Windows Authentication	16
What Gets Installed	17
Installing Bluebeam Studio Enterprise	17
Bluebeam Studio Enterprise Administrator	23
Status Page	23
Database Connection Page	24
Studio Session Page	24
Portal Page	24
E-mailer Service Page	25
Session Manager Service Page	25
User Notifier Service Page	26
Certificate Configuration Page	26
Job Queue Service Page	27
Projects Data Purge Service Page	27

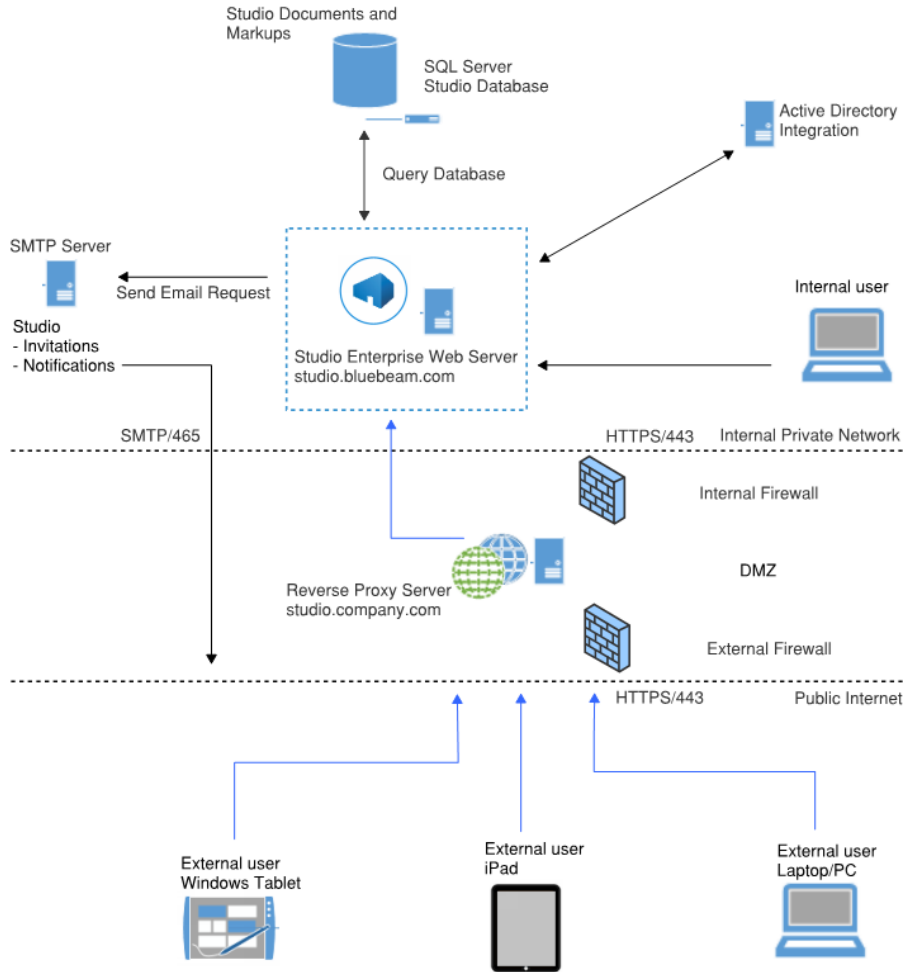
Enable Projects Data Purge.....	27
Enable Projects File Revision Management	28
The Bluebeam Studio Portal	28
My Profile Page	28
Studio Enterprise User Roles.....	28
Users Page.....	29
Documents Page	29
Control Panel Page	30
Studio Services	30
Reports and Notifications	30
Password Complexity	30
Project Undelete Page	31
Recovering a Studio Project	31
Recovering Studio Project Files.....	32
Reports Page	32
AD Integration Settings Page	32
Prerequisites	33
Confirm that all users in Active Directory have the first name, last name, and email address fields populated.	
Email addresses must be unique. Configuring Active Directory Integration	33
AD Manage Users Page.....	35
Manually Mapping or Un-mapping an AD Account	35
Server Permissions Page.....	36
Configuring Default Server Permissions.....	36
Security and Disaster Recovery.....	38
Troubleshooting.....	38

INTRODUCTION

This guide walks you through the installation, configuration, and administration of Bluebeam® Studio Enterprise, so that your organization can host Studio Projects and Sessions on an internal server. Before you get started, we strongly recommend taking a close look at the [System and Hardware Requirements](#), the prerequisites for installation and configuration, and certificate usage.

Note: For the purposes of this document, the term “Studio server” refers to the machine that Studio Enterprise is being installed on.

SYSTEM ARCHITECTURE OVERVIEW



SYSTEM & HARDWARE REQUIREMENTS

System Requirements

Supported Operating Systems

Bluebeam Studio Enterprise is compatible with the following Microsoft operating systems:

- Windows Server 2022
- Windows Server 2019
- Windows Server 2016
- Windows Server 2012 R2 64-bit
- Windows Server 2012 64-bit

Note: Windows Server 2016, 2019, and 2022 are supported only by Studio Enterprise 3.2. Please reach out to support@bluebeam.com for a download link and further assistance. See [How to upgrade to Studio Enterprise 3.2 for upgrade instructions](#).

Microsoft SQL Server

Microsoft® SQL Server® stores, organizes, and retrieves your Studio files and documents. Bluebeam Studio Enterprise is compatible with the following versions:

- Microsoft SQL Server 2022
- Microsoft SQL Server 2019
- Microsoft SQL Server 2016
- Microsoft SQL Server 2012

Note: The Express Edition of SQL can only be used for evaluation. It should not be used in a Production environment.

Note: SQL Server 2016, 2019, and 2022 are supported only by Studio Enterprise 3.2.

Note: If your SQL Server hasn't been installed, please see [Installing a New SQL Server Instance](#).

If it is already installed, please refer to [Configuring an Existing SQL Server Instance](#).

Microsoft Internet Information Services (IIS)

Microsoft IIS hosts the web services for Studio Enterprise. Bluebeam Studio Enterprise is compatible with the following IIS versions:

- IIS 10
- IIS 8.5
- IIS 8
- IIS 7.5
- IIS 7

Application Server and SQL Server Required Microsoft IIS Server Roles and Features

The Studio Enterprise application server and the SQL server must have specific MS IIS server roles and features installed and enabled. The following table lists the server roles and features required for each server OS version.

Server Role and Role Service	Application/SQL Server OS
Web Server (IIS)	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
HTTP Logging	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
Health and Diagnostics	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
ISAPI Filters	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
ISAPI Extensions	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
.NET Extensibility 4.8	Windows Server 2022
.NET Extensibility 4.7	Windows Server 2019
.NET Extensibility 4.6	Windows Server 2016
ASP.NET 4.8	Windows Server 2022
ASP.NET 4.7	Windows Server 2019
ASP.NET 4.6	Windows Server 2016
Application Development	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
Security	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
HTTP Errors	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016
Default Document	<ul style="list-style-type: none">• Windows Server 2022• Windows Server 2019• Windows Server 2016

Server Role and Role Service	Application/SQL Server OS
Static Content	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Common HTTP Features	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Static Content Compression	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Performance	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Web Server	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
IIS Management Console	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Management Tools	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Directory Browsing	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016
Request Filtering	<ul style="list-style-type: none"> • Windows Server 2022 • Windows Server 2019 • Windows Server 2016

Microsoft Message Queuing (MSMQ)

To ensure the security, correct routing, and delivery of messages from the Studio system to the Revu clients, Bluebeam Studio Enterprise requires the installation of MSMQ.

You can find installation instructions, as well as information about how MSMQ works, on the [Microsoft website](#).

SMTP Email Server

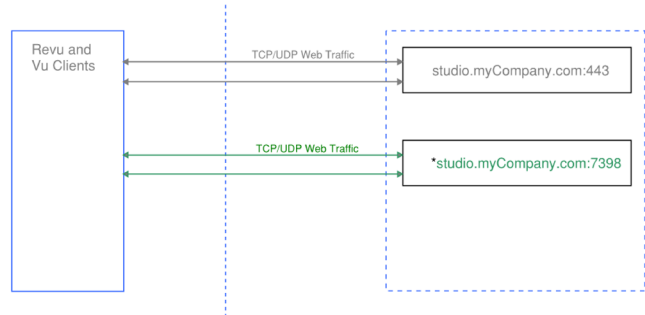
An important part of Bluebeam Studio functionality is the ability to send Session and Project invitations and notifications, as well as other information to hosts and attendees via email. For this to happen, your instance of Studio Enterprise [requires the following information for an email account on an SMTP server](#):

- SMTP Email server address
- SMTP Email server outgoing port
- Email address for Studio Enterprise
- Password for the email account
- The reply-to email address for email sent from the Studio Enterprise

Firewall

To ensure a proper connection between Studio Enterprise and Bluebeam® Revu®, you'll need to make sure the following firewall settings are properly configured:

- SQL Server ¹
- SMTP Email Server¹
- HTTPS on IIS
- Network Discovery to confirm that other machines can access it.²



* Required for Bluebeam Revu and Vu 12.1 and below.

¹Must be configured manually.

²Can be configured automatically if using Windows Firewall during the Studio Enterprise installation process.

Certificate Requirements

Both Studio Enterprise and your Revu clients use SSL certificate-based authentication for encrypted data connections. This being the case, all end user machines and the Studio application server must have these certificates installed.

You can set up a domain or wildcard certificate, and the installation process will let you create a self-signed certificate on the fly. Once a certificate is created, it can be distributed to individual workstations using Group Policy or manual installation.

Self-signed certificates are generally recommended for testing and internal purposes. For the best end-user experience, you should purchase an SSL certificate from a third-party Trusted Root Certificate provider. These certificates are automatically recognized and trusted by Windows clients and do not require manual distribution to each workstation.

Note: Apple iOS devices do not support self-signed certificates.

You can find lists of third-party Trusted Root Certificate providers for [Windows](#) on the [Microsoft](#) website.

Hardware Requirements

Our hardware requirements are based on a number of factors including the expected number of simultaneous Studio Sessions and connected users, the quantity and size of PDF files and markups within them, as well as the quantity and size of Studio Projects.

Processor

Bluebeam Studio Enterprise is a 64-bit application. For the best performance, you should run Studio Enterprise in a 64-bit, dual core environment or better.

RAM

We recommend at least 16 GB of RAM.

Recommended Minimum CPU and RAM Requirements for Large Scale Implementations

The information in this section is meant as a general guideline, and assumes that:

- Studio Enterprise and Microsoft SQL Server are installed on separate servers.
- Microsoft SQL Server has been installed and configured per Microsoft's recommendations.
- There is at least a one Gigabit connection between the MS SQL Server instance and your Studio Enterprise server.

Total registered users, 20% concurrent	1,000 users	2,000 users	4,000 users	6,000 users	8,000 users
<i>App server CPU</i>	4 CPU	6 CPU	8 CPU	10 CPU	12 CPU
<i>App server RAM</i>	16 GB RAM	24 GB RAM	32 GB RAM	40 GB RAM	48 GB RAM
<i>SQL server CPU</i>	4 CPU	6 CPU	8 CPU	10 CPU	12 CPU
<i>SQL server RAM</i>	32 GB RAM	48 GB RAM	64 GB RAM	80 GB RAM	96 GB RAM

Note: If you are going to scale up incrementally, you can do so in steps of two processors and 8 GB of RAM at a time.

Disk Space

Since Bluebeam Studio Enterprise should be installed on separate hardware from the SQL database (Microsoft SQL Server), there are two sets of space requirements:

Studio Enterprise Disk Space Requirements

You should have at least 100 GB of space available when installing Studio Enterprise.

Database Disk Space Requirements

Although we estimate that users will need at least 100 GB of disk space for the database, this really depends on the size of the files and markups held there. It may be a good idea to provision separate drives for: Data (MDF), Log (LDF), Tempdb, and Backups. If you do so, it's recommended to create multiple data files for Tempdb according to the number of CPU cores.

Network

Because network bandwidth tends to be the main bottleneck in Studio server performance, we recommend a gigabit network connection.

Minimum network bandwidths are not provided because there are too many factors to consider in determining these metrics.

INSTALLING AND CONFIGURING MICROSOFT SQL SERVER

Basic Microsoft SQL Server Configuration

The Microsoft SQL Server configuration for Bluebeam Studio Enterprise requires an SQL Server account with the following permissions:

- Create Databases
- Create/Drop Tables
- Create/Drop Indexes
- Create/Drop Foreign Key Constraints
- Create/Retrieve/Update/Delete Records

Note: The SQL Browser Service is disabled by default, so please make sure it is enabled and properly configured if your database is on a separate machine from your Studio Enterprise installation.

You can turn on the SQL Browser Service by going to **Properties > Service**, then setting Start Mode to Automatic. Read [Microsoft's TechNet article](#) for more detailed instructions.

Installing a New SQL Server Instance

Although this section describes the installation and configuration of a Microsoft SQL server 2022 instance, other versions are supported.

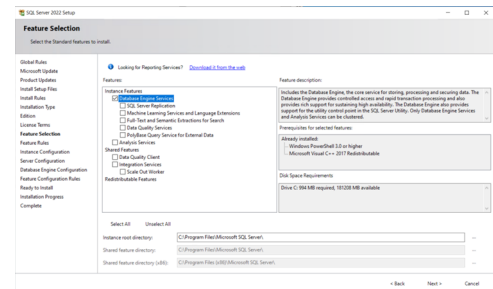
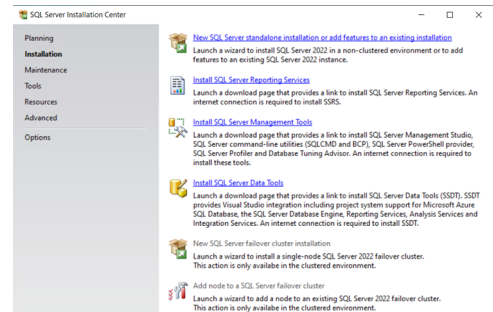
Please refer to [Configuring an Existing SQL Server Instance](#) for more details.

Note: For further details and references related to the installation and configuration of SQL Server, refer to the appropriate Microsoft documentation available on the Microsoft website.

Follow the steps listed below to install and configure a new SQL Server instance:

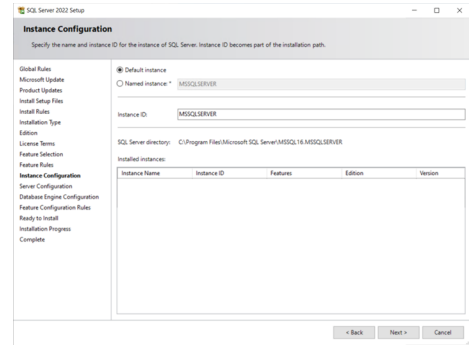
- 1 Load the SQL Server installer, click Installation on the left, and then select **New installation or add features to an existing installation** on the right.
- 2 When the installation wizard appears, click **Next** until you get to the **Feature Selection** page.

This is where you can select the feature **Database Engine Services** – the primary module that runs the SQL Server.



3 Continue through the wizard to the **Instance Configuration**.

Enter a custom name for the SQL Server instance in the **Named instance** box, or use the **Default Instance** to identify the database management system.

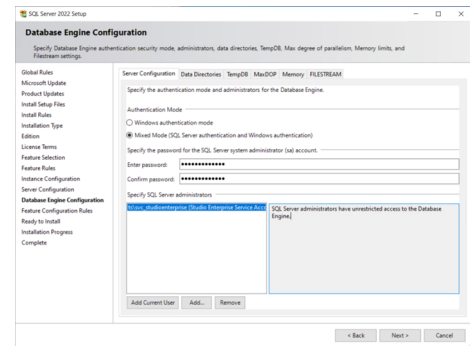


4 Keep clicking **Next** until you get to the **Database Engine Configuration** page.

Select **Mixed Mode** (SQL Server authentication and Windows authentication) as the authentication method.

Enter and confirm a new password for the SQL Server system administrator (*sa*) account

Add a Windows user account to the list in the **Specify SQL Server Administrators** section. The account specified will gain access to SQL Server using Windows Authentication.



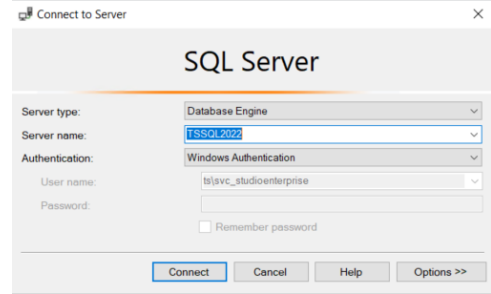
If separate drives have been provisioned for data, logs TempDB, and backups, configure them in the **Data Directories** and **TempDB** tabs.

5 Continue clicking **Next** to move through the rest of the wizard.

Note: Make sure you know the hostname of your Studio server, along with the database instance name and the “sa” account password, because you will need to enter this information during the rest of the Studio Enterprise installation.

Configuring an Existing SQL Server Instance

If SQL Server has already been installed, it will need to be configured so Bluebeam Studio Enterprise can connect to it. This section can be used as a guide to configure an SQL Server database that only uses Windows Authentication into one that uses Mixed Mode Authentication. If the state of the SQL Server is unknown, this section can also be used to verify that SQL Server is configured properly for Bluebeam Studio Enterprise.

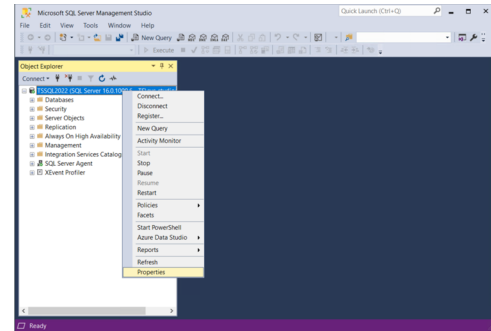


The best way to update SQL Server from an unknown state is to log into the machine hosting it and connect with Windows Authentication.

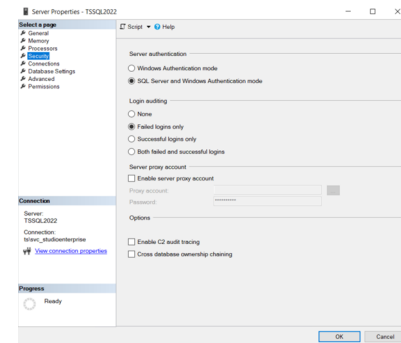
- 1 Log into the host machine using Microsoft SQL Server Management Studio and connect using Windows Authentication. This opens the Microsoft SQL Server Management Studio.

Note: The SQL Server login may fail, depending on the account used when it was originally set up.

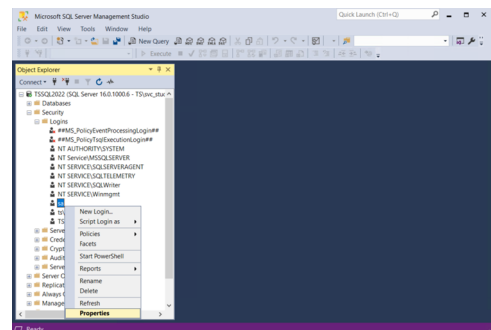
- 2 Right-click the Root node and select **Properties**.



- 3 Select **SQL Server and Windows Authentication Mode** and click **OK**. This changes the authentication method to **Mixed Mode**.

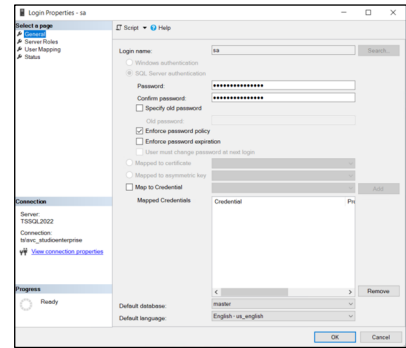


- 4 Expand the **Security** dropdown and the **Login** node below it, then right-click the "sa" account and select **Properties**. This opens the **Login Properties** dialog.



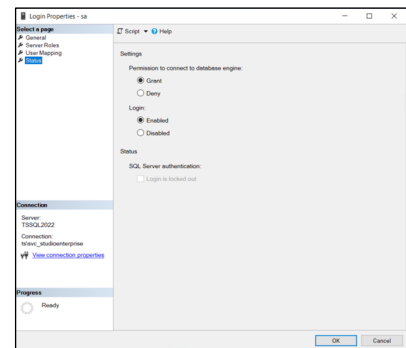
5 Select the **General** page on the left, and then click **SQL Server Authentication** and either update or reset the password for the “sa” account.

6 While remaining on the **General** page, select a database from the **Default database** dropdown menu. *Please do not leave this blank.*



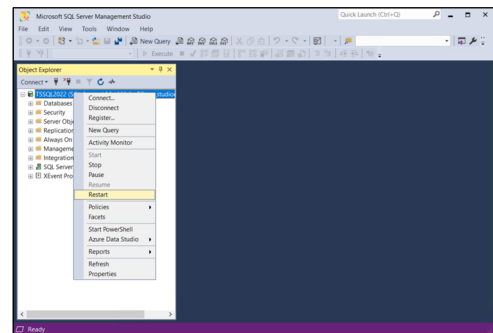
7 Select the **Status** page on the left, set **Permission to connect to database engine** to **Grant**, and **Login to Enabled**, then click **OK**.

You'll be taken back to the **Microsoft SQL Server Management Studio** dialog.



8 Restart the SQL Server by right-clicking the Root node and selecting **Restart**.

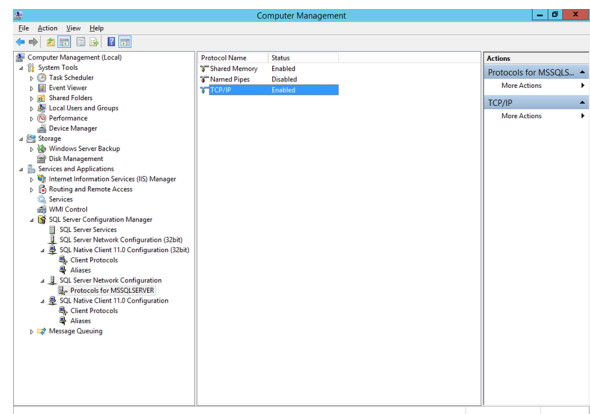
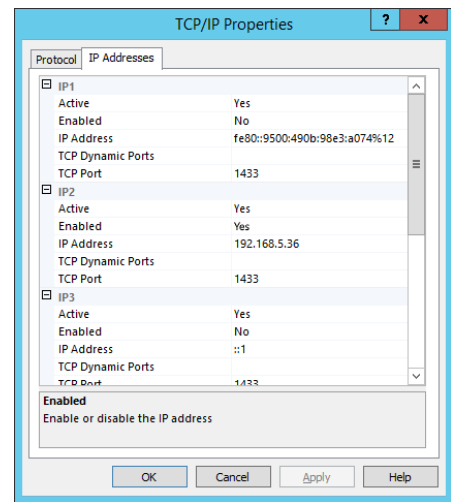
9 Once the restart has completed, test the configuration by using the “sa” account to log in to SQL Server Management Studio.



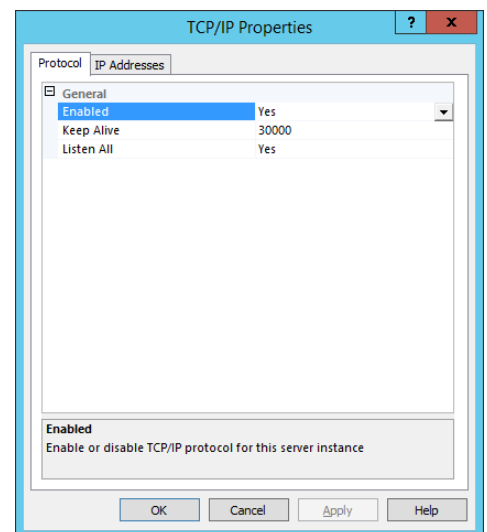
Configuring SQL Server Accessibility

If you have followed our recommendation to install Studio Enterprise and SQL Server on separate server hardware, you'll need to follow the steps listed below for configuring Microsoft SQL Server to accept remote connections:

1. Open the **Computer Management Tool** (*compmgmt.msc*).
2. On the right side of the Computer Management dialog, expand **Services and Applications** followed by **SQL Server Configuration Manager > SQL Server Network Configuration > Protocols for [Host Name]**.
3. Open the **TCP/IP Properties** dialog by double-clicking **TCP/IP** in the **Protocol Name** column, and verify this is enabled.



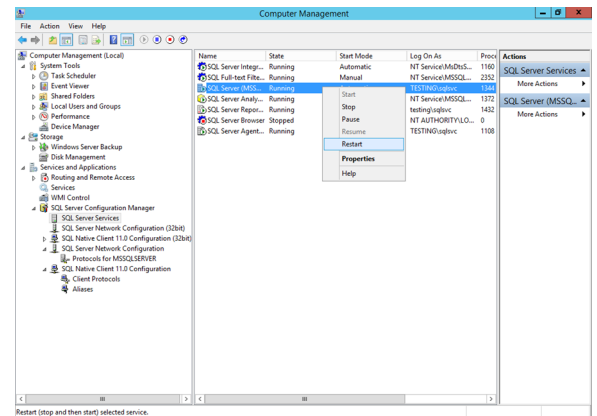
4. Enable at least one of the IP Addresses on the **IP Addresses** tab, and then click **OK**. You'll be returned to the **Microsoft SQL Server Management Studio** dialog.



- Restart the SQL Server Browser and SQL Server.

Click **Services and Applications** on the left side, and expand **SQL Server Configuration Manager** followed by **SQL Server Services**.

Locate **SQL Server Browser** and **SQL Server** in the **Name** column, and then right-click each of them, and select **Restart** from their corresponding pop-up menus.



WINDOWS FIREWALL CONFIGURATION

If you're going to use the Windows Firewall, **you'll need to add an Inbound Rule within the Firewall Manager to trust the SQL Server which is installed in `C:\Program Files\Microsoft SQL Server\MSSQL10_50.MSSQLSERVER\MSSQL\Binn\sqlservr.exe` by default. [we suggest using TCP port 1433. Learn more here.](#)**

CERTIFICATE INSTALLATION AND DEPLOYMENT

Because Studio Enterprise and your Revu clients use SSL certificate-based authentication for encrypted data connections between each other, they will all need to have access to the same certificate.

Using Self-Signed, Domain, and Wildcard Certificates

In addition to using an SSL certificate from a Trusted Root Certificate Authority, you also have the option of setting up a self-signed, domain, or wildcard certificate, which you'll deploy to your end-user workstations using either Group Policy or manual installation.

Certificate Deployment through Group Policy

For official instructions and additional resources, please refer to following information provided by Microsoft:

<http://technet.microsoft.com/en-us/library/bb742376.aspx>

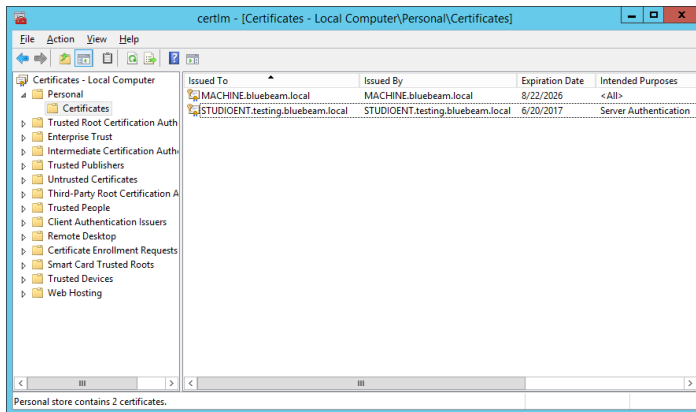
[http://technet.microsoft.com/en-us/library/cc770315\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc770315(WS.10).aspx)

<http://technet.microsoft.com/en-us/library/cc754841.aspx>

[http://technet.microsoft.com/en-us/library/cc733922\(WS.10\).aspx](http://technet.microsoft.com/en-us/library/cc733922(WS.10).aspx)

Note: Self-signed certificates are generally recommended for testing and internal purposes. For the best end-user experience, you should purchase an SSL certificate from a third-party Trusted Root Certificate provider. These certificates are automatically recognized and trusted by Revu and do not require “manual” distribution to each workstation.

iOS devices do not support self-signed certificates.



Using Trusted Root Certificates

When using a certificate from a Trusted Root Certificate Authority, you will need to follow their instructions to install it on your Studio server, via the **Microsoft Management Center** (*mmc.exe*). Certificates must be installed in the Local Machines Personal Store. This ensures it will be available for selection during the [Studio Enterprise installation](#). To view your installed certificates, use the Certificate Manager (*certmgr.msc*).

BLUEBEAM STUDIO ENTERPRISE INSTALLATION AND CONFIGURATION

This section refers to new installations only. If you are upgrading Studio Enterprise from an earlier version, please see [How to upgrade to Studio Enterprise 3.2](#) for upgrade instructions.

Pre-installation checklist

Here are some important prerequisites that need to be considered.

Requirements and Configurations

For the best possible performance, we strongly recommend that you do the following before you begin the installation process. *Please do not take any shortcuts:*

- Check the [System and Hardware Requirements](#) section of this installation guide to confirm that your whole environment meets or exceeds the specifications in each category.
- Make sure that [Microsoft SQL Server is correctly installed and configured](#).
- [Correctly install your SSL certificate](#).

- Make sure the hardware has a reliable internet connection.

Server Accounts

There are two accounts that are used to install and run Bluebeam Studio Enterprise: a Setup Account and a Service Account. These accounts require certain configurations to successfully install and run the software. These accounts will appear in the SQL Manager under **Security > Logins** on the left side.

Once you've located them, they'll need to be configured as described below:

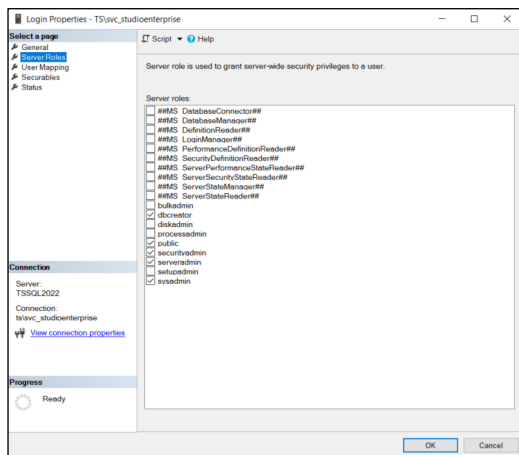
Setup Account

This account needs to be a member of the following server roles:

- **dbcreator** – This is used for creating and configuring the SQL database.

Note: This account is only used during installation.

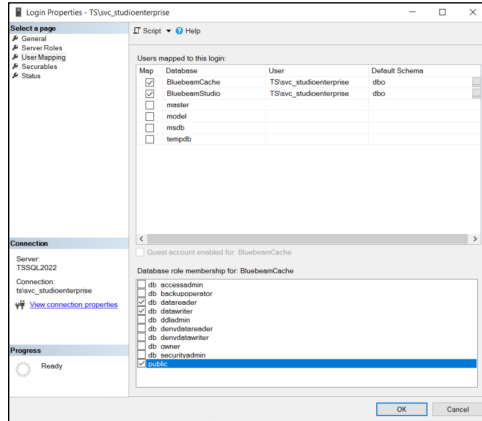
- **securityadmin** (during creation only) – For configuring the Service Account to run stored procedures and gain access to the database.
- **serveradmin** – For enabling CLR support on the database.



Service Account

The Service Account needs be a member of the following user mappings:

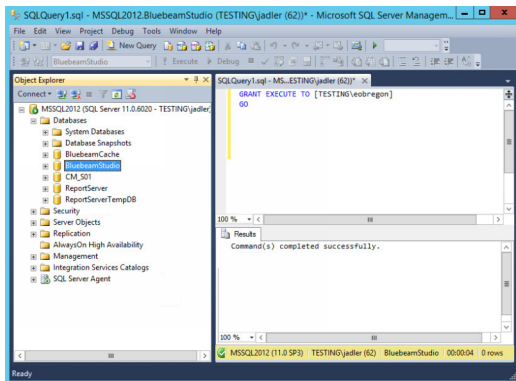
- BluebeamStudio
- BluebeamCache



Note: BluebeamStudio and BluebeamCache must have the db_datareader and db_datawriter roles in the SQL database.

The Service Account also needs explicit permission to the BluebeamStudio database in order to execute stored procedures. This is done by running the following query against the user in SQL:

```
GRANT EXECUTE TO [DOMAIN\user]  
  
GO
```



SQL Authentication vs. Windows Authentication

During the Studio Enterprise installation, you'll have the option of using either SQL authentication or Windows authentication.

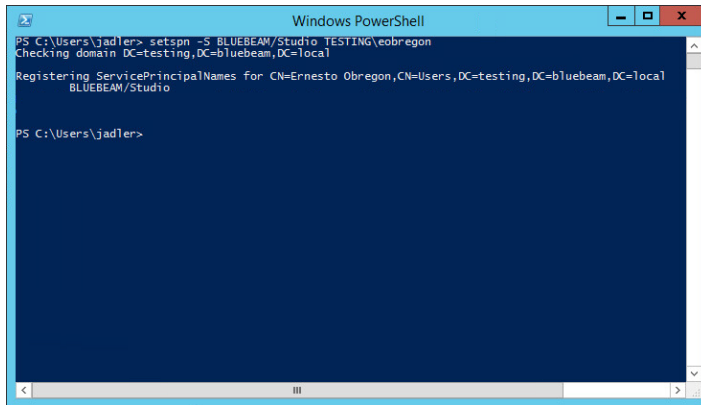
- Using **SQL Authentication** lets you specify the Setup Account, otherwise the *LocalSystem* account is automatically used as the Service Account.
- When **Windows Authentication** is used, you can specify the Service Account; the account currently logged into Windows is automatically used as the Setup Account (*this account must meet the conditions for the*

Setup Account as specified above). In order for the Service Account to authenticate users seamlessly when Windows authentication is used, it must be registered to the following Service Principal Name:

BLUEBEAM/studio

This can be done manually from a PowerShell command prompt using the following command:

```
setspn -S BLUEBEAM/studio DOMAIN\SERVICEACCOUNTNAME
```



If you ever need to change the Service Account, you must first unregister the *BLUEBEAM/studio* SPN from *DOMAIN\SERVICEACCOUNTNAME* before registering the new Service Account.

What Gets Installed

In addition to the application files, the Studio Enterprise installation wizard automatically installs the following items if they're not currently present or enabled:

- Microsoft .NET Framework 4.5. This is downloaded from [Microsoft](#) if required
- Microsoft SQL Server 2012 Native Client 11
- Microsoft System CLR Types for Microsoft SQL Server 2012 (*SQLSysClrTypes.msi*)
- Microsoft System CLR Types for SQL Server 2019
- Microsoft SQL Server 2012 Transact-SQL ScriptDom
- Microsoft SQL Server 2012 Data-Tier Application Framework (*dacframework.msi*)
- Microsoft IIS
- Microsoft Message Queuing (MSMQ)
- Microsoft OLE DB Driver 19 for SQL Server

Installing Bluebeam Studio Enterprise

This procedure applies to a new installation of Studio Enterprise 3.2. If this is a new installation, contact support@bluebeam.com for a link to the installer. If you're upgrading from a previous version, please see [How to upgrade to Studio Enterprise 3.2](#) for guidance.

To install Bluebeam Studio Enterprise:

1. Double-click the Bluebeam Studio Enterprise Installer.
2. Enter the following information under **Application Server Settings**:
 - The **Hostname** or **IP Address** of the Studio Enterprise server, and click **Reset** to populate this field with the computer name.

- The **Path to the Local Installation Directory** for the Studio Enterprise application.

*Note: This must be a local drive. Click **Browse** to navigate to and select a folder.*

- **An SSL Certificate** for the Studio Enterprise Server.

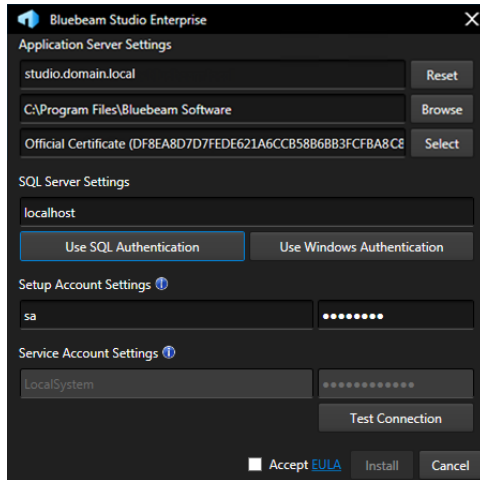
*Note: This certificate can be a self-signed certificate, if necessary, unless iPads are going to be used to access Studio Enterprise, in which case a certificate from a Trusted Root Authority is required. Click **Select** to choose from the certificates currently installed.*

3. Depending on your preferred authentication method, click either **Use SQL Authentication** or **Use Windows Authentication**:

Use SQL Authentication:

If you select **Use SQL Authentication**, enter the following under **SQL Server Settings**:

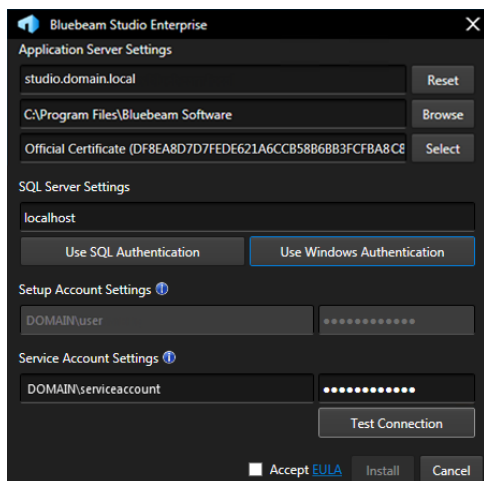
- The **SQL Server Hostname** and **Instance** for the SQL server that will be used with Studio Enterprise.
- The **SQL Server User Name** that Studio Enterprise will use as the Setup Account.
- The **Password** for the SQL Server User Name being used as the Setup Account.



Use Windows Authentication:

If you've selected **Use Windows Authentication**, you'll need to enter the following under **Service Account Settings**:

- The **Windows Account** that Studio Enterprise will use as the Service Account.
- The **Password** for the Service Account.



4. Click **Test Connection** to verify the Setup Account and Service Account connections.
5. Click **EULA** to fully read the End User License Agreement and then fill in the **Accept EULA** checkbox.
6. Click **Install**.

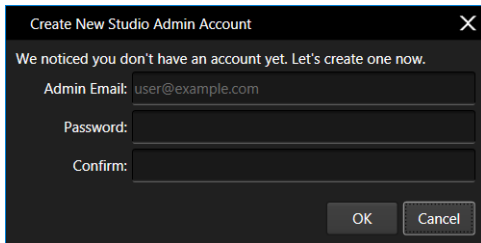
Based on whether this is a new Studio Enterprise installation or an upgrade from an earlier version, you'll be asked to either create or re-use and existing Bluebeam Studio database, as described below:

For a new installation:

When prompted to create a new Bluebeam Studio database, click **OK**.

to create an admin account for Studio Enterprise.

In the **Create New Studio Admin Account**, provide an Admin Email and Password and click **OK**.



Note: Passwords must be between 8 and 32 characters, contain at least one uppercase letter, one lowercase letter, one number, and one special character. These requirements may be changed to either Simple or Complex from the Bluebeam Studio Administrator Control Panel section.

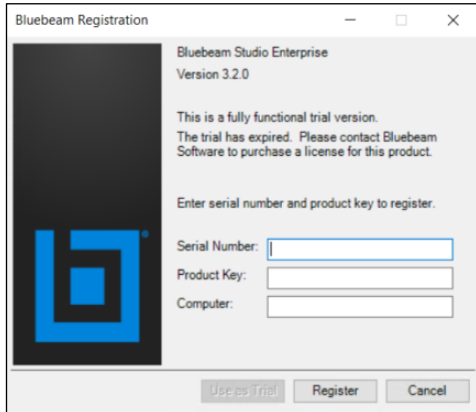
Important: During installation, it's best not to tie your account to the Active Directory in case it causes an accidental lockout of the Studio server. Tie an administrator account to the Active Directory only after setup is complete.

If this is an upgrade from an earlier product:

When prompted that an existing database will be used, click **OK**. See [How to upgrade to Studio Enterprise 3.2](#) for additional information.

A second message will appear telling you to back up your existing Studio database. You may have already done this prior to starting the installation, but you can never have enough back-ups. Click **OK**.

1. When the **Bluebeam Registration** dialog appears, enter your Serial Number and Product Key, and click **Register**.



Note: You can click **Use as Trial** if you'd like to use Studio Enterprise on a trial basis, but to ensure uninterrupted use, you'll need to register the software before the trial expires. You can do this in the Bluebeam Administrator under the **Tools** menu.

2. When the message appears letting you know that the installation was successful, click **Finish**.

After installation, Studio Enterprise starts, and one of the following occurs:

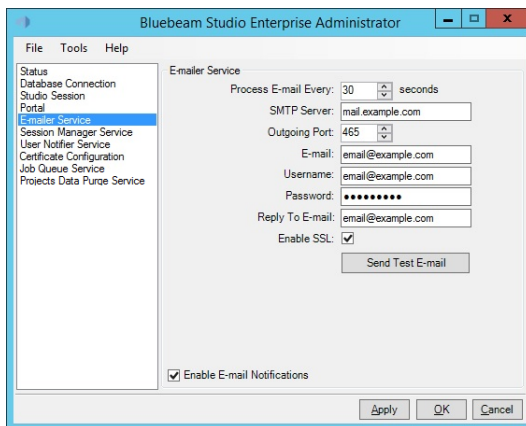
- A web browser automatically opens, displaying the Studio Enterprise web portal.

If this was a new installation, you'll be logged in automatically, using the Administrator user name and password created earlier.

If this was an upgrade, you will need to log in manually.

***Note:** JavaScript must be enabled for the Studio Portal to work. You can perform Portal configurations from another machine if JavaScript is not enabled on the server.*

- The **E-mailer Service** tab of the **Bluebeam Studio Enterprise Administrator** opens, and you can configure Studio Enterprise to send invitations and notifications for Sessions and Projects to hosts and attendees by filling in the **Enable E-mail Notifications** checkbox, entering the required SMTP server details, and then clicking **OK**.



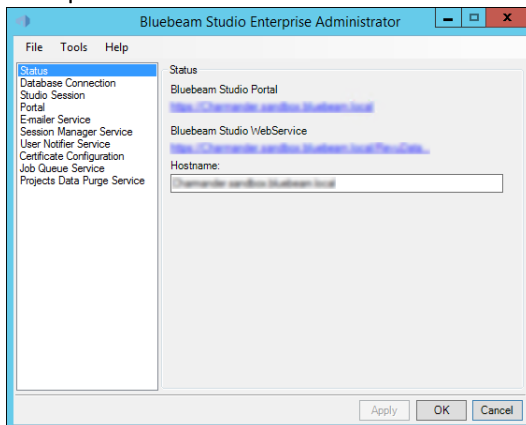
Note: An SMTP Server is recommended, but not required.

BLUEBEAM STUDIO ENTERPRISE ADMINISTRATOR

The Bluebeam Studio Administrator lets you configure and control Bluebeam Studio Enterprise using the functions and features of the various Tabs as described below:

Status Page

This is where you can easily access the Bluebeam Studio Portal and Web Service, as well as change the Studio Enterprise Hostname.



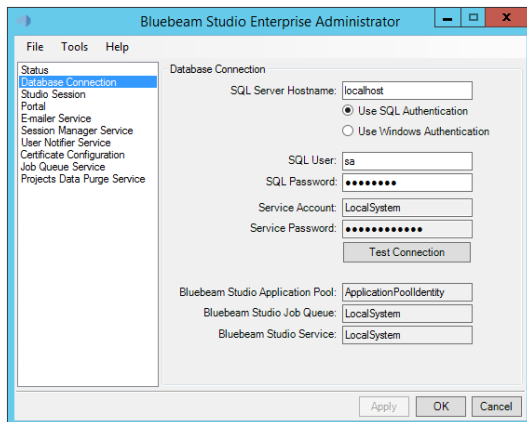
Please remember the following details:

- This is the same hostname that your end-users will connect to, as opposed to the Windows server name. For example, “studio.mycompany.com” and not “studio_server01”.
- If you are using a Self-signed certificate, the hostname on the Status page must match the hostname on the certificate.
- Hostname changes will not take effect until Studio Enterprise is restarted by clicking **Tools > Restart Server**.

Note: This will only restart the Bluebeam Studio Services. The Windows Server does not need to be restarted.

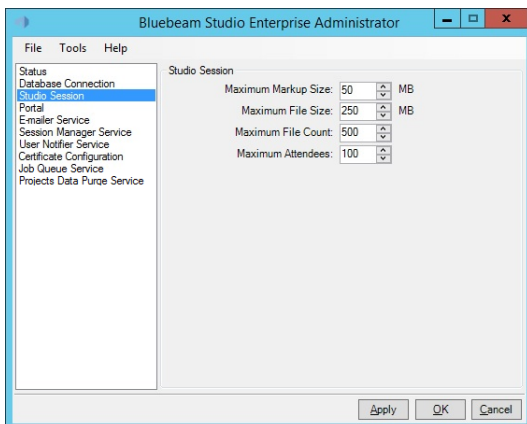
Database Connection Page

The **Database Connection** tab is where you'll be able to change the database connection and authentication method, which is useful if you ever want to move the Microsoft SQL Server to a different machine.



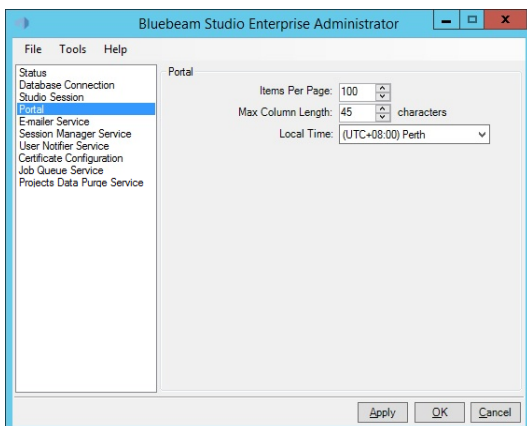
Studio Session Page

This page offers options for setting the maximum values for markup size, file size, file count, and maximum number of attendees for individual Studio Sessions.



Portal Page

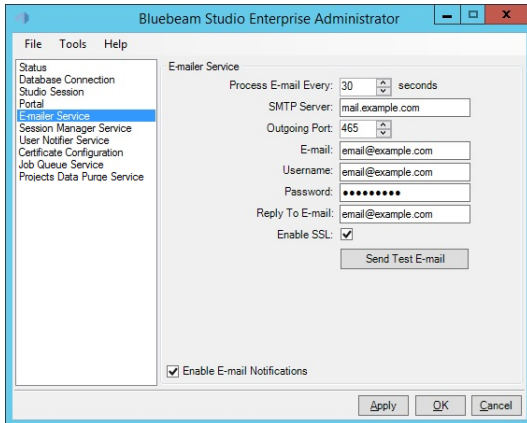
This is where you'll find settings that determine how the Bluebeam Studio Portal displays information.



Note: The **Max Column Length** parameter only applies to a subset of columns, such as the **Email Address** and **Name** columns.

E-mailer Service Page

This is where you can configure Studio Enterprise to send invitations and notifications for Sessions and Projects to hosts and attendees.



Once you've filled in the **Enable E-mail Notifications** checkbox, you'll be able to edit the **SMTP Server** details and other information on the page, then save the changes by clicking **Apply** and **OK**.

The Bluebeam Support site has more information about setting up notifications and alerts for [Windows](#).

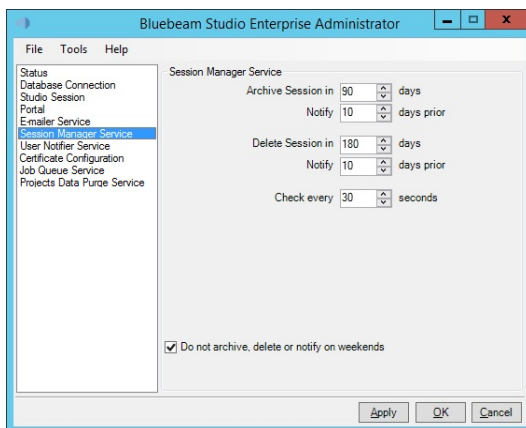
Session Manager Service Page

These settings control when inactive Sessions are archived and eventually deleted, as well as when the hosts are notified of these impending states:

Archive Session in:

Based on the default setting of 90 days, a Session will be archived after 90 days unless someone logs in. After logging into the Session, the archival/deletion periods are reset.

The host will receive an email 10 days before, notifying them this will happen.



Note: Archived Sessions can be recovered by the Session host or Studio Administrator by logging into Studio Web Portal, clicking on the Session owner's account, then **My Sessions**, and finally double-clicking the Session to recover and set the **Status** value from **Deleted** to **Active**.

Delete Session in:

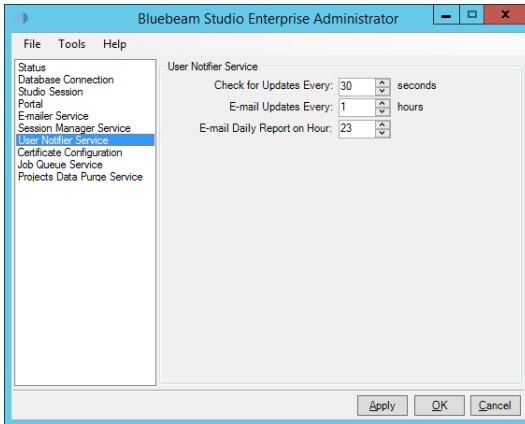
Based on the default setting of 180 days, a Session will be deleted after 180 days unless someone logs in.

The host will receive an email 10 days before, informing them of the impending deletion.

Note: When a Session is manually deleted, it is permanently purged from the system after 30 days, or the value set in **Days to Retain Deleted Sessions**.

User Notifier Service Page

This tab includes settings that determine how often hosts will receive notifications about their Sessions.

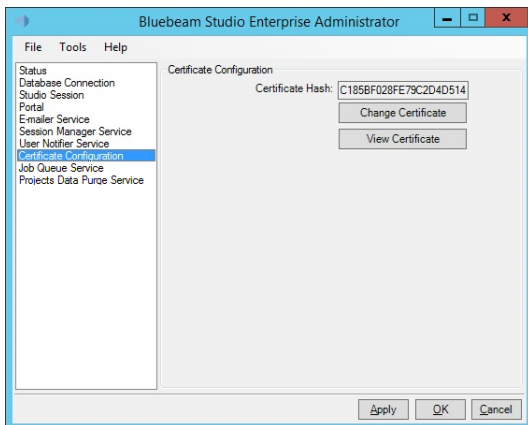


Note: An SMTP Server is required for these notifications.

The **User Notifier Service** queues messages based on the polling interval set by the **Check for Updates Every:** setting, and sends them based on the frequency determined by the **E-mail Updates Every:** value. The **E-mail Daily Report on Hour:** setting determines the time of day it will be sent out.

Certificate Configuration Page

If your SSL certificate expires, you can use this tab to update Studio Enterprise with a new one. Click **Change Certificate**, navigate to the new certificate, and then click **Apply** and **OK** to save the change.



If it's a self-signed Certificate, it will need to be installed on all Revu clients to connect to Sessions and Projects on your server.

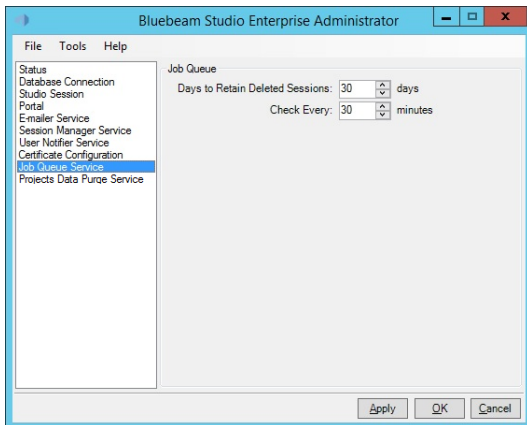
Note: Self-signed certificates are generally recommended for testing and internal purposes. For the best end-user experience, you should purchase an SSL certificate from a third-party Trusted Root Certificate provider, as Windows clients automatically recognize and trust these. This way you won't have to manually distribute them.

iOS devices do not support self-signed certificates.

You can find lists of third-party Trusted Root Certificate providers for [Windows](#) and [iOS](#) on the [Microsoft](#) and [Apple](#) websites respectively.

Job Queue Service Page

The **Days to Retain Deleted Sessions** setting determines how long deleted Sessions are retained on the server before being permanently removed. The **Check Every:** parameter specifies how often the system checks for deleted Sessions that should be removed.



Note: A deleted session is not recoverable.

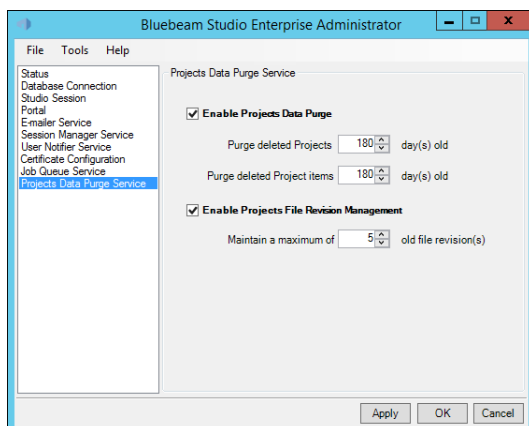
Projects Data Purge Service Page

Enable Projects Data Purge

Controls whether or not deleted Projects are eventually purged.

Purge deleted Projects - Specifies when Projects are purged after deletion.

Purge deleted Project items – Controls when files and folders are purged after their parent Project has been deleted.



Enable Projects File Revision Management

Determines whether file revisions are retained.

Maintain a maximum of – Sets the maximum number of retained file revisions.

Note: Versions older than the maximum are automatically purged, and some actions – such as moving or “undeleting” files – are tracked in their revision histories, but don’t count as revisions.

The **Project Data Purge Service** setting is disabled by default.

Be sure that your SQL server has sufficient hard drive space to hold all of your Studio Projects.

THE BLUEBEAM STUDIO PORTAL

The Bluebeam Studio Portal is a dashboard containing multiple pages from which you can perform various administrative tasks such as user management, reporting, and recovering deleted Studio Projects, Sessions, and documents.

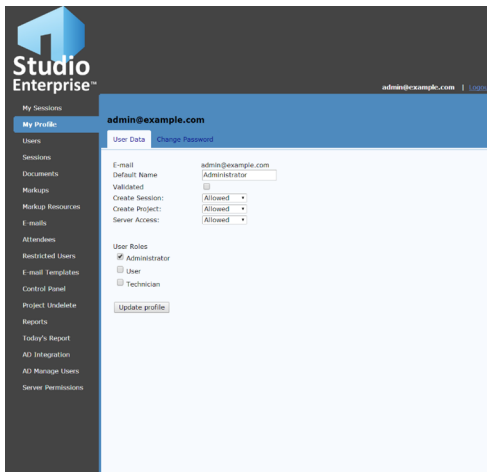
To access the portal you can click the link on the Status page of the [Studio Enterprise Administrator](#), or enter the URL (<https://<fully-qualified-machine-name>>) into a web browser. When the page opens, you can login using the [Studio Admin account](#) that was created during the Studio Enterprise installation.

Note: JavaScript must be enabled for the Studio Portal to work.

Studio users may also access this web portal to view their Studio Profile, change their passwords, and recover Sessions and Session documents. Users have a limited **User Role** by default.

My Profile Page

This page lets Studio users update their profiles and reset their Studio passwords. Studio Administrators will have additional options which let them assign different user roles to themselves or [other users](#).



Studio Enterprise User Roles

Administrator

This is the main user role for installing and managing Studio Enterprise. This user has the ability to change Studio Enterprise settings and run reports on usage, in addition to full access to the Admin web portal and so on.

Note: Only those requiring full access to the server settings should be set as an Administrator. Administrators can also recover user Sessions and documents as well as Projects and Project documents.

User

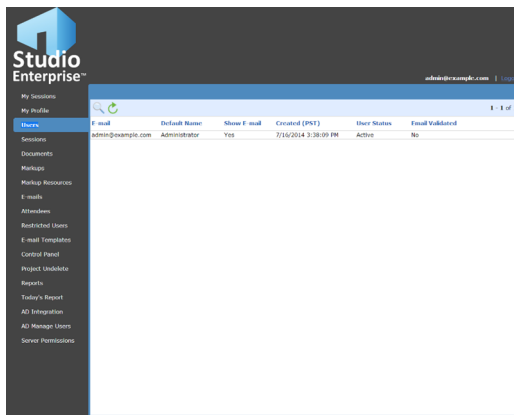
All new accounts are assigned this role by default. Although this allows them to create Sessions and Projects as well as invite attendees, it only lets them view Portal data for their own Sessions. Users can also recover Sessions and Session documents by clicking on the **Users** page, then on **My Sessions**, as long as the Session has not been permanently deleted.

Technician

As a Technician, a user is able to access any Session or Project for the purpose of verifying or troubleshooting any issues or problems. In this role, they'll be logging in without being an active participant, and therefore won't affect the Session or Project logs.

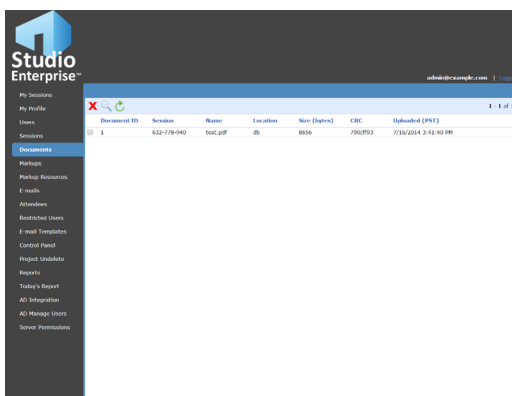
Users Page

This is where you can perform numerous user management tasks including password changes, permissions changes, and [role assignments](#). You can either double-click a user in the User List, or search for them by email address or user name, then double-click the result.



Documents Page

The **Documents** tab is used for managing Session files and their markups. You can select a Document ID in the Document List, or search for a file using the filename, Session ID, or date range. Double-click any file name to open it.



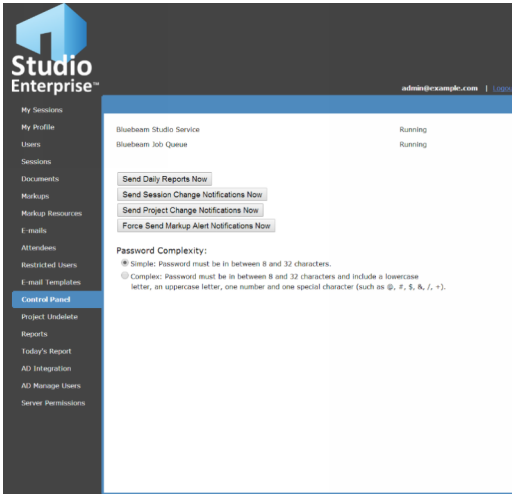
Control Panel Page

Studio Services

If either the Bluebeam Studio Service or Bluebeam Job Queue display **Stopped** (instead of **Running**), go to **Studio Administrator > Tools > Restart – Server**.

Reports and Notifications

In addition to displaying the status of the Bluebeam Studio Service and Bluebeam Job Queue, the **Control Panel** page includes buttons for immediately sending **Daily Reports**, as well as **Session and Project Change Notifications**, and **Markup Alert Notifications**.



Password Complexity

Additionally, you can control the complexity requirements for Studio accounts.

By default, Studio Enterprise allows users to create simple passwords between 8 and 32 characters. However, this setting can be changed at any time so that only complex passwords can be created which are between 8 and 32 characters long, and include at least one uppercase letter, one lowercase letter, one number and one special character, such as `!@#$$%^&*`.

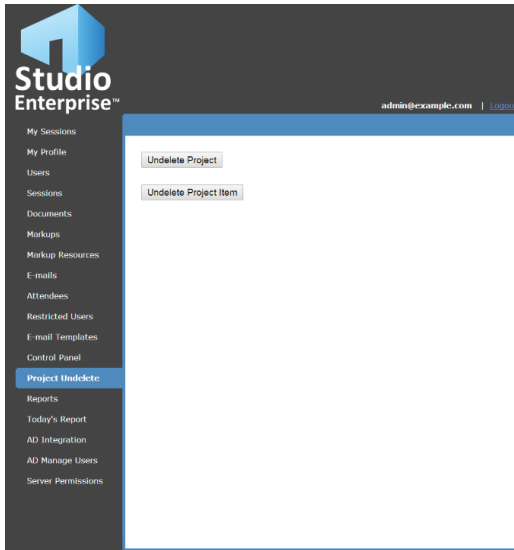
Note: Changing the password complexity requirements only affects passwords created after the setting takes effect. Existing passwords don't have to be changed, but if they are, they must meet the new requirements.

The following table describes the differences between simple and complex passwords for further clarification.

Simple vs Complex passwords in Studio Enterprise	Simple	Complex
Must be between 8 and 32 characters	Yes	Yes
Must contain at least 1 lower case letter	No	Yes
Must contain at least 1 upper case letter	No	Yes
Must contain at least 1 number	No	Yes
Must contain at least 1 special character	No	Yes

Project Undelete Page

The **Project Undelete** page is where you can recover deleted Studio Projects and Project documents.



Note: Only Studio Administrators have permissions to recover Projects and Project documents.

Recovering a Studio Project

- 1 Log into the Studio Enterprise Portal.
- 2 Select the **Project Undelete** tab.
- 3 Click **Undelete Project**.
- 4 Locate the Project to be recovered and click **Undelete**.

The Project will be recovered to the state it was in at the time of deletion.

To search for a specific Project, click **Search** and enter the search criteria in one or more of the fields at the top of the page.

If there are certain files you'd like to recover which were deleted before the Project was deleted, you'll need to recover those files individually.

Recovering Studio Project Files

- 1 Log into the Studio Enterprise Portal.
- 2 Select the **Project Undelete** tab.
- 3 Click **Undelete Project Item**.
- 4 Locate the Project file to be recovered and click **Undelete**. The recovered file will be added back to the Project as a new revision.

To search for a specific Project file, click **Search** and enter search criteria in one or more of the fields at top of the page.

If the file was located in a subfolder that was also deleted, that folder (and any relevant parent folders) will automatically be restored as well.

***Note:** Project files can only be recovered to an active Project. If you're unable to locate a particular file, make sure the relevant Project hasn't been deleted. If it has, you'll need to recover the Project first.*

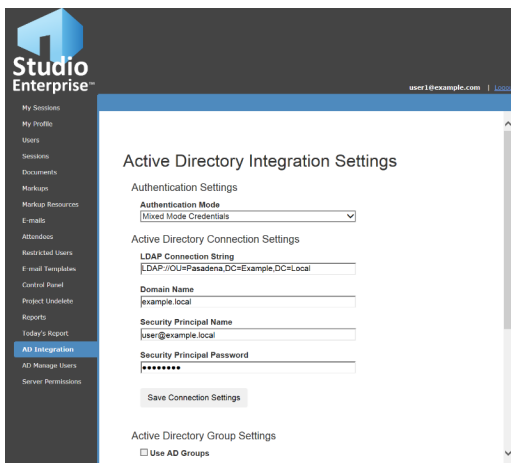
Reports Page

This page is used for generating reports based on **Sessions Created**, **Sessions with Activity**, and **Session Markups Created** settings.



AD Integration Settings Page

The **AD Integration** page lets you integrate Studio Enterprise with an Active Directory domain controller.



The screenshot shows the 'Active Directory Integration Settings' page in Studio Enterprise. The sidebar on the left is identical to the previous screenshot, with 'AD Integration' highlighted. The main content area is titled 'Active Directory Integration Settings' and contains the following sections:

- Authentication Settings:** A dropdown menu for 'Authentication Mode' set to 'Mixed Mode Credentials'.
- Active Directory Connection Settings:**
 - 'LDAP Connection String' field containing 'LDAP://OU=Pasadena,DC=Example,DC=Local'.
 - 'Domain Name' field containing 'example.local'.
 - 'Security Principal Name' field containing 'user@example.local'.
 - 'Security Principal Password' field with masked characters '*****'.
 - 'Save Connection Settings' button.
- Active Directory Group Settings:** A checkbox labeled 'Use AD Groups' which is currently unchecked.

Prerequisites

Please be sure to do the following before trying to configure your AD integration:

- Set up an Active Directory account to be used as the Security Principal.
- Prepare an LDAP connection string.
- Make sure the server has been added to the domain specified in the LDAP string.
- Have at least one Studio admin account ready to map to Active Directory.
- Make sure the Security Principal Account is also on the same domain.

Confirm that all users in Active Directory have the first name, last name, and email address fields populated. Email addresses must be unique.

Configuring Active Directory Integration

1. Log into the Studio Enterprise Portal.
2. Select the **AD Integration** tab.
3. Configure the following settings, as needed:

Authentication Mode:

Mixed Mode Credentials: Both Studio and Active Directory credentials can be used to access Studio Enterprise.

Note: This mode should be used if you want parties outside of your Active Directory to participate in document collaboration, like contractors or design partners.

Active Directory Credentials Only: Only Active Directory credentials can be used to access Studio Enterprise.

Note: Be sure to have at least one Studio user account with Studio Portal Administrator permissions that is not linked to your Active Directory. This will help prevent lock-out of your Studio Portal if anything happens to your Active Directory infrastructure.

LDAP Connection String:

Enter the desired LDAP connection string for your network. If you'd like to use an OU restriction, it can be added here as part of your LDAP Connection String. If you'd like to use AD groups, you can select them on the next screen.

Domain Name:

Enter the Active Directory domain.

Security Principal Name:

Enter or change the Security Principal.

Note: The Security Principal account is what Studio Enterprise uses to access your Active Directory server to authenticate AD users. It is strongly recommended that this account be one with a password that does not expire. If necessary, go to your Active Directory system and create a Security Principal account for Studio Enterprise (for example, "StudioServer@<yourdomain>") to use as the Security Principal.

4. Click **Save Connection Settings**.
5. To use Active Directory groups in addition to LDAP, select **Use AD Groups** and select the desired groups from the list below, then click **Save Group Settings**.

Note: When Active Directory groups are used, users must be in both the LDAP Connection String and at least one of the selected Active Directory groups in order to access the server. Active Directory Groups must be set up as **Distribution Groups** in the Active Directory.

6. After enabling Active Directory integration, you may want to map existing users to Active Directory accounts. This way, existing users with Studio accounts can continue accessing their existing Sessions and Projects once they switch to Active Directory credentials. There are two ways to do this:

Mapping users automatically:

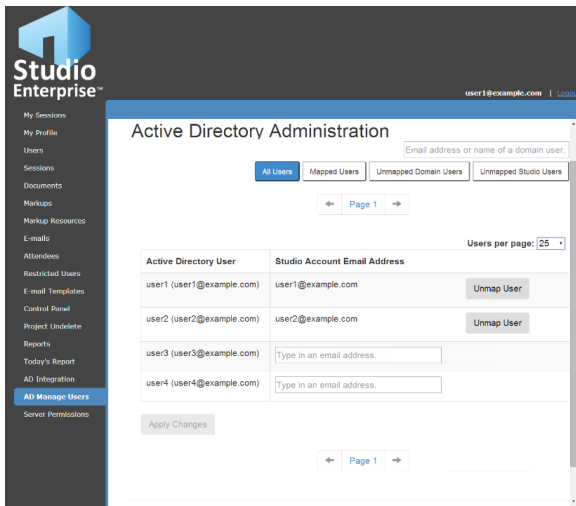
Click **Auto-Map Users**, which automatically maps users to AD accounts with matching email addresses. Once the mapping is complete, a report is generated listing the accounts that were mapped.

Mapping users manually:

Click **Manually Map Users** to jump to the **AD Manage Users** page, where you can manually map users to Active Directory accounts. This isn't necessary for users with matching Studio domain accounts and AD accounts, as they'll be mapped automatically the first time they log in.

AD Manage Users Page

The **AD Manage Users** page lets you map or un-map Studio Enterprise users to or from Active Directory accounts by following the steps listed below.



There is also an auto-mapping feature on the [AD Integration page](#) that automatically maps AD accounts to matching Studio accounts based on matching email addresses.

Manually Mapping or Un-mapping an AD Account

1. Log into the Studio Enterprise Portal.
2. Select the **AD Manage Users** page.
3. Locate the desired user.

To search for a specific user, use the search box in the upper-right corner of the page.

4. To un-map a mapped user, click **Unmap User**.

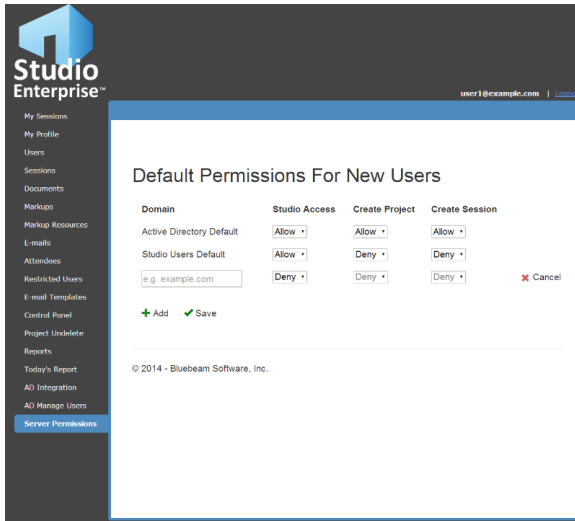
To map a user's AD account to its corresponding Studio account, enter an email address in the **Studio Account Email Address** field.

Note: The AD and Studio account must have been created with the same email address.

5. Click **Apply Changes** at the bottom of the page.

Server Permissions Page

This is where you can set default permissions for new users and AD users (when Studio Enterprise is integrated with AD) by domain.



Note: You can add and set default permissions for other domains, like "gmail.com". This could be useful if you need to block certain domains or limit permissions for outside contractors or design partners.

There are three permission types that can be enabled:

Server Access: Lets users log into Studio Projects and Sessions they are invited to. When Server Access is set to **Deny**, users will not be able to log into Studio or the web portal.

Create Project: Users can create Studio Projects, so long as they have Server Access permissions.

Create Session: Lets users create Studio Sessions, so long as they have Server Access permissions.

Note: When **Mixed Mode Credentials** and **AD Integrations** are enabled, you will see both **Active Directory Defaults** and **Studio User Defaults**. These Permissions are granular and can be adjusted per user on the **Users Page** for each user account.

If default permissions are set to **Allow**, but a user is not able to log into Studio or create a Session or Project, be sure to check their user account settings in the **Users** page.

Configuring Default Server Permissions


1. Log into the Studio Enterprise Portal.
2. Click the **Server Permissions** page.
3. Select the permissions for **Active Directory Default**, if applicable. These are the default permissions which are applied to all AD users added going forward.

Note: **Active Directory Default** only appears when the **Authentication Mode** is set to either **Mixed Mode Credentials** or **Active Directory Credentials Only** on the [AD Integration page](#).


4. Select the permissions for **Studio Users Default**.

For Studio accounts, default permissions are determined by domain. **Studio Users Default** defines the permissions that are applied to any user not captured by a domain-specific set of permissions.

5. To add domain-specific default permissions:

- a. Create a new row by clicking **Add** .
- b. Enter the domain for the permissions set in the **Domain** field. For example, "domain.com".
- c. Select the desired permissions from the corresponding options.

All permissions are disabled by default.

- d. Repeat this process to add more domains as needed.
- e. Click **Cancel**  if you want to remove a domain.

Note: *Active Directory Default and Studio Users Default cannot be removed.*

- f. Click **Save** .

Note: *Using domain-specific would be a good option if you need to set default permissions for specific outside parties, like contractors, design partners, or non-company specific domains, like Gmail™ users.*

SECURITY AND DISASTER RECOVERY

From time to time, we receive questions from Bluebeam Studio users about the safety of the files they're uploading to Bluebeam Studio. These concerns usually revolve around the overall level of document and system security, as well as what would happen in the event of an infrastructure failure. With this in mind, we've posted a [Bluebeam Security and Disaster Recover FAQ](#) on our website, to help address these concerns.

***Note:** These measures apply to Bluebeam Studio and Studio Prime. Since Studio Enterprise is hosted behind the customer firewall, it is up to their IT department to design, implement, and maintain their own security and disaster recovery protocols. However, they can use the information in this FAQ as a possible starting point.*

TROUBLESHOOTING

Please refer to our [Studio Enterprise Support page](#) for assistance with connectivity issues and general troubleshooting.



Bluebeam, Inc.
55 S. Lake Ave. Ste. 900
Pasadena, CA 91101, USA
www.bluebeam.com

